27th May 2020

Broadcom's response to Public Consultation on PDP Amendment Bill

Broadcom Inc.

1 Yishun Ave 7
768923
Singapore

For any information regarding this paper please contact:

Ilias Chantzos, LLM, MBA

Global Privacy Officer

Ilias.chantzos@broadcom.com

Introduction – Summary of Major Points and Statement of Interests

Broadcom would like to thank MCI and the PDPC for launching this public consultation. We believe that the proposed amendments are in the right direction and promote Singapore as a favourable location of doing business in Asia while maintaining a clear, balanced regulatory framework that is effectively protecting personal data.

Broadcom historically has been heavily invested in Singapore. The recent acquisition of the Symantec enterprise cybersecurity business has further enhanced this investment. Broadcom is providing a number of technologies to large organizations in market segments such as financial services and telecommunications. Several of these organizations have presence in Singapore.

We believe we have a unique perspective to bring in discussions around the amendments of PDPA because of the diversity of businesses Broadcom is currently engaged and its global reach. Broadcom is known historically for semiconductors manufacturing that enables communication and communication devices. In addition, Broadcom is having a thriving enterprise software business as part of its businesses, focusing mostly on information technology (IT) infrastructure management, in support of mainframe technology mostly for financial services, in cybersecurity to detect, prevent and mitigate cyberattacks as well as in payment security to detect and prevent financial fraud. A lot of our software is already or is in the process of becoming cloud enabled while we use cloud computing in our infrastructure extensively.

Our unique perspective comes from the different use cases of data processing we have as well as those we observe from our customers. In addition, as part of its diverse software and hardware business Broadcom will process different types of data. It will act as a service provider processing personal data on behalf and at the instructions of its customers. It will process pseudonymized or anonymized data, it will also process non-personal technical data as part of its IT infrastructure businesses, or data that carry high confidentiality requirements such as cybersecurity and fraud prevention.

We are overall supportive of the changes proposed to PDPA. We offer some comments, clarifications and observations around accountability, breach notice, consent, data portability, unsolicited communications and enforcement powers of PDPC. Broadcom believes that the updates to PDPA if done in a manner that takes into account the industry perspective can bring important benefits to the market. It can reinforce the image of Singapore as a top international destination that is in line with best practices and is safe to invest and do business.

Our comments in more detail

Accountability

The introduction of an accountability principle is welcomed and is overall supported as it is a concept that is already in place in several privacy legislative instruments. Broadcom believes that accountability and flexibility go hand in hand. The more accountable an organization is the more flexibility it should be able to have in the way it processes personal data. The challenge with introducing an accountability obligation is that the concept of accountability is so much broader than just risk-based approach and it is often used to encompass the sum of all requirements under privacy and data governance law. At the simplest way of summarizing accountability we would argue that it means to have transparent and enforceable policies that are available to the different stakeholders, that are enforceable by technological and organizational means and that evidence of that enforceability can be reproduced.

We would welcome further guidance from PDPC on aspects of accountability it would like to focus in Singapore. Data Privacy Impact Assessments (DPIA) and Privacy by Design mentioned in the consultation are certainly aspects of accountability that we believe could benefit Singapore and are in

line with international best practices. DPIAs can be a quite resource intensive exercise. Therefore, we would suggest that DPIAs should be a recommended best practice to consider the privacy impact of the activities of organizations. DPIAs should become a requirement only for a limited set of activities whereby there is a serious

risk to personal data. Moreover, when considering accountability, we would caution PDPC to avoid creating additional administrative burdens by requiring accountability obligations similar to what GDPR has created through the records of processing activities. Whereas documentation of privacy commitments in business contracts is certainly a good practice we would argue that the extensive record keeping imposed by GDPR is having a not so positive impact because it increases administrative burden, costs, complexity and risks creating a tick-box compliance culture.

In our opinion true accountability is better served through well-defined ownership of privacy responsibilities and controls, including within company management as well as transparency of policies, technologies and procedures. For instance, we would invite PDPC to look into the publicly available product transparency notices for our cybersecurity products, that we post under https://www.broadcom.com/privacy as an example of our accountability efforts.

Mandatory breach notification

The mandatory notification of personal data breaches is a best practice that is gradually becoming universally recognized. The regime described in the consultation is one that is in line with other jurisdictions, notably GDPR and therefore we can support and should be manageable by most organizations doing business internationally. The approach taken on the level of risk justifying notification, or on the threshold of 500 impacted individuals is in our opinion in the right direction and so is the technological protection exemption. The 72h notification deadline has advantages and disadvantages that have been extensively debated in other forums. As breach notification is a very resource intensive process, we would encourage PDPC to consider having a standard form to report breaches that is similar to other notification forms that major regulators use around the world. In addition, we would suggest considering including language in PDPA that similarly to the German privacy law protects organizations self-reporting an incident from self-incrimination, as an additional incentive that would encourage the right behaviour.
Finally, we would advise that there needs to be a level of flexibility in the otherwise very clear notification timeline/process. As it currently stands in the consultation it seems that PDPC prohibits notifying data subjects in any situation before it has received the formal notification of a breach. The whole idea behind a notification to the data subjects is that it is an emergency measure in circumstances of very high risk. For example, in cases where a breach exposes the victims to very imminent risk of harm (e.g. because their bank account might get wiped after a theft of their online banking credentials), it may be necessary to immediately lock all accounts and immediately prompt all victims to reset their passwords (in other words, notify them of the breach right away), before even a proper formal breach notice can be compiled and submitted to the PDPC within the 72-hour deadline.

New offences under PDPA for egregious handling of personal data

We understand the well-intended objectives of introducing the new offences in PDPA. We also believe in the importance of individual responsibility in protecting personal data especially in the workplace and that organizations should instil a data protection culture to its employees. Nevertheless, we remain sceptical to the idea of the introduction of the offences as described because we fear that organizations might try to shift the blame to employees for what could otherwise be a question of training or technical and organizational measures that ultimately sit with the responsible organization. Besides current employment law permits organizations to apply disciplinary measures including up to termination to employees who do not respect its policies for instance when managing personal data. Perhaps a way to address this point would be to separate between reckless behaviour that should be managed by the organization versus intentional behaviour which damages the organization and for which the organization is less culpable due to the insider threat that the employee represents.

Consent requirements

Broadcom is a company that is focused on business to business transactions, whereas the discussion around consent is usually focused on issues like direct marketing or industries that serve consumers. In several

jurisdictions that we operate consent is a less practical legal basis to use because it comes with considerable administrative burdens and may be invalid (for instance in cases of employment relationships). Therefore, unless in circumstances that consent is the appropriate legal basis, such as in cases of marketing communications, we will usually rely on legal or contractual obligations and sometimes on legitimate interest. For this reason, we welcome the initiative to include in PDPA deemed consent for contract, after notification, the legitimate interest, scientific research and product improvement. We would like to particularly highlight legitimate interest as a legal basis often used for cybersecurity and fraud prevention. Moreover, we would like to applaud the introduction of a product improvement exemption. We believe that it will be particularly important for the developments of technology such as artificial intelligence.

Data portability

Data portability is also mostly seen as a business to consumer right. Broadcom's business being enterprise focused means that we have much more experience with data subject access requests to view, rectify or delete information as well as requests from business customers to delete or hand over their data when a commercial relationship ends. Nevertheless, we would argue that any data portability obligation needs to come with exemptions for data that are anonymous or in cases where the data subject is disproportionally difficult to identify. In addition, it is important to clarify in PDPA there can be situations that a data portability obligation may need to be fulfilled but a copy of the data to still remain with the processing organization. For example, in the case of cybersecurity a data portability obligation may extract threat data for an identifiable individual, however a copy of that threat data may still have to remain at the possession of the providing organization in order to be able to detect the same type of threat in the future or for product improvement and testing purposes.

The consultation is making reference to both a pull and a push model for data portability. It is important to ensure that in any pull model scenario the organizations that would function as intermediaries and would pull the data on behalf of the consumer can demonstrate clearly and unequivocally that they have authenticated properly the consumer and that they are authorized by the consumer in question to exercise the portability right. The risk of using this right as an avenue to conduct social engineering cyberattacks cannot be underestimated.

We welcome the statement that derived data are not included in the data portability right. The consultation makes reference to prohibiting the porting of data where it is threatening the physical or mental health of an individual. We would invite policy makers also to consider not to limit this provision to physical security but whether there can be scenarios that the cybersecurity of an individual could be at risk by the porting of his/her data.

Finally, we would like to draw the attention of the policy makers to the example of GDPR on data portability. The limitations foreseen by the GDPR strike a reasonable balance between data subjects' rights, businesses' legitimate interests, and practicability. Singapore should consider similarly limiting portability to data that was (1) provided by the data subject, (2) processed on the basis of consent of the data subject / direct contract with the data subject, and (3) processed through automated means. Also, it would be advisable explicitly to exempt employee data / HR records from the portability rule, because the benefits to data subjects are negligible while the burdens on employers can be exorbitant. Which in some countries has resulted in highly disruptive weaponisation of the right to portability in employment disputes.

Unsolicited communications

We believe that the changes proposed in the consultation are in the right direction. We are especially supportive of the changes that organizations should not check DNC registry when conducting communications for an existing commercial relationship. This is in line with best in other legal instruments internationally and simplifies marketing activities for organizations.

New proposed penalties thresholds under PDPA and PDPC recourse

We believe it is extremely important for Singapore to have an effective data protection framework with an authority that is well resourced and can impose proportionate and dissuasive penalties. The additional measures as proposed in PDPA including the statutory undertakings and the options for mediation are in the correct direction and provide for a more flexible and adaptable enforcement regime.

We would like to thank MCI and PDPC for giving us the possibility to provide feedback to these important amendments to PDPA. We remain at your disposal to provide additional information.