

**RESPONSE TO
THE MINISTRY OF INFORMATION, COMMUNICATIONS AND THE ARTS (MICA)
CONSULTATION ON PROPOSED CONSUMER DATA PROTECTION
REGIME FOR SINGAPORE**



By Quotient Consulting (QC) Sdn. Bhd.
Data Diagnosis | Privacy Impact Assessment | Data Protection & Privacy Strategy
Training | Data Protection & Privacy Certification | Public & Private Consultations

Noriswadi Ismail
Co-Founder/Managing Consultant
<noris@qconsultant.com>

<<http://qconsultant.com>>

Questions 1 & 2: Objectives and principles of proposed DP framework

Impact of the proposed DP law in specific sectors

The proposed DP law should be regarded as the fundamental framework of informational privacy. The long-term impact, of which, will gradually pose potential reforms and amendments of other sectoral regulations. Such reforms should also take into account the whole spirit and motivation of the proposed DP law. Particularly, by incorporating clear and coherent definitions in its interpretation sections, the application, the guidelines, codes and related exemptions and exclusions (if applicable). This is to avoid ambiguity and interpretational issues that may laggard its application, in practice.

Anticipated impacts that may cause future practical applications:

- adequacy level of data protection that may differ from the respective specific sectors' legislation;
- adequacy of the proposed DP law from the European Commission (EC) Article 29 Data Protection Working Party (A29DPWP) endorsement. Thus far, as at 23 October 2011, the EC has recognised Switzerland, Canada, Argentina, Guernsey, Jersey, Isle of Man, the US Department of Commerce's Safe Harbor Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection;
- adequacy of the proposed DP law from the advisory viewpoint of ASEAN and its member states (anticipating that the ASEAN Community will be in place by 2015-2020); and
- the interaction of the proposed DP law that intersects with other sectoral regulations and other international guidance such as the APEC's privacy framework and the OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

Impacts that may cause challenges to the concurrent applications of the DP law vis-à-vis the existing sectoral regulations:

- related exemptions that may differ from one to another;
- different practices, applications and administrative formalities that may inhibit the speed of turnaround time (if, the spirit of the DP law is to be framed in a business-friendly manner);

- inter-relationship of such regional and global transactions between the private sectors and the government where third parties' data (non-Singaporean nationals) are involved; and
- compliance challenges in terms of implementation and enforcement between and amongst the regulators of sectoral regulations.

Question 3: "Personal data"

Definition

The proposed definition is brief, clear and concise. It also reflects APEC's privacy framework definition. Concomitantly, three (3) observations are relevant:

- There should be an extended definition of "Sensitive Personal Data (SPD)". Given Singapore as a preferred global data hub, and the inflow and outflow of data relates robustly to SPD (i.e., ranging from medical tourism, airlines passenger records, political stance, religious beliefs, sexual orientation, focused groups' organisation and to society memberships), appropriately, the urging priority to protect these are commendable;
- Subject to the sectoral regulations' requirements and applications on the SPD, it is - business-friendly – best, to include provisions on SPD in the proposed DP law, instead of, by contextually inferring it based on the diversified and different requirements of sectoral regulations; and
- A stark contrast is generally appraised through the proposed coverage of personal data of deceased individuals. If these are to be incorporated in the DP law, such data may contain SPD (if, for example, it originates from the EU member states, Canada and the US). If such coverage appears to be incorporated in the provisions of the proposed DP law, there should be a coherent and clear reference on SPD. The latter's definition would not be pragmatic, as a whole, if it is to be applied and defined contextually through sectoral regulations. If it remains to be applied, it may invite baggage of contextual challenges in interpretation, practice and enforcement.

Question 4: Personal data of the deceased

It is strongly recommended to cover the definition of personal data that is extendable to the deceased. In respond to items 3.15, although Canada's Personal Information Protection and Electronic Documents Act (PIPEDA, which only applies to private sectors) outlines the protection period less than 20 years, nonetheless, a reference to its sectoral legislation of the Ontario province (Ontario's Personal Health Information Protection Act, 2004 (PHIPA) is equally relevant. It protects a deceased's personal health information for a period of (120 years upon the creation of the information and 50 years after the death). This is depending upon whichever comes first.

Comparatively, provinces of Alberta and Saskatchewan adopt a period of 25 years after the death, whilst British Columbia, Nova Scotia and Prince Edward Island adopt a period of 20 years after death. The province of Manitoba adopts the period of 10 years after death whilst the province of New Brunswick adopts the discretionary approach.

Although the UK's Data Protection Act 1998 (DPA) covers personal data relating to living individuals, nonetheless, there are 3 sectorial legislation addressing this. First, medical records of the deceased (Access to Health Records Act 1990 (AHRA)). Second, Access to Health Records (Northern Ireland) Order 1993. And third, the Freedom of Information Act 2000 (FOIA). These are only applicable to medical records, but not all records of a deceased. Likewise, there are also no specific exemptions under the FOIA regarding the deceased subject to the applicable exemption in Section 41. This may be applicable if the data was originally obtained from the deceased is relevant for public authorities retaining data such as health or banking records.

The complexity to equalise similar level of protection for the deceased's personal data or SPD is a question of fact, depending upon a specific context. To mitigate this, the UK has favoured the principles of duty of confidence, which applies to the deceased's representative who administers the deceased's wills and probate.

In the Netherlands, the definition of personal data does not cover the deceased. Ultimately however, if the data of a deceased relates to a surviving relative (for example, data relating to hereditary disease that may affect children, the *bescherming persoonsgegevens (Wbp)* [Dutch Data Protection Act] applies. It provides guidelines on publication of personal data on the internet through an illustration regarding genealogical websites. The position adopted by the *Wbp* is that if such data relates to surviving relatives that constitute SPD (for example, in the case of a mother who passed away due to haemophilia and the illness is genetically passed on to her son or daughter), therefore the *Wbp* applies. The requirement to disclose this must be done through unequivocal consent. In any way, the *Wbp* does not take the 'silence lends consent' position. Should such reference is made, consent to disclose must be sought.

Interestingly, Slovenia is amongst the few EU member states, which has provisions on the deceased's data. In the Personal Data Protection Act of the Republic of Slovenia (Official Gazette of the Republic of Slovenia, No. 57/2001), Articles 17 (processing for historical, statistical and scientific-research purposes) and 23 (protection of personal data of deceased individuals) address specifically on the matter. However, it is silent on the period of retention.

Question 5: organisations and activities covered by the DP law

As the nature of data movements are fluid and borderless, the law should cover organisations in and outside Singapore. This is to achieve a reasonable adequacy of data protection measure. In New Zealand, the New Zealand Privacy Act 1993 is

considered as the only omnibus national data protection law outside the EU that covers both the public and private organisations. In practice, such complaints, investigations and enforcement could be integrated through mutual coordination and cooperation between the respective organisations' privacy and data protection authorities' jurisdictions. To mitigate the practical difficulties in practice, the law should develop its Singapore Adequacy Model that may be consistent with APEC, OECD, EU and Safe Harbor.

Question 6: whether the DP law should extend organisations located outside Singapore

As suggested to the respond in Question 5 above, in addition to the proposed Singapore Adequacy Model, the DP law should also take into cognisance these:

- harmonisation of the law with the EU Data Protection Directive 95/46/EC (DPD), Canada, United States, Australia, New Zealand, Ireland, Hong Kong and other members of APEC which have the similar laws;
- technical solutions (which covers any emerging technologies, at present and in the future) that may be supplemented as guidance notes to the DP law;
- geographical zoning approach through bilateral or multilateral cooperation with the privacy and data protection authorities (in line with Singapore's economic interest);
- determine the 'reasonableness of adequacy' (as the ideal approach to mitigate practical difficulties of implementation); and
- continual interaction between and amongst the abovementioned countries.

Questions 7, 8 & 9: proposed general exclusions from the DP law

A clear line must be drawn between balancing the fundamental interest in freedom of public expression within the exclusions. Once the line is drawn, the law should take into account the intersection of these exclusions with other sectoral regulations; whether it matches such applicable exclusions on the latter? Or whether such partial exclusion is considered necessary?

Taking the UK DPA's position, further exclusions also include: -

- national security and the armed forces;
- personal data that is processed for research, statistical or historical purposes;
- individual's physical or mental health (which only applies in specific circumstances and if such subject access is granted to which it would be

likely to cause serious harm to the physical or mental health of the individual or someone else);

- personal data that consists educational and social work records;
- personal data relating to human fertilisation and embryology, adoption records and reports;
- personal data processed for, or in connection with, such corporate finance services relating to price-sensitive information;
- examination marks and personal data contained in the examination scripts and documents; and
- personal data processed for the purposes of making judicial, Crown, or Ministerial appointments or for conferring honours

Apropos, the specific questions on artistic and literary purposes should be expanded. These are broad terms and could be interpreted *conjunctively*. Granted that by narrowing the terms may result to complexity in practice. Of relevance, special attention should be treated to such data that involves minor within the exclusions. This may be illustrated in guidance notes or code of practice.

In Ireland, the Data Protection (Amendment) Act 2003 has incorporated a provision on personal data that are processed only for journalistic, artistic or literary purposes. This is explained in Section 22A of the Act, which emphasises strongly on the *ground of public interest*. The same should also be consulted with any codes of practices that are prevalent under the Act.

Jersey, being one of the few countries which reached the level of adequacy by the A29WPDP, has incorporated the words "*special purposes*" under Article 3 of the Data Protection (Jersey) Law 2005 (L.2/2005). It relates to any one or more purposes of journalism, artistic and literary (by cross referencing to Article 32). The latter outlines the exemption requirements, which are comprehensively in-depth, having regard to the *special importance of the public interest in freedom of expression*. It also explains the duties of data controller to exercise the exemption based on *reasonable believe and grounds*.

Question 10: proposed general rules under the DP law

The suggested broad areas are deemed to be acceptable generally. It also reflects the fundamental applications across other international jurisdictions and practices. In the interests of this consultation, a reference is made to Switzerland's approach. The Federal Act on Data Protection (Swiss DPA) of 19 June 1992 (Status as of 1 January 2011). The DPA has 3 distinctive features that distinguish its approach as compared to other European Economic Area members and the 27 EU member states. First, it provides extensive protection of data relating to identified or identifiable legal entities. That covers personal data of *private individuals and*

corporations). Second, it increases the protection to the so-called 'personality profiles' – which means, any collection of data allowing the *appraisal of fundamental characteristics* of an individual's personality. This also applies to SPD. Third, it does not distinguish the obligations of data controller and data processor on the rationale that it's *both the responsibility of data controller and processor to ensure compliance* with the basic principles for processing personal data. In other words, both can be subjected to joint infringement of privacy suit although it is the sole responsibility of the data controller to comply.

The case for Singapore's proposed DP law is that, although it may not include the definitions of data controller or data processor, nonetheless, the law should make it clear to define the *concept of reasonableness* and how it may link the same to the general rules, principles and applications in practice.

Question 11: consent, representatives of individuals and accountability

Arguably, consent is the most complex and sophisticated subject when it is brought into practice. The EU DPD has in previous occasions, provided its advisory opinions under the A29WPDP on this. However, for the purpose of this submission, QC shall not outline the lengthy discussions, but, relating the same into 6 key observations that the DP law should consider:

- *excessive data collection* (whether online and offline) should not be permitted. The concept of reasonableness should be able to illustrate how this is applicable in practice;
- *proportionality, data quality and fairness* are the key principles that should be considered in consent;
- such *justifications, exclusions and purposes of transfer* should be taken into account contextually;
- the nature of consent that may be *withdrawable* subject to certain online and offline circumstances;
- the *adequacy level of consent requirements* if the data subject hails from outside Singapore; and
- clear divisions between the *employer-employees' consent* that covers pre-employment, present and post-employment stages.

Critically relevant, if the representatives of individuals are acting on behalf of the minor, the impact of such consent should be appraised on a case-by-case basis. The Swedish Personal Data Act (*Personuppgiftslag* (1998:204)) (PDA) generally explains this.

Besides the typical power of attorney or existing trustee modes, the issue on representatives of individuals should be handled cautiously when it comes to SPD.

This requires extra attention, especially whilst dealing with online and offline consent. In order to avoid excessive formality burden in practice, a cross reference to other sectoral regulations on the modes of representation should also be taken into account. This is to minimise such delays and backlogs of formality if such situation occurs.

The OECD, APEC and PIPEDA maintain accountability as one of the cornerstone principles in data protection. In practice, it is recommended for companies and organisations to embed data protection and privacy beyond than cultural compliance. It should be intersected with the companies and organisations' DNA, vision and mission. Once the data protection commission is in place, continual briefings, dissemination and campaigns on accountability for various stakeholders are highly recommended. In terms of resource allocation, companies and organisations should be able to strategise the level of working relationship, terms of reference and implementation. This is subjected to their budget and the needs to recruit talents that are capable to manage and lead. Depending upon the nature and purposes of the organisations and companies' setting, the guidance notes to the DP law should highlight the potential yielded dividends should data protection and privacy is positioned as business friendly as opposed to burdensome.

Questions 12, 13 & 14(a): proposed rules on collection, use and disclosure; proposed approach to the transfer of personal data outside Singapore

As reiterated in our response to Question 11 above, consent is and has been always the underpinning principle of such proposed rules on collection, use, disclosure, accuracy, protection, retention, access and correction. The similar responses on exclusion that may fall within these proposed rules are also outlined in responding to Questions 7, 8 and 9 respectively.

In consistent with these, the Swedish PDA has cross-referred to 4 specific sectoral legislation. Firstly, the Debt Recovery Act (*Inkassolagen* (1974:182)). This Act stipulates that anyone must secure a permit from the Data Inspection Board (being the Swedish Regulatory Authority – equivalent to the Data Protection Commission) who collects debt on behalf or another, or who has purchased debts for collection subject to certain exceptions. Secondly, the Credit Information Act (*Kreditupplyningslagen* (1973:1173)). This Act protects individual's privacy relating to credit information. It stipulates that such credit referencing of an individual can only be disclosed subject to qualified reasons of legitimate disclosure. Thirdly, the Electronic Communications Act (*Lagen* (2003:389) *om elektronisk kommunikation*). This Act outlines privacy rules concerning the processing of personal data relating to provision of electronic communication networks and electronic communications services. It implements the EU Directive 2002/58/EC on the protection of privacy in the electronic communications sector. Fourthly, the Patients' Personal Data Act (*Patientdatalag* (2008:355)), which provides the regulatory provisions on processing of personal data in the healthcare sector. The mission of this Act is to protect patients' data security and privacy. The unique position in Sweden is that, these Acts shall take over precedence, if there are inconsistencies with the Swedish PDA.

The case for Singapore's proposed DP law is that, if the proposed rules and its illustration are taken on board, it is recommended to relate the applications, conditions, exclusions and derogations with other sectoral regulations.

In relation to the transfer of personal data outside Singapore, there are different approaches and precedents that are procedurally complex. The EU Binding Corporate Rules (BCR), the proposed APEC Cross-Border Privacy Rules system, contractual clauses & obligations and other self-regulatory rules are the prevailing approaches that are prevalent.

A cursory look at Canada, Japan and Korea's approaches are worthy to consider for the Singapore's proposed law. Canada (via PIPEDA) and Japan (via the Act on the Protection of Personal Information, Law No. 57 of 2003 (PPI)) do not differentiate between cross-border and domestic transfers to such third parties (which cover affiliates, subsidiaries and parent organisations and companies). It applies the similar rules and obligations to all third parties irrespective of their location. The laws require organisations and companies to being accountable for protection personal data when such transfers to third parties take place.

The position and practice of PIPEDA is that organisations and companies that transfer personal data to third parties must oblige to include a privacy protection clause in contracts. Equal obligation is also applied to the third parties and the organisations and companies that originally collect the personal data.

The Japanese's PPI, in particular, outlines that in the event of transfers to third parties, organisations and companies must legalise it through contracts with service providers and any parties involved. The contracts must contain detailed data security provisions.

In Korea (Act No. 5835 [Promotion of Information and Communications Network Utilisation and Information Protection 2005, (PICNUIP)], cross-border agreements akin to the PIPEDA and Japan's PPI are not required. Nonetheless, Korea's PICNUIP requires opt-in consent to transfer data. At the time of this written response, Korea has a pending draft privacy law although it does not address the cross-border transfer of personal data.

The case for Singapore's proposed DP law is that it's best to combine the inclusion of privacy back-to-back contractual clauses with any parties who are involved in the cross border data transfers; obligatory data security-provision and opt-in consent to transfer data subjected to certain applications and exclusions. This should also be made fairly and coherently.

Questions 14(b) and 15: proposed rules on accuracy, protection and retention of personal data

The principle of security should be read together in these proposed rules. In the UK DPA, such personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

In practice, one needs to review the period of data retention; consider the purpose or purposes holding the data and its period of retention; delete the no longer needed data securely for this purpose or these purposes; and constantly update, archive and delete the data if it is outdated. These are reflected under Principle 5 (retaining personal data) of the UK DPA. Bearing in mind that Principle 5 is to be linked with the three standards (of the third, fourth and fifth data protection principles). They are; adequate, relevant and not excessive; accurate and, when necessary, kept up to date; and kept for no longer than necessary.

In view of the above, the DP law should, in principle, consider these:

- the stance and manner prior to deciding the period of data retention;
- the circumstances that determine the period of retention;
- the nature of data and what it is used for;
- the circumstances of the data once the period of retention ends;
- the circumstances of shared data once the period ends;
- sectoral regulations that address this; and
- such agreed industry practices that outline such period of retention.

Question 16: proposed rules on access and correction of personal data

The proposed rules on access and correction should be referenced to *data quality principle*. In Hong Kong, the Personal Data (Privacy) Ordinance 1995 (HK PDO), under Schedule 1, Data Protection Principle 6 and sections 22 to 29 stipulate this. PIPEDA, under part of Principle 9 and Schedule 1, 4.9.5 and 4.9.6, mirrors this obligation. Whilst these proposed rules are applauded, such existing sectoral regulations that provide the reasonable approach (if applicable) should not be ignored and abandoned. There is one possible assumption that may lie ahead, that is, it creates a 'hybrid approach' of access and correction, instead of a consistently comprehensive approach.

To mitigate, the Australian Privacy Act 1998 (Cth) (the Private Act) affecting private sector organisation that came into effect on 21 December 2001 provides a useful lead. It outlines the National Privacy Principles (NPPs) that consist 10 principles (collection, use and disclosure, data quality, data security, openness, access & correction, identifiers, anonymity, transborder data flows and sensitive information). In particular, NPP 6 (access & correction) gives individuals general right of access to the personal data, and the right to have that information corrected if it is inaccurate, incomplete or out-of-date. There are circumstances in which an organisation does not have to provide access. For example, if:

- it would be unlawful to provide the data;

- it would pose a serious and imminent threat to life or health of any individual; or

- the request is frivolous or vexatious.

NPP 6 further states that if providing access would potentially disclose a commercially sensitive decision-making process, then, the organisation may give an explanation rather than direct access to the information. If the data is inaccurate, the organisation must take reasonable steps to correct, provided that if the individual can establish that it is not accurate. Such refusal of correction by an organisation should be supplemented with reasons to the individual who requested it.

Questions 17 & 18: proposed penalty and enforcement regime

The proposed enforcement powers and appeals mechanism are commendable. In addition to that, the proposed DP law should take into the account potential extraterritorial enforcement between other countries, which have its data protection and privacy legislation. On this, the EU DPD model is worthy to consider.

The proposed financial penalties that may derive from the breaches are deemed to be amongst the best (if it is to be applied in practice). These financial penalties should be reviewed once in 2 or 3 years, subjected to the level of breaches, complaints and enforcements. Further, collaborative enforcement with other respective regulators of the sectoral regulations are indispensable. Such collaborative enforcement model and framework should be developed, as guidance and illustration in the DP law's regulations, codes of practice and guidelines.

Question 19: transitional arrangements

In the interest of dissemination to the businesses and consumers, specific guidelines should be able to cover fundamentals of privacy and data protection in plain English format. It is best to include practical applications, examples and illustrations that may be related to their daily engagements in data collection, sharing, transfer, processing, management, retention and deletion. Whilst it is very challenging to provide a standard guideline generally, nonetheless, such sectoral regulations that may intersect with the DP law should also provide the similar dissemination and commitment. In other words, industry specific joint-guidelines with the DP law would appeal and entice such awareness-building activities for businesses and consumers.

Question 20: 'sunrise period'

A two-year sunrise period is appropriate. This is to gauge the businesses and consumers' readiness, awareness and planning prior to the DP law being enforced.

Question 21: proposed treatment of existing personal data

The proposed treatment of existing personal data should take into account the existing contractual obligations' and sectoral regulations' requirements. There might be potential mergers and acquisitions or any commercial activities or renewal of agreements that involve outsourcing or other related commercial activities involving data. Depending upon when the proposed two-year sunrise period commences, the DP law should be able to specify the date as to when such treatment of existing personal data would be subjected to compliance. In other words, the cut-off date to which compliance to the DP law commences. The specified date should be informed beforehand to businesses and consumers so that they are able to conduct the necessary compliance, audit review and novation of contracts, agreements and internal controls' systems.

Question 22: different transitional arrangement

A tiered transitional arrangement period should be established depending upon the nature, setting, establishment and performance of the organisations. This can be inferred through their audited accounts and annual reports. For example, start-up, private limited and public limited businesses may have different periodic challenges to pursue the transition. To address this, the proposed transitional arrangement should be based on tiered approach. It is proposed to establish 3 tiers for different organisations (start-up – 2 years, private limited – 1 and a half year, public limited – 1 year), provided that it does not exceed the proposed 2-year period.

Question 23: National Do-Not-Call registry

It is an ambitious pursuit and commendable. We shall await the further publication consultation so that QC could impress MICA our stance on this.

Conclusion

This proposed response to the consultation has taken into consideration selected global practices on data protection. QC believes that it may add the value to other submitted responses to MICA. To reiterate, the proposed DP law should consider developing the Singapore Adequacy Model, which may be compatible with the other existing adequacy models in international data protection regime and practices. In sum, 2 additional observations are triggered. Primarily, whilst the proposed DP law shall interact sophisticatedly with other sectoral regulations, the need to interact with the public sector data must not be ignored although such guidelines and controls are in place. Lastly, although the proposed DP law covers organisations, by taking the simplification and less burdening compliance & formality approach, however, it is also best if MICA should be able to lead the interaction with personal data and SPD within the public sector. Perhaps, a future consultation on the proposed Singapore Freedom Of Information Law may be able to address these once the DP law has reached the maturity stage.