RESPONSE TO THE CONSULTATION PAPER FOR THE PROPOSED CONSUMER DATA PROTECTION REGIME FOR SINGAPORE
25 OCTOBER 2011

Submitted by : Nokia Pte Ltd

Lee May May / Raymond Choo

Nokia Legal and Intellectual Property

Email : maymay.lee@nokia.com , raymond.choo@nokia.com

---

1. INTRODUCTION

Nokia welcomes the opportunity to comment on the proposed consumer Data Protection regime for Singapore as described in the Consultation Paper issued by the Ministry of Information, Communication and the Arts on 13 Sept 2011. This paper outlines Nokia's position on the Consultation Paper and aims to provide practical recommendations on the future Singapore data protection framework.

Nokia welcomes the approach defined in the Consultation Paper. Globally interoperable data protection and privacy regimes, based on globally recognized privacy principles[1], are needed to ensure effective privacy protection in a globalized economy. Barriers to mutual recognition between different legal systems should be identified and removed. Ambiguity around applicable laws should be clarified. By drawing together recognised privacy principles from different legislative backgrounds, a realistic way forward for international businesses seeking consistency may be found. The overall approach defined in the consultation is an important step in the right direction.

This position paper starts by outlining some underlying basic principles that are essential for a successful new privacy regulatory framework. We will then provide more detailed comments on the topics raised in the Consultation Paper.

We have focused primarily on how private entities, such as Nokia, protect personal data.

2. KEY OBJECTIVES FOR THE DATA PROTECTION REGIME

The data protection regime should:

1. **Foster trust in digital life** by ensuring that users have fair and informed choices as to how their personal data is processed, users are offered with effective rights of access, erasure and blocking, data processing is proportionate and reasonably secure through application of appropriate organizational and technical security measures, on a state of the art basis, and that controllers are accountable for their data processing. A right balance between data protection and other legal

[1] See e.g. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the principles underlying the EU Data Protection Directive and the APEC Privacy Framework.

protections in a world where most human social behavior takes place in digital context needs to be found.

2. **Recognize the global nature of information flows** in the information economy by streamlining the legal instruments for international data transfers**.** A system based on holding the service provider accountable offers a meaningful basis for international data transfers. Companies should be able to certify their data processing on a worldwide basis. Work towards global privacy standards should continue.

3. **Be principle-based, technology neutral and focus on regulating the "what" instead of the "how"** to stand the test of time, to avoid a "chilling effect" on innovation and to cater for a large variety of different activities and business models ranging from offline transactions in public and private sector to internet banking, online shopping, location based services and social networking. The regulation should be clear on the objectives but avoid regulating in detail how those objectives are met to allow them to be met in a flexible manner in the context of different technologies and business models. Modalities, for example on consents or transparency notices should not be introduced.

4. **Be harms based** by distinguishing between different types of data processing based on the nature of the personal data in question, the harm that the processing may cause to individuals, the likelihood of such harm as well as the relationship between the controller and the individual concerned. Definition of personal data and transparency and consent requirements should reflect the harm pertinent to the activity in question. Enforcement should be harms based.

5. **Encourage companies to meet and exceed compliance requirements** not only through sanctions but also through positive incentives such as giving credit for participation in voluntary certification programs (for example "trust seals") and applying accountability and Privacy by Design principles. Self-regulation and co-regulation should be encouraged to find practical solutions to emerging issues in a principle-based regulatory environment.

6. **Foster creation of a privacy culture** in the society with co-operation between the public and private sectors. Privacy education, social awareness to common threats, creation of a privacy profession based on a privacy knowledge base and certification for categories of privacy professionals should be promoted. In addition, through continued public sector efforts, foster research into underlying technology standards and engineering processes for Privacy by Design principles to speed the availability of privacy-aware products.

Key concepts such as accountability, limitation of administrative burden and focusing on the outcomes of the regulation are all connected with and essential for reaching the above objectives.

3. STRENGTHENING INDIVIDUALS' RIGHTS

Ultimately users must be able to trust the digital ecosystem. Ensuring users are granted with appropriate rights is a key element of the trustworthiness of such an ecosystem. Nokia is committed to trust in digital life[2].

The world has become digital. Most forms of traditional social behavior already take place in a digital form. Social sharing, for example, is something that has always taken place and legal protections have always existed to discourage inappropriate behaviour, for example through criminalization of defamation. Digitalization, however, has brought about new dimensions that can aggravate the social impact of undesirable behaviors, such as the effect of instant worldwide and permanent publishing of an individual's activities in an unprecedented fashion.

Also, our physical surroundings and activities in public spaces are increasingly documented in a digital form. It will be ever more difficult, yet important to determine what privacy in public spaces mean in an era where digital cameras are everywhere and powerful technologies, such as facial recognition and data mining are widely available to the public.

As the users and society alike are still exploring the limits of appropriate behavior in a digitalized environment, the data protection regime needs to find an answer for the activities that should be governed by data protection rules and the activities that should be governed by other legal protections.

3.1 Concept of personal data (QUESTION 3 of Consultation Paper)

General observations: The concept of what constitutes personal data is fundamental to the application of any data protection regime. The proposed definition of personal data is binary in nature. In other words, if the definition is met, the regulation applies in full and where the definition is not met, no protection is available. This fails to recognize the difference in the potential harm pertinent in the data processing in question and is problematic in at least two dimensions: First, it places onerous obligations on organizations where the real harm to individuals is questionable. Second, where the definition is not met there is a risk of leaving certain data processing outside of protection where actual risks to the fundamental rights of individuals may be present.

One example is the use of various pseudonymous or indirectly identifiable data, such as IP-addresses, key-coded information, mobile device serial numbers or other such identifiers. These do not enable an individual to be identified directly as such, but can be ***linked*** to an individual if there is access to additional information enabling the association of the identifier with the individual. Often the service provider has neither the intention nor any practical or lawful means to access the needed additional information to identify the individual[3].

---

[2] Nokia is one of the founding partners of Trust in Digital Life –consortium. See http://www.trustindigitallife.eu/.

[3] In case of IP-address, the value added service provider typically has no lawful access to the ISP's DHCP log, which would be needed to enable the service provider to identify the individual to whom

On the other hand, not all unique identifiers are ***linkable*** to any specific individual. For example, the use of non-persistent unique identifiers that change from one session to the other make it not possible to link different sessions to same user. Typically the use of these identifiers makes the information not personally identifiable.

In some instances the sole purpose of data collection may be creation of non-personal statistical information based on information that is made anonymous upon its collection, for example by deleting or obfuscating any identifiers that may have been associated to the information upon its collection. It is not clear why full consent regime should apply to this kind of anonymous processing, at least when there are appropriate safeguards in place to ensure the anonymity of the collected information.

Furthermore, there are categories of more sensitive information that may warrant additional protections. For example, location data that can be linked to an individual, credit card details, information relating to health, sexual preferences and other similar types of information are often considered to be information for which more robust consent mechanisms and other safeguards should apply.

Modern analytical technologies increasingly allow relatively accurate estimation of the identity of an individual through combination of various pieces of information, fingerprinting and other such means. Indeed, it seems that the distinction between anonymous and personal data is increasingly difficult to make. In some instances, indirectly identifiable data types do warrant privacy protection as this data may sometimes be used to target activities to individuals.

3.2 Personal Data of Deceased persons (QUESTION 4 of the Consultation Paper)

While it seems reasonable to provide an element of privacy protection to a deceased person's personal data, there are practical issues which the regime should have answers/guidance for.

The deceased person's rights and obligations are typically passed on as a general succession in accordance with the applicable laws. To manage the deceased person's estate, access to his personal records is to a certain extent necessary. Furthermore, service providers may be asked to hand over passwords to email accounts or other such records as there may be invoices or other information that is needed to manage the estate of the deceased person concerned. Password protected cloud databases or local storages may contain for example pictures, contact books, letters, diaries or basically any information that may or may not be known to the family of the deceased.

Irrespective of the time period for privacy protection for the deceased, service providers and other parties will face difficulties in dealing with everyday incidents without clear rules on

---

the IP address relates. Similar analogy applies to IMEI codes. In fact the ISP has a legal obligation not to disclose that information and to protect that data against unauthorized access and use.

how to deal with these practical issues in case the Data Protection regime in Singapore extends to deceased persons' personal data.

Recommendation: We agree that the data protection regime should not prescribe what particular data item is personal data and what is not. However, the information classification system within the data protection regime should have the potential to allocate obligations on a more predictable and ***harms-based*** basis, appropriate to the processing at hand. For example, determining the prominence of notices towards the user, defining requirements on various types of consents and identification of the required level of technical and organizational measures to protect the data as well as identifying thresholds for breach notifications should be based on recognizition of the differences between various categories of information and the different nature of data processing even for the same categories of personal data. The extent to which privacy protection should also cover deceased persons and the duration of such privacy protection should be carefully considered to avoid practical difficulties.

3.3 Types of organizations and activities covered (QUESTIONS 5 and 6 of Consultation Paper)

The data protection regime should take note of the fact that commercial activity often takes place in the context of affiliated group companies. Any transfer of personal data within such a group should not be deemed as data transfer to a third party provided that there are adequate privacy protections in place within the group and the purpose of data processing does not materially change.

The question of applicable law is one of the most difficult questions in data protection today. Online services are provided over distance and often without regard to national borders. The rules governing governmental access to personal data, e.g. for law enforcement purposes, do not always follow the same principles as those adopted in data protection laws. Companies offering services in multiple countries often find themselves in a complex web of applicable laws for the very same data processing. This makes it difficult to implement group-wide privacy practices and policies without any clear benefit to data subjects.

However, and at least to the extent the service provider is established in a region where substantially the same level of protection for personal data processing is offered, a country of origin of the service provider principle, based on the service provider's establishment, should be applied or at least such should be a possibility of following the contract between the individual and the service provider.

Also, while it is understandable that the provision of services that are targeted and consumed in Singapore should receive appropriate privacy protection under the proposed Singapore data protection laws, it is less clear why Singapore regulation should apply in full to activities where both the data subject and the controller are non-Singaporeans or are not based in Singapore, the service is not consumed in Singapore and the only link to Singapore is that the data is processed in Singapore. A more meaningful connection to Singapore, in particular to Singapore data subjects, should exist for the Singapore data protection law to

be applied in full. Mere processing of personal data within Singapore should not attract application of the Singapore data protection law if the controller and its data subjects have no wider relationship within Singapore.

In case of mere processing of personal data in Singapore, the processed information should receive protection against unlawful access, modification, loss or alteration by any third party to achieve the objectives defined in the Consultation Paper. An exemption for the mere transit of data through Singapore should be considered.

Recommendation: The rules governing applicable law need to be carefully considered to ensure legal certainty, a level playing field and appropriate appreciation of increasingly globalized data processing environment. The ultimate objective should be a system of globally interoperable privacy law, sufficiently harmonized, based on same principles and applying the same accountability principles to ensure mutual trust between different countries. In such context, a country-of-origin principle, based on the service provider's establishment, is warranted provided that individuals have appropriate means of redress available in case of breach. In a world where data processing pertaining to same purpose physically takes place in numerous locations by various processors simultaneously it would not be practical to use the location of data processing as the criteria for defining the applicable law.

3.4 Exclusions (QUESTIONS 7, 8 and 9 of the Consultation Paper)

We believe the exclusions referred to in the consultation are generally appropriate. However, it should be considered whether or not it would be appropriate to add a household exemption, similar to that adopted in the European Data Protection Directive[4]. As many types of data processing takes place within a household for purposes relating to individuals' private life, for example managing family photo albums on the household computer. It should be considered whether it makes sense to extend the application of data protection laws to such activities.

In general we believe data protection rules should apply only to processing of structured sets of personal data. For example paper note books with information e.g. on meeting participants should not fall under the proposed law.

3.5 Data controller and processor distinction (QUESTION 10 of the Consultation Paper)

The regime should be clear on what the obligations are that an organization has to comply with. This allocation of responsibilities should reflect the role that organization has in the data processing in question.

[4] The individual handling and processing personal data is doing so "in the course of a purely personal or household activity" and according to Article 3 of the European Data Protection Directive 95/46 is exempted from the provisions of the European Data Protection Directive 95/46.

More and more data processing is outsourced by the organization having the relationship with an individual (controller) to service providers specialized in various types of processing activities to process personal data on their behalf (processors). Controllers often rely on their service providers to determine the most effective technological solutions to deliver outsourced processing.

However, such a processor is not and should not be involved in the relationship between the controller and the individual. For example the organization responsible for obtaining necessary consents or providing access to personal data of the individual should be the controller. In particular, the processor should not have the right or the obligation to start managing the relationship with the individual, as the purposes for which they process personal data are entirely mandated by the controller.

Not recognizing the fundamentally different roles different types of organizations play in data processing is bound to lead into confusion and serious data governance issues. It would also not be in alignment with the typical practice of sharing responsibilities of the service providers and their customers in commercial agreements regarding such data processing services.

As a starting point, controllers should be obligated to require appropriate safeguards from their processors. Processors should not be allowed to process personal data for other purposes than those defined by the controller. Processor should be allowed to define how to best process personal data accordingly. It should be considered whether or not to allocate certain obligations to processors directly based on law. Such requirements should primarily concern appropriate technical and other measures to protect personal data against unauthorized disclosure, modification, deletion or loss and perhaps define rules on how to deal with collected personal data in case the controller has ceased to exist or no longer is capable to live up to its obligations.

Recommendation: The regime should recognize the different roles organizations have in processing personal data and allow clear and flexible allocation of responsibilities accordingly. Dichotomy of a controller and processor serves as meaningful starting point. The definition of the controller should be based on the decision of the purposes for which personal data are processed (i.e. “why” the data are processed) rather than the means by which this is achieved (i.e. “how” the data are processed), as unclarity around this fundamental difference has lead to the current unclarity in the European data protection regime.

3.6 Consent (QUESTIONS 10 and 11 of the Consultation Paper)

Instead of focusing on consents, the emphasis should be in ensuring an informed choice for the individual. Transparency and openness are elementary to user choice. Without transparency, user choice is unlikely to be informed. Without true choice transparency is merely a formality, although an important one. Consumers should have the right to make an informed choice (by any suitable means) about how their data will be processed. Sometimes consent may be implied from individuals’ behaviour in appropriate contexts.

Users should know what personal information is being collected and processed and why; what their choices are regarding the use of this information; how this information may be shared and how it is protected.

The appropriate level of notice and user control over how information is used should be flexible and tailored appropriately for the nature of the information, to allow individuals to make informed choices.[5] The more sensitive the data being collected is or the more surprising its collection and use would be, the more prominent the notices should be, to ensure informed choices. However, companies should be able to innovate in the area of privacy notices, in line with these principles.

Users should be able to make meaningful, reasonable and informed choices. Users should be given meaningful choices to manage their personal data and preferences, fit for the situation and type of service at hand[6], offered with effective rights of access, erasure, modification and blocking. Consent can be obtained many ways (for example, opt-in, opt-out or implicit) and these should all remain valid options to ensure an informed choice, depending on the particular situation.

The Consultation Paper's approach to limiting the possibility to consent to processing that does not go "beyond what is necessary to provide the product or service" is problematic. While principles of proportionality and purpose limitation should provide boundaries to what the consent can cover, the proposed approach seems too narrow or it needs to be interpreted broadly. Certain types of data processing (e.g. use of cookies) may not be strictly necessary for the service provision in the technical meaning of the word, it may still be elementary for the business model as a whole. Without a possibility to obtain statistical information about service usage it is not possible to improve products and services based on factual information.

While consent is an important concept, in certain contexts consent is not an appropriate mechanism to legitimise data processing. For example, an employee's consent to its employer in context of the employer's standard routine data processing necessary for the administration of the employment relationship is very unlikely to be freely given due to the nature of the employment relationship. Withdrawing consent while remaining employed is typically not an option in this case. On the other hand, consent should not be totally abolished in employment relationships as employers may offer various voluntary services where the employee has a true choice without harmful consequences for refusal. Also, consent does not work for example in context of observing public spaces or managing data bases with pictures of individuals. Online shops are other example of practical difficulties. If a person wants to buy something as present for his family or friends, he needs to type in the recipients name and mail address. Consent does not seem like the right approach to manage the data protection dimension in these cases[7].

[5] For example, highlight notices and icons in the user experience, supplemented with more in-depth descriptions available to users and given at an appropriate time often provide best results.

[6] Different situations call for different choices. Social networking services typically require granular privacy settings suitable for that particular service whereas e.g. marketing consents are less complex (opt-in/out).

[7] While this holds, it is also clear that the other data protection principles would still need to apply.

When used as the sole basis for data processing, consent also presents challenges where individuals refuse to give, withdraw or condition their consent. Many business models require the use of personal data and in practice users are often presented with a “take it or leave it” choice. However, some categories and uses of data necessarily attract greater transparency and consent requirements.

Consent as a sole means to legitimize data processing should be reserved only for data processing of a sensitive nature. This should reflect the information classification system within the data protection regime (see our comments on the definition of personal data).

Recommendation: Rather than rely upon consumers’ understanding and policing the market through consent, the regime should require organizations to adopt an accountability approach to data governance. Modalities on consents, for example opt-in, or opt-out, should not be defined. Consent may also be implied through the individual’s actions. Controllers should be given room to innovate on the best means to provide informed choice in the appropriate context. The revised framework should allow controllers to legitimise their processing activities (particularly routine, organisational processing activities and those where consent is not a true option) other than in reliance on consent alone. Consent requirements should reflect a sliding scale - the more unusual the nature or use of data (e.g. sensitive data processing), then the greater the need to present individuals with prominent notice and choice. As a starting point, consent requirements must allow business models that necessarily entail the use of personal data without mandating a requirement to allow participation in the service without consent, provided that the user is offered an informed choice whether or not to participate at the outset of the service relationship. Instead of qualifying consent by limiting it to cases where data processing is “necessary”, consent should be qualified by principle of proportionality and purpose limitation.

3.7 Representatives of the individual (QUESTION 10 of the Consultation Paper)

Data protection should not be an area where concepts adopted for individual representation in most other legal contexts would not apply. Similarly, it should be possible for the individual to appoint a representative for himself. The controller should be allowed to trust such representation provided that adequate proof is expressed. On the other hand, controllers should be allowed to exercise caution. For example, in the context of individual access to personal data the controller should not be held liable for non-compliance if the controller refuses to accede to the request for information when the appointment of the representative of the individual is equivocal or ambiguous.

3.8 Accountability (QUESTION 10 of the Consultation Paper)

Companies must be accountable for their privacy practices. They should implement appropriate, effective and demonstrable data protection measures to ensure that they comply with their privacy commitments.

The ongoing efforts to clarify what those measures are, for example as explained in the Madrid Resolution[8], the APEC Privacy Framework[9] and the Accountability Project by the Centre for Information Policy Leadership[10] help to articulate what organizational accountability means and Nokia welcomes them.

Companies must have the flexibility to apply those measures in ways that take into account the type of the organization and business models, the nature of information being processed and the potential risks to individuals related to the data processing. Accountability is ultimately about reaching the most effective privacy protections with the minimum burden to regulators and companies alike.

Privacy by Design is a useful design methodology to make sure privacy considerations are baked into products and services from the R&D stage throughout the data processing lifecycle. Nokia sees Privacy by Design ultimately being a part of accountability.

Universally accepted criteria for appropriate organizational privacy protection measures would help create legal certainty and foster trust between companies and regulators. Indeed, accountability has the potential to bridge the gap between different legal regimes around the world, in order to achieve a globally interoperable regulatory framework for privacy.

Accountability helps shift the burden from less effective privacy protections, such as prior registration and approval by authorities, to more meaningful and truly effective privacy protections. Other incentives for accountability would include the easing of international data transfers and possible leniency in case of regulatory enforcement actions.

Apportioning privacy responsibilities to suitably competent and empowered staff is an important part of an accountable organization's privacy management structure. The revised framework should encourage larger controllers to appoint data protection officers ("DPOs").

However, having a DPO is neither sufficient to ensure nor a strictly necessary component of a solid privacy management framework. For example, companies may utilize a decentralized and integrated approach to privacy management when that is more appropriate for the way the company is otherwise organized. A single DPO being responsible for compliance may not be the appropriate solution in such an environment. Furthermore, such an approach risks privacy compliance becoming a matter of a separate team, distant from the actual business unit where Privacy by Design must be exercised, at least in the case where privacy responsibilities are not defined beyond the appointment of a DPO.

Without an exemption from personal liability, the risks associated with becoming a DPO will be too great for most employees to wish to accept the role. This, in turn, will adversely impact the success of the desired DPO culture. It should also be considered what would be

[8] http://www.gov.im/lib/docs/odps/madridresolutionno v09.pdf
[9] http://www.ema.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf
[10] http://www.informationpolicycentre.com/resources/

the most meaningful role for a DPO: A strict compliance officer or a true leader of privacy in an accountable organization.

Especially for larger corporations operating in a global context the processes through which the individual may exercise his privacy rights are typically regionalized and managed by dedicated resources other than the chief privacy officer of that company (for example in customer care). The utilization of normal business processes to deal with privacy related topics should be encouraged as opposed to centralizing all privacy topics for dedicated experts. This is important for the creation of true privacy culture within the organization where privacy competences are a matter of normal business competence.

Recommendation: Nokia welcomes accountability provided that there are appropriate incentives for organisations to take accountability measures (for example, leniency in case of enforcement and ease of international data transfer).

Whilst the appointment of Data Protection Officer ("DPO") should be encouraged, it must not be mandatory. Instead, companies should be encouraged to define appropriate privacy responsibilities within the organization in a way that best reflect the company's management structure in context of achieving an accountable organization. Controllers must have the flexibility to determine what are the appropriate role descriptions taking into account their size, structure, culture and resources. In any case DPOs must be exempted from personal liability in the event of a breach, unless the breach arises due to the intentional negligence or reckless act on the part of the DPO. For a group of affiliated entities a single DPO across the jurisdictions where the respective entities are located should be sufficient. Formal qualification criteria for a DPO should not be dictated. Professional certification should be encouraged to achieve a true privacy profession.

3.9 Rules on Collection, Use and Disclosure (QUESTIONS 12 AND 13 of the Consultation Paper)

While we in general endorse the rules as described in the consultation, we would like to emphasise that they be expressed in high level, principle-based terms only. We also refer to the points made in relation to exclusions, in particular to the household exclusion.

In context of the exclusion, it should be clear that, in order for the organizations to protect their valuable assets, organizations should not be obligated to provide personal data to researchers or other such third parties.

In context of defining the rules that govern the applicable law special attention should be given to defining the applicable laws pertaining to governmental access to personal data processed in Singapore.

Recommendation: Household exclusion should be introduced. Exclusions should not result to any obligations on organizations to disclose personal data. Governmental access to consumers' personal data should be based on clear and open legal provisions, be proportional and governed by due process.

3.10 Transfer of personal data outside Singapore (QUESTION 14 of the Consultation Paper)

In the globalized contemporary data processing environment transfers of personal data are the norm rather than the exception, taking place with a click of a mouse. Such transfers are an essential element of the reality we currently live in.

Nokia welcomes the simple approach presented in the consultation. Accountabilty is an important element a regime where the onus to ensure appropriate protection for personal data is left on the companies.

3.11 Rules on accuracy and retention (QUESTION 14 of the Consultation Paper)

While we in general endorse the rules proposed on the consultation, the regime needs to recognize the fact that 100% protection against all future threats is not achievable. The nature of security threats is very dynamic and global.

Nokia welcomes the emphasis placed on the need to ensure that personal data processing is subject to appropriate safeguards to protect personal data against foreseeable threats, such as unauthorized access, use, disclosure, modification or loss. Such measures are both technical (such as use of encryption, where necessary, firewalls, access control and other such technical and physical protection) as well as organizational (such as existence of a proper data protection program within the organization along the lines described in context of accountability principle). These measures should be based on the state of the art for technical measures and be in general reflective the nature of the personal data in question balanced with the likelihood and impact of a breach.

Recommendation: While some guidance on typical security measures may be warranted to ensure that the basics are in place, the emphasis should be in timely exchange of information between the authorities and organizations on threats and potential countermeasures directly and for example in the context of existing international computer emergency organizations.

3.12 Rules on retention (QUESTION 15 of the Consultation Paper)

We support a principle based approach instead of prescribing the retention period upfront to the individual at the point of collecting the personal data as this would be difficult to ascertain and not practicable for businesses.

Instances where data is stored without any deletion schedules are typical sources of privacy breaches. However, it should be left to the business to define the data retention period criteria, whether it be by way of purpose or by way of a retention period.

In addition to reasons mentioned in the consultation, organizations may need to retain personal data to be able to defend themselves against claims made by e.g. their former

customers. In these instances guidance on the appropriate retention times may be sought from rules governing the legal time limits during which a claim must be made.

Where any retention times are introduced for reasons relating to law enforcement, any such requirements should be clear, explicit and proportional. In case the retention period would exceed the normal business needs, it should be considered who carries the cost of such retention.

Recommendation: Retention times should not be prescribed in detail. Organizations should not be obligated to disclose their retention times. As part of normal data governance, organizations should define appropriate standards for data lifecycle management.

3.13 Rules on access and correction of personal data (QUESTION 16 of the Consultation Paper)

Together with the requirement to describe the organizations data processing practices, offering individuals with meaningful right to access, modify or even block unnecessary processing of personal data are fundamental measures in ensuring transparency of data processing and individual participation thereto.

It should be acknowledged that the broader the definition of personal data, the more difficult it gets to really identify in a reliable manner that the personal data for which access is sought really belongs to the individual requesting access to it. For example, in online context users are often identified through various accounts or identifiers that, while they may legally be seen as personal data, in practice it is not clear if the individual seeking access really is the individual to whom the transactions in question relates to. It may be impossible to provide sufficient evidence to one way or the other. At least sometimes providing information to the wrong individual may have more severe harmful consequences than not providing the information to the right individual.

Recommendation: Organisations should have a right to require individuals to identify themselves in sufficient detail as well as to provide organizations with sufficiently detailed access requests to enable organizations to find the requested information without undue burden and uncertainty concerning the identity to whom the information being disclosed relates to. Where sufficient online account management tools are available to individuals, they should be seen as appropriate means for providing access to their personal data.

3.14 Enforcement (QUESTIONS 17 and 18 of the Consultation Paper)

Enforcement activities should focus on harms to individuals. Companies that can demonstrate accountability in their overall activities should be given credit in case of enforcement on an individual breach. This would give companies increased incentives to really improve their privacy compliance and culture, as opposed to achieving just “mere compliance”. As part of the incentives for organizations to achieve and exceed compliance, those who are applying and adhering to accountability principles should not be subject to

private rights of action for inadvertent breaches. It is an important principle that the decisions of authorities are subject to appeal.

Recommendation: A scale of sanctions should be available, subject to and proportional to the seriousness of the violation, starting from enforcement letters advising organizations on the compliance ranging then into more serious sanctions. All enforcement needs to be based on an open investigation following a due process where the organization being investigated has a fair chance to provide their views on the subject matter which are appropriately considered in the process. In addition to sanctions, the enforcement regime should also provide appropriate incentives to promote accountable organizational behaviour.

3.15 Guidelines (QUESTION 19 of the Consultation Paper)

Regulation, whether comprehensive or sector specific, has never been successful in managing privacy on its own. Industry best practices, standardization and self-regulatory systems have always been essential for successful management of privacy issues.

Meaningful and effective self-regulation by industry, or co-regulation together with industry, regulators and other stakeholders, provides the best opportunity to rapidly adapt to new technologies and business models. This approach leads to increased efficiency, flexibility, incentives for compliance, and reduced cost.

Privacy by Design[11] is an important design approach for accountable organizations, to ensure that privacy considerations are integrated into processes, products and services from the early research and development stages throughout the entire data processing lifecycle. By nature, Privacy by Design will always remain a dynamic concept, not possible to define in regulatory detail, as new business models and technologies will create new privacy threats with new designs to mitigate those threats.

Privacy culture and Privacy by Design should be encouraged through the engagement and continued efforts of the whole privacy ecosystem, from companies to consumers, non-governmental organizations, regulators and academia. Privacy by Design as a privacy principle should not be prescribed in detail, to avoid a chilling effect on innovation.

Without a true privacy culture, based on social awareness for privacy threats, training and education of privacy professionals, encouragement and research for privacy aware technologies, technology standards and privacy engineering processes, any regulation will fall short of one of its key objectives, true protection for individuals.

Recommendation: Nokia encourages self-regulation and co-regulatory initiatives to deliver efficient, effective and timely protection for individuals. Before issuing guidelines the authorities should arrange open and accessible consultation processes where the whole privacy ecosystem (regulators, industry, academia and advocacy) are invited into open dialogue to reach practical, facts based outcome.

[11] See e.g http://www.privacybydesign.ca/

3.16 Transitional arrangements (QUESTIONS 20, 21 and 22 of the Consultation Paper)

The proposed one year sunrise period seems appropriate provided that the actual data protection law does not raise fundamental new types of requirements compared to existing regulations in other regions.

With respect to the existing personal data in organization's custody today, the proposed approach seems to strike the right balance.

3.17 National do-not-call registry (QUESTION 23 of the Consultation Paper)

Nokia endorses industry self-regulation and co-regulation between the industry and the authorities. However, where such measures prove to be ineffective to address a true privacy issue, regulation may be appropriate to the extent it is seen as an effective way to address the matter but should not result in undue burden to the organisations. Further, where this relates more to the control of spam / unsolicited electronic messages, this may be better provided for under the spam legislation instead.

THE END