ITI Comments on India's Draft Personal Data Protection Bill

September 29, 2018

The Information Technology Industry Council (ITI) welcomes the Srikrishna Expert Committee (the Committee)'s draft data protection bill and report. ITI is the premier advocate and thought leader around the world for the global information and communications technology (ICT) industry. ITI's membership is comprised of the world's leading innovative technology companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, cybersecurity, and Internet companies. Our members are global companies, headquartered around the world with business in every major market and deep investments in India. Privacy, security and trust are central to our companies' continued success and we take seriously our obligation to protect and responsibly use the personal information of our customers, consumers, users, and employees.

Because of our diverse membership and widespread business presence, our companies have extensive on site, practical experience with the privacy and data protection regimes of nearly every country. Informed by our global perspective and broad expertise, ITI encourages governments, as they consider developing or updating their privacy frameworks, to do so in a way that promotes the responsible use of personal information, encourages domestic innovation, attracts foreign investment, promotes the growth of trade and facilitates the free flow of information.

We are aware that each of the countries in which our members operate present a unique combination of challenges and opportunities in developing sustainable data protection policies. We welcomed the Supreme Court of India's recent ruling that privacy is "intrinsic to life and liberty" and is inherently protected under the fundamental freedoms enshrined in the Indian Constitution, as well as the formation of the Expert Committee on Data Protection, under the Chairmanship of Justice B. N. Srikrishna, by India's Ministry of Electronics and Information Technology (MEITY). These events and the proposal of this draft bill signal the beginning of a new stage in India's advancement on the world stage and we hope to be a resource during these discussions to support the development of a robust, globally interoperable data protection law in India.

We were pleased to see that several of the suggestions we made during the Committee's earlier request for input were reflected in the draft bill and report, and note that the draft bill has taken inspiration from many of the EU's General Data Protection Regulation (GDPR)'s strengths while retaining the Government of India (GOI)'s vision of growing India's digital economy, by providing for multiple legal bases for personal data processing, allowing beneficial uses of personal data while ensuring privacy and security through the use of anonymization and pseudonymization techniques, and ensuring exemptions for restrictions to personal data processing for research and employment purposes. However, we believe that certain sections of the proposed bill could unintentionally limit the ease of doing business in India, and hamper the country's growth, while offering minimal benefit to individual privacy.

We respectfully offer the following recommendations in response to the draft bill and report:

Summary of Recommendations

1. Remove Data Localization Requirements.
2. Remove Limits to Cross-border Data Transfers.
3. Clarify the Definitions of Personal, Sensitive and Anonymized Data.
4. Expand the Grounds for Personal Data Processing.
5. Lower Age of Consent for Children's Data.
6. Put Reasonable Limit on Data Breach Notification.
7. Narrow the Data Protection Impact Assessment Requirement.
8. Remove Local Residency Requirement for Data Protection Officer (DPO).
9. Limit Penalties and Remove Criminal Penalties for Offenses.
10. Create an Independent and Well-Resourced DPA.
11. Clarify Processor Fiduciary Liability.
12. Alter the Yearly Audit Requirement.
13. Narrow Data Access Powers and Clarify Safeguards.

Please see below for additional detail and analysis related to each of these thirteen recommendations, which we stand ready to discuss further at your convenience.

1. Remove Data Localization Requirements.

Under the draft bill, data fiduciaries are required to "ensure the storage, on a server or data center located in India, of at least one serving copy of personal data to which this Act applies." In addition, if the government designates a category of personal data as "critical" it "shall only be processed in a server or data center located in India.

We are deeply concerned by this section of the draft bill and would caution that the Committee's goal to ensure the growth of the digital economy while keeping personal data of citizens secure and protected is seriously undermined by this data localization requirement. The location of data is no longer relevant to the question of whether India has jurisdiction over that data. Both the protection and security of data -- as well as access to data for lawful purposes -- can be enabled without a requirement that data be stored in a specific physical location. In fact, local data storage requirements have been shown to render data more vulnerable to natural disaster, technical failure, and hacking or intrusion, because centralized storage presents a single point of vulnerability and a more attractive target to bad actors.

Mandating local storage of data also vastly increases the cost of doing business for companies. Data storage and processing relies on the economies of scale that can be found in large data centers. Companies, even very large multinational companies, use very few facilities for their global data processing needs. This allows them to provide effective low costs and high-quality services. Mandating that this process take place within certain borders can raise the cost for companies to procure data services by 30-60%.[1] Not only is this cost crippling for small and medium-sized enterprises (SMEs), it

[1] "Quantifying the Cost of Forced Localization" Leviathan Security Group, 2015.

translates to massive macroeconomic costs: economy-wide data localization in India could cost up to .8% of its GDP and decrease investments by 1.3%, causing economy-wide welfare losses per worker equivalent to 11% of the average monthly salary.[2] The result of these large costs includes a dampening of technological adoption and would be a significant challenge for firms to overcome in order to compete in the global economy.

We recognize GOI's legitimate concerns relating to law enforcement access to personal data, and would advise GOI pursue alternative globally oriented mechanisms, such as bilateral treaties and participation in multilateral fora and conventions to advance this objective. It is important to note that this is not an India specific problem. Many governments in the most significant economies in the world are currently grappling with similar frustrations, and our companies have been working with them to help develop international solutions to these problems. There are several noteworthy examples of good-faith efforts to advance solutions to the problem of law enforcement access to data, including:

1) The Brazilian Central Bank

The Central Bank of Brazil (BACEN) recently considered regulations similar to the RBI Directive, proposing implementation of a cybersecurity policy by financial institutions operating in Brazil that would have required localization of processing, data storage, and cloud computing services in Brazil. Following intervention by stakeholders to explain the potential negative consequences of forced localization on Brazil's economy and competitiveness, as well as the negative security implications, in April 2018, Brazil issued a revised policy allowing for financial data processing and storage outside of Brazil, provided certain compliance requirements are met by providers of such services. The revised policy requires that: (1) when contracting services abroad, financial institutions must indicate to the Central Bank the countries and regions where their services may be provided and where data may be stored, processed and managed; and, (2) ensure there is an agreement for the exchange of information between the BACEN and the central financial authorities of the countries where the services may be provided. -- in the absence of such an agreement, the contracting institution may request authorization from the Central Bank of Brazil and demonstrate that the laws of the countries where the services may be provided do not limit or impede access to data by the Central Bank of Brazil where warranted.

2) Europe E-Evidence Directive

The European Commission proposed draft legislation on e-Evidence (both a Regulation[3] and Directive[4]) in April 2018 to facilitate cross-border demands for communications data and metadata in criminal investigations. The proposed Regulation enables law enforcement authorities in EU member states to issue "production orders" of communications and cloud providers based in other member states or outside the EU, regardless of where the data is located, and also establishes mechanisms through which providers could challenge an access request based on a conflict between production obligations under the order and obligations under a third-country law. The Directive further requires EU member states to

[2] "The Costs of Data Localization: Friendly Fire on Economy Recovery" ECIPE, 2014.
[3] https://ec.europa.eu/info/sites/info/files/placeholder.pdf
[4] https://ec.europa.eu/info/sites/info/files/placeholder_0.pdf

establish legal representatives for the receipt of cross-border demands. Taken together, the Regulation and Directive would effectively give EU member states access for law enforcement purposes to the data of internet users not only across the EU, but worldwide. The EU's e-Evidence proposal, importantly, focuses on access, not location, and provides another potential model for addressing the law enforcement access problem in India.

3) Budapest Convention on Cybercrime

The Council of Europe Convention on Cybercrime (also known as the Budapest Convention) is at present the main international instrument on cybercrime. It aims to help its state parties harmonize their national laws, improve their investigative techniques and increase cooperation. In June 2017, the Cybercrime Convention Committee (T-CY) initiated a process to draft a second additional protocol to the Convention to create a clearer framework and stronger safeguards for existing practices of trans-border access to data.

4) Financial Action Task Force on Money Laundering (FATF)

The FATF has provided a list of recommendations for combatting money laundering and the financing of terrorism.[5] These recommendations encourage cooperation and coordination between competent authorities, emphasizing the use of mutual legal assistance. In addition, the recommendations focus on the timely production of information rather than the means of production of location of the data itself.

5) U.S. CLOUD Act

The Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943) is a United States federal law enacted in 2018 that modernized outdated data privacy and security laws to reflect modern technologies such as cloud computing. The CLOUD Act authorizes the U.S. government to enter into bi-lateral executive agreements with foreign governments to qualify them to make foreign law enforcement requests for electronic evidence related to its citizens directly to U.S. service providers, rather than via Mutual Legal Assistance Treaties (MLATs), provided that the foreign government counterparties have laws in place that sufficiently safeguard privacy, human rights and due process. The CLOUD Act thus provides a mechanism to resolve the conflicts of law issues that often impede the ability of countries such as India to access such data. While legitimate questions remain regarding how the CLOUD Act will be implemented, we urge the GoI to enter into discussions with the U.S. to determine what if any additional legal safeguards in India might be necessary (e.g., passage of GoI's contemplated Privacy and Data Protection law) to qualify GoI, or an entity within GoI, to enter into an executive agreement pursuant to the CLOUD Act.[6]

---

[5] "FATF Recommendations for International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation," FATF, 2018.

[6] The CLOUD Act additionally provides U.S. law enforcement with the ability to access electronic evidence regarding U.S. citizens stored outside of the U.S. by U.S. companies, pursuant to a valid warrant. The law also provides mechanisms for the companies or the courts to reject or challenge such requests if they believe the requests violates the privacy laws of the foreign country in which the data is stored.

We encourage GOI to explore collaborating through these and other mechanisms to create solutions to the shared global problem of law enforcement access to data. As the world has become more integrated and international, so too have cybercrimes, and any true solution to combatting the globalization of criminal data necessarily must involve cross-border mechanisms for cooperation.

While we would caution against any data localization requirement for the reasons explained above, given the heavy costs to privacy, security, and innovation, we suggest that GOI at minimum narrow the scope of the contemplates localization requirements to defined categories of specific high-risk data.

2. Remove Limits to Cross-border Data Transfers.

The free flow of data is fundamental to the health of the modern global economy, delivering countless benefits and enabling access to knowledge and tools for people around the world. India has historically understood and managed to leverage this reality, as evidenced by the rise of its booming outsourcing industry. It is equally important now for the GOI to acknowledge that international data transfers and meaningful privacy protection are not mutually exclusive or antagonistic goals.

Article 41 of the draft bill permits cross-border movement of data via certain legal bases, but limits these to standard contractual clauses, intra-group schemes, country adequacy and in the case of certain emergencies to be verified by the regulator on a case by case basis. It also includes a requirement for certification and periodic reporting under Section 40 that has no added personal data protection benefit while creating a superfluous compliance burden. We recommend that GOI remove these country-focused limitations and enable the free flow of data, with data fiduciaries remaining accountable and liable for their personal data processing regardless of the location of the transfer.

Many existing regimes reflect the need to preserve multiple approaches to cross-border data transfers without weakening privacy safeguards and India should leverage and take inspiration from these approaches, a few of which are highlighted in the below examples.

Mexico

Mexico's data protection law incorporates provisions that address "accountability" and acknowledge that personal data often needs to travel internationally. The law also avoids uncertainty as to what obligations and rights exist as personal data moves among data "controllers" and "data processors," and what documentation is needed to assure fulfillment of legal responsibilities. The controller remains accountable, together with anyone it transfers data to.

Canada

Canada, through The Personal Information Protection and Electronic Documents Act (PIPEDA), implements an organization-to-organization approach that is based on the concept of accountability. PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing. However, organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement. The Office

of the Privacy Commissioner of Canada can investigate complaints and audit the personal information handling practices of organizations.

APEC CBPRs

The Asia Pacific Economic Cooperation (APEC) forum endorsed a Privacy Framework in 2005, updated in 2015,[7] establishing an interoperable approach to data protection and promoting the free flow of information in the region. The Framework is an accountability-based privacy system that can be implemented in different economies via or alongside their own privacy legal and regulatory regimes. It also sets out an enforceable co-regulatory tool for data transfers, called the Cross Border Privacy Rules (CBPRs), which are flexible enough to be adopted on a broad scale and are gaining traction across the region. The principle of "accountability," a key underpinning of the framework, makes the original data collector legally "responsible" for data by making sure the obligations of the data controller follow the data as it crosses borders. The United States, Mexico, Canada, Japan, South Korea and Singapore are already participating in the CBPRs, while the Philippines, Chinese Taipei and Australia have all taken steps to participate, and other APEC economies have signaled their interest in joining. Operationalization of this system relies on certification bodies and third-party trust programs, backed by domestic enforcement. The APEC Privacy Framework and CBPRs together aim to improve information sharing among government agencies and regulators and facilitate the safe transfer of information between economies, while establishing a common set of privacy protections and providing technical assistance to those economies that have yet to address privacy from a regulatory or policy perspective.

3. Clarify the Definitions of Personal, Sensitive and Anonymized Data.

The current definition of "personal data" in the draft bill is broad and includes not only data that positively identifies an individual, but also data that is "indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such feature, or any combination of such features with any other information." This broad definition establishes a binary test of identifiability with no regard to the level of effort necessary to link the data to the individual and no relation to the degree of sensitivity of the data, creating unwarranted obstacles to the Committee's stated goal of "empowerment, progress and innovation." As data science advances, more and more data is potentially identifiable under the draft bill's definition and thus subject to regulation.

We agree that indirectly identifying information should be regulated as "personal data" in some cases. These cases should be determined by the amount of resources and effort that would need to be expended to re-identify the data and the possible risks resulting from this re-identification. Data should only be considered indirectly identifying (and thus protected personal data) if it is either the data

[7] https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

fiduciary's intent to identify the individual, or if it is reasonable for someone to attempt to identify given the nature and context of the data, the level of effort to identify individuals, and the risk of harm to the individual. Where the level of effort to identify an individual is low and the risk of harm is high, the indirectly identifying information should be categorized as "personal data." On the other hand, if the level of effort is high and the risk harm is low, the potentially identifiable data should not be considered personal data subject to the regulation. We therefore also suggest a qualification be added to "combination . . . with any other information." This "other information" should be legally available to the data fiduciary in order for such "other information" to transform the otherwise non-personal data into personal data.

The draft bill currently includes passwords and financial data in its list of sensitive data. The higher restrictions on sensitive data processing in the bill will inhibit many legitimate activities relating to security, fraud detection, and payment processing. We therefore suggest these be excluded from the definition to ensure India's outsourcing industry, which is a major source of jobs and economic growth, is not impacted negatively. We also suggest pictures be excluded from the definition of biometric data, to ensure that a vast amount of innocuous activity is not similarly hampered by the overbroad application of processing restrictions.

Article 2 of the bill defines anonymization as an "irreversible process of transforming personal data to a form in which a data principal cannot be identified." This is an impossibly high standard of anonymization under which data fiduciaries could almost never be certain that they have achieved sufficient levels of anonymization. This overly-narrow definition of anonymization may discourage data fiduciaries from attempting to de-identify data in the first place - particularly small companies and start-ups that lack the resources and technical know-how to invest in potentially expensive and time-consuming to maintain irreversible anonymization.

As an alternative, India should adopt an anonymization standard that permits data fiduciaries to engage in "reasonable efforts" to de-identify data. For example, The United Kingdom's Information Commissioner's Office (ICO) has laid out an advanced risk-based approach to anonymization and re-identification.[8] The ICO's approach recognizes the ideal of "perfect anonymization" is superfluous and often unachievable and opts instead to encourage companies to use technical and contractual measures to mitigate risk until the probability of re-identification is remote. Where anonymization is not possible, competent authorities should grant organizations decreased liability or lessen their compliance burdens as incentives for partially anonymizing, or "pseudonymizing" data. For example, the GDPR permits organizations pseudonymizing data to further process that data for additional purposes that are compatible with the original purpose of that data's collection – without needing to get consent again.

[8] Information Commissioner's Office, Anonymization: managing data protection risk code of practice.

4. Expand the Grounds for Personal Data Processing.

While we are pleased to see the draft bill contains various legal bases for personal data processing, we were disappointed to note that the committee identifies consent as the primary and preferable basis for processing, and further, and includes whether obtaining consent is possible in the consideration of whether consent should be the legal basis for processing. The possibility of obtaining consent is not always relevant to whether consent is the most appropriate legal basis for personal data processing and should not be a primary consideration in relying on the "reasonable purpose" ground. The bill should allow the reasonable purpose to be on equal footing with consent as a legal basis. Additionally, while the report makes mention of implied consent (p. 37), stating that except in the case of sensitive personal data, consent can be inferred in some cases based on the circumstances, there is no similar wording in the draft bill itself. We request that the permissibility of implied consent be explicitly codified in the draft bill.

We also suggest that the draft bill include an additional legal basis: processing to fulfill a contractual obligation. Without such a legal basis, businesses would be required to duplicate consent when processing is necessary to perform an existing contract. In keeping with the approach adopted by GDPR, India should adopt contractual obligations as an additional ground for processing, which allows data fiduciaries to perform various necessary functions including providing, developing and improving services, measurement, communication with the data principal, and transfer of data to data processors who don't have independent use rights.

We suggest that the Committee clarify that data processing associated with monetization of a service (either for processing of payment or delivery of advertising) is "necessary" to provide it, and that data fiduciaries can decline to provide services if data principals don't consent to receive advertising.

We also suggest that the Committee clarify data processing limitations in Article 17 (5/6/7) to enable reasonable uses of data, including sensitive data. Sensitive data processing should be permitted for reasonable grounds since the balancing test already includes "the effect of processing activity on the rights of the data principal," and "the reasonable expectations of the data principal." Both factors account for the risk associated with a given category of data. So long as the balancing test considers risk, the "reasonable purpose" residual ground should be available for sensitive categories of data. We also suggest that the reasonable purposes listed in the law include DPA discretion to specify additional reasonable purposes.

Article 14 provides a ground for processing personal data based on compliance with any law made by Parliament or any State Legislature, or compliance with any order or judgement of any Court or Tribunal in India. The law, however, would apply to multi-national companies that process the personal data of Indians. Such companies would also be subject to the laws of other countries that may require disclosure or other processing of their Indian employees or customers. To avoid the untenable position of requiring companies to choose which country's law they will follow, this ground for processing should be expanded to include compliance with any country's legal requirements.

Article 16 of the Bill provides for processing in various situations related to the employer/employee relationship. Article 16(2), however, limits all of the permitted purposes by allowing them "only where processing on the basis of consent of the data principal is not appropriate having regard to the employment relationship between the data fiduciary and the data principal, or would involve a disproportionate effort." The limitation on the valid employment purpose injected by (2) creates substantial unwarranted uncertainty on businesses. The draft law is devoid of guidance to businesses on how to conduct the subjective evaluation of the limitations set forth. As a result, compliance with this legal ground will have significant variations across businesses. Large risk-averse companies will likely always seek consent, but the vast majority of employers (and thus the vast number of Indians) that do not employ in-house legal counsel or have budget for external legal guidance, will not seek employee consent. A two-tiered system of data protection pivoting upon the nature of Indians' employers should not be an appropriate solution.

More importantly, consent, as set forth in Article 12 as a basis for data processing, should be reserved for situations where the data principal and the data fiduciary have appropriate bargaining power. In the employer/employee context, the employee rarely has the requisite bargaining power to make the consent (as contemplated under Article 12) freely given. We therefore suggest Article 16 (2) be removed.

5. Lower Age of Consent for Children's Data.

We request that any obligations relating to children's privacy include an "actual knowledge" standard, and that companies should not be held liable if they do not have knowledge that they are collecting information from a child. It is also important that the age of consent be reasonable and consistent with what is common in other parts of the world so as not to limit young people's participation and opportunities for learning. While the EU has allowed Member States to define their own ages (between 13 and 16), COPPA in the United States sets the age of consent at 13. We suggest India set the age of consent at 13 to encourage digital literacy and to prevent children in India being disadvantaged or excluded from online content and activity.

6. Put Reasonable Limit on Data Breach Notification.

The draft bill requires notification to the Authority of "any personal data breach . . . where such breach is likely to cause harm to any data principal" regardless of the degree of the harm. "Harm" is defined broadly in Article 3(21) to include subjective evaluations such as "loss of reputation, or humiliation." Without a qualifier as to the degree of harm necessary to trigger the notice obligation, any slight or trivial infraction of the inherently subjective reputation or humiliation would trigger the obligation of a notice to the Authority which is likely to create a high administrative burden on businesses as well as the Authority. We suggest that the harm from the breach must be significant to a reasonable person to obligate notification to the Authority.

The draft bill currently requires notification to the authority "as soon as possible" and subjects fiduciaries to a timing requirement determined by the Authority. We suggest that language be changed to "without reasonable delay" to prevent overloading regulatory institutions with incomplete or inaccurate information before the incident has been properly analyzed or addressed by the data fiduciary. Furthermore, we suggest the bill clarify how the breach notification requirements contained in this bill relate to breach notification mandates to other regulators in Indian law and to ensure there is no duplication.

7. Narrow the Data Protection Impact Assessment Requirement.

The draft bill requires that significant data fiduciaries always submit DPIAs to the Authority for review, which is likely to create a high administrative burden. The GDPR instead takes a narrower approach in requiring submission only when a high risk is identified, focusing the Authority's attention on processing activities that are most likely to harm data principals. We request clarification about whether processing may commence prior to the Authority's review and suggest imposing time frames within which the Authority must respond. The GDPR sets the limit to 8 weeks, thereby limiting business disruption from pending DPIA reviews.

We are also concerned by Article 33 which labels processing that involves "new technologies" as inherently risky and therefore, requiring of a DPIA. New technologies do not necessarily carry a high risk and such a broad DPIA review obligation could delay the adoption and growth of new technologies in India. DPIA review by the Authority should only be conducted if there is an assessed risk of serious harm under the general intent of Article 33, and not because of the technology that may be used for the processing. In addition, this provision could hamper large companies from setting up centers of innovation in India and impact the home-grown startup ecosystem. Article 33, therefore, should be technology neutral and focus on the risk of harm.

8. Remove Local Residency Requirement for Data Protection Officer (DPO).

We would like to note that there is no precedent for a legal requirement for foreign companies to hire a DPO who is based domestically. Companies should be able to rely on one DPO worldwide, while allocating a local point of contact for the company in India. This requirement sets an unworkable precedent, with companies potentially having to hire DPO's for each country they operate in. These additional costs, however, do not translate into more effective data protection. The draft bill should also permit companies to appoint a DPO based on the nature and volume of personal data being handled rather than setting up an expensive regulatory compliance regime for enterprises conducting low risk data processing.

9. Limit Penalties and Remove Criminal Penalties for Offenses.

The penalty structure laid out in the draft bill is disproportionately high and the language also does not sufficiently consider allocation of penalties on the basis of actors' intentions. It is important to ensure meaningful enforcement by creating an enforcement framework that distinguishes between (1) actors who willfully or in a grossly negligent way breach their legal obligations and cause harm to users from

(2) those who invest significant resources in not only complying with legal obligations, but often in putting in place data management practices, technologies and security measures that go beyond these requirements to ensure customer data is treated carefully. We suggest civil penalties be limited to a percentage of profits of the Indian entity rather than the global entity, and that authorities be encouraged to use discretion in enforcement to ensure dissuasive but fair penalties. This will foster an approach that promotes innovation, business and competitiveness, while putting the necessary controls and balances in place.

The proposed bill deems the head of a company or government department liable for the commission of an offense, which risks freezing business activity in this sector and discouraging qualified candidates from accepting these roles. We suggest the Committee limit personal liability of employees to cases where the corporate entity is acting as a shield for what is actually a single, individual actor.

10. Create an Independent and Well-Resourced DPA.

We believe that an independent regulatory body, separate from any governmental ministries, will be critical to the successful implementation and enforcement of the privacy law that is ultimately adopted in India. GOI will have to ensure a centralized and "expert" authority is provided with sufficient resources and can keep up with the rapid evolution of technology and global privacy trends. Articles 62 through 65 empower the regulator to issue directions, call for information, conduct enquiries and take punitive actions pursuant to an enquiry on the fiduciary and the processor. We suggest that the DPA take a collaborative and non-adversarial approach in its enforcement functions and ensure that the Appeals Tribunal remains independent and objective in its adjudications, to the extent possible, during implementation. Given the nascence of this space in India, as well as the potential for rapidly changing technological developments, ITI recommends that the DPA is mandated to first go through a consultative process with any industry body/ individual data fiduciary, prior to exercising any powers to issue orders or directions. The DPA should also be encouraged to reach negotiated settlements with parties prior to formal enforcement.

11. Clarify Processor Fiduciary Liability.

While we welcome the Committee's aim to establish clear roles for data fiduciaries and data processors, we recommend that Article 31 be modified to impose the primary responsibility for the determination of security safeguards on the data fiduciary. The data fiduciary should be responsible for contracting appropriately secure services from processors based upon its own assessment of the risks associated with the processing, given its unique understanding of the nature of the personal data within its control. Similarly, Article 75 should clarify that the data fiduciary should be primarily liable to the data principal for any compensation claims, unless the loss arises as a direct result of an act or omission of the data processor.

Data fiduciaries generally have the primary obligation for ensuring compliance with applicable data protection law, while data processors should be required to comply with data fiduciary's instructions and ensure the implementation of technical and organizational measures as well as the security of the

data they process. These are the customary responsibilities placed upon data controllers and data processors in other data privacy laws globally. A controller ensures that the data subject can exercise his/her rights and ensures respect for the established data protection principles. Data processors' responsibilities are determined bilaterally between controllers and processors depending on the circumstances and normally defined in a detailed contract.

12. Alter the Yearly Audit Requirement.

We recommend that the bill permit data fiduciaries to fulfill their yearly audit obligation via generalized privacy audits aligned with globally interoperable standards rather than compliance with this legislation specifically, which would create an additional compliance burden for companies who are operating in multiple countries and subject to various data protection and privacy laws. In addition, data auditors who allocate data trust scores should be required to follow clear and objective criteria and the bill should provide for rating dispute mechanisms for fiduciaries who wish to challenge a rating. To minimize the resource intensiveness of this privacy regime we suggest audits only be made compulsory for companies that have faced an enforcement action by the Authority or are otherwise deemed to be carrying out high-risk activities.

Finally, we believe the concept of a "significant data fiduciary" as laid out in the draft bill is unclear and risks becoming an arbitrary designation, creating the potential for discrimination against certain types of companies even if their activities are low risk and should not otherwise be subject to additional scrutiny.

13. Narrow Data Access Powers and Clarify Safeguards.

The bill creates powers for the "inquiry officer" to access large swathes of data indiscriminately. To maintain privacy, security, and protect companies' intellectual property, we ask that this access be narrowed to records specifically pertaining to what is necessary to the investigation around the processing of personal data and the protection of that data. At the same time, we recommend adding a provision that would require authorities and the Inquiry Officer to properly safeguard this information while in its custody, and to clarify whether this information would be subject to a Right to Information Act action. It is important that safeguards are in place to prevent competitors from inappropriately gaining this information through such a request.