ACC Response to White Paper of the Committee of Experts on a Data Protection Framework for India

The Association of Corporate Counsel (ACC) is pleased to have the opportunity to comment on the White Paper of the Committee of Experts on Data Protection Framework for India. ACC is a global bar association that promotes the common professional and business interests of in-house counsel who work for corporations, associations and other organizations through information, education, networking opportunities and advocacy initiatives.

As in-house counsel, our 40,000 members have a vested interest in data protection and security for their organizations. As many of our members work for multi-national companies, we favor an approach to India's data protection law that preserves India's important role in the global economy. In developing our comments on the white paper, ACC relied heavily on its India Corporate Counsel Forum, which serves as a peer-to-peer discussion platform on important regulatory developments impacting legal departments in India and beyond, and what these mean for in-house counsel on a day-to-day basis.

Part II – Chapter 1 – Territorial and Personal Scope

Q1. What are your views on what the territorial scope and the extra-territorial application of a data protection law in India should be?

The scope of the law should apply to organisations collecting and processing personal data of individuals in the context of business activities established in India. Personal data of individuals collected and processed by Indian entities on behalf of foreign entities should be governed by contractual obligations.

Q2. To what extent should the law be applicable outside the territory of India in cases where data of Indian residents is processed by entities who do not have any presence in India?

We agree with the provisional views that carrying on a business, or offering of services or goods in India shall be the parameters worth incorporating in the law in light of international practices. Thus the law may be applicable to entities located outside India even if they have no presence in India if the data of Indian residents is processed to offer

a good or service to Indian residents in India over the Internet or if entities monitor or track the behavior as far as their tracking of behavior takes place in India.

Part II – Chapter II – Other Issues of Scope

Q2. Should the law seek to protect data relating to juristic persons in addition to protecting personal data relating to individuals?

The law should apply to the personal data of individuals (natural persons), not data pertaining to corporate entities.

Q3. Should the law be applicable to government/public and private entities processing data equally? If not, should there be a separate law to regulate government/public entities collecting data?

The law should have a clear demarcation of applicable principles to public sector and private sector, and wherever they overlap. The approaches found in Japan and Australia are recommended in this regard.

Q4. Should the law provide protection retrospectively? If yes, what should be the extent of retrospective application? Should the law apply in respect of lawful and fair processing of data collected prior to the enactment of the law?

The law should not provide retrospective protection – this would be a difficult requirement for businesses to meet. With respect to personal data collected and processed prior to the enactment of the law, the law should allow organisations to process as before, provided such processing continues to remain valid under the new law.

Q5. Should the law provide for a time period within which all regulated entities will have to comply with the provisions of the data protection law?

Organisations will certainly require a transition time in order to implement new requirements of the law. The length of said transition time will depend on the final requirements of the data protection law, their complexity to implement, and how much of a departure they are from current practices in India. In no case should the transition time be less than 12 months, and it will likely be advisable to have a longer transition period.

Part II – Chapter 3 – What is Personal Data?

Q1. What are your views on the contours of the definition of personal data or information?

The definition of personal data should be limited to any data about individuals which can either directly identify, or along with other data sets, indirectly identify the individual.

Q2. For the purpose of a draft data protection law, should the term 'personal data' or 'personal information' be used?

As the term "personal information" can lead to ambiguity and confusion when used against the term "personally identifiable information," it is better to use the terminology "personal data." Moreover, personal information is best suited when the privacy laws and regulations are categorized by sector.

Q3. What kind of data or information qualifies as personal data? Should it include any kind of information including facts, opinions or assessments irrespective of their accuracy?

As per above definition, if the data (not information, as they are very different) either directly or indirectly with other data sets is able to identify the individual, it should qualify within the scope of the definition of "personal data." We would agree that if facts, opinions or assessments come within that definition, then they should be included irrespective of their accuracy.

Q5. Should anonymised or pseudonymised data be outside the purview of personal data? Should the law recommend either anonymisation or pseudonymisation, for instance as the EU GDPR does?

Anonymised data should be outside the purview of personal data, however, when the data is traceable to the identification of an individual, the law should apply. This would require adequate guidelines from the data protection authority to mitigate such risks.

With respect to pseudonymisation, the law should apply, but as in the case of GDPR, Article 11, the organisation should be exempt from responding to any rights that a data subject may claim relating to pseudonymised data.

Q6. Should there be a differentiated level of protection for data where an individual is identified when compared to data where an individual may be identifiable or reasonably identifiable? What would be the standards to determine whether a person may or may not be identified on the basis of certain data?

There should not be differing protection levels for data where an individual is identified compared to data where an individual may be identifiable. Businesses would face a huge challenge complying with such a requirement.

Q7. Are there any other views on the scope of the terms "personal data" and "personal information," which have not been considered?

Business contact information should not be included in the definition of personal data. There should be an exemption for business contact information, similar to what's found in the Singapore PDPA. This exemption should include an individual's name, position name or title, business telephone number, business address, business electronic mail

address or business fax number and any other similar information about the individual unless the personal data was provided by the individual solely for use in a personal context.

Part II – Chapter 4 – Sensitive Personal Data

Q1. What are your views on sensitive personal data?

The definition of sensitive personal data should be as defined as under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Sensitive personal data is defined in the said Rules to cover the following: (a) passwords, (b) financial information such as bank account or credit card or debit card or other payment instrument details; (c) physical, physiological and mental health condition; (d) sexual orientation; (e) medical records and history; and (f) biometric information.

Q2. Should the law define a set of information as sensitive data? If yes, what category of data should be included in it? E.g. Financial Information / Health Information / Caste / Religion / Sexual Orientation. Should any other category be included?

As mentioned above, the definition of sensitive personal data should be defined to cover the following: (a) passwords, (b) financial information such as bank account or credit card or debit card or other payment instrument details; (c) physical, physiological and mental health condition; (d) sexual orientation; (e) medical records and history; and (f) biometric information.

Part II – Chapter 5 – What is Processing?

Q2. Should the definition of processing list only main operations of processing i.e. collection, use and disclosure of data, and inclusively cover all possible operations on data?

The law should limit the processing scope to (1) Collection; (2) Use; (3) Dissemination; and (4) Invasion – similar to Daniel J. Solove's work on "Taxonomy of Privacy."

Q3. Should the scope of the law include both automated and manual processing? Should the law apply to manual processing only when such data is intended to be stored in a filing system or in some similar structured format?

Yes, the law should include both automated and manual processing, and should only apply to manual processing only when such data is intended to be stored in a filing system or in some similar structured format.

Part II – Chapter 6 – Entities to be Defined in the Law: Data Controller and Processor

Q1. What are your views on the obligations to be placed on various entities within the data ecosystem?

The entity collecting the data for processing towards its business value should own the accountability for managing the data throughout the life cycle. If a different entity acts on behalf of the collecting entity, it should provide adequate safeguards, but ultimate responsibility for the data should still rest with the collecting entity.

As the white paper notes, the GDPR model that allocates responsibility between data controllers and data processors and imposes direct statutory obligations on data processors is prescriptive and will impose high costs on data processors. Statutory allocations of responsibility are inflexible and cannot take into account the unique circumstances of a transaction – the data, the parties, or the commercial arrangements between them. Contractual allocations of responsibility are more sensitive and responsive to circumstances that may require special allocation of responsibility still consistent with the overall requirements of any data protection law. In practice, even with this flexibility, the multi-national organisations will still drive towards a consistent allocation of general responsibilities because businesses will want to implement a single global allocation of responsibilities (absent unique data or market requirements) to more efficiently operationalise common requirements across the globe. For example, a data processer for a mixed set of EU, Indian and US data will likely have a common set of privacy-related rules driven by the strictest set of national requirements (here, the EU), because it cannot efficiently segregate the data set by origin.

Q3. How should responsibility among different entities involved in the processing of data be distributed?

We favour an approach that makes a data controller primarily responsible for personal data under its control, including for information transferred to third parties for processing. As noted in our answer to Q1, we believe contractual means can be used to ensure a comparable level of protection while the information is processed by a third party. We generally support an approach in line with the PIPEDA law in Canada on this topic.

Part II – Chapter 7 – Exemptions for Household Purposes, Journalistic and Literary Purposes and Research

Q1. What are the categories of exemptions that can be incorporated in the data protection law?

We agree that there should be exemptions for data processed for household purposes; data processed for journalistic/artistic and literary purposes; and partially for research.

Research/Historical/Statistical Purpose

Q1. What are your views on including research/historical/statistical purpose as an exemption?

The law or the data protection authority should provide further guidance regarding exclusion of research activities in healthcare, due to the nature of the data collected. The law should also encourage either anonymising the data or pseudonymisation of the personal data with additional safeguards. This will reduce potential grievances and also mitigate risks.

Part II – Chapter 8 – Cross-Border Data Flow of Data

Q1. What are your views on cross-border transfer of data?

Cross-border transfer of data is the lifeblood of the global economy and has been a critical factor in the success of the Indian economy. Emerging research indicates that barriers to international data flows result in significant lost trade and investment opportunities, higher IT costs, reduced competitiveness and lower economic productivity and GDP growth. As a general premise, the Association of Corporate Counsel supports the free flow of data across international borders. As in-house counsel who are responsible for their companies' compliance with data regulations, we believe any regulation of cross-border transfers of data should have clear standards that are easy to comply with and present minimal disruption to business.

We also support the free flow of data across international borders because such flow is a necessary requirement for the detection of fraud and other corporate wrongdoing. To take the example of credit card fraud – credit account information is stolen from an Indian citizen, and used in another country to make a purchase. The credit card company's servers that can analyze this data and issue a fraud alert may be located outside of India. Restrictions of data flows between the three countries impede this sort of analytics operations along with many others that are part of multinational companies' programs designed to detect fraud and other corporate misdeeds. As in-house counsel, the lack of such analytical assistance makes the job of detecting fraud and ensuring a corporation's compliance with various laws much more difficult.

Q2. Should the data protection law have specific provisions facilitating cross border transfer of data? If yes, what should the adequacy standard be the threshold test for transfer of data?

India's data protection law should facilitate efficient cross-border transfer of data, as this is crucial for a number of organisations. The EU's approach to cross-border data transfers has proven to be rather restrictive, and India should seek a model that provides for easier transfer of data across borders.

The IT law currently provides for the transfer of data between organisations anywhere across the globe, provided that the transferee ensures the same or equal level of data protection required of the Indian organisation under national law. We recommend continuing with this approach as a starting point for India.

Q4. Are there any other views on cross-border data transfer which have not been considered?

Cross-border data flows are also essential to human resource management. Multinational companies may need to move employees' personal data between various locations to perform routine operations incident to employment. If the final data protection law has restrictions on cross-border flow of data, those restrictions should not apply to employers' processing of employee data outside of India for legitimate purposes.

Part II – Chapter 9 – Data Localisation

Q1. What are your views on data localisation?

The white paper gives a detailed summary of the potential negative impacts of a data localisation policy on the Indian economy. As a global bar association, with many members employed by multi-national corporations, the Association of Corporate Counsel does not support barriers to doing business across borders. As India has already experienced with its data localisation mandate in the telecom sector, such requirements are a hindrance to business, particularly global businesses.

Q2. Should there be a data localisation requirement for the storage of personal data within the jurisdiction of India?

India should not require data localisation for the storage of personal data. Even if the requirement were just applicable to storage of personal data, from a functional standpoint, it would require data localisation across all data, due to the difficulty of distinguishing personal data from non-personal data. If the government has concerns about the security of data stored outside of India, the data protection law may provide for security standards for storage of data that contains personal data. The government may also consider developing a list of nations where data cannot be stored due to security concerns.

Part III – Chapter 1 – Consent

Q1. What are your views on relying on consent as a primary ground for processing personal data?

Consent should be treated at par with other grounds for processing. It is critically important to establish grounds for processing data that are still lawful but do not require the data subject's consent.

Q2. What should be the conditions for valid consent? Should specific requirements such as 'unambiguous', 'freely given' etc. as in the EU GDPR be imposed? Would mandating such requirements be excessively onerous?

Consent should be allowed to be obtained in a number of different ways: E.g., opt-in, opt-out, deemed consent, privacy settings on a website. The key requirement to a valid consent should be that the organisation is able to prove that it has notified the individual of the collection, use and disclosure of his personal data and has obtained consent. Consent should be considered valid if the individual has been notified of the purposes for which his personal data will be collected, used or disclosed and the individual has provided his consent for those purposes. The consent should provide clarity and certainty for both organisation and individual. Only if the organisation chooses to adopt an approach to consent that does not require a positive action of the individual (e.g., an opt-in approach), would the burden of proving a valid consent lie with the company. This is a more flexible approach than GDPR that we feel is more suitable to India.

Q4. Should different standards for consent be set out in law? Or should data controllers be allowed to make context-specific determinations?

We recommend that India follow an approach similar to Canada's, where express consent is only required for the processing of sensitive personal data. Implied consent should be sufficient for non-sensitive information. We believe this approach balances the Supreme Court's declaration of privacy as a "fundamental right," without adding unnecessary burden to business or needlessly contributing to consent fatigue among the public.

Q5. Would having very stringent conditions for obtaining valid consent be detrimental to day-to-day business activities? How can this be avoided?

As stated in our answer to Q2, we believe India should adopt a flexible approach to consent requirements. Overly stringent conditions for obtaining valid consent are very difficult to operationalise, especially in a society that has not previously had a requirement for consent to process personal data.

Part III – Chapter 3 – Notice

Q1. Should the law rely on the notice and choice mechanism for operationalising consent?

Yes. The transparency in providing the information towards processing will help organisations in validating the consent mechanism. As mentioned in our comments on consent, organisations must inform individuals of the purposes that a reasonable person would consider appropriate in the circumstances for which their personal data will be

collected in order to obtain consent. The notice should highlight purposes which may be of particular concern to the individuals (e.g. for marketing purposes), use a layered notice (i.e. lists the basic or most important information more prominently), headings, titles and sections. The notice should be legible and in simple language that's easy to understand for the target audience.

Q3. Should the effectiveness of notice be evaluated by incorporating mechanisms such as privacy impact assessments into the law?

An organisation may take a proactive and systematic approach in adopting appropriate measures and tools to address the effectiveness of notice like the lawfulness of processing, purpose specification and security safeguards. One of the ways can be a Privacy Impact Assessment, but it should be left to the organisation to determine the most appropriate measures to evaluate the effectiveness of notice to be adapted for its specific circumstances.

Q4. Should the data protection law contain prescriptive provisions as to what information a privacy notice must contain and what it should look like?

The proposed data protection law should not contain prescriptive provisions or specify a specific manner or form in which an organisation should issue a notice to inform an individual of the purposes for which it is collecting, using or disclosing the individual's personal data. It should be left to the organisation to take into account its own circumstances and requirements to determine what information a privacy notice must contain such that the individual is provided with the required information to understand the purposes for which his personal data is collected.

Part III – Chapter 4 – Other Grounds of Processing

Q1. What are your views on including other grounds under which processing may be done?

Including grounds other than consent under which processing may be done is essential to the ability of businesses to comply with the data protection law.

The "legitimate interest" ground is especially critical to business interests, and indeed the public's interest. Certain types of data processing that rely on the legitimate interest exception serve important interests such as deterring fraud and money laundering. For example, companies in the financial industry will usually vet potential vendors for anti-money laundering, know-your-customer, and anti-bribery purposes. This review may involve the processing of personal data held by the vendor, and under the GDPR model, would not fall within any ground for processing other than the legitimate interest exception to consent. Therefore, we find the white paper's skepticism of the legitimate interest ground troubling. The white paper acknowledges the need for some sort of residuary ground under which processing activities could take place, but states that such

processing must be for the benefit of the individual. Under that standard, such vendor review still would not qualify.

There are other processing activities that would be impossible to conduct with the elimination of the legitimate interest ground for processing, so we recommend proceeding with caution in that regard. The law or the data protection authority should define adequate guidelines to interpret the balancing test to be considered by the data controllers against the individual's interest and privacy harm.

We also wish to call special attention to the processing of employee data by the employer. Data processing activities should be laid out clearly to avoid significant impact to an organisation's processing of personal data. With no clear guidelines, businesses would face a huge burden in handling employee/labor concerns.

Q2. What grounds of processing are necessary other than consent?

1. Performance of Contract
2. Legal Obligations
3. Data Subject's Vital Interest
4. Legitimate Interests of the Data Controller
5. Public Interest

Part III – Chapter 7 – Storage Limitation and Data Quality

Q2. On whom should the primary onus of ensuring accuracy of data lie especially when consent is the basis of collection?

When consent is the basis for collection, the primary onus should vest with the individuals in providing the correct information. Much data provided by individuals is not accurate. Businesses should not be made responsible for the accuracy of such data.

Q3. How long should an organisation be permitted to store personal data? What happens upon completion of such time period?

We do not agree with alternative "a": "data should be completely erased." A requirement for data deletion would be harmful to India's business interests. Big data is a key source of value that businesses are just starting to tap for identifying market trends, analyzing performance and forecasting future outcomes. To do this, businesses must be able to use large data sets, some of which will include personal data, which are collated and analysed to detect patterns and make optimal decisions.

As "data is the new oil," we recommend exploring alternatives to mandating deletion of data. An approach similar to GDPR, Art. 5(1)(e), could be a model to allow further use of personal data. It allows storage of data for longer periods than necessary for the purposes for which the personal data was processed, if the purpose of the longer period is for

archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. Such an exception could be expanded to explicitly include business research applications and perhaps require anonymisation with such uses. Additionally, GDPR requires that such data be kept with adequate technological and organisational safeguards.

Part III – Chapter 8 – Individual Participation Rights-1

Q4. Should there be a fee imposed on exercising the right to access and rectify one's personal data?

The organisation should be able to charge the individual a reasonable fee to recover any incremental costs of responding to an access request.

Q5. Should there be a fixed time period within which organisations must respond to such requests? If so, what should these be?

Reasonable time should be provided to the organisation to provide access to the requested personal data. If the organisation is unable to provide access within 30 days, it can inform the individual as soon as possible of the time in which the organisation will be able to provide access.

Q6. Is guaranteeing a right to access the logic behind automated decisions technically feasible? How should India approach this issue given the challenges associated with it?

Any requirement to disclose the logic behind algorithm-based predictive analytics must be done in a manner consistent with intellectual property rights.

Q7. What should be the exceptions to individual participation rights?

Where personal data is anonymised, or pseudonymised, the rights to access, deletion, or correction should not apply.

There may be certain other exceptions or prohibitions that may be applied by the organisation when providing such access to data. For example, if personal data requested by the individual also contains personal data of another individual, legal or regulatory proceedings or court orders.

Part IV – Chapter 1 – Enforcement Models

Q2. Does co-regulation seem an appropriate approach for a data protection enforcement mechanism in India?

We agree that co-regulation is the appropriate approach for data protection enforcement in India.

Part IV – Chapter 2 – Accountability and Enforcement Tools

Q3. Should the lack of organisational measures be linked to liability for harm resulting from processing of personal data?

Yes, the lack of organisational measures to adequately protect privacy should be linked to liability for harm resulting from the processing of personal data. Organisations that fail to implement processes and systems to protect personal data should be treated more harshly under the data protection law. This will incentivise greater compliance with the law.

Q4. Should all data controllers who were involved in the processing that ultimately caused harm to the individual be accountable jointly and severally or should they be allowed mechanisms of indemnity and contractual affixation of liability inter se?

We do not think the principle of joint and several liability should be applied between all data controllers involved in processing. Requiring this form of liability can be unfair to those data controllers that have been diligent in safeguarding personal data, and may increase overall transactions costs, as businesses will be less certain of overall liability for processing data. Therefore, liability should be allocated based on fault.

Q5. Should there be strict liability on the data controller, either generally, or in any specific categories of processing, when well-defined harms are caused as a result of data processing?

Subjecting data controllers to a strict liability regime, either generally or in specific categories of processing, lessens the incentives of data controllers to take effective protective measures, as their liability would be the same regardless of the measures taken. For this reason, we do not support the imposition of a strict liability regime for harms caused by a data incident. Rather, liability for such harm should be based on an organisation's failure to implement required privacy protections.

Part IV – Chapter 2B – Personal Data Breach Notification

Q3. When should personal data breach be notified to the authority and to the individuals?

In general, it is a good practice to notify individuals affected by a data breach. Not only will this encourage individuals to take preventive measures to reduce the impact of the data breach, it will also help an organisation rebuild consumer trust. Organisations should be required to prepare and implement a good data breach management and response plan.

Notification to the individual may be required for affected individuals if a data breach involves sensitive personal data and the organisation has determined there is a likelihood the individuals will suffer harm as a result of the breach. The law should not set a specific time period for this notification, but should impose a reasonableness standard. Notification to the authorities should be only for matters that might cause serious public concern or where there is a risk of harm to a large group of affected individuals. We recommend this approach because a lower threshold for reporting to the authorities may not result in meaningful disclosures, given the frequency of security incidents at most organisations (not just within India, but worldwide).

Part IV – Chapter 2C – Categorisation of Data Controllers

Data Protection Impact Assessment

Q5. Are there any alternative views on this?

With the evolving technological evolutions and day-to-day use of personal information processing, a requirement for "privacy by design" should also be included in the scope of the law. The concept (defined by Dr. Ann Cavoukian) was earlier used as a best practice for organisations involved in technological innovations. The EU GDPR mandates privacy by design in Article 25 as one of the accountability requirements. The concept not only helps in mitigating privacy risks, but also provides considerable opportunities for new innovations.

Data Protection Officer

Q1. What are your views on a data controller appointing a DPO?

We do not believe there should be a general requirement for a data controller to appoint a DPO. Rather, appointment of a DPO or similar officer to oversee privacy concerns should be considered a best practice and considered by the data protection authority as an indication of a company's level of compliance with the data protection law. Further, the data privacy law should not proscribe specific duties and responsibilities of the officer in charge of privacy. Companies need to have flexibility in designing the systems for compliance best suited to their individual circumstances and their workforce. For example, a company may find it better to divide some of the roles of the DPO among different officers. A Chief Privacy Officer responsible for the company's compliance with the data protection law, but then a privacy counsel who serves as the company's contact point with the regulator. Companies should not be prevented from designing the most efficient compliance mechanisms by overly prescriptive legal requirements.

Q2. Should it be mandatory for certain categories of data controllers to designate particular officers as DPOs for the facilitation of compliance and coordination under a data protection legal framework?

We do not think there should be a mandatory requirement for DPOs, for any category of data controllers. Having a universal requirement for DPOs would be overly burdensome to small and medium size businesses, and even a requirement limited to certain categories of data controllers can be difficult to define, as can be seen from the GDPR experience. Therefore, we believe a more flexible and efficient approach would be to incentivize companies to create a robust overall compliance program, rather than mandate the creation of specific officers and responsibilities.