Centre for Information Policy Leadership
Hunton & Williams LLP

20 September 2017

CENTRE FOR INFORMATION POLICY LEADERSHIP RESPONSE

SINGAPORE PUBLIC CONSULTATION FOR APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

The Centre for Information Policy Leadership at Hunton & Williams LLP (CIPL) welcomes this opportunity to respond to the Singapore Personal Data Protection Commission (PDPC) on its Public Consultation for Approaches to Managing Personal Data in the Digital Economy.

CIPL is a privacy and data protection think tank in the law firm of Hunton & Williams LLP and is financially supported by the law firm and 54 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure effective privacy protections and the effective and responsible use of personal information in the modern information age. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton & Williams.

This response is focused on Part II of the PDPC's proposal for an enhanced framework for collection, use and disclosure of personal data. Although consent has been traditionally viewed as the processing ground which most empowers individuals, as it gives them control over the use of their personal data, CIPL believes that consent is no longer always the best or only way to empower individuals, especially given the development of new technologies and business practices in the digital era. The PDPC, recognising this reality, is proposing two additional bases for the processing of personal data without obtaining consent. CIPL agrees with both recommendations and sets out its reasoning below, including some additional suggestions.

CIPL attaches its white paper on Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR as an Annex to this submission.

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@hunton.com, Markus Heyder, mheyder@hunton.com or Sam Grogan, sgrogan@hunton.com.

Issues with Obtaining Consent in Certain Contexts

CIPL agrees with the PDPC's characterisations of the challenges of consent. Indeed, in the modern information age, there may be many contexts and circumstances in which obtaining valid consent for certain processing operations may have become impractical, impossible, ineffective or simply not meaningful. For example:

- In contexts where there is no direct interaction with individuals;
- Where individuals do not have a relationship with organisations that may process their data in the context of machine learning or in an ecosystem of mobile devices and the Internet of Things (IOT);
- Where large and repeated volumes of data are processed (seeking consent at every instance may not be feasible);
- Where the use of data is common, expected or trivial, or privacy risk to the individual is limited;
- Where the practical implementation of consent would unduly burden individuals and lead to consent fatigue (i.e. there may be many instances where individuals simply will no longer be willing or able to keep providing consents in the face of a deluge of requests for consent generated from data users in the digital economy, even where they might not have an objection to the processing);
- Where consent may not provide effective protection to the individual, because consent does not require the organisation to take certain other protective measures that are required by other grounds for processing (such as risk assessment and mitigations);
- Where consent may not be practicable (i.e. no ability to seek or provide consent);
- Where consent is counterproductive (e.g. processing to prevent fraud or crime, or to ensure information and network security); or
- Where consent is not meaningful because there is no genuine choice on the part of the individual.

In addition, requiring consent at every instance calls into question how "informed" such consents can be. Some processing operations are so complex that individuals cannot practically be provided with the necessary information to make meaningful and genuine choices.

Therefore, other processing grounds, which place greater responsibility on organisations to demonstrate accountability in ensuring the protection of personal data and safeguarding the interests of individuals, sometimes can be more appropriate than consent.

Furthermore, requiring consent across the board regardless of context, function or actual risk to individuals may prevent many types of legitimate, safe and beneficial data processing in the digital economy. In that connection, CIPL welcomes the PDPC's recognition that the consent approach erroneously assumes that individuals will always "weigh the costs to themselves and the benefits to the wider public" when exercising informed choice or consent. That may not actually be the case. As such, it may create obstacles to processing activities that may have been legitimate, beneficial and harmless in the first place, or may undermine societal progress in general.

The PDPC put forward two additional bases for data processing — "notification of purpose" and "legal or business purpose" — which would allow organisations to process personal data where consent may not be the most effective, practical or appropriate basis for processing.

1. **Notification of Purpose**

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

Answer: Yes. Providing individuals with notification of the purpose of the collection, use and disclosure of their personal data with an option to opt-out, where appropriate and feasible, can be more effective and realistic than seeking consent in cases like those mentioned above. Notification of purpose requires that organisations be transparent about how they are going to use data. Such transparency is critical for trust and digital confidence. By informing individuals about the protection and use of their personal data, individual acceptance and support of certain data uses will increase.

CIPL agrees with the PDPC's approach not to prescribe how the notification is to be done, leaving it to organisations to assess and determine the most appropriate mechanism. Providing notification is specific to context. What works for one scenario may not work for another. However, strong examples and guidelines would be helpful on what constitutes appropriate elements of notification that can then be adapted by organisations based on their needs, modes of communication and processing operations. Such guidance should be developed with input from affected stakeholders.

CIPL believes notification of purpose can be practically implemented through effective privacy policies and notices. Organisations should ensure that notification goes beyond providing standard legal notices. Notification (both of the "organization to individual" variety and "one-to-many" variety mentioned in the PDPC proposal) should instead be user-centric and effectively explain to individuals in plain language the current and potential uses of data, the benefits of such uses, and how the data will be protected. Where appropriate, acknowledging and addressing potential future uses that are not yet known are also imperative to providing effective notification of purpose to individuals. Explaining the rationale and benefits of possible additional data uses is important to creating trust and enhancing the customer relationship with the organisation. Furthermore, the notification of purpose should not be hidden but

instead presented to the individual in a practical, transparent and user-friendly manner, through an appropriate mechanism (such as dashboards, portals, interactive apps, signage, etc.). Where appropriate and feasible, the notification should outline how an individual may opt-out of the data processing should they wish to do so.

For some time, CIPL has been advocating for a new approach to transparency, one that is more user-centric and promotes effective engagement and good relations with customers, rather than solely focusing on legal compliance. Organisations need to step up and create effective and innovative ways of interacting with individuals and providing necessary information, with the help of multidisciplinary teams of technologists, user design specialists, behavioural economists, marketers and lawyers. Equally, data protection regulators should incentivise and showcase such best practices of user-centric transparency.

CIPL reads the opt-out element of the notification of purpose ground in the proposal as one that applies only where providing opt-out is feasible (see paragraph 3.9 of consultation proposal). CIPL agrees that opt-out cannot be a required element under this processing ground. If providing opt-out under this processing ground is not feasible or appropriate, then organisations should still be able to proceed with processing, provided the other conditions of the notification of purpose approach are complied with. However, some may read the proposal as indicating that this processing ground may only be used where it is feasible for the organisation to allow individuals to opt-out of the processing. In other words, if it is not feasible to offer an opt-out, then the processing cannot take place on this ground. The PDPC should make clear that this is not the case. One of the examples provided in the proposal of when the notification of purpose approach could be used where opt-out is not possible is where organisations wish to deploy recording devices or drones in high traffic situations that are likely to capture personal data. However, such processing should still be allowed to occur, provided appropriate notice is provided and the other elements of the proposed approach are satisfied (as discussed below in question 2).

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).

Answer: As an initial matter, CIPL believes that all processing grounds set forth in the PDPA should be of equal status, including consent and the two additional grounds proposed by the PDPC. It should be made clear that no processing ground is privileged over the others. An example for this approach can be found in the six different legal bases for processing under the EU Data Protection Directive and the incoming EU General Data Protection Regulation (GDPR).

Furthermore, CIPL agrees that these different grounds must be distinguished by certain elements that describe the situations in which it would be appropriate to use them. The PDPC, in its proposal to expand and strengthen the parallel bases for collecting, using and disclosing personal data under the PDPA, should describe these elements (as it has done), but make clear that it is up to the organisation to decide which processing ground is most appropriate and

suitable for the processing operation at hand, noting that the organisation must be able to justify and defend its decision in light of the elements of the processing ground.

This approach is consistent with CIPL's long-standing advocacy for organisational accountability/corporate digital responsibility, whereby organisations should implement policies, procedures and measures to ensure the protection of personal data through comprehensive privacy programs and be able to demonstrate the reasonableness of their decisions and accountability measures. We are delighted to see the PDPC reference and recognise accountability in their proposal. The defined elements of a processing ground can be used by organisations to determine the appropriateness of this ground for a given processing operation and can assist regulators in assessing whether the organisation made the right choice should the selection come into question.

The notification of purpose ground will allow organisations to provide sound protections and ensure their customers' confidence in cases where it is impractical, impossible or unnecessary to obtain consent or where another basis for processing is not more appropriate or relevant, such as "legal or business purpose." Valid consent requires that it is possible to provide clear and understandable information to an individual and that the individual has a genuine choice to decide whether or not to accept the processing. It must also be possible to withdraw consent at any time. Also, the consent should be meaningful and not overused in cases where there is minimal privacy risk. If these conditions to consent are not present, then organisations should be able to rely on the notification of purpose ground for processing or on another appropriate ground, provided the relevant elements of the alternative ground are met.

CIPL agrees with the PDPC that the notification of purpose approach is a suitable processing ground when the collection, use and disclosure of personal data is not expected to have any adverse impact on the individual. Organisations should be expected to understand the impact and risks to individuals from a proposed data use. This approach is in line with the modern trend of risk management and risk assessments in many areas of legal compliance, and most recently in data privacy law and compliance. This, however, cannot mean that organisations must guarantee with absolute certainty that no adverse effects will occur from the processing, but only that the processing operation must not be expected, or not be likely to, result in such effects because the organisation has taken the necessary steps to identify and minimise any such adverse effects. Thus, CIPL agrees that organisations wishing to rely on the notification of purpose ground should conduct a risk and impact assessment prior to notification and processing to determine the likely risks of the processing, balance the risks involved against the benefits, and devise appropriate mitigations. This risk-based approach to privacy protection places the burden of protecting the individual on the organisation, and is consistent with organisational accountability.

Finally, terms such as "impractical" (e.g., "it is impractical for the organization to obtain consent", Section 3.8(a)), necessarily and appropriately entail a degree of subjectivity in the application of the described elements. Thus, it is imperative to recognise that, in some cases, multiple processing grounds might be available in a given context and that it must be left to the

judgement of the company to decide which one it should rely on, provided it can reasonably justify its decision in light of the elements set forth in the PDPA. For instance, in cases where consent might be technically possible, this should not act as a bar to utilising the notification of purpose ground, which may be more appropriate for the circumstances.

2. Legal or Business Purpose

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?

Answer: Yes. The PDPC, in its consultation proposal, recognises that there may be circumstances when organisations need to collect, use or disclose personal data without consent for a legitimate purpose apart from those currently authorised by the PDPA or other laws. The PDPC cites sharing and use of data to detect and prevent fraud as one example, which is a benefit to the company, its customers, and the public.

As noted by the PDPC, a similar ground for processing to the proposed "legal or business purposes" ground is included in the EU Data Protection Directive and the GDPR, where it is referred to as the "legitimate interest" ground for processing. CIPL has previously outlined the importance of including a legitimate interest-type ground for processing personal data in data protection laws designed for the modern information age.[1]

While the proposed "legal or business purpose" ground is similar to the "legitimate interest" ground, under the GDPR, the legitimate interest at issue may also be that of a third party, which can be interpreted to include the interest of society. Indeed, this is also implied in the PDPC's second condition for this ground of processing in Section 3.15(b) (benefits to the public must be weighed against risks to the individual). However, note that we do not believe that it is always or only the interests to the public that must necessarily outweigh such risks to rely on this processing ground; it could also be the benefits to, or interests of, the company, an individual or a group of individuals that may outweigh such risks. See page 8 of this response. Indeed, the benefits or interests against which risks must be weighed are more likely to be those for the company or its customers rather than any potentially more abstract benefits to the public.[2] We suggest that the PDPC clarify the benefits/interests to be assessed are all applicable benefits/interests to the business, other third parties, customers, the public and/or society.

We further note that identifying benefits to the public and society may be difficult for businesses in contexts where such benefits have not formally been recognised or established in

[1] See CIPL paper on Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR. (May 2017) https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2017/06/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf, attached as an annex to this submission, and also https://iapp.org/news/a/empowering-individuals-beyond-consent/.

[2] Of course, this also depends on the meaning of "benefit to the public (or a portion thereof)", which could, for example, include customers. The PDPC might want to clarify its understanding of this phrase.

some legal or regulatory framework or through custom or consumer expectation. In such situations, businesses would have to be able to use their own judgement and be confident that regulators would honour these judgements if they are well-reasoned, justifiable and supported by sufficient evidence. CIPL recommends that this aspect be further considered and elaborated in terms of how organisations can identify and assess such public benefits and how their assessments will be recognised by regulators.

We also recommend that the PDPC rename this ground to "legal purpose or legitimate interest" to clarify the broader application of the ground to any organisation and the interest to include third parties. In addition, in a globalised data protection environment, where interoperability between privacy regimes and cross-border transfer mechanisms becomes increasingly important,[3] using similar terminology for similar concepts makes creating such interoperability easier.

The legitimate interest (or legal or business purpose) ground can, in a multitude of contexts provide more effective protection for individuals than consent, given that it requires a risk-assessment, a balancing of interests and appropriate mitigations for any identified risks. See discussion below under Question 4.

Under a legal or business purpose processing approach, organisations will not need to notify individuals of the collection, use or disclosure of personal data for such purposes. This is a key distinction between this approach and the notification of purpose approach, which does require some form of notification. This makes sense, as in some instances providing a detailed notice about a processing based on the legal or business purpose ground may prejudice the purpose of processing (e.g. processing of personal data for anti-fraud purposes, or for ensuring information or network security), or where it may be impossible to provide notice, or where it is completely unnecessary, such as in cases of low or no risks to individuals.

Some may conflate the two approaches in cases where an opt-out is not feasible for the notification of purpose approach, because both approaches require an assessment of risks and impacts on individuals and the implementation of necessary measures to mitigate such risks. Due to their similar requirements, the line between both approaches may be blurred. Hence, it is important that the PDPC sets out the different nature of the two legal grounds by highlighting that notice is not required under the legal or business purpose approach and by providing more examples where these processing grounds may be employed.

However, it is not possible to predetermine all contexts or processing activities where the legal or business purpose approach may apply. The PDPC, in recognising that the regulatory environment must keep pace with evolving technology while providing effective protection for individuals, should not limit this processing ground to a rigid list of activities. Certainly, examples of legal or business purposes (or "legitimate interests") are welcomed, but the essence of this processing ground is that it must be future-proof and adaptable to new

[3] See the ongoing efforts on creating interoperability between APEC CBPR and EU transfer mechanisms.

processing operations by virtue of its risk-based approach that allows the data user to precisely assess and deal with the specific risks at hand regardless of the nature of the technology or business practice. Recitals 47, 48 and 49 of the GDPR set out an array of non-exhaustive legitimate interest processing examples (such as, preventing fraud, ensuring information and network security and processing for marketing purposes) and a similar approach could be taken in the PDPA to illustrate the types of processing operations that fall under the legal or business purpose approach without restricting its application to a strict list of processing activities. Additionally, in CIPL's paper on Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR[4] we provide, grouped in several categories, examples of the use of the legitimate interest ground, gathered from current business practices of CIPL members.[5] These examples may provide a useful source for a similar illustrative list from the PDPC and we would be happy to elaborate and work with the PDPC on this matter.

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[6] clearly outweigh any adverse impact or risks to the individual)?

Answer: As with the notification of purpose approach, CIPL agrees that the PDPA must describe the general elements for a legal or business purpose approach. To re-emphasise CIPL's view, we believe that all grounds for processing should be on equal legal footing, whereby no one processing ground is viewed as privileged. It should be up to the organisation to decide which ground of processing is the most appropriate under the circumstances, provided that it fully complies with the requirements or elements of the ground it selects and that such a ground is appropriate and lawful with respect to the type of data to be processed. Thus, CIPL agrees that processing grounds similar to the proposed legal or business purpose approach (such as the legitimate interest ground under the European regime) are typically relevant or appropriate where obtaining consent is not relevant, practical or possible. However, this is not to say that in cases where consent might be technically possible, consent must under all circumstances be employed. Instead, there may be cases where either ground may be feasible. In such cases, it should be left to the organisation to decide which ground would be more appropriate or effective in protecting the individual. Of course, organisations should be able to explain and justify their decisions.

The most important condition that should be placed on the use of this ground of processing should be that organisations undertake an appropriate risk assessment and ensure that they

[4] See footnote 1 above.
[5] See pages 32-43 of attached annex for a list of legitimate interest categories and case studies prepared by CIPL.
[6] In Question 4, the PDPC appears to agree that the "benefits to the public" are relevant in the context of "legal or business purpose", which is consistent with CIPL's recommendation on page 7 above to change the name of the ground to "legal purpose and legitimate interest" so that societal benefits and interests are explicitly included in this ground for processing.

can demonstrate that they have done so, i.e. that they can justify to a regulator or other relevant third party the outcome and any decision to proceed with the processing operation.

Such risk assessments may typically involve:

- Identifying the specific adverse impacts on individuals and potential risks and harms of the proposed processing;

- Assessing the desired benefits of processing to the business and/or society. In this respect CIPL believes that the condition should not be limited to benefits to society alone, as seems to be suggested in Section 3.15(b) of the proposal and Question 4. Instead, it is the legitimate business purpose or interest of the organisation and/or the legitimate interests of third parties, including an individual, a group of individuals, the public (or a section thereof) or society, that must be considered in this analysis;

- Balancing and weighing the involved risks, benefits and competing interests;

- Implementing context-specific mitigations and safeguards that minimise the risks as much as possible without undermining the desired benefits; and

- At the end of this process, the organisation must make a defensible judgement call as to whether to proceed with the processing in light of the benefits and residual risks after mitigation. Where a processing operation poses a high risk, is particularly intrusive or is harmful to an individual's privacy and such risks cannot be mitigated against, legal or business purpose (or legal or legitimate interest) may not be appropriate and consent should be sought.

Conclusion

CIPL agrees that the addition of the notification of purpose and legal or business purpose (or, possibly, "legal purpose or legitimate interest") approaches to processing is vital for Singapore to keep pace with the constantly and rapidly developing digital economy. Both proposed approaches signify a move away from the over-use of consent, in the traditional sense, and pave the way for an approach that holds organisations accountable to act responsibly. Both approaches relieve individuals of the burden of unreasonable expectations and demands to unilaterally protect their interests in an increasingly complex and incomprehensible data economy. This is the only viable way forward for many future processing operations, as it not only ensures the protection of individuals, but also enables data innovation and growth in the information society. Furthermore, by introducing these two grounds Singapore can ensure that consent is reserved for cases in which it is truly required, meaningful and effective.

If you would like to discuss any of these issues further or require additional information, please contact Bojana Bellamy, bbellamy@hunton.com, Markus Heyder, mheyder@hunton.com or Sam Grogan, sgrogan@hunton.com.