Advancing Singapore's Next Generation Data Protection Regime

Microsoft's Response to the Public Consultation
Issued by the Ministry of Information Communication and the Arts
on the Proposed Consumer Data Protection Regime for Singapore

For more information please contact:

John Galligan
Regional Director, Government Relations
Microsoft Operations Pte Ltd
#22-02, 1 Marina Boulevard
Singapore 018989
jogallig@microsoft.com

Microsoft

Introduction

Singapore has an enviable reputation as a policy innovator. It leads the region and the world on many key indices, among them network readiness, prioritisation of ICT, efficiencies of legal system, and global competitiveness.[1] But, as the Ministry of Information, Communication and the Arts ("MICA") recognises in its consultation document, Singapore's lack of a comprehensive framework for the protection of personal data has been an area where the market has not kept pace with global regulatory trends and technology developments.

The explosive growth of the internet economy, cloud computing, the proliferation of computers and handheld mobile devices, and the expansion of e-commerce, e-government, e-health and other web-based services have brought us tremendous social and economic benefits. At the same time, these technologies have fundamentally redefined how, where, and by whom data is collected, transmitted and used – reinforcing the need for new rules for the protection of personal data.

Singapore is now in a unique position to develop a truly 21st century data protection regime that not only meets the privacy needs of its citizens and promotes responsible information stewardship by organisations that collect personal data, but that also reflects modern computing and internet paradigms. To achieve this, however, Singapore must focus its efforts on crafting a regime that is "future-proof" to the greatest extent possible – in other words, a regime that can withstand the rapid pace of technological change and protect personal data not only on the day of adoption, but also five, ten and even fifteen years into the future. Based on what MICA has outlined in its thoughtful and pragmatic public consultation paper, we believe that the Proposed Consumer Data Protection Regime for Singapore (the "proposed DP law") is well on its way to becoming just such a "next generation" data protection regime.

As one of the world's largest digital technology and services providers, Microsoft's success depends on users having confidence in our ability to responsibly manage and protect their data. We have worked hard to ensure that all of the company's products, services, processes and systems incorporate measures designed to help protect user privacy. We also work closely with regulators, industry and civil society organisations across the world to develop responsible business practices and strengthen national and international legal frameworks for data protection.

---

[1] The Global Information Technology Report 2010–2011: Transformations 2.0. World Economic Forum 2010

Given our commitment to data protection, Microsoft welcomes the opportunity to participate in this important consultation on the proposed new data protection regime for Singapore. In our opinion, this review, and the advancement of a comprehensive data protection regime, is essential for Singapore to realise its ambitions to be a major cloud computing and data processing hub by providing technology companies like Microsoft with the opportunity to provide next generation services to customers and consumers right across the the Asia-Pacific region.

These are unquestionably challenging times – but also exciting ones – for those concerned with the protection of data in an ever-more connected world. Microsoft stands ready to work with MICA and other stakeholders to help improve Singapore's regulatory foundations so that it is better equipped for today's more complex data protection environment and continues to be among the world's most vibrant and successful digital economies. Our comments on the specific questions raised in the consultation paper follow.

Summary of Major Points

Key Objectives and Principles (Questions 1-2)

- Microsoft strongly endorses the objectives outlined by MICA. Providing strong safeguards for personal data, and ensuring industry has certainty and clarity regarding their obligations to protect that data, are essential if Singapore is to remain a global hub for innovation and online services.

- We agree that it makes good sense to introduce the DP law so that it applies concurrently with existing sectoral regulations. We encourage MICA to work with other regulators and industry to review existing sector-specific regulations and modernise them as needed to ensure that *all* data protection rules in Singapore protect users' privacy while enabling innovation and facilitating the productivity and cost-efficiency offered by new computing paradigms like cloud computing.

Scope: Types of Data Covered (Questions 3-4)

- We believe that the proposed definition of "personal data" strikes an appropriate balance between under and over inclusion of data types and is flexible enough to encompass future types of personal data. We welcome the recommendation that rather than establish definitive lists in law, the Data Protection Commission (DPC) will provide guidance for organisations regarding what is and is not personal data (and "sensitive" data).

Scope: Types of Organisations and Activities Covered (Questions 5-6)

- Microsoft supports the broad application of the proposed data protection law to all private sector organisations.

- We commend MICA for taking a practical and realistic approach to the difficult issue of extra-territorial application of the proposed DP law. While there are no easy answers, one approach that merits consideration is an applicable law test that is based on the "country of origin principle" – i.e. which would subject data controllers to the law of the jurisdiction where their primary data centre is located. More broadly, we also encourage Singapore to work closely with its trading partners to agree baseline norms of data protection that will ensure personal data is safeguarded regardless of its geographic location.

Rules and Exclusions: General Exclusions (Questions 7-9)

- Overall, Microsoft agrees with the proposed general exclusions from the data protection law.
- Although it can be difficult to define exclusions for artistic and literary purposes, especially in a digital age, we believe that the new DP law should provide for them. Privacy and data protection law should not be used to stifle freedom of expression.

Rules and Exclusions: General Rules and Rules on Collection, Use & Disclosure (Questions 10-14)

- ***Data controllers/data processors****:* We agree that all organisations should be required to protect data under their custody and control. That said, many of the fundamental responsibilities under the law - such as providing notice, obtaining consent or otherwise establishing a legal basis for processing the data, ensuring data are accurate, and responding to data subject access requests - should continue to rest primarily with data controllers. Processors' primary responsibility should be to comply with general requirements of the law such as securing all data that they process, as well as to fulfil contractual obligations that their controller customers impose.

- ***Legal bases in addition to consent***: We agree that in many circumstances it is important and appropriate to obtain an individual's consent in order to collect and use his or her personal data. As the consultation document recognises, however, in some cases obtaining consent is neither practical nor necessary. For example, where secondary processing of personal information falls within an individual's reasonable expectations given the context of the processing, additional notice and consent become less important. Similarly, where processing is necessary for the purposes of legitimate interests that the organisation is pursuing, consent may not be needed (except in cases where the organisation's interests are overridden by the need to protect the fundamental rights and freedoms of the individual).

- ***Mechanisms for obtaining consent***: The optimal means for obtaining consent can vary depending on the specific context of the collection. We also note that as technology evolves, the ways in which consent is obtained will also change – and mechanisms that are commonplace today may be obsolete in a few years' time. Mandating how consent is to be provided, or preferring certain mechanisms over others, will result in an inflexible regime that may soon be outdated. We therefore support MICA's proposal not to prescribe in detail the manner in which consent may be given in the DP law.

- ***Accountability***: We encourage MICA to consider the introduction of a broad accountability requirement in the new law. Such a measure could apply to *all* organisations that process data, and require them to put in place appropriate, proportionate and effective measures to ensure that they comply with data protection rules in practice.

- ***Disclosing the purposes for collecting data***: We support efforts to enhance transparency, including the requirement that data controllers disclose information to users about their rights to access or correct their data. We believe that organisations collecting data are best placed to determine the most appropriate formulation of notices to data subjects, depending on their services and the context in which they are providing the information.
- ***Transferring personal data outside of Singapore***: We *strongly agree* with the consultation paper's recommendation that the onus should be on the organisation transferring personal data outside of Singapore to ensure that the appropriate measures are taken to protect that data. This is fully in line with the adoption of rules obligating all entities handling personal data to be accountable for their actions. More broadly, we encourage Singapore to take the lead in multilateral discussions – including with APEC and ASEAN lawmakers – involving international data transfer, with the aim of agreeing baseline data protection principles that will facilitate efficient international data flows and that will give users confidence that their data is safe wherever it travels.

Rules on Accuracy, Protection and Retention of Personal Data (Questions 14-15)

- Microsoft believes that it is the responsibility of data controllers to take reasonable efforts to maintain accurate records of data subjects and to protect this data from unauthorised access, collection, use, copying, modification, disposal and disclosure. We support the proposal for the new DPC to develop guidelines for data controllers on data security and governance.
- We agree that, as the consultation document notes, it is not always practical for organisations to specify the retention period for personal data at the collection point. Instead, we support the right for individuals to be informed of the retention period for their personal data upon request.

Rules on Access to and Correction of Personal Data (Question 16)

- Microsoft supports individuals' reasonable right to access and correct their data where possible. We also agree that data controllers should be required to provide information about the ways in which personal data is being used. In order to ensure these obligations are workable in practice, we recommend that controllers be allowed to provide the *categories* of organisations to which data has been disclosed rather than individual names that may mean little to data subjects. We also recommend that access to personal data should only be granted to individuals who can be authenticated, to prevent the accidental sharing of personal data with third parties.

Penalty and Enforcement Regime (Questions 17-18)

- Effective regulatory regimes require both consistent oversight to deter organisations from contravening the rules, and clear and meaningful sanctions for violations when they occur. We support the creation of an independent and well-resourced DPC with statutory enforcement powers. To maximize its resources, we encourage the DPC to target violations of the rules that create a real risk of serious harm and repeat offenders who consistently disregard the law.

Regulations, Code of Practice and Guidelines (Question 19)

- We agree that the DP law should be flexible, and that where further guidance is needed DPC codes of practice or guidelines may be appropriate. To ensure the DPC is both well-informed and has credibility, we encourage it to operate in a transparent manner and to consult openly and regularly with stakeholders.

Transitional Arrangements (Question 20)

- We agree that there should be a transition period for the new DP law, but would also submit that the longer the delay the greater the risk to Singapore-based data controllers competing for international customers. We also accept that many small businesses may need more time than large enterprises to comply with the new procedures and submit that one approach may be the implementation of the DP law in two stages: a sunrise period of 12 months after enactment for all large private sector enterprises and a sunrise period of 24 months after enactment for all small and medium size enterprise (SMEs). An SME could be defined in line with the Government's own definition, namely; a business with annual sales turnover of not more than S$100 million, or, employment size of not more than 200 workers sector. This definition would apply to over 99% of all SMEs in Singapore.

Comments

A. Key Objectives and Principles (Questions 1-2)

We agree strongly that the time has come for Singapore to establish a general DP regime. As the consultation recognises, new technologies offer tremendous opportunities for Singapore. At the same time, these technologies are testing Singapore's existing and fragmented data protection rules. A coherent and robust a forward-looking DP regime is essential if Singapore is to achieve its aspirations to become a leading market for new data-based services, including cloud computing. Without such a regime, consumers may lack the confidence necessary to try new online services, and enterprises may lack the legal certainty necessary to make operational and strategic decisions.

We also believe that the objectives and principles outlined in the consultation document - ensuring adequate safeguards to protect consumers' personal data and promoting trust while given businesses legal certainty, managing compliance costs, and ensuring consistency with international standards – are consistent with the development of a next generation data protection regime. Indeed, we see the development of the data protection regime as necessary for the advancement of Singapore's cloud computing ecosystem, and we are encouraged by Minister Lui's comments on the launch of the review that:

> *"The Government will be introducing a data protection law that will provide a baseline standard for data protection in Singapore….It will also enhance Singapore's overall competitiveness and strengthen our position as a trusted hub for businesses and a choice location for global data management and processing services."*

Of course, achieving these objectives will be more complicated than establishing them. To ensure that the DP regime Singapore ultimately adopts is indeed fit for purpose, we recommend that each provision of the proposed legislation be tested against certain fundamental criteria, among them:

Certainty. The proposed regime is intended to create certainty via baseline legislation on which other laws and codes can be applied; however, this baseline must not only meet local privacy and data protection needs, it must also interoperate with other regional and global regulatory frameworks. The current patchwork of regulatory frameworks governing data protection across the world has become increasingly difficult for companies of all sizes to comply with as ever-larger volumes of data move across geographic boundaries. Even in Singapore today, the sectoral regulations in healthcare and financial services do not only affect the free flow of information within Singapore, they also influence the decisions of regulators in other jurisdictions

in framing their data protection laws.[2] Any reform within Singapore should consider the local and global regulatory ecosystems more broadly, and seek to further promote the harmonisation of data protection laws to provide greater certainty for data subjects and the organisations handling personal data in multiple markets. Without this interoperable policy framework, Singapore-based data processors could find themselves unable to service customers in markets where the local laws preclude the exporting of data to jurisdictions without comparable data protection regimes.

Flexibility. We believe that a greater focus on achieving substantive outcomes rather than prescriptive and rigid rules will render data protection laws more resilient and more durable. A DP law crafted in this way gives organisations the flexibility to adapt their policies and practices to meet changing scenarios, while still subjecting them to the obligation to provide strong privacy protections. We are therefore pleased that the Government is proposing a principles-based approach to allow for a degree of flexibility in interpretation, enforcement and penalties and empowering the DPC to issue guidelines and codes of practice. We are also supportive of the scope for the Minister to make further regulations under the Act to ensure that the laws keep pace with community attitudes, technology innovations and evolving bet practice in privacy law.

Simplified data flows. Today, data is no longer constrained within organisational or geographic silos. Instead, personal data regularly crosses national and international borders. It is important to acknowledge this trend and improve existing mechanisms for international data transfer to ensure that they continue to protect users while facilitating the data flows necessary to enable more efficient, more reliable, and more secure delivery of online services to Singapore's citizens and those organisations that use Singapore as a data hosting and processing hub. Accordingly, we are encouraged that the final data protection model will be informed not just on regional models and international standards such as the APEC Privacy Framework and OECD Guidelines, but also best practices in jurisdictions such as the European Union, Canada, the United Kingdom and New Zealand.

Technology neutrality. There is no question that technology will continue to change – and change quickly. Legislative preferences for particular services, solutions or mechanisms to protect data will quickly be superseded by new technologies. Today, for example, there is significant debate over how best to secure effective user consents to cookies by means of Internet browser settings, website notices, and the like. Preferences for one approach over another can chill innovation, deterring providers from developing alternative approaches to protect data. To this

[2] http://www.scmagazine.com.au/News/235977,singapore-regulator-casts-doubt-on-banking-clouds.aspx

end, we endorse the objective outlined in the consultation paper that the data protection regime will be "technology-neutral as far as possible".

Finally, regarding the proposal to apply the DP law as a baseline concurrent with existing sectoral regulations (e.g., in the financial services sector), we agree that this approach recognises the different needs of different sectors and is preferable to enacting a law that either wholly supersedes or is superseded by sectoral regulations. That said, we encourage MICA to work with other regulators and industry stakeholder to revisit existing sectoral regimes to be sure that they reflect the principles outlined above – and where possible facilitate a transition towards more flexibility in the movement of data with respect to cloud computing and third party hosting in these sectors.

B. Scope of Coverage (Questions 3-6)

1. *Types of Data Covered (Questions 3-4)*

Perhaps the most important element of any data protection legislation is the definition of "personal data." An overly broad definition can have the unintended consequence of over-inclusion of data types – driving up compliance costs for businesses and organisations and impeding the free flow of information while providing little in way of enhanced protection for data subjects. An overly narrow definition can dramatically undermine the confidence of data subjects that the regime is seeking to protect.

The consultation paper proposes the following as the definition of "personal data":

> "*Personal data" means information about an identified or identifiable individual; where "individual" means a natural person, whether living or deceased.*

In our view, this definition is a good starting point, as it is broadly in line with the definitions in other data protection legislation around the world, strikes a balance between under and over inclusion of data types, and retains a degree of flexibility that will ensure it can encompass future data types. This flexible approach is preferable to creating a definitive list of personal data that would no doubt become out-of-date as new types of personal data emerge. "Fixed" lists of what is and is not personal data (or sensitive data) also fail to recognise that what constitutes personal data is generally context specific.

We also support the consultation paper's proposal to permit the new DPC to provide guidance on what information may constitute personal data, and in which contexts. This approach will no doubt provide organisations and data subjects with helpful guidance on how the law should be interpreted. At the same time, it will ensure that Singapore's DP law is better able to address new technologies

that rely on data that may or may not be personal depending on the context, such as the cookies and IP addresses that underpin many of the digital services we take for granted today.

2. *Types of Organisations and Activities Covered (Questions 5-6)*

Microsoft supports the broad application of the proposed data protection law to all private sector organisations, and would limit exemptions for particular types of organisations or sectors as this is likely only to increase the complexity of the regime and thereby increase compliance costs.

With respect to the application of the proposed regime to organisations *outside* of Singapore that collect or process data *in* Singapore, the consultation paper correctly points to the practical difficulties of extra-territoriality and enforcing any data protection law where an organisation has no physical or operational presence in Singapore. This is a concern shared by data protection authorities around the world.

While there are no easy solutions, there are models that merit exploration to address difficult issues of applicable law and cross border enforcement. One model – currently being considered in the EU – would base the determination of which country's data protection rules apply on a country-of-origin principle. More specifically, EU Member State regulators have endorsed an approach under which the data protection law that applies would be determined by the location of the company's "main establishment." While "main establishment" can be defined in various ways, we endorse a definition that looks to the location of the company's primary data centre, on the grounds that this approach ensures that the law that applies is that of the market with the closest nexus to the actual processing. Applying this rule to Singapore and in the context of cloud services would mean that Singapore's DP law would apply if a company has a primary data centre in the country.

The above approach helps to ensure that companies operating at multinational level are not subject to multiple (and sometimes inconsistent) legal obligations flowing from the different jurisdictions in which they operate. Of course, it is equally important that data subjects have confidence that their data is safe wherever it is stored. To this end, we also believe that Singapore should work closely with its trading partners to agree harmonised, robust international baseline standards of data protection and mechanisms for ensuring compliance with those standards – such as the progressive work being achieved around the APEC Data Privacy Pathfinder projects and the more recent development of the APEC Cross Border Privacy Rules (CBPRs). These rules provide both businesses and regulators with greater clarity over the accountabilities of sharing information across jurisdictions. Moreover, the CBPRs provide greater coordination and sharing between data protection authorities in the area of compliance and enforcement. As a long-term partner to APEC on its Pathfinder projects and the

development of the CBPRs, Microsoft has confidence that this coordination will protect consumers' personal data while simultaneously taking into account the regulatory conditions and data ecosystems across Asia-Pacific.

While seeking to apply Singapore law to the operations of off-shore data collectors will remain challenging whatever framework is adopted, the reach of a data protection law also poses an interesting counterpoint – namely, should Singapore law apply to foreign data customers using data hosting services here in Singapore? In other words, should the data or service hosted by a cloud provider in Singapore for a foreign customer be subject to local law when that data or service is not being accessed or used by anyone in the provision of a service in Singapore. The closest analogy would be a 'free-port' where the goods that are in transit or storage and not destined for local use or consumption do not attract any compliance with many local laws.

How this applies to the virtual trade in goods and services remains an interesting question, but one that is being posed with greater frequently. For instance, a recent report on the future of cloud computing in Australia floated the concept along these lines:

> *Superior regulation could help facilitate export growth in two ways:*
>
> 1. *Firstly we could pioneer a careful separation between the regulation of local supply and export so as to exempt foreign purchasers of Australian cloud services from any regulatory requirements that exist in Australia solely to protect Australian users;*
>
> 2. *Secondly we could allow foreigner purchasers of cloud services to "opt in" to that regulation should they wish.* [3]

We do not endorse this approach as a substitute for greater international harmonisation of data protection laws, but, given Singapore's heritage as an attractive and efficient transit point for physical goods, we encourage further innovative policy approaches to data importation into Singapore by removing local compliance burdens on Singapore-based data controllers handling international customer data assets.

---

[3] The Potential for Cloud Computing Services in Australia: October 2011. Page (vi) http://www.lateraleconomics.com.au/outputs/The%20potential%20for%20cloud%20computing%20services%20in%20Australia.pdf

C. Rules and Exclusions (Questions 7 – 16)

1. *General Exclusions (Questions 7-9)*

In order to increase legal certainty, Microsoft believes that any baseline law should be as comprehensive as possible with few exemptions. That said, we agree that some of the proposed exclusions from the data protection law, as listed below, are appropriate:

- personal data recorded in a court document;
- personal data contained in a record under the control of a public agency;
- disclosure of personal data by a public agency to a specific organisation or the public generally;
- collection, use or disclosure of personal data by a news organisation in the course of a news activity; and
- collection, use or disclosure of personal data of an individual's business contact information for the sole purpose of enabling the individual to be contacted in relation to the individual's employment, business or profession.

The consultation paper also asks whether the DP law should provide exclusions for the collection, use and disclosure of personal data solely for literary and artistic purposes. Although it can be difficult to define such exclusions, especially in a digital age, Microsoft believes that these should exist in the new law. Privacy and data protection laws should not be used to limit free expression and creativity when there are other avenues for aggrieved data subjects to seek redress, including defamation and civil litigation.

2. *General Rules (regarding controllers/processors, consent and accountability) (Questions 10-11)*

Data Controller/Data Processor: As one of the world's leading online service providers, Microsoft has substantial experience managing the personal information of not only our enterprise customers through our Office 365, Windows Azure and Dynamics CRM Online products, but also of hundreds of millions of individual subscribers information through services such as Windows Live Hotmail, Xbox Live, Bing search and Office Web Apps. We are both a data processor and data controller and few companies have the experience that Microsoft has in managing these responsibilities on a global scale for so many data subjects.

We agree that *all* organisations should be required to protect data under their custody and control. This reflects the state of data management for organisations of all sizes, especially in the current cloud

computing environment. Many businesses, large and small, may have email systems, personnel records, customer relationship databases, corporate websites, even payments systems hosted by third party data processors. This is likely to only increase given the growth of cloud computing services and the compelling economics behind data controllers moving to a third-party provider model. One way to ensure the robust protection of data across the controller/processor spectrum is to adopt broad-based accountability requirements that apply to both controllers and processors (an option we discuss in more detail below).

That said, while all organisations should be required to protect data under their custody or control, certain responsibilities should belong to companies that control the data as opposed to those that are simply processing or hosting the data on their behalf. For example, many of the primary responsibilities under the law --such as providing notice, obtaining consent or otherwise establishing a legal basis for processing the data, ensuring data are accurate, and responding to data subject access requests -- should rest with the data controller. Such obligations should not be imposed on mere processors, who only act on behalf of controller customers; instead, processors' primary responsibility should be to comply with general requirements of the law such as securing all data that they process, as well as to fulfil contractual obligations that their controller customers impose. Indeed, imposing obligations on processors, such as the giving of notice or the collection of consent, in many situations will be unworkable; processors, for example, may be unlikely to interact with data subjects in ways that permit the gathering of consent. Similarly, a processor's typical method of providing notice to data subjects could be at odds with that of the controller, in which case the controller's method should apply.

Consent: We agree that in many circumstances it is important and appropriate to obtain an individual's consent in order to collect, use or disclose his or her personal data. As the consultation document recognises (at 3.42 - 3.48) however, there scenarios where obtaining consent before collecting personal data may be neither practical nor necessary. For that reason, we recommend that the proposed DP law should also include other legal bases to justify the collection and processing of data.

For example, in addition to the exceptions to consent that are outlined in the consultation document, we recommend that the new DP law expressly provide that organisations may process an individual's personal data (without having to obtain his or her consent) where this is necessary for the purposes of legitimate interests that the organisation is pursuing, except where these interests are overridden by the interests for the fundamental rights and freedoms of the individual. For guidance, we encourage MICA to consider Article 7 of the EU Data Protection Directive (95/46/EC), which lists several

conditions that justify the processing of data, including consent and many of the exceptions listed in the consultation document, as well as this "legitimate interests" basis.

Where it *is* necessary to obtain consent, we agree with the consultation document that the type of consent should be allowed to vary depending on the specific context of the collection. We therefore strongly support the proposal not to prescribe in detail the manner in which consent may be given in the DP law. Indeed, the consultation document notes that consent "may be explicit or implied, depending on the circumstances." This is a very practical viewpoint that ensures that organisations are able to choose the most effective means of obtaining consent. We believe equally that consent should be permitted on the basis of "opt-out" or "opt-in" depending on the scenario (as described in section 3.35). Currently there are a wide range of mechanisms that enable users to control and consent to collection and use of their information, and some of the more robust opt-out mechanisms provide stronger protection for consumer privacy (with fewer disruptions for Internet users) than weaker opt-in mechanisms. For example, given that modern websites increasingly pull content from multiple sources, requiring users to provide separate opt-in consents in relation to every site that is the source of content would result in users receiving a significant number of opt-in requests every time they go online – a situation which often leads to users opting-in as a matter of routine, even when their privacy would be better served by their opting out. We thus believe that any final data protection laws should recognise the validity of a range of mechanisms for consent, including an informed opt-out and should require that all such mechanisms enable meaningful consent in the particular context in which they are deployed.

Accountability: To implement principles of "accountability" into the new DP law, the consultation proposes requiring organisations to designate one or more individuals responsible for compliance. We encourage MICA to consider the introduction of even broader accountability requirements in the new law that would apply to *all* organisations that process data.

Although there has been considerable discussion in international data privacy circles about "accountability" recently, as noted the basic principle is not new. Accountability was included nearly 30 years ago in the OECD's 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; today, it finds expression in the Canadian Personal Information Protection and Electronic Documents Act, the APEC Privacy Framework and in other data protection regimes around the globe. The principle also appears in the privacy standards released at the conclusion of the 2009 international commissioners' conference in Madrid and meant to serve as a basis for a global privacy standard. Unhelpfully, however, the principle of accountability has been variously formulated in these legal texts, making it challenging to define what it means precisely. Some legal frameworks see

accountability as a mechanism to facilitate cross-border data flows, whereas others understand it as ensuring compliance more broadly.

Thus, at the threshold, it is vital that there be a shared understanding of the principle of accountability. We at Microsoft understand an accountability-based privacy regime to mean that data protection standards and requirements are enshrined in law, but that individual organisations are made more responsible for determining how best to meet those standards in practice. This approach places responsibility directly on the shoulders of the organisations that process personal data, mitigating the burden on individuals to police the use of their data (an obligation that is increasingly challenging in the new information economy). Accountability also means that the law moves away from simply trying to conform to prescriptive rules – regardless of their underlying purpose – and focuses on securing good substantive outcomes, in data protection terms.

Within Microsoft, accountability is a core component of our approach to data privacy, and permeates our own collection and processing of personal data, as well as our interactions with our business partners and vendors. We set ourselves a high standard of data protection based on legal requirements, self-regulation and best practices. We adopt a combination of measures that include policies and practices, technology, training and collaboration to achieve this standard – among them ensuring that privacy and data protections are systematically incorporated into the development and deployment of our products and services; providing users with clearly worded privacy policies; offering users tools to empower them to control their information online; and working with a range of online stakeholders to improve laws, strengthen self-regulatory mechanisms and create a more trustworthy online ecosystem.

Microsoft believes that to be truly accountable, organisations that process personal data must embrace data protection as an important value in its own right. We agree with the consultation document that organisations should be transparent with individuals about their policies and practices regarding how they manage personal data. But being accountable should involve more than simply designating one or more individuals to be responsible for ensuring that they comply with the DP law. Organisations should be required to put in place appropriate and effective measures to ensure that they comply with data protection rules in practice -- including adopting and implementing written policies and procedures regarding the processing of personal data and controls to ensure such policies and processes are effectively implemented (e.g., by educating and training staff); making appropriate summaries of those policies available; adopting appropriate security measures; and appointing an individual at senior management level for responsibility for data protection compliance. To be workable across the full spectrum of organisations that handle personal data, these measures

should be scalable – i.e. proportional to the nature and volume of the personal data that the organisation processes, the nature of the processing, and the risks to the rights and freedoms of individuals whose data are being processed.

3. *Rules on the Collection, Use and Disclosure (including Transfer outside of Singapore) of Personal Data (Questions 12-14)*

Collection and disclosure: As described above in response to questions 10-11, while consent is a key basis for legitimizing the use and disclosure of data, in some contexts obtaining consent may not be necessary or possible. We thus support the exceptions outlined in sections 3.42-3.48 and 3.52-3.59. We also encourage MICA to consider the additional grounds we outline above, relating to use and disclosures aimed at facilitating an organisation's legitimate purposes.

We further recommend that MICA consider a narrow exception to the need for "fresh" consent (section 3.49). The consultation paper suggests that fresh consent must be obtained where data is to be used for a purpose other than that for which the individual has given consent. We would also suggest an additional grounds or exception for the secondary processing of personal information that falls within an individual's reasonable expectations given the context of the processing. In such circumstances, notice and consent become less necessary. For example, when individuals provide their contact information to a company, they generally understand and accept that the company might use the data for the secondary purpose of sending advertisements about its own products, and consent should not be required in these circumstances. Practices that are commonly accepted today include product and service monitoring, support, and fulfilment; internal operations; fraud prevention; authentication; legal compliance; protecting life or personal safety; first-party marketing; acting against security threats; carrying out an employment relationship; corporate mergers; improvement of existing services or development of new services; and sharing data with affiliates that are subject to the same privacy policy.

Turning to the question of *what* disclosures an organisation must make to a data subject when collecting data, we agree that organisations should be required to disclose the purposes for the data collection. Indeed, one of the central tenets of Microsoft's own privacy principles is that users must have choice over how we use and disclose their personal information. Our customers can only exercise this choice in a meaningful way if they are clearly informed about how we intend to process their data. For this reason, we have been at the forefront of efforts to promote transparency in the online space, including being one of the first companies to deploy so-called "layered notices" to better inform users regarding our data handling practices.

Our own experience has demonstrated that providing notice in ways that are clear and easily accessible has helped to promote the uptake of our technologies and services, and encourages users to exercise informed consent. We thus support efforts to enhance transparency by requiring data controllers to disclose information to users about their rights to access and correct their data, and to provide a contact point for any complaints or enquiries. On this latter point, we recommend that the DP law allow organisations to provide contact details for a dedicated privacy office/customer liaison department, which in practice will be in a better position to field inquiries and complaints than a major organisation's Chief Privacy Officer.

In terms of the *content* of notices, we believe that individual data collectors are in the best position to determine the most appropriate formulation of the relevant language in any notice to data subjects, depending on their service and the context in which they are providing the information. To that end, we support the consultation paper's recommendation that the DP law remain silent on the means of obtaining consent and the language of supporting notices to data subjects. Indeed in providing information to data subjects, we believe that prescriptive rules around notice, consent, collection and use can inhibit flexibility and at times have unintended consequences. For example, prohibiting organisations from requiring "an individual to consent to the collection, use or disclosure of personal data beyond what is necessary to provide a product or service" could dissuade organisations from providing free products and services in exchange for information to be used for subsequent product marketing. For example, if a company held a contest giving away t-shirts, they would only be permitted to require name and postal address (strictly necessary to provide the t-shirts to the winners), and not non-pertinent information such as NRIC number, age and ethnicity for example.

Transfer of personal data outside of Singapore. In today's networked world, data knows few geographic boundaries. Instead, data travels regularly across national and regional borders – enabling many of the online services that we now expect and rely on as part of our daily lives. We are therefore encouraged that one of the guiding principles for this review has been to facilitate the international transfer of data – and we *strongly endorse* the consultation's recommendation that the onus be on organisations to ensure that appropriate measures are taken to protect personal data where such data is transferred outside of Singapore. As described above in our earlier comments on accountability, this approach allows data to flow across international borders based on data exporters remaining accountable for the protection of the data regardless of geographic location – placing responsibility on the shoulders of individual organisations that process data to determine how best to meet high standards of data protection. We believe such an approach would ensure the robust protection of data, but at the same time give organisations adequate flexibility to accommodate current data transfer needs.

We also believe that it is vitally important that jurisdictions across the world – Singapore included – work together to develop and agree better harmonised standards of data protection. Broader consensus on international baselines of protection will lessen the perceived need of some markets to restrict data transfers -- and hopefully will lead these markets to adopt more flexible rules that permit data to travel across national and regional borders with fewer impediments.

Microsoft recognises that industry has an important role to play to address this challenge and to foster the emergence of a more uniform and global data protection regime. As a leading technology developer and provider of cloud-based services for consumers and enterprises, Microsoft participates in various industry groups and initiatives whose aim is ensuring that appropriate rules are in place for addressing new technologies and critical issues like data privacy and security. For instance, we are a member of the Digital Due Process coalition, comprising privacy advocates, online companies and think tanks, which has urged the U.S. government to update the Electronic Communications Privacy Act to ensure that data stored in the cloud is subject to the same level of protection as data stored locally, possibly through enactment of a new Cloud Computing Advancement Act. In 2008, we helped form the Global Network Initiative, which remains dedicated to advancing Internet freedom and promoting transparency and user notice online. We also are actively involved with APEC, and have lent our support to the APEC Privacy Framework and Data Privacy Pathfinder project. Through these and many other initiatives, Microsoft is working hard to find solutions.

But industry on its own cannot create the much-needed international framework, despite its best efforts. Policymakers and governments have a vital role to play and Microsoft urges the Government of Singapore to take the opportunity to take a leadership role in working towards a set of universally agreed data protection principles. As a first step toward the long-term solution that is required, we urge the Government of Singapore to commence discussions with APEC and ASEAN lawmakers and regulators – as well as with industry from those markets – with the aim of agreeing to a set of baseline data protection principles applicable to information stored in the cloud. A precedent for such an effort already exists, in the form of the EU-U.S. High Level Contact Group, which is now developing rules for transatlantic data sharing in order to fight terrorism and serious crime.

These initiatives should offer fertile ground for opening up fruitful bilateral discussions between Singapore and the U.S. Ideally, these initial discussions will lead us on a path to more formal multilateral solutions – perhaps in the form of a treaty of similar international instrument under the aegis of the APEC, Trans Pacific Partnership, G20, OECD or another international organisation. In the meantime, the current bilateral and multilateral agreements that Singapore has entered into such as

Free Trade Agreements, Mutual Legal Assistance Treaties and Double Taxation Agreements could also be refined to further promote the free trade in information.

4. *Rules on Accuracy, Protection and Retention of Personal Data (Questions 14-15)*

Microsoft believes that it is the responsibility of data controllers to take reasonable efforts to maintain accurate records of data subjects and protect this data from unauthorised access, collection, use, copying, modification, disposal and disclosure. We thus support the inclusion of provisions in the DP law requiring organisations to ensure that the personal data they collect is reasonably accurate and complete. We also support rules obligating organisations to deploy reasonable security arrangements to protect that data. As the consultation document notes, however, the question of what security measures are appropriate in a given context will depend on the types of data and of processing involved – making it all but impossible for the law to prescribe specific security measures that should apply in all instances. Instead, we support the proposal for the DPC to develop flexible guidelines for data controllers on data security and governance. We also recommend that the DP law include express language making clear that the security measures adopted by an organisation should be appropriate to the risks presented by the nature of the data and its processing.

Turning to the question of the retention of data, we agree that, as the consultation document notes, it is not always practical for organisations to specify the retention period for personal data at the collection point. Different pieces of data collected simultaneously may be retained for varying lengths of time; for example, it is common industry practice to retain credit card numbers for 18 months following the date of a transaction (as per Payment Card Industry rules), while other data collected at the same time may be retained for longer for tax or other purposes. Oftentimes, mandating disclosure of retention timeframes at the point of collection would make privacy policies and other notices more complicated and more difficult for consumers to digest. Rather than requiring organisations to routinely disclose retention times, we believe a more balanced and workable solution would be to give individuals the right to be informed of the retention period for their personal data upon request.

5. *Rules on Access to and Correction of Personal Data (Question 16)*

Access and correction by data subjects: Microsoft supports individuals' reasonable rights to access and correct their data where possible – rights that we believe are essential elements of an individual's ability to control his or her personal data more broadly, particularly online. Indeed, Microsoft is working hard to empower consumers to control their personal data "footprint" online. For example, Tracking Protection in Internet Explorer 9 helps consumers choose which third-party sites

can track them online. Ordinarily, when a consumer visits a website, he will automatically share information with that site such as cookies, IP address, etc. If the website contains content provided by a third-party site (for example, a map, advertisement, or web measurement tools such as a web beacon or scripts), some information about the consumer may be automatically sent to the third-party site. Although that kind of arrangement may benefit the consumer by providing easy access to third party content, it can also impact his privacy because he could be tracked across the Internet by the third-party sites. If the consumer uses a Tracking Protection List in Internet Explorer 9, the consumer can choose which third party sites can receive his information and track him as he browses the web. In our Bing search business, our current practice is that as soon as Microsoft receives a Bing search query we take steps to de-identify the data by separating it from account information that could identify the person who performed the search. Then, at 6 months, we take the additional step of deleting the IP address, and at 18 months, we delete the de-identified cookie ID and any other cross-session IDs associated with the query.

While we thus support the consultation paper's recommendations regarding data access and data correction, we would suggest certain refinements. For example, while we agree that data controllers should be required to provide data subjects with information about the use and disclosure of personal data, we would suggest that controllers be allowed to provide the categories of organisations to which data has been disclosed rather than individual names that may mean little to data subjects.

We also agree that there are circumstances where an organisation should not be required to provide individuals access to personal data. In addition to the scenarios described in paragraph 3.72, we suggest that data protection legislation or guidance from the DPC explicitly note that access should only be granted to individuals who can be authenticated, to prevent the accidental sharing of personal data with third parties. For example, if a consumer forgets his password for an email account, he should be authenticated (perhaps via a secondary email address or text message to a mobile number previously collected) before being granted access to the account.

Government access: We also encourage Singapore to consider data access in a broader context – and more specifically to look beyond the right of data subjects to access their data, and to consider when third parties, and particularly domestic and foreign government authorities, are permitted to access such data. Governments, confronted with the challenge of online crime and the use of the Internet in connection with threats to public safety or national security, increasingly are focused on obtaining access to user content and other data held by cloud service providers.

In the consultation paper, it is proposed that in circumstances of a national security, defence, public safety, the conduct of international affairs or similar matters of such interest, a data subject would not be notified if their personal data were accessed in the course of such an investigation. While we are sensitive to the need for confidentiality and secrecy in the conduct of law enforcement and national security investigations, we also submit that more transparency is needed about the circumstances under which government authorities can search, seize, or intercept data held by data controllers and processors. This is important not only for due process, but in the absence of this transparency, customers may actually lose confidence in the security of their data being hosted in Singapore and choose to host their data in another jurisdiction. Consistent with these views, as a general rule when Microsoft maintains data within a specific country and is required to comply with legal process from a governmental entity for records held in its custody, we use reasonable efforts to provide the customer with notice that a demand for its records has been made when providing such notice is permissible. Microsoft may, however, be prohibited by law in some circumstances from providing such notice, in which case notice would not be provided.

In addition to questions involving transparency, cloud providers often face the further dilemma of trying to comply with inconsistent laws in this area, especially where multiple jurisdictions may have an interest in a single matter, each seeking access to user information. There are, however, no universally agreed upon rules governing such access by law enforcement. The result is that service providers are increasingly subject to divergent, and at times conflicting, rules governing access to user generated content and data.

This global thicket of competing and conflicting laws presents a significant obstacle to the delivery of cloud services that meet users' reasonable expectations of privacy. Where the rules of different nations conflict, a cloud provider's decision to comply with a lawful demand for user data in one jurisdiction may place that provider at risk of violating the privacy laws (or other laws) of another jurisdiction. Equally troubling, this situation makes it extremely difficult for providers to give their customers accurate and adequate notice of the conditions under which their data might be accessed by law enforcement.

Many governments have attempted to establish procedures to avoid such conflicts, but the mechanisms for doing so have not been successful in practice. International legal instruments for the sharing of information have in some circumstances (such as when a government is attempting to thwart an on-going crime) proven slow and cumbersome. As such, some countries have begun to ignore established procedures and simply demand that local employees, under threat of personal legal jeopardy, disclose data regardless of where it is located or to which jurisdiction the relevant

service is provided. To encourage continued investment in cloud computing services, there must be greater clarity and consistency on rules that will protect the privacy and security of user data, encourage cloud providers to operate within Singapore, and ensure legitimate law enforcement needs are addressed.

To achieve this objective, Singapore can take several steps. One ambitious solution would be for Singapore to promote a multilateral framework on these issues in the form of a treaty or similar international instrument. While this option would undoubtedly require significant diplomatic leadership and resources, it offers perhaps the best hope of addressing legitimate government needs in a coherent fashion while ensuring that business and consumer interests in privacy and freedom of expression are adequately met on a global scale.

A less formal option would be for Singapore to engage independently in consultations and consensus building on procedures for resolving data access issues in ways that avoid conflicts through enhanced Mutual Legal Assistance Treaties (MLATs) for example. Even bilateral discussions on these issues will increase awareness of the problems created by conflicting claims of jurisdiction and pave the way for a longer-term, more formal solution.

Cloud computing will only reach its full potential if providers can establish data centres and offer services in multiple jurisdictions, without fear that each step will invite competing claims of jurisdiction and government access to data. The rules must balance the legitimate needs of law enforcement, industry, and users, and it is vital that all stakeholders are represented in any deliberations. Singapore has much to gain from promoting an enhanced dialogue on the international rules on government access to cloud-based data given its ambitions to be a global data hub. Equally, though, Singapore has much to lose if there is a perception that there is an opaque approach to government access is not addressed in this data protection review and other regulations. [4]

D. Penalty and Enforcement Regime (Questions 17-18)

Effective regulatory regimes require regular oversight to ensure that organisations do not contravene the rules and clear and meaningful sanctions for violations when they occur. The establishment of a Data Protection Commission to enforce the data protection law will be a critical element to fostering

[4] For instance, a recent paper from an Australian cloud computing provider provides the following statement: "*There is tangible risk that data stored in Singapore may be exposed to extremely onerous police investigative powers granted under the Computer Misuse Act….Therefore you should consider that data transferred and stored in Singapore may be at greater risk of being accessed by government and law enforcement agencies, than data stored in Australia*."
http://www.macquarietelecom.com/Portals/0/Downloads/whitepapers/Macquarie_Telecom_Cloud_and_Cross_Border_Risks_Singapore_2011.pdf

trust and promoting compliance. To be effective, the DPC should be independent and well-resourced, and should have statutory enforcement powers, including the right to commence an investigation without a complaint and referring investigations to other regulators when there is the potential for breach of sectoral regulations. In carrying out its responsibilities, we would encourage the DPC to adopt a strategic, risk-based approach to enforcement, focused on those violations that create a real risk of serious harm. [5] Repeat offenders – i.e. those who consistently ignore the data protection rules – should also be a target of the DPC.

In assessing the proposed framework in Singapore, we endorse the tiered enforcement and penalty regime commensurate with the severity of the violation, including orders for corrective action, mediation between contending parties and financial penalties for serious offences. We also support the establishment of an Appeals Board to allow for a review of the DPC's rulings.

E. Regulations, Codes of Practice and Guidelines (Question 19)

As we noted at the outset of our comments, we believe that the most durable data protection regimes are those that are not overly prescriptive, and that instead build in a degree of flexibility. However, clarity as to how rules work is also important both for the confidence of data subjects and for organisations seeking to operate within the boundaries of the law. We agree with the consultation paper that empowering the DPC to issue on-going guidance on issues under the regime will help to achieve these ends. In addition to the issues identified above (such as the scope of personal data), another area where DPC guidance may be useful is accountability. As notions of what constitutes best practice in accountability evolve and expand, DPC leadership in this regard would be welcomed.

To ensure that the DPC has credibility in issuing guidance, we recommend that its operations be made transparent through measures such as engaging in regular dialogues with stakeholders and opening certain discussions and debates to the public. We also recommend that the DPC engage actively with industry in formulating its positions and generating guidance, to ensure that they remain fully informed and accurate as possible. This is especially important where guidance disproportionately impacts an industry sector or particular company or companies, or where the DPC is focusing on technology related issues, where sophisticated technical input is often essential

[5] The UK's data protection regime provides a good example of a risk-based approach to enforcement. In the UK, the Information Commissioner now has the power to impose significant fines when a contravention is serious and is likely to cause substantial damage or substantial distress, and where the data controller either (i) deliberately contravened the UK Data Protection Act or (ii) knew or ought to have known that there was a risk the contravention would occur, and that it would be likely to cause substantial damage or distress, but still failed to take reasonable steps to prevent it from happening. Such an approach provides a meaningful deterrent and is likely to lead to improved privacy protection for individuals; at the same time, the sanctions are properly limited to truly bad actors.

Transition Period:

Microsoft strongly believes that the enactment of a DP law is a priority and that any unnecessary delay to its implementation may not only result in Singapore being further out-of-step with regional and global policy frameworks, but also affect the ability of Singapore-based data controllers to effectively compete for international data customers in many jurisdictions across the world. We therefore submit that there is no time to lose.

As already suggested in the consultation paper, for many organisations the enactment of the DP law will simply formalise their existing procedures, especially those organisations that comply with industry codes of practices, including the Model Code. Other organisations, such as small and medium enterprises (SMEs), may have no such data protection or privacy procedures in place.

While Microsoft does not endorse separate DP regimes based on the size of an organisation, we do recognize the need to maintain policy momentum and foster certainty for large enterprises (such as those seeking to invest in local data centre infrastructure or external customers seeking to host their data in Singapore) and the needs of smaller organisations to adjust to any new DP law requirements. To that end, one option that merits consideration is a two stage implementation process before the application of the DP law: a sunrise period of 12 months after enactment for all large private sector enterprises; and a sunrise period of 24 months after enactment for all small and medium size enterprises.

A small and medium size enterprise could be defined in many ways, but it might prove useful to reference the Standards, Productivity and Innovation Board ("SPRING") definition which, as of 1 April 2011, has adopted the following criteria: enterprises qualify as SMEs as long as they satisfy at least one of two parameters; 1) annual sales turnover of not more than S$100 million or 2) employment size of not more than 200 workers sector.[6] A similar definition could be applied to the transition arrangements for the DP law noting that under these criteria, more than 154,100 SMEs - making up 99.3% of total enterprises in Singapore - would have 24 months to comply with the new arrangements.

Conclusion

[6] http://www.spring.gov.sg/NewsEvents/PR/Documents/Fact_Sheet_on_New_SME_Definition.pdf

Modern computing paradigms – the cloud foremost among them – provide new opportunities for Singapore and its citizens. At the same time, these paradigms also create new challenges, particularly around the processing of personal data. Addressing these challenges is critical if Singapore is to become among the world's leading cloud centres.

Microsoft believes that the proposals in the MICA consultation paper go a long way toward establishing a policy framework that will promote consumer confidence, create a legal infrastructure where organisations can innovate and grow, and foster the cloud computing marketplace. We are confident that any data protection law enacted in Singapore will achieve the right balance between efficiency and privacy, innovation and security.

But the reforms do not end there. Continual policy refinement around core issues such as data security, technology standards, data governance and access, and the promotion of international trade in data are essential for Singapore to retain its reputation as a policy innovator and technology hub. Microsoft stands ready to apply its experience and expertise to help achieve these aims and further advance Singapore's ambition to be Asia's preferred destination for the technology sector.