COMMENTS OF THE AMERICAN BAR ASSOCIATION
SECTIONS OF ANTITRUST LAW AND INTERNATIONAL LAW
ON THE PERSONAL DATA PROTECTION BILL, 2018

September 27, 2018

The views stated in these Comments are presented on behalf of the American Bar Association Sections of Antitrust Law and International Law. They have not been approved by the House of Delegates or the Board of Governors of the American Bar Association and therefore may not be construed as representing the policy of the American Bar Association

I. Introduction

The Sections of Antitrust Law and International Law ("the Sections") of the American Bar Association respectfully submit these comments on The Personal Data Protection Bill, 2018.[1] These comments are intended to further this dialogue and reflect the Sections experience in international and cross-border privacy and data security issues. The Sections' long involvement in these issues rests on the participation of both private and public sector lawyers, economists, and market participants, reflecting the interests of all those who engage in, benefit from, and enforce legal rights relating to, digital as well as traditional commerce in which personal data plays an important role. The Sections do not advocate on behalf of any particular interest or party; rather, we offer our comments as constructive input of the type invited by the Committee of Experts.

The Sections commend the Committee of Experts for presenting a comprehensive, thoughtful analysis that takes into account the vast technological changes and legal developments in the global data marketplace. In these Comments, the Sections make several suggestions that we believe will further the goals "to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation."

II. Executive Summary

The Sections' comments make the following suggestions:

Jurisdiction: The Sections respectfully submit that the proposal provides for excessive extraterritorial reach. The draft seeks to replicate Article 3 of the European Union's (EU) General Data Protection Regulation ("GDPR"),[2] but because it does not include its limiting recitals, the proposal is, in effect, far broader than the GDPR. The draft would apply to all companies incorporated outside of India that offer goods or services in India. The Sections believe adopting such an expansive regulation will deter companies from offering services in India and overburden them with excessive regulations from India and the EU. The costs may prove prohibitive, particularly for small and medium-sized entities. The Sections continue to believe that even the GDPR approach is too aggressive, and that the approach of the 1995 EU Directive is preferable, regulating a controller when the processing was "carried out in the

[1] http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.
[2] The General Data Protection Regulation (EU) 2016/679, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

context of the activities of an establishment . . . on the territory of the Member State." This approach avoided the major conflict-of-laws issues that arise under the overbroad jurisdictional reach of the GDPR and reduces obstacles to the growth of the digital economy that promises to bring new goods, services, and opportunities to India's economy. The Sections at a minimum would urge the Ministry of Electronics and Information Technology ("MeitY") to conform to the entirety of the GDPR's approach – including its recitals and common law underpinning – rather than the current incomplete statement of the GDPR.

Data Fiduciary, Data Principal, and Data Processor: Applying the concept of fiduciary to the data controller is inapposite, because personal data is often made available in a public or arms-length commercial context and artificially imposing that relationship in India will simply exclude India from the global data market. The GDPR model of specifying the duties and obligations of the data controller and data processor are more appropriate for the treatment of personal information collected and used in non-fiduciary relationships.

Definition of "Personal Data": Absent from the Bill is any express reference to the likelihood of the data fiduciary, or any other person, identifying the natural person so that data may constitute "personal data" even if it would not be feasible for the data fiduciary or the other person to carry out such identification. The Sections would recommend consideration of an approach similar to that adopted in the GDPR and the U.S. Federal Trade Commission's (FTC) privacy framework,[3] which is to focus on the means reasonably likely to be used, either by the controller or by a third party, to identify the natural person to whom the data relates and refer to factors such as the cost of identification and the time required for identification, having regard to available technology.

Consent/Reasonable Purposes: The Sections recognize that the "reasonable purpose" approach features the flexibility of the GDPR's legitimate interest lawful basis. However, this approach does not, but in the Sections' view should, feature a balancing test to determine when the data fiduciary can process data for reasonable purposes. The Sections therefore recommend a balancing test that takes into account the interests of the controller, the effects on rights of the data subject, the public interest, etc. This is similar to the balance test used in a "legitimate interest" analysis. The Sections would also recommend additional guidelines for when the use of reasonable purpose is inappropriate.

Processing of Sensitive Personal Data in the Employment Context: There are likely to be circumstances in which it is necessary for employers to process sensitive personal data relating to their employees, but that are not currently covered in Chapter IV. The Sections recommend that consideration be given as to whether it may be necessary either to expand the conditions in Chapter IV or for these conditions to be extended through delegated legislation.

Processing for Functions of the State: The Bill gives wide latitude to a data fiduciary processing data for functions of the State, without limiting such processing to reasonable purposes. The Sections recommend limiting such processing to purposes related to national security, counterterrorism and the investigation of serious crimes.

---

[3] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, FTC Report (Mar. 2012) ("2012 FTC Privacy Report"), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

Data Trust Score: The Sections reiterate the concerns we raised in our prior submission about the disproportionate impact on smaller data fiduciaries seeking to comply with the Act and recommend that the Data Protection Authority of India ("Authority") register and properly incentivize data auditors to serve smaller data fiduciaries.

Cross-Border Data Transfers and Data Localization: The Sections recommend dropping the cross-border data transfers and data localization restrictions from the Bill in order to encourage and facilitate cross-border data flows. This would provide the Bill with a more flexible framework, which could evolve to take account of technological developments, increased global data flows and the interests of global entities considering doing business in India.

Cybersecurity & Breach Notification: The draft bill avoids creating a specific standard for when a data breach should be reported, either to regulators or data subjects and instead leaves this critical issue to be determined by the newly formed DPA. The Sections recommend that the draft provide that notification of significant data breaches be made "without unreasonable delay."

Right to be Forgotten: Privacy Regulation and Freedom of Expression: The Sections commend the Committee for advocating a balancing test. However, we note that while broad-based restrictions on the dissemination of personal data may be laudable in theory, they are not free from error costs that may manifest in regulation (*e.g.,* stunted innovation).

Automated Decision Making and Profiling: The Sections reiterate the concerns they expressed in connection with the White Paper that any disclosure of business proprietary information in, *e.g.* the Data Protection Impact Assessment submitted to the Authority, be subject to the protection of intellectual property rights so as to protect the ability of businesses to innovate and compete.

The Broad Authority Delegated to the Regulator: The draft bill empowers the DPA to make legislative determinations that the Sections view as properly within the province of the legislature rather than of a newly created privacy regulator. The Sections have identified a number of legislative determinations that are delegated to the DPA by the draft bill and suggest in each case that the draft bill be amended to provide that these essential determinations be made by the legislation itself rather than a new and untested administrative agency.

Accountability/Penalties: The imposition of penalties of up to four percent of total worldwide turnover in the preceding financial year (which may include the worldwide turnover of group companies) often will be disproportionate to the revenue earned from data processing activities or to the harm suffered by individuals, even for major infractions of the law. In addition, the factors the Adjudicating Officers are required to consider when imposing civil monetary penalties are narrower in some respects than the GDPR. The Sections therefore recommend that the Bill be amended to add additional factors when imposing civil monetary penalties focusing on the responsibility of, and actions taken by, the data fiduciary or data processor; the degree of their cooperation with the Data Protection Authority; and the categories of personal data affected. The Sections are also concerned that criminal penalties may be applied too broadly. The Sections recommend that the Bill be amended to narrowly circumscribe and specifically define potential infringements that constitute criminal offenses and that the Committee remove individual criminal liability for corporate offenses from the Bill.

III. Specific Suggestions

1. Jurisdiction

The proposed jurisdiction provisions of the draft bill allow substantial extraterritorial reach, and clearly seek to emulate the parallel provisions of the GDPR. The Committee included an exception for processing foreign nationals' data that is not present in the GDPR, which is helpful. The draft does not, however, include the qualifications expressed in the GDPR's recitals relating to jurisdiction, potentially making it even more far-reaching than the GDPR.

The proposed regulation applies to both in-country and out-of-country data processors.

First, it applies to the processing of personal data that is "collected, disclosed, shared or otherwise processed" in India.[4] However, collection of Indian data principals' personal data by data fiduciaries outside of India is exempted from this provision *unless* the data fiduciary is (a) carrying on business in India; (b) offering goods and services in a targeted and systematic manner to persons in India; or (c) processing data for profiling of data principals in India.[5] This provision does not, however, apply to fiduciaries outside of India engaging in "irregular and ad hoc collection of data of persons present in India."[6]

Second, the regulation applies to processing personal data anywhere in the world "by the State, an Indian company, any Indian citizen," or any entity incorporated in India.[7] It provides that the Central Government may exempt processors in India that only process the data of foreign nationals.[8] Anonymized data, in addition, is exempted.[9]

This proposal is helpful in that it exempts the processing of foreign nationals. India's business process outsourcing industry is a major source of jobs and economic growth. If this exception is clarified to include all organizations processing only foreign nationals' data (rather than only Indian companies), this regulation will safeguard this high-value industry in India. We suggest that this clarification be made, and that non-Indian companies be included. We also support the exemption for the processing of anonymized data.

However, the proposal provides for excessive extraterritorial reach. The draft seeks to replicate Article 3 of the GDPR, but the proposal is, in effect, far broader than the GDPR. The draft would apply to all companies incorporated outside of India that offer goods or services in India. Adopting such an expansive regulation will deter companies from offering services in India and overburden them with excessive regulations from India and the EU. The costs may prove prohibitive, particularly for small- and medium-sized entities.

As noted above, the draft proposal uses terms from the GDPR but does not include its limiting recitals (or, of course, the EU common law principles that undergird those terms). In particular:

"Offering Good or Services." In respect of the first prong concerning parties offering services in the EU, recital 23 of the GDPR contains a useful clarification:

---

[4] Draft Bill, art. 2 §1(a); Committee Report at 18-19, 21.

[5] Draft Bill, art. 2 §2(a)-(b); Committee Report at 19-20, 21.

[6] Committee Report at 1-20.

[7] Draft Bill, art. 2 § 1(b); Committee Report at 19, 21.

[8] Committee Report at 20-21.

[9] Draft Bill, art. 2 §3.

> Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.[10]

Accordingly, the mere accessibility from the EU of a company's website or the use of a certain language are not sufficient to trigger jurisdiction under the GDPR. The targeting of EU users must be more obvious and "envisioned," for example, by allowing them to order goods and having them shipped to the EU, by using the Euro as a currency option, or by offering content in languages adapted to EU users.

These principles sound in EU common law. In the *Pammer* case,[11] the Court of Justice of the EU ("CJEU") was asked to clarify when an Internet service can be considered to target a Member State. The CJEU held that mere accessibility of a website does not suffice. Similarly, the indication of the trader's address, e-mail address, or phone number (without international code) cannot be construed as targeting. To the contrary, the CJEU highlighted the following examples of activities that can demonstrate an intention to target:

- the express mentioning that the service is provided to users in a Member State;
- paying search engines to have its website favorably indexed in order to facilitate access by consumers in particular Member States;
- the international nature of the services;
- the provision of international telephone numbers;
- the use of internet domain levels other than those of where the service provider is established (or general ones, such as .eu, or .com); and
- the mentioning of international clientele, and accounts written by such customers.

"Monitoring the Behaviour." The draft law also uses the terminology of the GDPR for tracking individuals within India, but again does not include the limiting language of the corresponding recital. Recital 24 of the GDPR provides:

> In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

The recital assumes tracking of behavior that is quite extensive. The tracking should occur with the intention of influencing the user based on an analysis and prediction of personal preferences. Whether this description of "monitoring" would apply to generally accepted Internet advertising techniques is an open question. Current Internet advertising strategies rely on data that does not contain contact or identifying information of "natural persons," but might rely on device identifiers, IP addresses, cookies, and other proxies for identifying a particular advertising subject on the Internet. It may be that "monitoring" that focuses on serving targeted advertising to a user based solely on device identifier, IP

[10] GDPR, Recital 24.

[11] Peter Pammer v. Reederei Karl Schlüter GmbH & Co., KG (C-585/08) and Hotel Alpenhof GesmbH v. Oliver Heller, (C-144/09) (December 7, 2010), available at http://curia.europa.eu/juris/liste.jsf?language=en&num=C-585/08.

address, or other identifier that cannot be used to identify a "natural person" should not fall under the definition. It remains to be seen how the EU will interpret this provision of the GDPR.

The Sections continue to believe that even the GDPR approach is too aggressive and believe the approach of the 1995 EU Directive is preferable. The Directive had limited extraterritorial application, regulating a controller when the processing was "carried out in the context of the activities of an establishment . . . on the territory of the Member State." This approach avoided the major conflict-of-laws issues that arise under the overbroad jurisdictional reach of the GDPR. It also reduces obstacles to the growth of the digital economy that promises to bring new goods, services, and opportunities to India's economy. The Sections at a minimum urge MeitY to conform to the entirety of the GDPR's approach – including its recitals and common law underpinning – rather than the current incomplete statement of the GDPR.

2. Data Fiduciary, Data Principal and Data Processor

The Bill defines the relationship between what in other jurisdictions are referred to as the data controller, the processor, and the data subject as a fiduciary relationship.[12] As explained in the accompanying Report, "depending on the nature of data that is shared, the purpose of such sharing and the entities with which sharing happens, data principals expect varying levels of trust and loyalty."[13]

We are mindful that in proposing novel terminology, the Committee of Experts was seeking a custom tailored approach to India, that data controllers should have legal obligations, and data principals should have legal rights. However, the Sections are concerned that with respect to personal data, applying the concept of fiduciary to the data controller is confusing and inapposite. The imposition of this relationship was not proposed in the *White Paper of the Committee of Experts and the Ministry of Electronics and Information Technology on a Data Protection Framework for India* (the "White Paper"). Nor has any other jurisdiction adopted the framework of a fiduciary relationship between the data subject and data controller. The Sections believe this is for good reasons, including that it would preclude the collection of even non-sensitive personal information because any collection would violate the no conflict, no profit, and confidentiality rules of fiduciary relationships, and the collection of any adverse information needed to prevent fraud, abuse, and illegal activity would violate the undivided loyalty rule. The GDPR model of specifying the duties and obligations of the data controller and data processor are more appropriate for the treatment of personal information collected and used in non-fiduciary relationships. An alternative approach would be to look at the controller/processor relationship as a principal/agent relationship, as in the Privacy Shield Framework.[14] Under the terminology of the proposed bill, a controller would be a "data agent" to a data subject who is a "data

---

[12] THE PERSONAL DATA PROTECTION BILL, 2018, CHAPTER I, Section 3: (13) "Data fiduciary" means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data; (14) "Data principal" means the natural person to whom the personal data referred to in sub-clause (28) relates; (15) "Data processor" means any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary; … (36) "Significant data fiduciary" means a data fiduciary notified by the Authority under section 38."

[13] *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (Report), http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf at 8:

[14] *See* Federal Trade Commission, The EU-U.S. Privacy Shield Framework, *available at* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield.

principal." The data subject would also be the "data principal" in the relationship with the data processor.

> As noted in the landmark India Supreme Court case, *Reserve Bank of India and Ors. v. Jayantilal N. Mistry and Ors* (December 16, 2015), fiduciary relationships usually arise in one of four situations:
>
> (1) when one person places trust in the faithful integrity of another, who as a result gains superiority or influence over the first,
>
> (2) when one person assumes control and responsibility over another,
>
> (3) when one person has a duty to act or give advice to another on mattes falling within the scope of the relationship, or
>
> (4) when there is specific relationship that has traditionally be recognized as involving fiduciary duties, as with a lawyer and a client, or a stockbroker and a customer."

As stated by the Supreme Court, a fiduciary must adhere to the:

(i) No Conflict rule – A fiduciary must not place himself in a position where his own interests conflicts with that of his customer or the beneficiary. There must be real sensible possibility of conflict.
(ii) No profit rule – a fiduciary must not profit from his position at the expense of his customer, the beneficiary;
(iii) Undivided loyalty rule – a fiduciary owes undivided loyalty to the beneficiary, not to place himself in a position where his duty towards one person conflicts with a duty that he owes to another customer. A consequence of this duty is that a fiduciary must make available to a customer all the information that is relevant to the customer's affairs;
(iv) Duty of confidentiality – a fiduciary must only use information obtained in confidence and must not use it for his own advantage, or for the benefit of another person.[15]

The India Supreme Court there held that the Reserve Bank of India (RBI) does not place itself in a fiduciary relationship with the Financial institutions (though, in word it puts itself to be in that position) because, the reports of the inspections, statements of the bank, information related to the business obtained by the RBI are not under the pretext of confidence or trust. In this case neither the RBI nor the Banks act in the interest of each other. By attaching an additional "fiduciary" label to the statutory duty, the Regulatory authorities have intentionally or unintentionally created an *in terrorem* effect.

The same *in terrorem* effect applies here as well, where the label does not reflect the true relationship of the data controller and data subject. The assumption that all, or even most, personal data is provided in the context of a trust and loyalty relationship is incorrect; the Sections submit that artificially imposing that relationship in India will impair India's participation in the global data market. There should be no presumption of a fiduciary relationship, for example, where a data subject voluntarily makes his or her personal information public (*e.g.*, posting business-related or other personal

[15] http://www.dhirassociates.com/images/Fiduciary-Relationship-RBI-NEW.pdf, *citing* The Advanced Law Lexicon, 3rd Edition (2005).

information on the internet) or providing personal information to government agencies for a public purpose (*e.g.*, to obtain a license).

Nor should there be a presumption of a fiduciary relationship with respect to personal information provided in arms-length commercial contexts, which would be contrary to well accepted contract law. For example, a data subject knows that if she purchases a product on credit and does not pay, the creditor may file a lawsuit disclosing the name and conduct of the defaulting debtor and report that information to a credit reporting agency. The data subject knows that the creditor does not owe it a duty of loyalty or confidentiality and so will not disclose the failure to pay without the express permission of the debtor. To render every arms-length commercial transaction into a fiduciary relationship could make doing business in India impossible and, in the credit scenario, would encourage fraud. Indeed, the integrity of the credit reporting system itself could be hampered to the detriment of the underserved who depend on a credit reporting system to advance their economic well-being. That potential outcome would conflict with the goal of empowering rural Indians. The imposition of a fiduciary relationship between the data controller and the data subject would also preclude the collection of personal data required by law in many countries to perform due diligence on vendors and suppliers, which includes the collection of personal information related to officers, directors, and principals. Those wishing to work with Indian businesses simply could not do so and would have to look elsewhere.

3. Definition of "Personal Data"

The Bill defines "personal data" as "data about or relating to[16] a natural person who is directly or 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 features, or any combination of such features with any other information."

The reference point of data relating to an identifiable natural person is consistent with the approach taken in the OECD Guidelines,[17] the FTC's privacy framework, and the EU GDPR and Data Protection Directive[18] that preceded it. Similarly, the reference to an individual being *directly or indirectly* identifiable is consistent with GDPR and its predecessor and takes account of the range of means by which a natural person may be identified.

However, absent from the Bill is any express reference to the *likelihood* of the data fiduciary, or any other person, identifying the natural person. This means that, in principle, data may constitute "personal data" if it is merely theoretically possible that the natural person may be identified, either by

---

[16] It is unclear whether there is intended to be any substantive distinction between "about" and "relating to." In the Sections' view it would be sufficient to refer to either "relating to" (consistent with legislation such as GDPR) or "about" (consistent with legislation such as the Singapore Personal Data Protection Act 2012). "About" suggests that the relevant natural person must be the subject of the data, whereas "relating to" suggests a looser relationship between the data and the natural person and may result in a broader application of rights such as confirmation and access (section 24).

[17] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, updated in 2013, http://www.oecd.org/sti/ieconomy/privacy-guidelines.htm.

[18] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.

the data fiduciary or by some other person, even if it would not be reasonably likely that the data fiduciary or the other person could carry out such identification. This may lead in practice to data fiduciaries treating all data as personal data, even in circumstances where this is plainly not warranted, on the basis that the possibility cannot be ruled out altogether that another person (including, potentially, the relevant natural person himself) may be able to determine the natural person to whom the data relates.

The Sections recommend considering an approach similar to that adopted in GDPR and the FTC's privacy framework, which is to focus on the means reasonably likely to be used, either by the controller or by a third party, to identify the natural person to whom the data relates.[19] The Bill might, as in the GDPR and the FTC's privacy framework, refer to factors such as the cost of identification and the time required for identification, having regard to available technology. This would provide the Bill with a flexible concept of identifiability, which could evolve over time to take account of technological developments, while at the same time allowing data fiduciaries to avoid incurring the cost and effort of treating data as personal data in circumstances in which there is no reasonable likelihood of a natural person being identified from it.

An alternative approach is that previously taken in the UK Data Protection Act 1998[20] (now repealed in relevant part),[21] which was to consider whether the relevant natural person could be identified from the information in question, either by itself or taken together with other information in, or likely to come into, the possession of the controller. A similar approach is taken by the Singapore Personal Data Protection Act 2012. There are several benefits to this approach, not least of which is that it sets a reasonably objective standard for data controllers to apply. One issue with this approach, however, is that it does not consider the likelihood of identification by a person other than the controller itself, which may be difficult to assess, but may also lead to different outcomes in the case of indirect identifiers such as dynamic IP addresses.

3. **Consent / Reasonable Purposes**

The Sections note that the reasonable purpose approach for data processing activities promises specificity from the Authority for reasonable purpose related activities identified under Section 17(2). The Sections also recognize that the reasonable purpose approach features the flexibility of the GDPR's legitimate interest lawful basis. Specifically, the reasonable purpose approach balances the interest of the data fiduciary, whether the data fiduciary can reasonably obtain consent, public interest, data principal rights, and the reasonable expectations of the data principal.

---

[19] Recital 26 to GDPR provides: "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments." In our view that reference to "singling out" is not a helpful addition to the recital and does little to clarify what is intended. *See also* 2012 FTC Privacy Report at 18-22.

[20] https://www.legislation.gov.uk/ukpga/1998/29.

[21] It was replaced by Data Protection Act 2018, http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf.

Notably, the reasonable purpose approach does not feature a balancing test to determine when the data fiduciary can process data for reasonable purposes. The Sections therefore recommend a balancing test that takes into account the interests of the controller, the effects on rights of the data subject, the public interest, etc. This is similar to the balance test used in a "legitimate interest" basis. The Sections would also recommend additional guidelines for when the use of reasonable purpose is inappropriate.

The Sections also note that, unlike the GDPR, the legislative proposal does not explicitly include contractual necessity as a basis of implied consent. While "reasonable purpose" may be sufficiently flexible to take into account contractual necessity, the Sections recommend that this be made more explicit.

4. Processing of Sensitive Personal Data in the Employment Context

Sensitive personal data may be processed only in strictly limited circumstances, which are set out in Chapter IV (see section 7(2)). There are likely to be circumstances in which it is necessary for employers to process sensitive personal data relating to their employees, but that are not currently covered in Chapter IV. Whereas section 16 provides a basis for the processing of non-sensitive personal data in the employment context in circumstances in which it would not be appropriate to rely on consent, this does not provide a basis for the lawful processing of sensitive personal data.

Examples of circumstances in which it may be necessary for employers to process sensitive personal data include:

- Biometric data – it may be necessary for employers to process biometric data for purposes of authentication of employees' access to resources (such as fingerprint scanning or facial recognition). There is no obvious ground in Chapter IV for such processing.
- Dietary requirements – employers and their service providers may need to process details of employees' dietary requirements for purposes of ensuring that catering accommodates religious beliefs or allergies or food intolerances. Again, there is no obvious ground in Chapter IV for such processing.
- Legal proceedings – employers frequently need to process personal data for purposes of bringing or defending legal proceedings involving employees, and it is not uncommon for this to involve the processing of sensitive personal data. Section 44(1) exempts *disclosures* of personal data from section 7(2) and Chapter IV in circumstances where such disclosures are required for legal proceedings, but this does not apply to processing more generally. (Section 44(1) is to be contrasted with section 44(2), which refers more generally to "processing".)

While recognising that the types of data enumerated under "sensitive personal data" are rightly considered sensitive and should be processed only under limited conditions, the Sections suggest that it may be necessary either to expand the conditions in Chapter IV or for these conditions to be extended through delegated legislation.

5. **Processing for Functions of the State**

Sections 13(1), and 19 of the Bill allow a data fiduciary to process personal and sensitive data, respectively, if the processing is necessary or strictly necessary for any function of Parliament or any

State Legislature.[22] Section 20(a) of the Bill, permits a data fiduciary to process sensitive personal data if the processing is explicitly mandated under any law made by Parliament or any State Legislature.[23]

The Sections are concerned by the potential scope of "*any function of Parliament or any State Legislature*" and "*any law made by Parliament or any State Legislature*" and note that this language provides the State, as a data fiduciary, with the means to process data in a manner inconsistent with data principal rights. The Bill gives wide latitude to a data fiduciary processing data for functions of the State, without limiting such processing to compelling state purposes such as processing related to the national security. The Sections recommend limiting such processing to purposes related to national security, counterterrorism, and the investigation of serious crimes. The Sections further recommend limiting such processes absent a judicial warrant based upon the required standard under applicable law, which in the U.S. is an individualized showing of probable cause.

The Sections further note that the public interest (and state functions) are much broader than those described in the bill. Other interests include consumer protection, competition, health, safety, environment, education, tax, public benefits, etc. Further, it is not clear that permitting state functions as a basis for processing means that it will be "inconsistent with data principal rights." The remainder of the bill would still apply to this processing.

6. Data Trust Score

The Bill notes that the Authority will register data auditors, who will evaluate data fiduciary compliance with the Act, and who may assign a rating in the form of a data trust score to the data fiduciary pursuant to a data audit conducted under this section.[24]

The Sections reiterate the concerns we raised in our prior submission about the disproportionate impact on smaller data fiduciaries seeking to comply with the Act. Although external and independent auditors may promise transparency and credibility, the Sections note that data principals may realize these benefits only when they interact with larger data fiduciaries, who have the resources to engage a data auditor to annually audit policies and processing. The Sections recommend that the Authority register and properly incentivize data auditors to serve smaller data fiduciaries. Absent such efforts, small data fiduciaries will have difficulty complying with Section 35.1 and the data trust score will only have relevance for larger data fiduciaries.

7. Cross-Border Data Transfers and Data Localization

The Sections commend the Committee of Experts for its detailed and comprehensive analysis in the Report accompanying the Bill. In the Report the Committee notes that there has been an explosion in the globalization of data and acknowledges the challenges with maintaining the flow of data necessary for a "healthy digital economy," while at the same time providing a reasonable level of protection when data is transferred. The Report specifically indicates that "(p)ersonal data that is maintained in India will always have the protection of India's data protection regime. However, national interest would require that at least an adequate level of protection should be accorded to personal data transferred abroad. Given the mobility and seamless transferability of data, a failure to impose such a restriction would

[22] *Id*. CHAPTER III, Section 18(1); CHAPTER IV, Section 19.
[23] *Id*. CHAPTER IV, Section 20.
[24] *Id*. CHAPTER VII, Section 35.

seriously compromise the efficacy of the substantive protections the law provides. It is thus necessary that rules ensuring such adequate protection be implemented."[25]

The Bill currently requires all companies doing business in India to store a copy of all information on a server in India. Moreover, the Bill compels the Indian Central Government to develop categories of critical personal data, which may be processed only in a server or data center in India. Finally, the Bill contemplates standard contractual clauses or intra-group schemes that must be approved by a new data protection authority in order to transfer data and outlines a prescriptive process to ensure compliance.[26]

Despite the assurances provided in the Bill and the Report, the Sections are concerned that the Bill currently includes significant restrictive cross-border data transfer and data localization requirements.

Cross-Border Data Transfers

With regard to cross-border data transfers, we reiterate the Sections' view that the adequacy test does not ensure a smooth flow of information, but rather heightens uncertainty for cross-border data flows. As noted in the initial Indian White Paper only a few countries have been deemed adequate by the EU, excluding most key non-EU markets.[27] The adequacy framework, coupled with proposed EU-styled standard contractual clauses could increase the cost, time and resources associated with doing business

---

[25] *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (Report), http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf, at 83-96.

[26] THE PERSONAL DATA PROTECTION BILL, 2018, CHAPTER VIII

Section 40: Restrictions on Cross-Border Transfer of Personal Data.

(1) Every data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which this Act applies.

(2) The Central Government shall notify categories of personal data as critical personal data that shall only be processed in a server or data centre located in India.

(3) Notwithstanding anything contained in sub-section (1), the Central Government may notify certain categories of personal data as exempt from the requirement under sub-section (1) on the grounds of necessity or strategic interests of the State.

(4) Nothing contained in sub-section (3) shall apply to sensitive personal data.

Section 41. Conditions for Cross-Border Transfer of Personal Data.

(1) Personal data other than those categories of sensitive personal data notified under sub-section (2) of section 40 may be transferred outside the territory of India where—

(a) the transfer is made subject to standard contractual clauses or intra-group schemes that have been approved by the Authority; or

(b) the Central Government, after consultation with the Authority, has prescribed that transfers to a particular country, or to a sector within a country or the Authority approves a particular transfer or set of transfers as permissible due to a situation of necessity; or

(c) the Authority approves a particular transfer or set of transfers as permissible due to a situation of necessity;

(d) in addition to clause (a) or (b) being satisfied, the data principal has consented to such transfer of personal data; or

(e) in addition to clause (a) or (b) being satisfied, the data principal has explicitly consented to such transfer of sensitive personal data, which does not include the categories of sensitive personal data notified under sub-section (2) of section 40.

[27] White Paper at 64.

in India and negatively impact the economy. Supporting the seamless cross-border flow of information will continue to ensure India's presence in the global economy.

Data Localization

In addition, the Sections share a concern, expressed by many stakeholders, regarding the negative impact of data localization laws and rules that limit the storage, movement, or processing of data. The protection of personal data and ensuring data security are often cited as reasons for imposing data localization requirements. The Sections agree that data security and privacy are important objectives, but do not embrace the approach outlined in the Bill.

The Sections reiterate the concerns they expressed in connection with the White Paper in that lowering barriers to data transfers across national borders play a critical role in the development of innovative technologies and digital goods and services, as well as contributing to the growth of the broader economy. Data transfer and related data localization requirements are not necessary for, and are indeed unrelated to, privacy protection or security concerns. As previously noted, they raise barriers to entry for cross-border competitors since the security of data depends on the administrative, physical, and technical safeguards that are put in place to protect the confidentiality, integrity, and availability of the data.

Moreover, mandating localization of personal data as proposed in the Bill may become a trade barrier and create technical difficulties in certain markets. Businesses of all sizes, including Indian startups as well as larger Indian businesses with international operations, may not be able to leverage global cloud platforms and could face barriers to entry as they expand and conduct business in global markets. Data localization also may lead to mirroring of data in multiple jurisdictions. This outcome conflicts with data minimization and may create additional potential sources of data compromises.

The Sections understand that certain critics of the Bill have indicated that it negates the core tenets of cross-border data flows, which made India a global IT hub. There are also reservations regarding passwords and financial data being categorized as sensitive personal data since many Indian companies are managing financial and health data from over 80 countries.

There is tension in many jurisdictions, including the United States, regarding these same matters. It is therefore essential to have a data protection enforcement agency, with flexible authority, coupled with a self-regulation framework to appropriately address data protection issues and to achieve maximum compliance. For example, the FTC is the main U.S. privacy agency, focusing on commercial consumer privacy issues. Although the FTC does not enforce laws that govern cross-border data flows, Section 5 of the FTC Act provides the FTC with the authority to investigate and prevent abuses of personal data as an issue of consumer protection and substantive data protection (under its authority to investigate "unfair and deceptive acts or practices").[28] The FTC also serves as the backstop enforcement authority for the Privacy Shield Framework,[29] which provides a transparent method for companies to transfer personal data to the United States from the European Union (EU) consistent with EU law, and the APEC Cross-Border Privacy Rules System, which facilitates data transfers among participating APEC economies.[30]

---

[28] The FTC also has certain other data protection authority. For example, it enforces the Children's Online Privacy Protection Act.

[29] *See* Federal Trade Commission, The EU-U.S. Privacy Shield Framework, *available at* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield.

[30] *See* APEC Cross Border Privacy Rules (CBPR) System, *available at* http://www.cbprs.org.

The FTC has undertaken enforcement actions and international cooperation against numerous companies for violating Section 5 of the FTC Act and other legislation.[31]

The Sections would recommend dropping the cross-border data transfers and data localization restrictions from the Bill in order to encourage and facilitate cross-border data flows. This would provide the Bill with a more flexible framework, which could evolve over time to take account of technological developments, increased global data flows, and the interests of global entities considering doing business in India.

8. Cybersecurity & Breach Notification

One of the most important issues in legislating data breach notification is the benchmark for when a data breach should be reported, either to regulators or data subjects. The draft bill avoids creating a specific standard in this regard, however, and instead leaves this critical issue to be determined by the newly formed DPA.[32] Although this approach is superior to the GDPR's arbitrary and unrealistic standard of requiring notification within 72 hours,[33] relying on a future administrative determination for such an essential part of the law is inappropriate. We recommend that the draft bill be amended to state a standard for when notification is appropriate.

As the Sections noted in their comments to MeitY earlier this year, we recommend that the draft provide that notification of significant data breaches be made "without unreasonable delay."[34] This more flexible standard gives data fiduciaries the time to properly investigate the incident before expending limited government resources on incomplete or inaccurate assessments of the situation. This approach has proved effective in the United States, which has had data breach notification laws at the state level, and for certain types of data also at the federal level, for more than a decade. This approach prevents data fiduciaries from imposing unreasonable delay but permits them to undertake an appropriate investigation before making a notification that may contain a number of "false positives" and have very little actionable information for regulators and data subjects.

9. Automated Decision Making and Profiling

---

[31] For example, the FTC and international partners from Australia and Canada recently received an award from the International Conference of Data Protection and Privacy Commissions for cooperation on the Ashley Madison data breach. *See* https://www.ftc.gov/news-events/press-releases/2017/09/ftc-earns-prestigious-international-award-ashleymadison om-data.

[32] *Id.*, at 64; Draft Bill, art. 32 § 1.

[33] EU GDPR, art. 33 § 1.

[34] ABA Comments at 2.

In the proposed bill, profiling[35] impacts: (1) jurisdiction,[36] (2) the definition of sensitive personal information,[37] (3) protection of data collected with respect to children,[38] (4) the right to data portability,[39] and (5) performing Data Protection Impact Assessments.[40] With respect to automated decision making[41] the accompanying Report notes the impact of "Big Data" (defined as "processing vast amounts of data at scale to discern patterns of individual behaviour or market trends")[42] on data minimization and purpose limitation[43] and data principal rights.[44] The Committee of Experts expressed their view that the response by the EU to emerging challenges from Big Data and AI -- the right to object to automated decision-making and to access the logic behind it – and the EU's underlying concerns for protection against prejudice and discrimination in output data owing to evaluative determinations without human review, is better achieved through the accountability framework, more specifically, (i) privacy by design, with periodic audits and monitoring by the DPA and (ii) the right of individuals to go to court for breach of fiduciary duties.

The Sections reiterate the concerns they expressed in connection with the White Paper that any mandatory disclosure of such business proprietary information in periodic audits by the Authority or otherwise be subject to the protection of intellectual property rights so as to protect the ability of businesses to innovate and compete. One concern relates to the scope of the disclosures to the Authority under Section 33(3) relating to the Data Protection Impact Assessment. That section provides that "[a] data protection impact assessment shall contain, at a minimum— (a) detailed description of the proposed processing operation, the purpose of processing and the nature of personal data being

---

[35] Chapter I, Section 3(33) "'Profiling' means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interest of a data principal."

[36] Chapter I, Section 2(2) "… the Act shall apply to the processing of personal data by data fiduciaries or data processors not present within the territory of India, only if such processing is … (b) in connection with any activity which involves profiling of data principals within the territory of India."

[37] Chapter IV, Section 22(3): "The Authority may also specify categories of personal data, which require additional safeguards or restrictions where repeated, continuous or systematic collection for the purposes of profiling takes place and, where such categories of personal data have been specified, the Authority may also specify such additional safeguards or restrictions applicable to such processing." See also Chapter XV, Section 108(f).

[38] Chapter V, Section 23(5): "Guardian data fiduciaries shall be barred from profiling, tracking, or behavioural monitoring of, or targeted advertising directed at, children...."

[39] Chapter VI, Section 26: "(1) The data principal shall have the right to— (a) receive the following personal data related to the data principal in a structured, commonly used and machine-readable format—(iii) which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained."

[40] Chapter VII, Section 33(1): "Where the data fiduciary intends to undertake any … large scale profiling … or any other processing which carries a risk of significant harm to data principals, such processing shall not be commenced unless the data fiduciary has undertaken a data protection impact assessment in accordance with the provisions of this section."

[41] Chapter I, Section 3(7) "Automated means" means any equipment capable of operating automatically in response to instructions given for the purpose of processing data."

[42] Report at 54: "This is made possible by algorithms that enable machines to process at scale, learn from such processing, remember their learnings to gain intelligence and analyse such learnings constantly to generate useful, results. These results are then used to more precisely target products, services, interventions to audiences now identified as receptive. Needless to say, such results are probabilistic though their widespread use in the digital economy perhaps suggests that they are more often right than wrong."

[43] Report at 54-58.

[44] Report at 74-75.

processed."[45] This may require the disclosure of business proprietary information. Specifically, would the required description of:

- the "proposed processing operation" result in the public disclosure of the logic behind automated decisions or any other intellectual property information; and
- "the purpose" result in the public disclosure of business proprietary marketing plans including proposed new products and services? This would also have competition law impact as competing businesses inadvertently signal future marketing plans.

The same concern would be present with respect to audit reports of "privacy by design" measures audited under Section 35(b) that must be filed with the Authority under Section 60(h).

10. Right to be Forgotten: Privacy Regulation and Freedom of Expression

In its Report, the Committee rightly notes the inherent tension between privacy and free speech rights.[46] This is a debate that has not been resolved under U.S. law, although the U.S. Supreme Court's opinion in *Sorrell v. IMS Health, Inc.*[47] is instructive in this regard. That case originated in a challenge to a Vermont statute that sought to deny IMS Health access to prescribing physician data, which IMS Health used, in part, to create analyses that allowed pharmaceutical companies to engage in more targeted and data-driven marketing activities. The Vermont legislature believed that these marketing activities were causing the price of healthcare to rise as more physicians switched from using generic drugs to higher cost branded alternatives. The clear statutory intent was to deny marketers the ability to make data-based arguments in favor of higher cost branded drugs, thereby bringing down the cost of healthcare.

Writing for the majority, Justice Kennedy opined that the statute violated the U.S. Constitution's First Amendment right to free speech, since the statute prohibited only the marketers' speech and not that of other speakers: "The State has burdened a form of protected expression that it found too persuasive. At the same time, that the State has left unburdened those speakers whose messages are in accord with its own views. This the State cannot do."[48] The Court's holding was therefore a straightforward application of U.S. free speech law: the sale of prescribing physician data was protected by the First Amendment; the statute restricted only the sale of that data for marketing purposes while preserving the right to sell that data for other (*e.g.*, research) uses; therefore, the statute created content-based and viewpoint-based restrictions on expression. Under U.S. law, that is presumptively unconstitutional and would survive only if the state could show a "compelling interest" that could not be achieved with a less restrictive means. Vermont could not do so; indeed, the Court reasoned that there were several less restrictive market-based alternatives.[49]

The Court could have stopped there, and *Sorrell* would have little relevance to the broader question of whether free speech rights prevent broad privacy-based protections of the use of personal data. But it

[45] Section 33(4) requires the submission of the data protection impact assessment to the Authority "in such manner as may be specified."
[46] Report at 9, 78-79.
[47] 131 S. Ct. 2653 (2011).
[48] *Sorrell*, 131 S. Ct. at 2672.
[49] *Id.* at 2669-70 (noting that doctors could simply decline to meet with marketers, post "no solicitation" signs, or otherwise instruct their receptionists not to make appointment with representatives of pharmaceutical companies).

did not: the Court specifically held that the "creation and dissemination of information are speech within the meaning of the First Amendment."[50] The Court continued, "[f]acts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes."[51] The Court then framed the key issue thusly: "The state asks for an exception to the rule that information is speech"[52] before concluding that the question itself was irrelevant in that case because of the content-based restriction in what was, in the end, a clumsily-worded statute. But the Court's point was clear: under U.S. law, the default position is that data is speech. Accordingly, any regulation of the dissemination of data must pass heightened scrutiny by a showing of a compelling state interest and the lack of viable, less restrictive alternatives.

The Sections commend the Committee for advocating a balancing test. As we noted in our comments on the White Paper, "a principle-based approach would provide a vehicle for balancing individuals' interest in limiting permanent use of their data with the legitimate needs of those to whom they provided their data in the first place." In the U.S., as noted in *Sorrell*, our law favors the disclosure of information over any restriction of it. For example, while newspapers may incur liability for the publication of salacious personal information, the truthfulness of that information is an absolute defense against such claims, even if the information published serves little to no broader societal purpose. Artificial restrictions on the dissemination of data will inevitably produce error costs. Taking the Vermont statute that was at issue in *Sorrell*, while it is likely true that marketing activities resulted in higher healthcare costs, it is also true that, in some cases, improved prescribing practices would save lives. The Sections thus note that while broad-based restrictions on the dissemination of personal data may be laudable in theory, they are not free from error costs that may manifest in regulation (*e.g.,* stunted innovation).

11. The Broad Authority Delegated to the Regulator

Like the GDPR, the draft bill creates a new national data protection authority (the "DPA"). Markedly unlike the GDPR, however, the draft bill empowers the DPA to make legislative determinations that are truly the province of the legislature rather than of a newly created privacy regulator. Here, we outline a number of legislative determinations that are committed by the DPA by the draft bill and suggest in each case that the draft bill be amended to provide that these essential determinations be made by the legislation itself rather than a new and untested administrative agency.

Determination of "Reasonable Purpose" for Lawful Processing. A determination of whether processing data is lawful is arguably one of the core purposes of any data protection legislation. Here, however, the DPA is empowered to identify particular types of processing that satisfy the "reasonable purpose" provision for determining whether data processing is being undertaken for a lawful purpose.[53] Accordingly, unless the DPA determines that a given type of processing qualifies as a "reasonable purpose," data fiduciaries cannot rely on this basis for processing. The draft bill does provide guidance to the regulator, in that requiring that the DPA consider (1) the interest of the data fiduciary in processing, (2) whether the data fiduciary can reasonably be expected to obtain consent, (3) any public

[50] *Id.* at 2667 ("[I]f the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct.") (citations omitted).

[51] *Id.*

[52] *Id.*

[53] Committee Report at 118 (explaining that "any freely constituted residuary ground would be too capacious.").

interest in processing, (4) the effect of the processing on the rights of the data principal, and (5) the reasonable expectations of the data principal.[54] But even within these rather broad parameters, it is extraordinary to delegate such an essential legislative determination to a regulator.

This approach is at variance from the GDPR, which provides that data controllers—not the DPA—should engage in a multi-factor balancing test to determine whether the "legitimate interests" ground is available, with the statute defining the factors that must be considered. The GDPR requires data controllers to document that "legitimate interests" analysis; as a result, European DPAs can perform ex-post reviews to ensure that data controllers do not adopt overly-expansive interpretations of the "legitimate interests" ground. This approach has the benefit of requiring that legislatively determined factors be considered, and that determinations of "legitimate interest" are tailored to the facts of the situation rather than to assumptions of a regulator.

New Categories of Sensitive Data. Under the draft bill, the DPA would be responsible for identifying new categories of sensitive data.[55] One consequence of this approach is that data fiduciaries will not be able to predict which types of data may be classified as sensitive in the future. Given that the Committee's proposal calls for significantly more onerous processing restrictions on sensitive data, this uncertainty may deter companies from processing the data of Indian citizens.[56] Businesses and entrepreneurs would be better served by a procedural approach that ensures that the categories of data that qualify as sensitive are as consistent and predictable as possible.

"Significant" Data Fiduciary Determinations. The DPA has discretion to determine if an entity should be classified as a "significant data fiduciary," which carries added responsibility and higher penalties. Significant data fiduciaries will be notified by the Authority of their classification and must register with the Authority.[57] Additionally, *only* significant data fiduciaries are required to complete Data Protection Impact Assessment, adhere to record-keeping requirements, conduct data audits, and appoint data protection officers, unless the Authority makes an exception.[58] Leaving this essential determination to a newly formed administrative agency means that regulated entities will have no means to determine their regulatory status before investing significantly in India. On the other hand, all entities considering entering the Indian market must assume that they may be later determined to be "significant," because there are no statutory definitions or other indicia of reliability that can assure them to the contrary. the Sections respectfully submit that the legislature, rather than an agency, should determine a definition for this important category of regulated entities.

12. Accountability: Penalties

The Sections are concerned that the civil and criminal penalties in the Bill may be disproportionate and excessively punitive. Such penalties could deter legitimate data processing activities in India that would bring valuable societal benefits.

The Report states that civil monetary penalties should "make it unprofitable for data fiduciaries to be engaging in the wrongful act in the future and . . . proportional to the harm suffered by the data principal." However, the imposition of penalties of up to four percent of total worldwide turnover in the preceding financial year (which may include the worldwide turnover of group companies) often will be

[54] Draft Bill, art. 17.
[55] Draft Bill, art. 22 §1.
[56] *See, e.g.,* Draft Bill, Ch. IV.
[57] *Id.*, art. 38 § 2.
[58] *Id.*, § 3.

disproportionate to the revenue earned from data processing activities or to the harm suffered by individuals, even for major infractions of the law. For example, unlike competition law violations, which by their very nature increase revenue for the company and cause financial harm to individuals, data protection law infringements do not necessarily benefit the data fiduciary or cause material harm to individuals. The Sections therefore recommend that the Committee reduce the amount of civil monetary penalties under the Bill.

The Sections commend the Committee for requiring that Adjudicating Officers consider various factors when imposing civil monetary penalties. Similar to the GDPR, this approach provides assurances that civil monetary penalties will not be excessive. However, the factors listed in the Bill are narrower in some respects than the GDPR. The Sections therefore recommend that the Committee amend the Bill to require that the Adjudicating Officer consider the following additional factors when imposing civil monetary penalties:

- the degree of responsibility of the data fiduciary or data processor taking into account technical and organisational measures implemented by them;

- the degree of cooperation with the Data Protection Authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

- the categories of personal data affected by the infringement;

- the manner in which the infringement became known to the Data Protection Authority, in particular whether, and if so to what extent, the data fiduciary or data processor notified the infringement; and

- where measures have previously been ordered against the data fiduciary or data processor concerned with regard to the same subject matter, compliance with those measures.

With respect to criminal offenses and penalties, the Sections are concerned that criminal penalties may be applied too broadly. For example, infringements that result in "significant harm to a data principal" may constitute a criminal offense if committed knowingly, intentionally, or recklessly, but the Bill does not define the circumstances under which such "significant harm" may occur. The Sections recommend that the Bill be amended to narrowly circumscribe and specifically define potential infringements that constitute criminal offenses.

The Bill also extends liability for criminal offenses committed by a company to "persons in-charge" or, in some cases, to directors, managers, secretaries, or other officers. Although the Sections understand the Committee's desire to hold responsible parties accountable, the Sections nevertheless believe that extending criminal liability to individual employees or officers will deter individuals acting in good faith from engaging in data processing activities on behalf of the company. Accordingly, the Sections recommend that the Committee remove individual criminal liability for corporate offenses from the Bill.

IV. Conclusion

The Sections appreciate the opportunity to comment on the Personal Data Protection Bill, 2018. If the Sections can clarify any of the matters discussed herein or answer any questions, we would be pleased to do so.