Centre for Information Policy Leadership
Hunton Andrews Kurth

26 September 2018

# Centre for Information Policy Leadership

# Comments on the Indian Ministry of Electronics and Information Technology's Draft Data Protection Bill 2018

Centre for Information Policy Leadership
Hunton Andrews Kurth

26 September 2018

## Introduction

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to submit comments to the Indian Ministry of Electronics and Information Technology on its Draft Personal Data Protection Bill 2018 (Draft Bill or Draft).

CIPL commends the drafters for developing a Draft that addresses a wide array of key protections that must be included in a modern-day data protection law. We also support the government's intention to develop a law for the data-driven economy that enables effective privacy protections and at the same time ensures India's economic competitiveness in the fourth industrial revolution. In this regard, our comments should be viewed as suggestions for further improvement of the text of the Draft.

As a general point, for global organisations that operate and/or process data in India, it would be most important to align the Draft Bill as much as possible with existing global privacy laws and standards. In addition to ensuring such alignment, building and improving upon existing models to devise more effective solutions to the challenges of the modern digital economy should be a key consideration in finalising the Draft Bill.

We recommend that India look to not only the EU General Data Protection Regulation (GDPR),[2] but also privacy regimes in other jurisdictions and regions (including the APEC region) in ensuring such alignment. This will allow it to draw only what is best from each of them and maximise its ability to interoperate with all of these regimes, based on the most appropriate provisions of all of them, thus enabling the free flow of personal data and effective privacy protections.

In this regard, we support the drafters' recognition and inclusion of several key data privacy concepts and best practices in the Draft. In particular, we welcome the Draft Bill's recognition of the need to protect personal data as an essential facet of information privacy while still ensuring progress and innovation in the digital economy. CIPL also commends the inclusion of concepts such as data protection principles, a variety of grounds for processing personal data, the distinction between data fiduciaries and data processors, the inclusion of transparency and accountability and the ability to take personal data outside the scope of the law through anonymisation. On the other hand, CIPL believes that the Draft would benefit from several clarifications and modifications in certain areas, as outlined in more detail below.

---

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 65 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this paper should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

CIPL endorses the establishment of a single and effective national data protection authority (DPA) in the Draft Bill. However, the Bill appears to grant the DPA an unusually high number of responsibilities, powers and tasks, many of which might be better placed either upon the legislature or on regulated organisations, subject to DPA oversight (e.g. the ability to define new categories of sensitive data, to specify the types of activities for the reasonable purposes processing ground, to define the standard for anonymisation, to specify instances where data protection impact assessments are mandatory, to decide when a data breach should be notified to individuals, etc.). For the sake of an efficient, effective, predictable and not overly bureaucratic data protection system, we would advise against any unnecessary overextension of the DPA's responsibilities, powers and tasks. CIPL notes various instances of such overbroad powers and responsibilities throughout this comment.[3] Where the law ultimately does provide for DPA discretion to modify or add to the requirements of this law, any changes or additions should be subject to public notice and consultation processes to ensure regulatory predictability for both organisations and individuals. Providing the DPA with such discretion must be carefully thought through by the legislature and it must carefully consider the best approach to ensuring a principles-based law that still provides for flexibility and remains future-proof.

Finally, CIPL recommends including a risk-based approach in a number of the Draft Bill's provisions, such as in the provisions on accountability, privacy by design and notification of data breaches, as further explained in this comment.

We hope that our recommendations below will assist the drafters in finalising the Draft in a way that fully realises its promise. In that connection, we commend the drafters for initiating a consultation process on the Draft Bill and would suggest that a second round of consultations might be appropriate on a revised version of the Draft before its enactment.

**Summary of CIPL Key Recommendations**

1. **Extraterritorial Scope**: The law's extraterritorial jurisdiction should only extend to data fiduciaries located outside of India that specifically direct their services to and purposefully collect personal data of Indian residents (see pages 5-7).

2. **Anonymisation**: The definition should be revised to reflect the more realistic standard of reasonable anonymisation coupled with legal and administrative safeguards and the need to re-identify data in certain circumstances for the benefit of individuals (see pages 7-9).

[3] In that connection, we urge you to consider CIPL's 2017 white paper "Regulating for Results – Strategies and Priorities for Leadership and Engagement", 10 October 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement__2_.pdf, which sets out a framework for maximising the effectiveness of a DPA through prioritising its various roles and activities within these roles, constructive engagement with industry to improve compliance, and leveraging accountability schemes with third party, non-DPA, front-line oversight, such as certifications and codes of conduct (e.g. APEC Cross-Border Privacy Rules (CBPR) and similar accountability schemes).

3. **Notice**: Notice requirements should be set out in the law rather than left to DPA discretion. Data fiduciaries should only be required to provide individuals with information on categories of their data sharing partners (rather than each one individually) and joint data fiduciaries should be able to give notice on behalf of each other where appropriate (see pages 10-11).

4. **Accountability and the Risk-based Approach**: Specific reference to the risk-based approach to compliance should be included as part of the accountability provision and throughout the law where appropriate (e.g. in section 29 on Privacy by Design). Such an approach will also enable the transfer of many of the current DPA responsibilities to organisations with an opportunity for *ex post* review and enforcement by the DPA (see pages 11-13).

5. **Legal Basis for Processing**: Consent is too dominant and narrowly defined. A separate ground of contractual necessity should be included in the law and the scope of the reasonable purposes ground revised in line with the concept of legitimate interest in other global privacy laws (see pages 13-19).

6. **Sensitive Personal Data**: The category of "sensitive personal data" should be dropped. Instead, a risk-based approach to privacy protection that requires organisations to subject all their processing activities to a risk analysis and establish appropriate mitigations and controls should be adopted to provide more contextual, targeted and appropriate protections (see pages 20-22).

7. **Children's Data**: The age threshold for children should be amended to 13 years in line with other data protection laws and a risk-based test to determine whether a service is directed at a child should be developed together with industry to avoid a situation where every site or service must age-verify its users (see pages 22-24).

8. **Right of Confirmation and Access**: The right should only apply to current data being processed at the time the data principal makes the request and limits should be placed on the right of access for requests that are excessive or vexatious (see pages 24-25).

9. **Right to Data Portability**: The law should make clear that data generated in the course of provision of services or use of goods by the data fiduciary does not include "inferred" or "derived" data. Data processed on the basis of the "reasonable purposes" ground should be excluded from the right to data portability (see pages 25-26).

10. **Right to Be Forgotten**: The law should permit the DPA to create detailed guidelines to guide the adjudicating officer in making decisions on right to be forgotten cases to ensure that the power to restrict information distribution is used sparingly to avoid any undue concealment of legitimately available public information while still permitting the right to be exercised by individuals in appropriate cases (see pages 26-27).

11. **Personal Data Breach**: Notification to the DPA should occur "without undue delay" after the data fiduciary has awareness and sufficient information about the nature of the breach. Notification to data principals should be a decision of the data fiduciary (rather than the DPA) if the breach is likely to result in a high risk or significant harm to individuals (see pages 29-30).

12. **Data Protection Impact Assessment**: Section 33 should set forth "likely high risk" as the relevant standard for a DPIA requirement and list broad, non-exclusive example criteria or high risk factors for when a DPIA is required. DPIAs should be subject to *ex post* review by the DPA on request rather than submitted to the DPA upfront (see pages 30-32).

13. **Record-keeping**: Section 34(2) should be deleted. The precise manner of forms of records should not be left to the DPA but rather to the data fiduciary to devise its own appropriate form of record-keeping (see page 32).

14. **Data Audits**: Requiring mandatory annual audits by an independent auditor is excessive, burdensome, costly and unnecessary. The law should provide for a more targeted approach to audits and use them in response to a specific violation or in connection with an investigation or enforcement action or response to such actions upon DPA request or order (see pages 32-33).

15. **Data Protection Officers**: There should be no specific location requirement for the DPO. At most, the law should follow the GDPR model of requiring a legal representative of the data fiduciary in India (see pages 33-34).

16. **Significant Data Fiduciaries**: This concept should be removed from the law. Requirements for DPIAs, record-keeping, data audits and appointment of the DPO should be laid out in their respective sections. The requirement for such data fiduciaries to register with the DPA should also be removed with an emphasis on organisational accountability instead (see pages 34-35).

17. **Data Localisation**: Requirements around data localisation should be reconsidered as they do not serve to improve data protection and will severely disrupt the operations of data fiduciaries and processors and negatively impact India's data economy (see pages 35-38).

18. **Cross-border Transfer Mechanisms**: Organisations should be able to adapt and tailor their contracts to the specific context of a transfer rather than be forced to use non-modifiable standard contractual clauses. The scope of application for intra-group schemes should mirror that of the APEC CBRP and section 41 should, in general, be designed with interoperability with the CBPR system in mind. Consent should be framed as a separate basis for transfer rather than an additional requirement to use other transfer schemes. The law should include other key transfer derogations recognised by other privacy laws (see pages 39-43).

19. **Codes of Practice**: Section 61 should be broadened to also include privacy seals, marks and certifications. The law should also provide that companies may submit codes for approval by the DPA (see page 44).

20. **Timeline for Adoption**: The timeline for the law to enter into effect should be at least 3 years from the enactment date or preferably 3 years from 12 months after the notified date as organisations will have a clearer picture in regards to the requirements created by the DPA as laid out in its codes of practice (see pages 46-48).

**Comments**

The below comments are ordered by reference to the Chapters of the Draft Bill and the numbered headings correspond to the relevant section within the Draft Bill.

**Chapter I — Preliminary**

*2. Application of the Act to Processing of Personal Data*

Given that data processing is inherently global and that India is a primary hub for data processing and IT services, CIPL welcomes the inclusion of a specific provision on the Draft Bill's territorial scope. However, CIPL recommends this provision be further revised and refined in relation to the following points below.

Section 2(1)(a) notes that the Act applies to the "processing of personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India" and section 2(1)(b) notes that the Act applies to the "processing of personal data by the State, any Indian company, any Indian citizen or any person or body of persons incorporated or created under Indian law".

This wide scope and cumulative application of both provisions may lead to conflict of laws with other countries' data privacy laws. It could extend to cases where Indian processors process data on behalf of foreign clients. In such cases, the Indian processors must be able to meet the requirements of the relevant foreign law that applies to the data at the point of collection. For example, if an Indian processor processes data on behalf of a Belgian data fiduciary, the Indian processor must be able to apply the relevant Belgian law to such data, since as a data processor it is under an obligation to act under the instructions of the data fiduciary that is subject to Belgian law — not Indian law. If Indian law applied instead of Belgian law, and Indian law were in conflict with some of the Belgian law provisions, the data processor would be in breach of its contractual obligations with its client in Belgium.[4] However, as currently drafted, section 2(1)(a) suggests that since such data is processed in the territory of India, that Indian law would apply. Similarly, section 2(1)(b) refers to data processed by "any Indian company", and Indian data processors (including subsidiaries of non-India based companies or of purely Indian companies) would fall under this category.

CIPL recommends that this point be clarified in section 2 of the Draft Bill. This is in line with section 37(3) of the Draft Bill (processing by entities other than data fiduciaries) which states that the "data processor…shall only process personal data in accordance with the instructions of the data fiduciary…" and section 104 which provides the Central Government with the power to exempt certain data processors from the application of the Act. Otherwise, the data processor industry in India will be severely impacted as data fiduciaries may be unable to

[4] In practice, the effects of complying with the foreign law may be limited, depending on the privacy law of the foreign jurisdiction. There may be significant overlap in legal requirements between jurisdictions so that in many cases there may not be any conflicts, but there may also be significant differences. Thus, conflict of laws are possible and the Draft Bill should clarify such situations.

ensure that their data processors in India comply with the relevant foreign law to the standard to which they are required.

In addition, in the context of data localisation,[5] a situation could arise where a data fiduciary allows employees in its Indian operations to remotely access, view or edit an offshore dataset. This situation may arise frequently as groups of companies often use global systems and applications that are accessible, used and maintained globally, including in India. Such access, viewing or editing would be considered "processing" and as such may (1) bring the offshore dataset within the scope of Indian law and (2) require a copy of the dataset to be stored in India or, in the case of critical data, subject it to the requirement to only process the data in India. CIPL recommends that the Draft Bill make clear that such remote access by employees of a global organisation's Indian operations does not bring the offshore data within the scope of Indian law.

CIPL recognises that section 104 allows the Central Government to exempt certain data processors from the law with regard to data principals not within the territory of India. However, this provision continues to provide for a large amount of discretion and uncertainty, which may stifle the business process outsourcing industry in India. For instance, data processors often process personal data of principals that are both in and out of the territory of India and segregation of data is not always technically possible.

As a possible way forward, CIPL would like to mention the Philippines Data Privacy Act[6] which relieves a processor located in the Philippines of complying with parts of the Philippines Data Privacy Act and the Implementing Rules and Regulations[7] in relation to data collected outside of the Philippines, where the foreign controller collected the data in compliance with the laws of their jurisdiction.[8]

With respect to the extraterritorial reach of the Draft Bill, section 2(2) currently states that the Act applies to the processing of personal data by data fiduciaries or data processors outside of India if such processing is in connection with any business carried on in India, any systematic activity of offering goods or services to data principals in India, or any activity involving profiling of principals in India.

---

[5] See discussion below on page 35 for CIPL's recommendations in respect of data localisation.
[6] Republic Act 10173 — Data Privacy Act of 2012, available at https://www.privacy.gov.ph/data-privacy-act/.
[7] Implementing Rules and Regulations of the Data Privacy Act of 2012, available at https://www.privacy.gov.ph/implementing-rules-and-regulations-of-republic-act-no-10173-known-as-the-data-privacy-act-of-2012/.
[8] *Supra* note 6 at Section 4 — "This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to the immediately succeeding paragraph: Provided, That the requirements of Section 5 are complied with. This Act does not apply to the following: […] g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines".

This raises the following potential issues:

- By making the Act applicable to data fiduciaries or data processors located outside of India if the processing is "in connection with any business carried on in India", foreign data fiduciaries or data processors could become subject to the Act solely by virtue of their contracting with a separate business that, unbeknownst to them, outsources work or otherwise transfers their data to a data processor in India.

- For example, where a Japanese bank contracts with a Japanese IT service provider and the IT service provider outsources the service to India, such relationship between the Japanese bank and the Japanese IT service provider is made in connection with business carried on in India. This could lead to the Japanese bank being subjected to Indian law by virtue of the relationship with the Japanese IT service provider. This would raise significant concerns among global organisations about having their data potentially transferred to India in all their business relationships. CIPL recommends that this provision be deleted or, at the very least, narrowed to clarify this situation.

- Conversely, the broad reach of the Draft Bill risks hampering innovation and growth for domestic companies and may impede their ability to operate internationally. Reluctance from foreign, multinational data fiduciaries to do business in India will not only impact their own operations but will ultimately reduce the level of business in India for domestic companies, particularly with respect to processing, outsourcing and other IT services.

CIPL recommends that this section be refined to reduce the wide scope of the Draft Bill's applicability, keeping in mind the issues above that may arise with an overly expansive territorial scope. CIPL recognises that provisions of any data protection law on jurisdiction are complex, especially in light of different roles of data fiduciaries and data processors and must be thought through carefully and in detail, with the help of real case scenarios. In CIPL's view, the law's extraterritorial jurisdiction should extend only to those data fiduciaries located outside of India that specifically direct their services to Indian residents and purposefully collect personal data of Indian residents.

*3.* *<u>Definitions</u>*

(3) Anonymisation

The importance of anonymisation of personal data as a tool to exclude such data from this law to enable a broad range of beneficial uses, such as big data analytics for purposes of scientific research and product improvement and development, cannot be overstated. The Draft Bill clearly recognises that fact in section 2(3) by providing that "…the Act shall not apply to processing of anonymised data".

However, section 3(3) defines anonymisation as the "irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, meeting the standards specified by the Authority". This definition is problematic for the following reasons:

- "Irreversible" is a very high standard to meet as nothing is completely irreversible. Data should be excluded from the scope of this law when data principals are not identified, having regard to all means reasonably likely to be used, by the data fiduciary or any other person, to identify the data principal. This more realistic standard provides an incentive for organisations to anonymise data using measures appropriate to the risk of identification, which can be assessed through appropriate risk assessment processes for a specific context. When this is coupled with procedural, administrative and legal protections against de-anonymisation (see discussion below), data principals are effectively protected; and

- The standard for anonymisation should not be left solely to the DPA. Instead, any standards specified by the DPA should be viewed as guidance that organisations may follow. Organisations should also have the ability and responsibility to identify different or additional anonymisation measures that are appropriate for their specific contexts, subject to being able to justify their decisions. This type of shared responsibility for setting reasonable and effective standards would improve the likelihood that personal data are effectively protected and would avoid the legal uncertainty that would result if the standard were left only to the discretion of the DPA.

Therefore, CIPL recommends that:

- The definition of anonymisation be revised to reflect that anonymisation is a process of transforming or converting personal data to a form in which a data principal cannot be identified having regard to all methods reasonably likely to be used by the data fiduciary or any other person to identify the data subject. The (non-exclusive) standard for anonymisation should be laid out in the law or in guidelines developed by the DPA following a public consultation process to allow for relevant stakeholder input;

- In addition, the standard for anonymisation could also be provided by, or informed by, standards developed by independent standardisation bodies, such as the ISO, rather than left to the discretion of the DPA;

- The Draft Bill incorporate procedural, administrative and legal protections, such as internal accountability measures and a commitment of organisations not to re-identify data, enforceable contractual commitments with third parties not to re-identify anonymised data, as well as legal prohibitions on unauthorised re-identification by any third party. This will ensure that all anonymised data may be recognised as such and excluded under the law;[9]

[9] For a discussion of this approach, see "Protecting Consumer Privacy in an Era of Rapid Change — Recommendations for Business and Policymakers", US Federal Trade Commission, March 2012, available at

- The law should provide for reasonable standards or allowances for re-identification where appropriate. Anonymised data sometimes must be re-identified to provide the benefits derived from the insights gained by analysing anonymised data to individuals. For example, a fitness device could provide a certain insight regarding a detected health condition to a user or the data fiduciary may need to send an alert to a certain user to improve their daily habits based on such insights. This is another reason to supplement technical anonymisation measures with procedural, administrative and legal measures.[10]

(21) Harm

The definition of "harm" is overly broad and lacks any limiting criteria. For example, it includes "discriminatory treatment", which could effectively bar any form of targeted advertising. The wide ambit of "harm" could also result in contraventions under the Draft Bill which are not otherwise punishable under other laws dealing with the same issues. Further, including "any denial or withdrawal of service, benefit or good resulting from an evaluative decision" would risk application of this concept to any such denial or withdrawal regardless of its impact, materiality or significance. Thus, we suggest including limiting criteria in the definition that indicate the need for an appropriate level of materiality of the harm at issue. For example, under the GDPR's provision on automated decision-making (Article 22), the effect of a covered automated decision must produce "legal effects" or be "similarly significant".

**Chapter II — Data Protection Obligations**

*4. Fair and Reasonable Processing*

Section 4 requires that any person processing personal data owes a duty to the data principal to process such personal data in a "fair and reasonable manner that respects the privacy of the data principal". While the incorporation of such a principle is commendable, the requirement for demonstration of compliance with an inherently subjective and ambiguous standard ("fair and reasonable") without corresponding guidance for interpretation of this standard by a data fiduciary is problematic. Without more, this would likely leave the provision open to contradictory interpretations and expose organisations to business risks and uncertainty in an enforcement context. The Draft Bill should, therefore, provide that compliance with this principle is deemed satisfied when a data fiduciary adheres to the requirements of organisational accountability as further explained in this comment below, conducts appropriate risk assessments with respect to its processing activities and implements effective mitigations

https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; and "Anonymization and Risk", Ira Rubinstein and Woodrow Hartzog, September 2015, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2646185.

[10] Such an approach has already been adopted in other jurisdictions. For example, the Japanese privacy law uses a combination of anonymisation techniques and bans unnecessary re-identification in its provisions regarding anonymisation.

based on such risk assessments, and/or complies with approved codes of practice (and similar schemes addressed below).

*5. Purpose Limitation*

Section 5(2) provides that personal data shall be processed only for purposes specified or for any other incidental purpose that the data principal would "reasonably expect" the personal data to be used for. Burdening the data fiduciary with a subjective interpretation of what might constitute the "reasonable expectation" of a data principal could result in widespread misinterpretation of such expectations as well as undermine the ability to demonstrate compliance. We would therefore recommend that Section 5(2) be amended to allow processing "only for purposes specified or for other purposes compatible with the specified purpose" (and consistent with the grounds for processing provided in sections 12-17). The law should also provide for criteria for determining compatibility, such as any link between the specified purpose and the further purpose, the context of the collection of the data, the nature of the data, the possible consequences of the processing to the data principal and the existence of appropriate safeguards (see Article 6(4) GDPR). An additional consideration in determining compatibility should be whether the further processing conflicts with or undermines the specified purpose, which, if it did, would most clearly indicate incompatibility.

*8. Notice*

Section 8(1)(g) requires the data fiduciary to provide the data principal with information on the individuals or entities, including other data fiduciaries or data processors, with whom the principal's personal data may be shared, if applicable. Not only is there no discernible benefit to providing such detailed information to data principals, it is almost impossible to provide and maintain such detailed information on third party recipients in a privacy notice, as data fiduciaries' suppliers, other business partners and data recipients change regularly. Modifying a privacy notice is generally quite burdensome and, in the case of global companies, requires a need to address all countries in which they operate. In order not to unduly burden companies and to make this provision more manageable and useful to data principals, CIPL recommends that this should be changed to information about the categories of individuals or third party entities with whom the data may be shared.

Where data is not collected directly from an individual, section 8(1) notes that the data fiduciary shall provide the data principal with the information listed in section 8 "as soon as is reasonably practicable". The law should clarify that there may be instances where it may never be reasonably practicable to provide such information to data principals. For example, in situations where the data fiduciary has no direct relationship with the data principal[11] and providing notice would be impossible or involve disproportionate efforts.

[11] An example of where a data fiduciary may not have a relationship with a data principal is when a nomination is made in favour of a third party (for example, where a life insurance policy-holder designates a beneficiary who does not have a relationship with the data fiduciary). In such cases, the details of the third party are collected

Moreover, in the situation of joint data fiduciaries, it should be possible for one data fiduciary to give notices on behalf of the other where appropriate, given that not all data fiduciaries have a direct relationship with the data principal. Also, even if the data is collected directly from the data principal, it may not always be appropriate to provide all information at the time of collection, for example, where a customer is on a support hotline where one would not expect individuals to wait on the line for a recording of a notice to be played. Section 8 of the Draft Bill should more clearly address the method and timing in these types of situations.

In addition, section 8(1)(n) requires the data fiduciary to provide the data principal with any other information as may be specified by the Authority. Again, changes to data privacy notices require comprehensive changes through a complex process, especially in the case of multinationals where such changes have to be global. CIPL recommends that the notice requirements be laid out in the Draft Bill and not left to the discretion of the DPA.

Moreover, having "stable" privacy notices that do not need to be constantly adapted to new changes enables better predictability and understanding by data principals, which is in line with the obligation in the Draft Bill to provide information in a clear manner (see discussion below).

Finally, section 8(2) requires the data fiduciary to provide the information as required under this section to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person and in multiple languages where necessary and practicable. This raises the question of how necessity on multiple languages is determined and may require further clarification generally.

*11. Accountability*

CIPL welcomes the inclusion of accountability as a requirement in the Draft Bill in section 11. We suggest the addition of a specific reference to the risk-based approach to compliance, either in this section or elsewhere. An example can be found in Article 24(1) of the GDPR.[12]

Essentially, this approach enables organisations to modulate or calibrate their specific compliance measures to the specific nature and risks of their processing. The underlying concept of this risk-based approach is that organisations should always assess and understand the risks of all of their processing activities within their specific purposes and contexts. This would provide for a more effective, efficient and targeted deployment of compliance resources, and benefit both individuals and organisations. As explained in CIPL's previous work on the role of risk management in data protection and privacy risk frameworks, modern data protection

without notice or consent (e.g. bank accounts, insurance policies, financial securities, postal deliveries, secondary/add-on users of a service).

[12] See Article 24(1) GDPR ("Taking into account the nature, scope and purposes of processing as well as the risks of varying likelihood and severity...the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation").

laws should formally enable and incorporate this approach as foundational to any effective data governance and compliance.[13]

Further we recommend clarification of section 11(2). The current wording that the data fiduciary must be "able to demonstrate that any processing undertaken...on its behalf is in accordance with the provision of this Act" is unduly broad. When having data processors work on their behalf, data fiduciaries are going to be limited in terms of what they are able to demonstrate by way of what their processors are doing. The language in this section should accurately reflect these limits. Demonstrating that processing by their data processors is at all times in accordance with this law is an impossible task. It would require constant and continuous audits of all processors, which could be in the hundreds. Instead, the type of demonstration of accountability required by this section should be that processors have provided sufficient guarantees that they are capable of complying with their relevant obligations imposed by this law and by the data fiduciary. This can also be achieved by relying on certifications, codes of practice or other accountability frameworks in which processors participate, such as BCR for processors or the APEC Privacy Recognition for Processors (PRP),[14] and this should be specifically made clear in the final law.

Finally, we urge consideration of two recent CIPL white papers on the issue of Accountability.[15] The first of the two papers explains, among other things, the essential elements of

[13] See CIPL's white papers on Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, 21 December 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf; A Risk-based Approach to Privacy: Improving Effectiveness in Practice, 19 June 2014, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf; The Role of Risk Management in Data Protection, 23 November 2014, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf; Protecting Privacy in a World of Big Data, The Role of Risk Management, 16 February 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf; and Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679," 19 May 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_wp29s_guidelines_on_dpias_and_likely_high_risk_19_may_2017-c.pdf.

[14] *Infra* note 40.

[15] See CIPL papers on "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society", 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; and "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability", 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf.

accountability and how they can be implemented and demonstrated by organisations. The second paper addresses how DPAs and policy- and law-makers can specifically incentivise organisational accountability beyond the incentive that comes from having to comply with legal requirements.

The essential elements of organisational accountability — leadership and oversight, risk assessment and DPIAs, policies and procedures, transparency, training and awareness, monitoring and verification, and response and enforcement — directly correspond to the requirements of most data protection laws, including the Draft Bill. For the sake of global harmonisation, consistency and interoperability, it is important that there be broad consensus and a common understanding of the concept of accountability and how it should be deployed. For example, one of the features and advantages of accountability is that it places an *ex ante* burden to protect individuals on the organisation (by implementing measures that correspond to all elements of accountability and/or the corresponding legal requirements), subject to *ex post* enforcement by the DPA. Throughout our comments herein, we have pointed to examples where a proper application of the concept of accountability would improve the effectiveness and efficiency of India's data protection regime by reducing the *ex ante* tasks and administrative burdens of the DPA (such as authorising, approving, specifying or notifying various items) and leaving these issues to the accountability obligations of the data fiduciaries, subject to *ex post* enforcement. In addition, when implemented correctly, organisational accountability enables an effective data protection framework that reduces the burden on individuals to protect themselves in the complex digital economy (see, for example, the discussion on consent below).

**Chapter III — Grounds for Processing of Personal Data**

*12. Processing of Personal Data on the Basis of Consent*

While consent is an important ground for processing data, it is not appropriate for all data processing in the modern information age, where data processing is ubiquitous and persistent in all aspects of people's digital lives. An effective and comprehensive data protection law should include a range of different processing grounds which data fiduciaries can select from depending on the specific data processing context. While the Draft Bill does provide for a variety of different processing grounds, the majority of them are tailored for specific situations and this will lead to most data fiduciaries having no choice but to rely on consent for the processing of personal data. For example, processing of personal data for functions of the State, for compliance with law or court order, for prompt action (i.e. medical emergencies and disasters) and employment purposes all relate to very specific data processing scenarios. Processing of data for reasonable purposes could be very promising but at present is limited to purposes specified by the DPA.

Given the growing complexity and sheer volume of personal data processing, obtaining valid and informed consent is becoming increasingly challenging for organisations as well as burdensome for individuals. Reliance on consent for the majority of processing operations is problematic for several reasons:

- **High standard for valid consent**: The Draft Bill sets out similar requirements for valid consent as the GDPR[16] (i.e. the Draft Bill notes that consent must be free; informed; specific; clear, having regard to whether it is indicated through an affirmative action; capable of being withdrawn; and not conditional on the performance of a contract). This is a very high standard to meet and not appropriate or possible for all processing operations.

- **Overreliance on consent undermines its quality and creates consent fatigue**: Overreliance on consent will undermine the quality of consents that are obtained and may unduly burden individuals and lead to consent fatigue. There may be many instances where individuals simply will no longer be willing or able to keep providing consents in the face of a deluge of requests for consent generated from all the different data users in the digital economy, even where they might not actually have an objection to the processing. This will undermine legitimate and harmless data uses for no good reason.

- **No direct interaction with individuals**: Consent is not appropriate in contexts where individuals do not have a relationship with the organisation that may process their data. For instance, in the context of business-to-business products and services, AI and machine learning services or in an ecosystem of mobile devices and the Internet of Things (IoT). One example would be the provision of location based services (LBS) through the detection of wireless access points (e.g. Wi-Fi routers and cell towers) and comparing those access points to data stored on individual mobile devices. LBS provide significant value to individuals and are a key feature of many products and services today. Maintaining an up-to-date list of locations of Wi-Fi routers is a continuous process, however, because such routers are frequently added or removed from the Internet. Companies collect this information through a variety of sources including from individual smartphones as they move about the environment. However, this is only possible through the legitimate interest processing ground as the companies that collect such information often do not have a direct relationship with the owner of the Wi-Fi access point, making it impractical and unfeasible to obtain their consent.

- **Volume of processed data and common data uses**: Where large and repeated volumes of data are processed or where the use of data is common, expected or trivial or the privacy risk to the individual is limited, seeking consent at every instance may not be feasible or beneficial.

- **No ability to seek consent or seeking consent would be counterproductive**: There may be instances where the data fiduciary does not have the ability to seek consent from the data principal or where seeking such consent would be counterproductive (e.g. processing to prevent fraud or crime or to ensure information and network security).

[16] See Article 7 GDPR.

- **No genuine choice for the data principal**: Consent is not meaningful in instances where there is no genuine choice on the part of the individual. Additionally, some processing operations are so complex that the individual cannot practically be provided with the necessary information to make meaningful and genuine choices.

- **Management of physical notice and consent forms**: The potential burdensomeness of notice and consent is exacerbated in the context of physical, paper-based forms, which we understand are widespread and common in India. It is unclear how such volumes of physical forms can be realistically managed and recorded without tremendous pressures on available resources. The Draft Bill makes no provisions for this.

Moreover, even in cases where consent is appropriate and effective, it is important to consider the nature of consent that is appropriate in a given context. For example, the Data Protection Committee Report (the Committee Report) that accompanies the Draft Bill[17] acknowledges that consent is not a one-size-fits-all solution to privacy, correctly observing that different types of data processing need to be governed by different standards — noting that "implied consent may be sufficient" to process personal data in limited circumstances. However, the Draft Bill only allows for the indication of implied consent through affirmative action (section 12(2)(d)). An example of such affirmative action would be where a user proceeds with filling out a free-text field to fill out a profile as a necessary step to proceed with a service, thereby implicitly indicating through affirmative action that he or she wishes to proceed with the service. We believe the Draft Bill should make clear that implied consent also must include — and would be just as valid — clear and informed inaction, such as that enabled by opt-out mechanisms, whereby a data principal would be given the clear choice to opt-out of a certain processing of his or her personal data. This is a widely used form of indicating agreement with data processing around the world and should be enabled in India as well. There are many circumstances where this method, when combined with clear information to individuals, provides an efficient way to proceed with legitimate and common processing activities without burdening the data principal with unnecessary affirmative tasks that would only exacerbate general consent fatigue and without placing unnecessary and costly administrative burdens on organisations.

While CIPL believes that consent has an important role to play in circumstances where it can be effective, the situations described above demonstrate that it is not an appropriate ground for processing in all cases. Therefore, other processing grounds, which place greater responsibility on organisations to demonstrate accountability in ensuring the protection of personal data and safeguarding the interests of individuals, sometimes can be more suitable than consent. Equally, the other concepts and requirements of a data protection law have the objective of ensuring individuals are empowered and protected in relation to their data, rather than

[17] See A Free and Fair Digital Economy — Protecting Privacy, Empowering Indians, Indian Ministry of Electronics and Information Technology Committee of Experts on Data Protection under the Chairmanship of Justice B N Srikrishna, Former Judge, Supreme Court of India, July 2018, available at http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf at page 37.

achieving this solely by consent (e.g. compliance with data protection obligations, rights of individuals, transparency requirements, accountability requirements, risk assessments, etc.).

Therefore, given the limitations of the other processing grounds in the Draft Bill as outlined above, CIPL recommends the Draft Bill be amended, particularly with respect to the reasonable purposes ground as discussed below.

*Contractual Necessity*

Additionally, CIPL strongly recommends that the Draft Bill provide for a separate ground of contractual necessity and that such scenarios are not bundled into the consent ground as described by the Committee Report.[18] The Committee Report notes that "where a data principal consents to a contract that requires personal data processing, such consent would have to meet the heightened standard under data protection law".[19] This would effectively require every contractual arrangement and transaction to be accompanied by a separate consent. This could lead to companies having to manage a huge number of additional consents to the already high number that they must otherwise deal with. Furthermore, individuals may enter into multiple contracts or transactions daily and over burdening them with consent requests can lead to consent fatigue. In addition, providing a different standard for contractual necessity in India may create problems for global companies that operate and offer their goods and services both in India and elsewhere. The Committee Report itself even highlights several problems with this proposed approach[20] and CIPL urges the legislature to revisit this topic and add the contractual necessity ground into the Draft Bill as a standalone processing ground and to design it with interoperability in mind to avoid differing standards globally.

*17. Processing of Data for Reasonable Purposes*

Many organisations rely on other available grounds to collect and process data when consent is not appropriate. The processing ground of legitimate interest, which is incorporated in multiple global data privacy laws, has proven vital to enabling data fiduciaries and processors to collect and process data while ensuring organisational accountability and respecting data protection rights of individuals. CIPL has previously written on the importance of including a legitimate interest-type ground for processing personal data in data protection laws designed for the modern information age[21] and has specifically collected real examples of the current and common uses of the legitimate interest ground for processing among leading global organisations.

As mentioned, other jurisdictions have recognised the value of the legitimate interest processing ground. For example, it is included in the GDPR as one of the six legal bases for

[18] *Id*. at page 42.
[19] *Id.*
[20] *Id*. at pages 40-42.
[21] See CIPL White Paper on Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR, 19 May 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf.

processing,[22] none of which are privileged over the other. In addition, Brazil's recently approved comprehensive data protection law includes the legitimate interest ground.[23] Furthermore, the Singapore Personal Data Protection Commission (PDPC) sought feedback on legitimate interest under the "legal or business purpose" processing ground in July 2017 as part of its review of the Singapore Personal Data Protection Act (PDPA). The PDPC said that, based on the feedback it received, it intends to adopt this concept under the term "legitimate interest".[24]

The "reasonable purposes" ground in the Draft Bill appears similar to the legitimate interest ground but there are some concerning differences:

- **Residuary rather than equal ground**: The Committee Report describes the reasonable purposes ground as a residuary ground for processing activities rather than an equal ground.[25] This forces data fiduciaries to primarily rely on consent and the other narrow processing grounds which can be problematic for the reasons outlined above.

- **Limited to purposes identified by the DPA**: The reasonable purposes ground for processing is limited to specific purposes to be identified by the DPA relating to very narrow types of activities (e.g. fraud prevention, whistle-blowing, mergers and acquisitions, network and information security, credit scoring, recovery of debt and processing of publicly available data). Such activities do not take into account processing necessary in other contexts such as AI and machine learning applications where consent is not appropriate or practicable. Indeed, in the Committee Report, the Committee states that relying on consent may hinder the evolution of new technologies relying on data analytics, which may hold significant benefits.[26]

The Committee Report raises a concern that the "existence [of the legitimate interest ground] as a standalone ground for processing appears to be designed to provide latitude to data fiduciaries, without entirely securing the rights of data principals. This may be remedied under the Indian data protection law by circumscribing the ambit of the provision". Moreover, it places the requirement to conduct the balancing test on the DPA rather than on the data fiduciary as is customary in other jurisdictions.

This concern is unfounded. In so far as the legitimate interest ground for processing requires a risk assessment and balancing of interests implicated in the involved processing, it is an element of, and supports, a data fiduciary's accountability under the data protection law. In

[22] See Article 6(1)(f) GDPR.
[23] See Article 7(IX) of Lei Geral de Proteção de Dados Pessoais, available at http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.
[24] See "Response to feedback on the public consultation on approaches to managing personal data in the digital economy", available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/PDPC-Response-to-Feedback-for-Public-Consultation-on-Approaches-to-Managing-Personal-Data-in-the-Dig.pdf at page 8.
[25] *Supra* note 17 at page 117.
[26] *Id*.

many instances, the legitimate interest ground is a more rigorous and effective tool for protecting individuals than other grounds, including consent. The balancing test under legitimate interest requires a context-specific risk/benefit assessment and implementation of potential mitigations as part of organisational accountability. The data fiduciary must also be able to demonstrate that they have carried out this balancing test by documenting the risk-analysis and being able to justify to a regulator or relevant third party the outcome and any decision to proceed with the processing operation, or face enforcement and sanctions.

Typically, such risk/benefit assessments involve:

- Identifying the specific adverse impacts on individuals and potential risks and harms of the proposed processing;

- Assessing the desired benefits of the processing to the business and/or society;

- Balancing and weighing the involved risks, benefits and competing interests;

- Implementing context-specific mitigations and safeguards that minimise the risks as much as possible without undermining the desired benefits; and

- At the end of this process, making a defensible judgment call as to whether to proceed with the processing in light of the benefits and residual risks after mitigation. Where a processing operation poses a high risk, is particularly intrusive or is harmful to an individual's privacy and such risks cannot be mitigated against, legitimate interest may not be appropriate and seeking consent may be the only option.

Such a detailed risk-analysis and balancing exercise clearly intends to secure the privacy rights of individuals while still enabling important data processing operations to take place where consent is not appropriate and practicable.

CIPL recommends the following with respect to the Draft Bill's reasonable purposes processing ground:

- The reasonable purposes ground should be considered to be an equal ground with consent and not a residuary ground. All processing grounds should be placed on equal footing and data fiduciaries should be able to select the ground which is most appropriate for a specific processing operation. Consent should not be the default processing ground and is unlikely to be suitable for many modern-day processing operations.

- The reasonable purposes ground should not be limited to a rigid list of processing activities determined by the DPA (nor should the processing of sensitive personal data be excluded from this ground for processing (see discussion below)). As demonstrated in CIPL's paper on "Examples of Legitimate Interest Grounds for Processing of Personal

Data",[27] there are likely to be a growing number of situations in which organisations need to collect, use or disclose personal data without consent for a legitimate purpose apart from those authorised by the DPA. It is essential that data protection law stays future-proof and provides organisations with the ability to process data responsibly in the context of evolving technology and in a way that does not create risks to individuals. Of course, examples of reasonable purposes are welcomed and the DPA can spell out which types of processing activities may fall under this ground, but this should not be exclusive. Moreover, the DPA should not be put in a position of constantly having to update and add to the list of "reasonable purposes". This would undermine one of the key features and benefits of this ground for processing — the efficient, risk-based and context-specific assessment of what is a reasonable (or legitimate) purpose — and replace it with a potentially lengthy bureaucratic process. The essence of this processing ground is that it must be future-proof, adaptable to new processing operations and evolving technologies and industry practices by virtue of its risk-based approach that allows the data fiduciary to precisely assess and deal with the specific risks at hand regardless of the nature of the technology or business practice. Such a balancing test by the data fiduciary ensures data privacy rights and protections for individuals.

- In the Draft Bill, the "reasonable purposes" ground is applicable only for the processing of personal data under Chapter III, and not for the processing of sensitive personal data. To the extent that the concept of "sensitive personal data" is retained in the final law (which we do not recommend — see discussion below), this ground should additionally be included as a separate ground for processing of sensitive personal data under Chapter IV of the Draft Bill.

- The "reasonable purposes" ground should be renamed to "legitimate interest". In a globalised data protection environment, where interoperability between privacy regimes and cross-border transfer mechanisms becomes increasingly important,[28] using similar terminology for similar concepts makes creating such interoperability easier. In addition, many companies operate on a global scale and having different terminology for the same concepts will be unduly disruptive to business operations and commercial data negotiations (e.g. if a foreign party is not familiar with the term reasonable purposes but is familiar with the concept of legitimate interest). Also, having consistent terminology and concepts is ultimately helpful to individuals, who are increasingly mobile and access global services and products.

[27] CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data, 27 April 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_27_april_2017.pdf.

[28] See the ongoing efforts on creating interoperability between APEC CBPR and EU transfer mechanisms.

**Chapter IV — Grounds for Processing of Sensitive Personal Data**

*3. Definitions (See Chapter I – Preliminary)*

(35) Sensitive Personal Data

CIPL does not recommend establishing a category of pre-identified "sensitive data", as sensitivity of processing and data is very much context driven. Instead, we recommend a risk-based approach to privacy protection that requires organisations to subject all their processing activities to a risk analysis and requires them to establish mitigations and controls appropriate to the risks involved. This does not mean that the law cannot include examples of what kinds of personal data might be particularly sensitive but such examples should be treated as guidelines to take into account when conducting a context-specific risk assessment rather than as automatic and invariable triggers of heightened requirements or limitations on the use of such data. However, to the extent that the Indian legislature decides to include such a category in its law, CIPL has some concerns around the Draft Bill's definition of sensitive personal data.

The definition currently includes "passwords", "official identifiers" and "financial data" as types of sensitive data. Such types of data are all regularly processed by data fiduciaries and processors and including them in the definition would hinder many common data operations that include the processing of such data. For example, workplaces often process financial data for payroll and salary purposes. Financial data is further processed in contexts such as fraud prevention and credit scoring. The Committee Report even notes in relation to these activities (which are included under the reasonable purposes processing ground) that resorting to consent in such situations, as a ground for processing, may prove burdensome and may raise concerns of consent fatigue among data principals. Moreover, financial information is already heavily regulated and protected by industry specific laws. Furthermore, including "passwords" within the definition would mean that a separate consent would be required from an individual every time he or she creates a password. This would make it impossible for companies offering password manager products to operate and risks depriving individuals in India of a tool expressly designed to provide better security online and stronger passwords to better protect their personal data.

CIPL recommends narrowing the definition of sensitive data (if this concept is retained at all) by removing "passwords", "official identifiers", "financial data" and "caste or tribe" from the definition and by specifying that "biometric data" is included in so far as the processing is for the purpose of authenticating the identity of a natural person. As to "caste or tribe", many Indian surnames indicate caste or tribe but names of individuals cannot realistically be treated as sensitive personal data. In addition, the available grounds to process sensitive data should be widened to include the ground of "reasonable purposes" and a separate specific ground for "employment purposes".

Also, the definition is open-ended as it includes "any other category of data specified by the Authority under section 22". Sensitive data (if the concept is used at all) should be clearly defined through a law making procedure and not subject to additional definitions. The inclusion

of an open-ended ability to specify additional categories of sensitive data will create legal uncertainty and lead to unrealistic expectations on data fiduciaries to stop processing existing data that is subsequently deemed to be sensitive and to seek consent from data principals. Additionally, given that the norms for processing are far more restrictive and the penalties for non-compliance far higher on processing of sensitive personal data, the open-ended nature of the definition poses an unjustifiably high and unpredictable compliance cost. However, to the extent the Authority is given the ability to add to the categories of sensitive data, the law should provide for a public consultation process to allow for proper notice and stakeholder input.

*18. Processing of Sensitive Personal Data Based on Explicit Consent*

Processing of sensitive personal data should not be limited to explicit consent. It should be permitted on all the other available processing grounds, including "reasonable purposes" (or "legitimate interest"). Indeed, the risk/benefit assessment inherent in the legitimate interest ground for processing is uniquely suited to ensure the appropriate level of protection for any given level of sensitivity of personal data. In addition, the processing of sensitive personal data (if the concept is retained) should be permitted in the following circumstances:

- Where the context of the processing does not raise a risk of significant harm (e.g. for employment purposes, such as registering a new employee for company health insurance coverage);

- Where such processing is necessary for the performance of a contract (e.g. employment or insurance);

- Where appropriate safeguards for the security and privacy of the information are in place;

- Where the data principal is adequately informed about the collection and use of the sensitive data prior to sharing the data and has legitimate options to refrain from sharing the data;

- Where adequate de-identification, subject to sufficient technical and organisational measures preventing re-identification, is employed;

- Where processing is performed in the context of identifying, supporting and addressing diversity and inclusion within organisations; or

- Where processing in the context of customer and vendor checks is performed, including processing financial data to ensure firms meet Know Your Customer (KYC) requirements and performing risk intelligence assessments on potential vendors and partners to ensure they comply with anti-bribery obligations, laws on modern slavery, counterfeiting laws, etc.

Given the broad definition of sensitive data, the limited grounds available for processing is troubling. Processing sensitive data on the basis of explicit consent, for certain functions of the State, in compliance with law or court order or for prompt action is too narrow to support all of the common and essential data processing operations around sensitive data that take place today. Furthermore, restrictions on the processing of sensitive data could potentially provide less protection to individuals in certain circumstances. For example, many AI and machine learning applications have the potential to avoid many of the irrational biases that infect human decision-making and make detecting bias and errors easier and more reliable through the processing of extensive data, including sensitive data. Denying access to or preventing retention of sensitive data will only make it harder to detect and remedy bias while also denying all segments of society the full potential of AI benefits.

*22. Further Categories of Sensitive Personal Data*

In addition to the DPA's ability to specify further categories of sensitive data (see discussion on the definition of sensitive data above), section 22 also provides that the DPA may specify categories of personal data, which require additional safeguards or restrictions where repeated, continuous or systematic collection for the purposes of profiling takes place. The power to define further categories of sensitive data in this regard will create real uncertainty for local businesses, as well as for foreign companies to invest in India, especially in new technologies based on data processing and analytics, such as AI and machine learning. Nevertheless, to the extent the Indian legislature intends to provide the DPA with discretion to define such new categories of sensitive personal data, the Draft Bill should impose consultation obligations on the DPA to seek feedback from industry and government on any proposed changes.

**Chapter V —Personal and Sensitive Personal Data of Children**

*3. Definitions (See Chapter I – Preliminary)*

(9) Child

The definition of a "child" in the Draft Bill is "a data principal below the age of eighteen years". CIPL believes that age 18 is too high, and recommends that the age be amended to 13 years to align with both US practice under COPPA,[29] the recently enacted Brazilian privacy law and the 10 EU Member States that selected age 13 for the age of digital consent under Article 8 of the GDPR.[30] As outlined in CIPL's white paper on GDPR Implementation in Respect of Children's Data and Consent,[31] having multiple diverging age ranges for children in international data protection law is highly problematic. By selecting an age of 13, India will ensure that its data

[29] 15 USC § 6501 ("The term 'child' means an individual under the age of 13").
[30] See GDPR: Updated State of Play of the Age of Consent across the EU, Ingrida Milkaite and Eva Lievens, Ghent University, 28 June 2018, available at https://www.betterinternetforkids.eu/en_US/web/portal/practice/awareness/detail?articleId=3017751.
[31] CIPL White Paper on GDPR Implementation in Respect of Children's Data and Consent, 6 March 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf.

protection law aligns with the most common international age threshold for children's data in data protection law.

It is also pertinent to note that while the definition of a child as a person below 18 years has been retained in the Draft Bill in deference to the age of consent for contract as per the Indian Contract Act, 1872 read with the Indian Majority Act, 1875, the Committee has explicitly acknowledged that *"*from the perspective of the full, autonomous development of the child, the age of 18 may appear too high*"*,[32] recognising that mandating 18 years will not be reasonable in light of the varied nature of online activity. This is also in line with the observations of the Delhi High Court in the case of *K.N. Govindacharya v. Union of India* [W.P. (C) 3672/2012] where the Court recognised the general practice of mandating 13 years as the lower (age) limit in the case of social media.

At the same time, CIPL wishes to underline that lowering the age to 13 years does not mean the Government's role in protecting children will be reduced. The Government could play an important role in raising awareness on the safe use of the Internet by providing educational workshops to minors, teachers and parents. The Government could also help private sector efforts by supporting NGOs and others including enterprises that engage in raising awareness among young adults.

*23. Processing of Personal Data and Sensitive Personal Data of Children*

Section 23(2) notes that appropriate mechanisms for age verification and parental consent shall be incorporated by data fiduciaries in order to process personal data of children. CIPL recommends that the following points be considered with respect to this provision:

- Age verification may not be the most effective way to protect the child, given the risk of minors' feeling compelled to circumvent these measures. The mandate to use age verification could result in a perverse incentive that hinders the development of more effective privacy protections. A more reasonable approach would be in-context settings that are easily accessible and easy to use. The mechanism chosen to verify the age of a data principal should involve an assessment of the risk of the proposed processing and should not lead to excessive data processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are or are not a minor.

- It will be important to avoid a system where every site or service, even those not intended for or attractive to children, must age-verify their users. CIPL recommends that data fiduciaries that do not explicitly direct their services at children be exempt from the age verification requirement, and that a risk-based test to determine whether a service is directed at a child (including whether it processes large volumes of children's data and the intent of the data fiduciary to target children) be developed within the framework of the Draft Bill. Such a test should be created in collaboration with industry. Furthermore,

[32] *Supra* note 17 at page 44.

it should be taken into account that given the potentially onerous nature of implementing such solutions, many businesses may — out of abundant caution — choose to stop servicing children or any users suspected to be children under a specific age. This will exclude large parts of the Internet from use by children — including valuable sources of information, learning, and communication.

- As set forth above, CIPL recommends that the threshold age be reduced to 13 years. Alternatively, if the current age threshold is retained, the Draft Bill should implement a sliding scale approach, where parental consent is only required for certain children (e.g. those under the age of 13) but other relevant requirements may still be applicable for data principals between 13 and 18. Requiring parental consent for all data principals under the age of 18 could cut off young adults from crucial Internet or mobile app-based services and is likely to also impact their own data protection and privacy rights. This request for change is in fact supported by the observations of the Committee in its own Report, as well as the recognition of the reality of Internet use by young adults by the Indian Courts.

- The Draft Bill should recognise situations in which children's data will be processed without age verification or parental consent where such processing is necessary to comply with a legal obligation, an order of a court or tribunal or for prompt action, including the need to guard the health or ensure the physical integrity of the child. Moreover, blanket restrictions on online tracking in respect of children such as under section 23(5) could lead to restricted ability to provide relevant information to the data principal, especially in edutech and over-the-top (OTT) services, or could prevent the provision of key services such as fraud prevention in the banking sector through the monitoring and tracking of children's savings accounts and financial activities to prevent and detect suspicious transactions.

**Chapter VI — Data Principal Rights**

*24.* *Right to Confirmation and Access*

Section 24(1)(b) states that the data principal shall have the right to obtain from the data fiduciary "a brief summary of the personal data of the data principal being processed or that has been processed by the data fiduciary". The right to confirmation and access should only apply to current data being processed at the time the request is made by the data principal to the data fiduciary. Retaining data that has previously been processed by the data fiduciary in case a data principal might exercise their right to confirmation and access would be contrary to section 10 on data storage limitation.

Additionally, section 24(1)(c) provides principals with the right to obtain "a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal". Providing for such a right would require all data fiduciaries to maintain metadata on all processing operations at the individual level. Conveying this information in the manner specified in section 24(2) (i.e. in a clear and concise manner that is easily

comprehensible to a reasonable person) would be very costly. Indeed, the relevant information is already provided for in the notice obligations under section 8(1)(a)-(b).

CIPL recommends that access to data under section 24 be limited to data being processed at the time the request is made by the data principal. Obligations under section 24 should cease after the data is deleted by the data fiduciary according to law and its internal policies. Furthermore, a brief summary of the processing activities undertaken by the data fiduciary should be provided in the privacy notice at the general level rather than requiring data fiduciaries to keep a log of all processing activities at the individual level. Additionally, in line with the Committee Report, section 24 should make it expressly clear that the basis of the rights of confirmation and access "is to ensure that the data principal can understand, gauge and verify the lawfulness of processing".[33]

CIPL further recommends that a subsection be added to the provision to clarify the limits on the right of access. In particular, the Draft Bill should make clear that if a data fiduciary considers an access request to be manifestly unfounded, excessive, technically impossible or vexatious, then it should be able to refuse the request or charge a reasonable fee to assist with complying with the request. In cases where the data fiduciary refuses the request, it must be able to (1) demonstrate the manifestly unfounded, excessive or vexatious character of the request and (2) justify its decision.

*26.* *Right to Data Portability*

Section 26(1)(a)(ii) provides that the data principal shall have the right to receive personal data relating to him or her which has been generated in the course of provision of services or use of goods by the data fiduciary in a structured, commonly used and machine-readable format. This provision should clarify that such generated data refers to personal data that is either collected directly from the individual or observed from the activities of data principals as they use the goods or services of the data fiduciary. Observed data includes data generated by the data principal such as his or her search history, location data, traffic data or tracked health information. It does not include, however, "inferred" or "derived" data generated by the data fiduciary on the basis of data provided by or observed from the data principal. The Article 29 Working Party (WP29), in its guidelines on data portability,[34] provides the examples of "the outcome of an assessment regarding the health of a user" and "the profile created in the context of risk management and financial regulations (e.g. to assign a credit score or comply with anti-money laundering rules)" as constituting "inferred" or "derived" data. Applying the data portability right to such data would in most cases hinder the protection of other rights, such as trade secrets or other intellectual property rights, or other commercial interests, such as competitive advantage.

[33] *Supra* note 17 at page 69.
[34] Article 29 Working Party Guidelines on the Right to Data Portability, as last revised and adopted on 5 April 2017, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.

In addition, section 26(1)(a)(iii) provides that the data portability right is available for data which forms part of any profile on the data principal. It should be further clarified that inferred or derived data contained within such profiles is outside the scope of the data portability right.

Moreover, data processed on the basis of the "reasonable purposes" ground should be excluded from the right to data portability. For example, section 17(2)(a) and (d) on the reasonable purposes processing ground notes that the DPA may specify reasonable purposes related to (a) the prevention and detection of any unlawful activity including fraud and (d) network and information security. Enabling the portability of data processed exclusively for such purposes would affect and weaken fraud detection and network security systems.

CIPL recommends that the Draft Bill clarify that data portability only applies to raw data provided by the individual or data observed about the individual through their use of the data fiduciary's goods and services. It does not apply to data inferred or derived from the analysis of data provided by the data principal (either directly or observed).

Finally, it is crucial to ensure the security and reciprocity of portability. That means that data fiduciaries or providers of portability on each side should have strong privacy and security measures, such as encryption in transit, to guard against unauthorised access, diversion of data or other types of fraud. It is also important that a data principal's decision to move data to another provider should not result in any loss of control over that data. It should be noted that to realise such security and reciprocity, it is important to encourage private sector initiatives to develop applicable standards that will provide for greater flexibility than prescribed formats or other relevant rules on portability being defined by public bodies.

*27. Right to Be Forgotten*

Section 27 (1) of the Bill states that the right to be forgotten is a data principal's right to restrict or prevent continuing disclosure of personal data by a data fiduciary under specific circumstances that have to be balanced against criteria listed in section 27(3). These criteria are designed to address other important rights such as free speech and the right to know and other interests of other data principals. In this respect, sections 27(2) and (3) of the Draft Bill provide that the adjudicating officer shall weigh the right to be forgotten against the right to freedom of speech and expression and the right to information of any citizen.

The right to be forgotten is a problematic concept and difficult to implement in practice. In Europe, where the right to be forgotten was first recognised as a right, there are ongoing legal disputes in courts to further define and shape its scope. In all instances, a careful balancing is required to assess the appropriateness of the exercising of this right against the public interest in retaining data, including in accordance with data retention policies and practices. Removing data from active processing should be distinguished from removing data altogether, which may have significant and adverse implications. For example, it is essential for anti-money laundering, anti-terrorism, sanctions screening and credit scoring checks that data is retained. Retaining data is also essential for employers to check CV credentials and for tax authorities to verify employment history. From a societal perspective, it is important that individuals are not able to

"erase" inconvenient truths about themselves, or to play the system to improve their credit score or conceal relevant facts. This is especially important in the context of background checks on individuals working with children or vulnerable adults.

In order to address some of these challenges, CIPL recommends that the law allow the DPA to create detailed guidelines to guide the adjudicating officer in making a decision. This could help ensure that the power to restrict information distribution is used sparingly to avoid any undue concealment of legitimately available public information through the right to be forgotten while still permitting the right to be exercised by individuals in appropriate cases.

*28. General Conditions for the Exercise of Rights in this Chapter*

Section 28(1) states that the exercise of any right under this Chapter, except the right under section 27 (the Right to Be Forgotten), shall only be on the basis of a request made in writing to the data fiduciary. This provision should be less prescriptive. The data principal should be able to make a request to exercise his or her rights in the same manner as he or she provided the data (for instance, via web form). In addition, this provision would preclude self-service modules for data correction or user information portals for access to data which are common methods of exercising individual rights online.

Section 28(3) notes that the DPA may specify a reasonable time period within which the data fiduciary shall comply with the requests under this Chapter. The time period to respond should be provided by law and not subject to change by the DPA at any given time. This ensures consistency and predictability for data fiduciaries who must comply with the requests and data principals in the exercise of their rights. A response period of 30 days, with the possibility of extension in certain circumstances (including challenges preventing an appropriate response in the given timeframe) is a popular model adopted in other data protection laws.

Section 28(4) notes that where any request is refused by the data fiduciary, it shall provide the data principal making the request with adequate reasons for the refusal in writing. The Draft Bill should clarify that "in writing" can include electronic notifications. Traditional paper notifications to individuals would be too cumbersome and unduly burdensome on data fiduciaries.

Section 28(6) provides that the manner of exercise of rights under this Chapter shall be in such form as may be provided by law or in the absence of law, in a reasonable format to be followed by each data fiduciary. CIPL recommends amending this provision to remove the reference to additional law as data fiduciaries should have as much flexibility as possible to design their internal processes for compliance on the basis of accountability.

**Chapter VII — Transparency and Accountability Measures**

*29. Privacy by Design*

CIPL welcomes the inclusion of the concept of privacy by design in the Draft Bill. As a general matter, CIPL wishes to underline that a privacy by design requirement needs to reflect a risk-

based approach to data processing. Thus, it must be calibrated to the likelihood and severity of the risks of harm to the rights and freedoms of individuals. Such risk calibration should take account of the state of the art, cost of implementation and the nature, scope, contexts and purposes of processing.

Section 29(c) states that every data fiduciary shall implement policies and measures to ensure that technology used in the processing of personal data is in accordance with commercially accepted or certified standards. CIPL recommends that this be deleted as such a requirement will impact an organisation's ability to innovate around design standards. As long as the data protection principles and other relevant measures are followed and data principals are appropriately protected, including through privacy by design, then the objectives of the data protection law will be met.

In addition, CIPL recommends that the wording in section 29(g) be revised from "the interest of the data principal is accounted for at every stage of processing of personal data" to "the protection of the rights and freedoms of the data principal is accounted for at every stage of processing of personal data".

*30. Transparency*

Section 30(1)(h) of the Draft Bill notes that the data fiduciary shall take reasonable steps to maintain transparency regarding its general practices related to processing personal data and shall make any other information as may be specified by the DPA available in an easily accessible form. Similar to the discussion of the Notice principle above, modifying a privacy notice, especially for a large multinational corporation, is not an easy endeavour. Leaving transparency requirements to the discretion of the DPA creates undue uncertainty for organisations and could require multiple changes every time the DPA specifies a new requirement. CIPL recommends that such requirements be specified upfront in the Draft Bill.

In addition, in the context of vendor assessments and KYC checks, whether conducted by an organisation engaging directly with an individual or by a third party providing expert services to firms, it is not always possible nor desirable to notify individuals that such processing is taking place. Furthermore, lengthy notice requirements run the risk of creating barriers to innovation and adversely impacting the online experience for customers, particularly for mobile phone services, where screen size and text limitations are key issues. Notices are important, but layered notices and a risk-based approach should be followed to reflect the realities of data being processed.

Moreover, section 30(2) notes that the data fiduciary shall notify the data principal of important operations in the processing of personal data related to the data principal through periodic notification in such manner as may be specified. CIPL recommends deleting this provision as this could potentially create spam, overburden individuals or may be misused by bad actors to create vulnerabilities (such as phishing attacks). This provision is superfluous given the notice requirements, breach notification requirements and the provisions of the Draft Bill on individual rights.

*31. Security Safeguards and 37. Data Processors*

Under an accountability model the data fiduciary is accountable to the data principal for the proper processing of their data. The data fiduciary is in the best position to understand the benefits and risks of their processing activities and provides instructions to the data processor based on their knowledge of the data principals, the personal data that is to be processed and the risks attached to the processing. Often the data processor may not have visibility to the personal data and may not be aware of the particular risks unless informed by the data fiduciary.

The Draft Bill specifically recognises the data processor in a number of ways. First, under section 37, the data fiduciary is required to enter into a valid contract with the data processor. Although this is a normal arrangement, section 37 mandates that the contract contain specific requirements, such as restrictions on sub-processing and treating personal data as confidential. We see no reason for the law to impose these particular requirements on the data processor when these are commercial matters to be resolved between the parties taking into account the risks associated with the processing.

Secondly, section 31 (Security Safeguards) imposes a joint obligation on the data fiduciary and processor to implement "security safeguards". The Draft Bill confuses what should be a clear separation between the responsibilities of data fiduciaries and processors. Consistent with an accountability model, CIPL recommends that this section be modified to impose the primary responsibility for the implementation of security safeguards on the data fiduciary, with the data fiduciary contracting with the data processor for services based upon the data fiduciary's assessment of the nature of the processing (and any associated risks) given its unique understanding of the nature of the personal data within its control.

*32. Personal Data Breach*

The definition of personal data breach (see section 3(30) in Chapter I – Preliminary) should include permanent loss of data that is accessible to unauthorised parties, but not temporary loss of access to data principals. Otherwise, whenever a system is undergoing maintenance or temporarily offline for other reasons, there would be a data breach under the current definition. The definition in the Draft Bill should be clarified to avoid this result.

Section 32(1) requires notification to the DPA of a personal data breach where such breach is "likely to cause harm to any data principal". In turn, under section 32(5) the DPA determines whether the breach has to be notified to the data principal, "taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm".

We recommend that the decision of whether the data principal should be notified be left to the data fiduciary and that the threshold for such notification be more clearly stated as "likely high risk" or "significant harm". This standard is not inconsistent with the current wording (taking into account the severity of the harm), but would be more clear and help avoid over-inclusive notification, as such notification would result in notice fatigue and, over time, diminish the

usefulness of such notices to data principals. It would also avoid the additional burden on the DPA to have to review and determine if a notification to individuals is required in every single data breach, which are likely to be numerous and on a daily basis.

In addition, there should be exceptions to such a notification requirement where the data fiduciary has in place protective measures with respect to the affected data, such as encryption, that make the data unintelligible; or the data fiduciary has taken measures that reduce any "high risks" so they are no longer likely to materialise; or the notification would require a disproportionate effort, in which case an alternative way to notify the breach via public communication or similar methods should be permitted. Finally, placing the burden on the data fiduciary to decide when to notify data principals aligns well with their own interest in promptly giving their data principals the opportunity to limit any harm from a data breach. Of course, the DPA should retain the ability to require such notification where necessary.

Further, section 32(3) requires that the notification to the DPA be "made…as soon as possible and not later than the time period specified by the Authority, following the breach after accounting for any time that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm". As to the timing of the notification to the DPA, we would advise against stating in the law or subsequently through the DPA any specific time (e.g. 72 hours). Rather, it should simply be made clear that the notification should occur "without undue delay" after the data fiduciary has awareness and sufficient information about the nature of the breach, including of its likely impact and general significance. Except for the current language allowing the DPA to specify a time period, the current proposed standard for the timing of the notification ("as soon as possible" and "after accounting for any time that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm") actually captures part of this concept already. However, we would specifically add to that standard the time that may be required to gather sufficient information on what happened and the scope and significance of the breach. The time required for these activities cannot be universally defined in advance and any premature notification may lead to unnecessary and wasteful engagement of the DPA. However, data fiduciaries should be able to defend their timing of notification under an "undue delay" standard.

*33. Data Protection Impact Assessment*

Section 33 provides for data protection impact assessments (DPIA). DPIAs are important tools in data protection to identify and assess the risks of data processing operations and to implement appropriate mitigations and controls in response. Certain clarifications and changes to the current draft section could improve its effectiveness and also obviate the need for section 38 on the classification of "significant data fiduciaries", which we strongly recommend removing (see discussion below).

Section 33(1) would be more clear and effective if it initially set forth "likely high risk" as the relevant standard for a DPIA requirement, and listed broad, non-exclusive example criteria or factors for when such high risk might be present and data fiduciaries must conduct a DPIA (which are already included in the current Draft Bill). This approach would give organisations

the necessary guidance as to when they must comply with this obligation and would be reviewable after the fact by the DPA and subject to enforcement if the organisation failed to comply with the obligation.

As to the specific examples of factors for possible high risk, it should be clarified that the listed factors do not necessarily in and of themselves signify higher risk levels that would automatically warrant a DPIA. For example, merely using a new technology may not increase the risk profile of an organisation or processing operation or, by itself, justify a full-blown DPIA or data audit (if that concept is retained). (Note that the opposite might be the case as well!) In fact, requiring new technologies to undergo a DPIA (and DPA review) before being able to be implemented in India is most likely to have an adverse impact on innovation in India and the progress of technological adoption.

It should be made clear in this section that data fiduciaries must make an individual, case-by-case judgment on whether there is likely high risk and/or if the sample factors, in fact, create a likely high risk in the circumstances at hand, and only if they do, perform a full-blown DPIA. Of course, data fiduciaries must be able to demonstrate and defend their decision-making process in that regard, which they are required to be able to do under the enforceable accountability requirement in this law. This approach to DPIA would be both more inclusive in that it potentially captures more high risk processing than covered by the sample factors alone, and less inclusive in that it enables data fiduciaries to avoid unnecessary DPIAs, and thus improves the cost effectiveness and efficiency of their compliance operations. Indeed, allowing organisations to focus their resources on truly harmful activity ultimately improves privacy and data protection for individuals overall.

The same approach would also obviate the need for specifying circumstances, classes of data fiduciaries, or processing operations where DPIAs are mandatory, as currently envisioned by section 33(2). We do not believe that such categorical "pre-designations" of high risk activities are capable of being consistently accurate or useful, especially if the test in section 33(1) for when to conduct a DPIA is articulated and applied appropriately and accountability measures are properly implemented and enforced.

Section 33(2) also envisions the DPA specifying instances where a "data auditor" must be engaged by the data fiduciary to conduct a DPIA. Again, we do not believe that this mechanism is necessary or useful, if the DPIA standard is properly articulated, applied and enforced against under accountability principles. This process would have the potential of being overly broad by capturing unnecessary audit targets and impose huge potential administrative costs on organisations with no commensurate benefit to data protection. Conducting DPIAs and engaging, where appropriate, internal data privacy experts, DPOs or even internal auditors for the most mature organisations to help in the process, is an important part of organisational accountability and ensures data protection is embedded in the processes and culture of an organisation.

Section 33(3) lists the required minimum elements of a DPIA. An important element that is missing and should be explicitly included is an assessment of the benefits of the processing to

all relevant stakeholders, including individuals, society and the organisation. Any proper risk assessment and tailoring of appropriate mitigations must involve the weighing of the relevant countervailing equities, i.e. a cost/benefit assessment. This is important because any mitigations and controls for the identified risk might also reduce or remove the benefits. Thus, a processing activity with high risk but also high benefits at stake might mandate a different response than a similarly risky activity with only minor benefits. At a minimum, full awareness of the benefits can inform a decision of whether to proceed with the processing, even in light of any residual risk that cannot be avoided. In short, section 33(3) should explicitly acknowledge the relevance of benefit assessment in the context of risk assessment. This is particularly important given an increasing role of data-driven innovation and technology in delivering societal, economic and individual benefits in the fourth industrial revolution.

Finally, section 33(4) would require all DPIAs to be submitted to the DPA. CIPL strongly recommends that this provision be deleted. The purpose of a DPIA should be to force the data fiduciary to undertake a detailed risk assessment and devise appropriate mitigations. Moreover, the DPIA must be in a form that is capable of being produced to and examined by the DPA upon request, such as in an enforcement context, to determine whether the data fiduciary has complied with the law in a demonstrable fashion. This is sufficient to give full effect to the purpose of the DPIA. To require the routine submission of all DPIAs would add tremendous volumes of work and administrative burdens both to the data fiduciaries and to the DPA, potentially paralysing the effectiveness of the Authority. For example, the sheer burden of routinely creating versions of the DPIAs (and some companies conduct hundreds of them) devoid of confidential business information and trade secrets is difficult to overstate. The overall global trend in data protection regulation is to move away from *a priori* reviews and authorisations to accountability and post-facto checks and balances as a result of a complaint, investigation or other incident.

*34.* *Record-Keeping*

Section 34(2) provides that the data fiduciary shall maintain records "in such form as specified by the Authority". CIPL believes that this unnecessarily restricts the flexibility of organisations to devise their own appropriate forms of record-keeping. It also imposes an unreasonable and excessive micro-management obligation on the DPA relating to matters not within its core competence. Instead, records should be kept in a manner that allows them to be produced to the DPA on request, consistent with section 11(2) on accountability. But the precise manner of form of records should be left to the discretion of the data fiduciary. CIPL recommends deleting section 34(2).

*35.* *Data Audits*

Section 35(1) provides that data fiduciaries shall undergo an annual audit with respect to their processing operations by an independent data auditor. We believe that this is an excessive, burdensome, costly and unnecessary measure. It would be more effective to take a more targeted approach to data audits and use them in response to a specific violation or in connection with an investigation and enforcement action, or in response thereto, upon request

or order of the DPA. Indeed, not only the high costs but the practicalities of such audits on a routine basis would have to be considered. Many data fiduciaries have global operations with respect to which constant routine audits by one jurisdiction would be extremely difficult to manage and sustain over the long run. In short, this provision should be amended to reflect a more limited and targeted use of third party data audits. Audits and verifications are an important part of organisational accountability and both data fiduciaries and processors should be conducting these as a matter of their own compliance strategy and privacy management program, as opposed to such audits being required and specified by law.

Further, Section 35(5) and (6) empower a "data auditor" to assign a rating in the form of a "data trust score" to the data fiduciary. However, the evaluation made by a data auditor would necessarily be subjective, leading to inconsistencies in evaluation by different auditors and making the score an unreliable metric of the data fiduciary's actual performance. Thus, to the extent the provision on data audits is retained at all, we recommend that these subsections be deleted, or, in the alternative, that the power to assign data trust scores be vested in a neutral body such as the DPA, upon application by the data fiduciary.

*36. Data Protection Officer*

Section 36(1) relating to the appointment of a data protection officer (DPO) is unclear as to whether the DPO must be located in India. It appears from section 36(4) that the only DPOs who must be based in India are those of data fiduciaries that are not present within India but are engaged in processing to which Indian law applies.

To clear up this ambiguity, CIPL recommends that there be no specific location requirement for the DPO under any circumstance. Requiring an organisation processing personal data that is subject to Indian law outside of India to have a DPO based in India is unreasonable and burdensome. Such a requirement would potentially apply to a large number of organisations with no physical operations in India to appoint DPOs there. If India wanted certain organisations established outside of India but processing Indian personal data to have some kind of representation in India, it might follow the GDPR model of requiring a legal representative[35] of the data fiduciary in India.

Further, specifying the geographical location of a DPO would add additional administrative burdens on organisations without any direct corresponding benefit to individuals' privacy and would create barriers and costs to doing business in India.

Also, with respect to section 36 generally, the DPO responsibilities and tasks described in the Draft Bill can be (and generally are) performed regardless of the physical location of the DPO. Thus, the DPO should be able to be located anywhere in the world, as long as they are able to perform the tasks and duties effectively and with authority. Imposing a residency requirement in India will impose unjustified costs and undermine the ability to appoint the best person available for this role.

[35] See Article 4(17) and 27 GDPR.

Finally, we recommend that section 36 include the criteria for when organisations will have to appoint a DPO. Currently, the need for a DPO depends on the classification of data fiduciaries as "significant" data fiduciaries under section 38, providing, in essence, that only those organisations that are designated to be "significant data fiduciaries" must have a DPO. However, because we recommend removing the concept of "significant data fiduciaries" from this law for the reasons discussed in detail below, we also suggest that the criteria for when to appoint a DPO be moved to the DPO provision. However, we suggest that the criteria be further refined to define more clearly when an organisation, based on its risk profile, is required to appoint a DPO, taking guidance, perhaps, from Article 37 of the GDPR.

*38. Classification of Data Fiduciaries as Significant Data Fiduciaries*

Section 38(1) would give the DPA the power to "notify certain data fiduciaries or classes of data fiduciaries as significant data fiduciaries". It also sets for the relevant factors: volume and sensitivity of personal data processed, turnover, risk of harm, use of new technologies and any other factor relevant in causing harm. Section 38(2) requires significant data fiduciaries to register with the DPA. Further, section 38(3) provides that all or any of the following obligations — DPIA, record-keeping, data audits and DPO — shall apply only to such significant data fiduciaries. Finally, the DPA may require any data fiduciary that is not a significant data fiduciary to nevertheless comply with any or all of these measures if the DPA "is of the view that any processing activity undertaken by such data fiduciary or class of data fiduciaries carries a risk of significant harm to data principals".

We see several problems with this proposed provision.

Firstly, it would likely impose significant administrative and oversight burdens on the DPA, which would have to identify individual, or classes of, significant data fiduciaries in a process that would have to be repeated and re-assessed constantly in the ever-changing environment of digital and data-driven organisations. This would be a task of potentially enormous proportion and complexity, given not only the size of India's economy but also the broad extraterritorial reach of the Draft Bill.

Secondly, the factors identified as relevant to such classification do not necessarily in and of themselves signify higher risk-levels that would warrant the automatic application of the identified obligations. For example, merely using a new technology may not increase the risk profile of an organisation or processing operation or, by itself, justify a full-blown DPIA or data audit (if that concept is retained).

Indeed, the current proposal under section 38 appears to be at once both too broad and too narrow. It would capture organisations whose processing, in fact, does not involve the risk-level that might justify the specified obligations. And it may not capture organisations whose processing is not covered by the factors set forth in the law or by the DPA.

CIPL suggests that the more effective and efficient approach to applying the requirements of DPIAs, record-keeping, data audits (if retained at all) and appointing a DPO would be to address the standard for when they are required within each of their respective sections. Thus, for

example, the section on DPIA would set forth likely high risk as the relevant standard for a DPIA and then set forth broad, non-exclusive, criteria for when such high risk might be present and data fiduciaries must conduct a DPIA (which the current Draft already partially does). This approach would give organisations the necessary guidance as to when they must comply with this obligation and would be reviewable after the fact by the DPA and subject to enforcement if the organisation failed to comply with the obligation in line with the accountability principle as per section 11 of the Draft Bill. Another approach would be to address this through the accountability requirement, which would be risk-based and would include examples of accountability elements, measures and controls expected of organisations that engage in high risk processing.

The additional layer of up-front designation of "significant" data fiduciaries thus seems to add unnecessary complexities to the system, imposing unnecessary pressures on the resources of the DPA, with little or no countervailing benefit to data protection. Indeed, such an approach could cause serious harm to India's ambitions to emerge as a hub of innovation and technology, sending a message that entities which undertake innovation and deploy new technology will be penalised by the imposition of additional compliance requirements. Instead, the proposed framework should aim to incentivise and to facilitate to the maximum extent possible and only intervene where articulated harm to any specific party results.

Thirdly, the registration requirement for significant data fiduciaries is problematic and would serve no purpose that couldn't be achieved through more efficient means. It would impose significant administrative burdens and costs on both organisations and the DPA. Also, it is not clear who and what would be included. Will this registration capture an entire organisation or just the particular processing operation that is captured by a factor for "significant data fiduciary"? What if the majority of an organisation's processing is not captured? Do they have to register? How do organisations unregister?

In addition, most recent and mature data privacy laws, such as the GDPR, have just moved away from registration models that have proved to be inefficient and overly bureaucratic to move to accountability schemes with compliance responsibilities being entirely on the organisation under the *ex post* control of the DPAs.

CIPL strongly recommends against this registration requirement as any discernible value of such a registration seems vastly outweighed by the costs.

**Chapter VIII — Transfer of Personal Data Outside India**

*40. Restrictions on Cross-Border Transfer of Personal Data*

For India to maintain its status as a magnet and destination for global businesses and a centre of technological progress and innovation required in the fourth industrial revolution, it is important that India get the rules on data flows and cross-border transfers right. The free flow of data is a key element of economic growth. This fact has been supported by multiple

studies.[36] Indeed, over the past decade, cross-border data flows have boosted global GDP by 10.1 per cent.[37] As a result, CIPL strongly urges India to reconsider its proposed data localisation provisions.

Data localisation requirements, including the general obligation to store a copy of data in India and to process "critical data" only in India, do not serve to improve data protection, severely disrupt operations of both data fiduciaries and processors and will have a negative impact on India's data economy. For instance:

- In many cases, it is not possible to process all data locally and maintain the same quality of service as could otherwise be achieved (for example, round-the clock, follow-the-sun customer service);

- The trend towards micro-services in service architecture and increasing distribution of data processing means that data localisation restrictions are likely to result in companies choosing not to serve the Indian market or significantly reducing the functionality of their services;

- Data localisation restrictions risk significantly impairing innovation by raising costs to potentially prohibitive levels for small and medium sized enterprises;

- Data localisation restrictions undermine India's ability to leverage emerging technologies that rely significantly on global and distributed networks, like cloud computing, data analytics and AI/machine learning;

- Data localisation requirements create complex conflict of laws situations with other data protection laws globally, especially the GDPR. For example, holding data longer than necessary or using data for different purposes than for which it was originally collected (including for localisation requirement purposes) would likely be a contravention of the GDPR;

- Data localisation is a costly effort that impacts on an organisation's ability to operate with consistency and to invest in focused data security measures. The more fragmented the location of the data, the greater the corresponding risks to the data being compromised, given the additional and unnecessary "touch points"; and

[36] A recent study published by GSMA summarises existing studies regarding the value of data flows. See Annex B of "Regional Privacy Frameworks and Cross-Border Data Flows — How ASEAN and APEC can Protect Data and Drive Innovation", GSMA, September 2018, available at https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf.

[37] See "Digital Globalization: The New Era of Global Flows", James Manika et al., McKinsey Global Institute, March 2016, available at https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx.

- Data localisation obligations may further weaken security by reducing the probability of network redundancy whereas a distributed network is crucial for securing data, making it possible for data to be restored in case of data loss due to natural disasters or cyber-attacks.

Section 40(1) currently provides that a "serving copy" of all personal data be kept in India. Such a localisation requirement would impose significant costs on companies of all sizes operating in India, both foreign and domestic, and is not necessary to ensure privacy protections for such data. On the contrary, the requirement to maintain a serving copy in India would force foreign companies to use or create data storage facilities within India, thereby creating substantial additional security risks and threats of leakage and thus compromising user privacy. This requirement would also lead to a move towards centralisation of data storage, which would be extremely dangerous from the point of view of harm likely to be caused by a potential cyber-attack. Cross-border data flows should be protected, and the appropriate level of privacy protection for personal data flowing across borders ensured, through an "adequacy" finding of a country or international organisation, or a sector within a country, or through technical and legal measures, including contracts and/or accountability-based frameworks such as enforceable corporate rules, codes of practice, codes of conduct and certifications, some of which are already included in the Draft Law. The addition of a mirroring requirement as contained in Section 40(1) is unlikely to serve this purpose. The objective behind the inclusion of this requirement is not clear and may not be proportionate to the burden and risks being imposed. Thus, in situations where personal data flowing across borders is protected through such other means, CIPL strongly recommends removing the concurrent data localisation provision.

CIPL understands that one of the possible reasons for the data localisation requirement in the Draft Bill lies with the need to secure the lawful access to data in cross-border investigations of serious crimes. Given the consequences of data localisation requirements as described above, CIPL suggests that the Indian government encourage bilateral and multilateral instruments to make data sharing work in such instances without resorting to localisation. For example, the CLOUD Act recently enacted by the United States enables bilateral agreements with qualifying countries which would allow non-US qualified governments to get access to data in the context of criminal investigations in a much more efficient way. India should aim for such an agreement to resolve such issues while avoiding the negative economic impact of data localisation. This issue has also been dealt with in trade agreements, such as the recent US-Mexico agreement whereby financial institutions are no longer required to store data locally as long as the relevant authorities are able to access the information they require.[38]

Section 40(2) provides that "[t]he Central government shall notify categories of personal data as critical…that shall only be processed…in India". Other than in very narrow, thoroughly justified and specific cases related to State security, classified information or national defence

[38] See "U.S.-Mexico Trade Pact Aims to Allow Banks to Move Data", Daniel Stoller, Bloomberg Law: Privacy & Data Security, 27 August 2018, available at https://www.bna.com/usmexico-trade-pact-n73014482039/.

related matters, such an extreme localisation measure is not necessary to protect personal data, nor is it necessary to ensure proper access to data by the authorities. Both objectives can be achieved through technical and legal measures that do not impose similar unnecessary costs on efficient economic activity within India. In addition, we are concerned about the opinion expressed in the Committee report that says "[i]t is our considered view that the size and potential of the Indian market trumps the additional cost that some entities may have to bear on account of a mandate to process personal data locally".[39] The "potential" of the Indian market could be hampered by data localisation obligations which will reduce options for Indian companies, especially small and medium-size players that rely on India's current open and free data flow policy to compete with international players that have access to cutting-edge technologies and tools in accessing various markets.

For example, many businesses rely on 24-hour customer service. That requires access to personal data outside of India's time zone. It would not serve India well to force companies to choose between functionality and efficiency on the one hand or establishing or maintaining a business presence in India on the other. Both should be possible. It would also not serve Indian companies well that would like to expand beyond the Indian market or do business with such companies. We understand that for some of our member organisations, the inability, for example, to move health data out of India would likely lead to the elimination or reduction of operations and offerings in India. In addition, it would also stifle international research efforts and prevent advancement in key sectors of the global economy (e.g. international medical research).

We recommend that, save for the very narrow and specific cases mentioned above, the law does not include such special categories of data that can only be processed in India. However, while we are not advocating for or recommending such categories of data, to the extent the Indian legislature does see fit to include such critical categories of personal data, we would recommend (1) that the law itself define such critical personal data, rather than giving the Central Government the ability to identify such categories, and (2) that copies of such data should always be able to be transferred across borders, subject to appropriate technical and legal protections and to the possible above-referenced narrow exceptions relating to State security, classified information or national defence.

Finally, the proposed broad and open-ended authority of the Central Government to "notify categories of personal data as critical personal data" that can only be processed in India will create significant legal uncertainty. Businesses that are considering establishing or maintaining business operations in India will have no way of knowing whether they will be impacted by future notifications in that regard. Thus, at a minimum, the law should explicitly limit this broad authority to extraordinary circumstances and provide for a process for notifying such categories of personal data that is open to public consultation.

[39] *Supra* note 17 at page 94.

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

Section 41 sets forth several conditions or mechanisms for transferring personal data across borders. We recommend several clarifications as well as additions.

- **Standard Contractual Clauses**

First, with respect to standard contractual clauses, section 41(1)(a) of the Draft Law envisions that they be approved by the DPA. We advise against the use of non-modifiable standard clauses and the pre-approval requirement because they are inefficient and undermine the effectiveness of the contracts.

Contractual arrangements between transferors and transferees that establish legal obligations and the conditions under which data processing activities may take place are widely used by organisations globally, both for purposes of controller-to-controller transfers and, even more frequently, controller-to-processor transfers. They are an effective means to ensure that the legal obligations that attach to the data continue to apply as the data moves between countries, thereby ensuring a high level of protection of the data.

Because data flows occur within varying and specific business contexts, parties to a transaction must remain free to use contractual language that suits their specific business needs and information flows while also imposing the appropriate data privacy and security obligations applicable to the data. For example, the needs of businesses in the financial sector, health services sector, insurance sector and advertising sector vary greatly and each sector has unique business and regulatory needs that are best handled by contractual provisions customised to their specific situations and data-handling needs.

Indeed, this context-specific flexibility in contracting is essential. Therefore, we strongly discourage an approach that requires the use of non-modifiable standard contractual clauses for transfer purposes, as, for example, is currently the case under the GDPR. Under that model, businesses are forced to have multiple contracts (one to meet their individual data processing needs and one merely to "tick-the-box" of privacy regulatory compliance), which is inefficient and ultimately does little to improve privacy protections. Rather, organisations should be able to adapt and tailor their contracts to the specific circumstances of the transfers to maximise both efficiency and privacy protections so long as they comply with and implement the relevant data protection requirements and elements in their contracts with third parties. This more flexible approach is evident in the privacy laws of countries such as Australia, Hong Kong and Singapore.

Moreover, for reasons of efficiency and resource management both for organisations and the DPA, regulatory or governmental review and pre-approval of the contracts should not be required. It is sufficient that the data privacy regulators or individuals have the ability to challenge non-compliance with data transfer requirements through appropriate legal processes.

- **Intra-Group Schemes**

Second, as to "intra-group schemes" that have been pre-approved by the DPA (section 41(1)(a)), we recommend that their scope be broadened beyond "intra-group" and that regulatory pre-approval not be required.

The proposed "intra-group schemes" appear to resemble the EU GDPR's Binding Corporate Rules (BCR), and, indeed, they can be a valuable and important transfer mechanism. However, their scope should be broadened to be at least as broad as the EU BCR, but, ideally, should be broadened even further. Moreover, they should not have to be pre-approved by the DPA.

Under the BCR system, groups of corporate affiliates may transfer data to non-EU countries within their corporate group if the group has a set of rules, or BCR, that have been approved by EU data protection authorities. These BCR establish uniform internal rules for transferring personal data across the corporate group based on EU data privacy requirements, and are binding on all relevant entities and personnel in the group. BCR exist both for organisations acting as controllers (data fiduciaries) and as data processors. The GDPR has expanded their potential application from use of BCR only within a corporate group to a group of enterprises "engaged in a joint economic activity". At a minimum, India should recognise the same scope of BCR. Ideally, however, the scope of application for any type of BCR-like scheme should mirror that of the APEC Cross-Border Privacy Rules (CBPR)[40] (see discussion below), which do not have "within-group" or "joint economic activity" limitations. In other words, it should be possible for two BCR companies to share data between themselves, based on the fact that both have BCR and provide for an adequate and high level of privacy protection and a comprehensive privacy program.

To ensure wider uptake and scalability in the future of such schemes, especially for SMEs, any corporate rules system should not require prior approval by a DPA. Instead, such corporate rules could either be self-certified or reviewed by a third party "Accountability Agent", as in the case of the CBPR (see discussion below), as appropriate, and, with respect to government or regulatory oversight, companies that employ such corporate rules should stand ready to demonstrate their compliance on request.

- **Interoperability with APEC Cross-Border Privacy Rules (CBPR)**

Third, section 41 should be designed with an eye on interoperability with the APEC CBPR system developed by the Asia-Pacific Economic Cooperation (APEC) forum. The CBPR are a fast-growing cross-border transfer mechanism for the entire APEC region, which comprises 21 member economies and more than half of the world's population and economy.

[40] See APEC CBPR and PRP system documents, available at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx. The APEC CBPR and PRP have emerged as significant accountability and cross-border transfer frameworks in the Asia-Pacific region (see www.cbprs.org).

The CBPR are an enforceable corporate code of conduct or certification mechanism for intra- and intercompany cross-border data transfers that have been reviewed and certified by an approved third party certification organisation (Accountability Agent). The CBPR's objective is to uphold privacy protections to the standard embodied in the APEC Privacy Framework, a statement of privacy norms endorsed by the APEC forum in 2005.[41] Enforcement of the CBPR is provided by APEC data protection and privacy authorities that have joined the APEC Cross-border Privacy Enforcement Arrangement (CPEA).[42] To date, six APEC economies have joined the system, two more have announced their intent to join in the course of 2018 and several others are preparing to join in the near future. All APEC economies have endorsed the system and stated their intention to join the system at some point. APEC has also developed a corollary system for processors, called the APEC Privacy Recognition for Processors (PRP).

The advantage of this system is that it allows transfers not only within a global corporate group (or within a group of enterprises engaged in "joint economic activity" — such as under the BCR), but also between unaffiliated companies and to companies that are not CBPR-certified anywhere in the world. The CBPR-certified company remains liable for the protection of the information at the level of the originating APEC country and the CBPR, regardless of where or to whom the data is transferred. The CBPR system thus enables data flows among participating economies while assuring personal data is protected. CIPL would like to stress that both data flow and data protection can be achieved simultaneously and that there is no trade-off between cross-border data flow and personal data protection.

We strongly urge India to explicitly include a transfer mechanism modelled on the CBPR in its data protection law to enable such future interoperability between the APEC region and India. Non-APEC countries that adopt similar mechanisms could make their cross-border rules mechanisms interoperable with the CBPR (and other similar schemes) if and so long as there is substantial overlap in the data protection requirements within each system. This will have the effect of creating a global certification mechanism requiring only one approval process. Creating transfer mechanisms with global applicability would be a significant efficiency gain to multinational and global businesses and would also help regulators and, ultimately, benefit individuals. The EU and APEC have taken initial steps to explore and develop interoperability between EU transfer mechanisms (e.g. BCR and future GDPR certifications) and the APEC CBPR. Moreover, it is not inconceivable that the APEC CBPR may at some point be amended to allow participation by non-APEC countries. Thus, India should devise its cross-border transfer mechanisms, certifications and code of conduct schemes (see discussion below) with CBPR in mind.

Indeed, the Draft Law already takes a step in that direction, although in a seemingly roundabout way. Section 61 on Codes of Practice allows the DPA to approve or issue "codes of practice" submitted by various types of industry associations, regulators or government bodies.

[41] See APEC Privacy Framework, available at https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf.
[42] See APEC Cooperation Arrangement for Cross-Border Privacy Enforcement, available at http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf.

These codes of practice may be used, among other things, for "cross-border transfer of personal data pursuant to section 41 of this Act". This mechanism closely resembles that of the APEC CBPR, which can be described both as a code of conduct and as a "certification", participation in which signifies a commitment to adhere to a defined standard of privacy protection as described by the CBPR program requirements. As a result, we recommend that India make that overlap explicit, include the use of codes of practice and certifications as additional transfer mechanisms in section 41 (similar to how the EU has in the GDPR[43]) and, furthermore, add certifications to section 61 (see discussion below).

- **Consent as a Basis for Transfer**

Section 41(1)(d) and (e) require that, in addition to having contractual clauses or intra-group schemes or the transferee country being adequate, the data principal must also consent to the transfer, with respect to both regular personal data and sensitive personal data. However, consent should not be required in addition to such other transfer conditions or mechanisms. It is difficult to see how this would even work in a multitude of situations. For example, a multinational company headquartered outside of India may need to transfer the personal data of its India based employees to the main foreign office location for purposes of performance assessments. In some instances, this may just include enabling the access of personal data of Indian employees to their managers located outside of India. The company may rely on an intra-group scheme to make such a transfer. Given the imbalance of power in the employment context, obtaining the employees' consent on top of transferring the data through the intra-group scheme may not be practical or appropriate. Such a requirement also renders invalid other bases of processing which would be more appropriate. For instance, in this situation, section 16(1)(d) permitting the processing of personal data for any other activity relating to the assessment of the performance of the data principal who is an employee of the data fiduciary would be a more suitable grounds for transfer.

As a result, CIPL believes that, at most, consent should be a standalone condition or derogation for transfers and not cumulative with other derogations or mechanisms. This is the position taken under the GDPR (Article 49 — Derogations for specific situations).

- **Other Conditions for Transfer (Derogations and Exceptions to Data Transfers)**

The proposed data protection law appears to be missing several key transfer conditions that typically are included in other privacy laws as derogations or exceptions to their cross-border transfer restrictions. At a minimum, India should include the following derogations and exceptions in its data protection law:

- the transfer is necessary for the performance of a contract between the data principal and the data fiduciary or between the data fiduciary and a third party and (i) is entered into at the request of the data principal or (ii) is in the interest of the data principal;

[43] See Articles 40-43 GDPR.

- the transfer is for the purpose of legal proceedings, including investigations by regulatory authorities, or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;

- the transfer is necessary to protect the vital interests of the data principal or of other persons;

- the transfer is necessary for a legitimate interest of the data fiduciary or a third party that is not outweighed by the fundamental rights or freedoms of the data principal;

- the data principal has consented to the transfer;

- the transfer is necessary for reasons of public interest;[44] and

- the transfer is made from a public register.

This list is not comprehensive and may include additional grounds, derogations or exceptions. For the sake of global interoperability and harmonisation, we recommend that the list of transfer grounds, derogations or exceptions be as inclusive and comprehensive as possible, taking into account, at a minimum, all grounds, derogations and exceptions that exist in current Indian law as well as comparable laws in other countries.

**Chapter IX – Exemptions**

*45. Research, archiving or statistical purposes*

Section 45(1) provides that "where processing of personal data is necessary for research, archiving or statistical purposes, such processing may be exempted from such provisions of this Act as the Authority may specify except section 4, section 31 and section 33". CIPL recommends that the final data protection law include relevant examples of categories of processing for these purposes, including medical and related research, to provide for more certainty and reduce the ambiguity associated with leaving all specification of covered processing to the DPA. Also, for the same reason of certainty, the final text of section 45(1) should state that "such processing shall be exempted" rather than "may be" exempted. In addition, as to conducting DPIAs in connection with such processing related to research, we refer back to our recommendations on DPIAs above (see page 30), including not requiring the submission of each DPIA to the DPA for approval.

[44] Transfers in this context include transfers by public bodies or private sector organisations for public interest reasons, for example, in the case of private sector organisations, the transfer of data for regulatory approvals for life-saving research and safety monitoring of widely distributed medical products in the pharmaceutical industry.

**Chapter X — Data Protection Authority of India**

*61. Codes of Practice*

As stated above in the transfers section, section 61 on Codes of Practice allows the DPA to approve or issue "codes of practice" submitted by various types of industry associations, regulators or government bodies. CIPL welcomes the inclusion of such codes of practice in the Draft Law. Codes of practice (and similar schemes — see below) are an important tool for ensuring compliance, organisational accountability and responsible data use. They also play an increasingly important role in creating global interoperability between different privacy regimes as well as cross-border transfer mechanisms. As such, we suggest that the Draft Bill further strengthen the provisions around codes of practice to ensure the widest possible uptake among the industry of such schemes.

Under the current Draft, codes of practice may be used, among other things, for "cross-border transfer of personal data pursuant to section 41 of this Act". CIPL recommends that this section be broadened to include privacy seals, marks and certifications, similar to the GDPR. It would also help improve the ability to leverage the Indian codes of conduct and certifications in other regions (such as APEC and the EU) for purposes of interoperability and global harmonisation.

Moreover, section 61(2) limits the ability to "submit" such codes for approval by "an industry or trade association, an association representing the interest of data principals, any sectoral regulator or statutory authority, or any departments or ministries of the Central or State Government". We recommend that the proposed law be broadened to include companies in this list of entities that may submit codes. In many cases, large companies create their own codes of conduct for their suppliers and distributors. Such company codes that similarly implement the requirements of India's data protection law should also be open for approval by the DPA.

Also, section 61(4) currently provides that a code of practice "shall not be issued unless the Authority has undertaken a requisite consultation process with relevant sectoral regulators and stakeholders including the public and has followed the procedure for issuance of such code of practice, as may be prescribed". We recommend a more nuanced approach here and would add "where appropriate" between "consultation process" and "with relevant sectoral regulators". A consultation process as described in this provision, though generally desirable, would not necessarily be appropriate or helpful in all contexts and may also unnecessarily encumber and slow down, if not completely undermine, the uptake and use of certain reasonable and effective codes of practice (and certifications, seals and marks, if included). An example would be if India ever wanted to approve the APEC CBPR as a code to the extent its requirements are consistent with India's data protection law. In that case, because the CBPR are already final and operational, there would not be a role for a public consultation on the code or certification itself. Instead, the CBPR or similar existing codes might be subject to approval (or rejection) by the DPA alone.

**Chapter XI – Penalties and Remedies**

*69. Penalties*

The Draft Bill specifies penalties for breach of data fiduciary obligations based on "total worldwide turnover", which is defined to include the total worldwide turnover of the data fiduciary and the total worldwide turnover of any group entity of the data fiduciary in certain cases.

The penalties specified in the Draft Bill are extremely high and potentially unreasonable and arbitrary. They are calculated on the basis of "total worldwide turnover" of the company, and not limited to the revenue generated in India or the actual harm that any non-compliance may have caused a data principal. Moreover, in view of the restrictive data localisation provisions as currently envisaged, which in some cases of critical personal data will potentially limit business to and within India, extending liability across total worldwide turnover and turnover of any group entity of the data fiduciary which has no reasonable nexus to such "India only activity" will be unreasonable and excessive.

We thus recommend that if the metric of turnover must be retained, a proportionate approach would entail fixing a cap on penalties and computing such penalties on the basis of any non-compliance by the data fiduciary and relevant impacts in the Indian market. The penalty should not extend to the data fiduciary's group entities located outside of India. To support this proposition, reliance may be placed on existing jurisprudence in India in other areas, such as competition law, where the Supreme Court of India has limited the calculation of penalties in relation to the "relevant turnover".

Furthermore, the DPA should approach sanctions from the perspective that the law merely provides a maximum threshold ("a penalty which may extend up to…") and not a method of calculation. As a result, sanctions should be determined by the DPA under a two-step approach: (1) The amount of the fine should be calculated in light of the circumstances as specified in the previous paragraph and (2) once this determination has been made, the DPA must verify that this figure is not in excess of the amount or percentage provided for by the law. This ensures that any threshold of turnover is viewed as a maximum boundary rather than the default standard.

**Chapter XIII — Offences**

Section 90 provides for fines and the imprisonment of up to three years of individuals who have knowingly, intentionally or recklessly obtained, disclosed, transferred, sold or offered to sell personal data in violation of this law. Section 91 provides for fines and imprisonment of up to five years for the same violations in relation to sensitive personal data. Section 92 provides for fines and imprisonment of up to three years for violations in relation to improper re-identification of personal data. Finally, section 95 provides for liability of any persons in positions of responsibility regarding the violating processing or activity, unless they could prove lack of knowledge and due diligence on their part. Subsection (3) also provides for liability of directors, managers, secretaries or other company officers where the violation has been

committed with that person's consent or connivance, or is attributable to their neglect (see also section 78 on Recovery of Amounts, providing for the attachment (and/or sale) of a person's movable property, accounts, immovable property, arrest and detention, etc.).

We believe that including criminal sanctions and imprisonment for individuals in the data protection law is excessive. To the extent that violations create criminal as opposed to civil liabilities, they are better addressed within the criminal code in relation, for example, to fraud and cybercrime.

Also, from a policy perspective, natural persons acting in their official capacity on behalf of a legal person that employs them should not be personally liable for violations of this law, unless they are top officers or directors and have acted wilfully or with gross negligence and for the purpose of financial or similar gain. Imposing criminal liabilities for such violations on individuals, especially internal data privacy experts/DPOs would undermine the ability of organisations to find qualified data protection officers and similar staff responsible for the handling of personal data and, thus, undermine the goals of this law. Similarly, the possibility of a criminal investigation being launched against a company for data protection violations can cause irreversible damage to an organisation's reputation, even if it the investigation later concludes with a finding of no criminal liability on the part of the organisation. Thus, it may also create perverse incentives towards less openness, forthrightness and constructive engagement with the DPA.

Finally, the Draft Bill also provides that when a company contravenes any provision, every person who was in charge and had responsibility for the company will be deemed to be guilty of the offence and places the burden of proving innocence on the person instead of the prosecution. This provision is unduly harsh and would inevitably lead to businesses and their leadership being less likely to carry out significant innovation or research activities within the country — preferring jurisdictions which adopt a more rational and harm-based approach to criminal penalties. It is also questionable how one would identify, in practice, true offenders in such situations when the provision holds every person who was in charge of, and was responsible to, the company at the time of the offence to account. This could potentially include thousands of employees.

**Timeline for Adoption**

Once enacted, the Indian government must select a "notified date" within 12 months. On the notified date, Chapter 10 on the Data Protection Authority of India and provisions on the power for the government to make rules to carry out the purposes of the Act and the power of the DPA to make regulations consistent with the Act will come into effect. The DPA must be established within 3 months of the notified date and must no later than 12 months from the notified date specify the exact list of activities that qualify for the reasonable purposes processing ground and must also issue codes of practice on various matters. All the remaining provisions of the Act (apart from section 40 on data localisation) will be in force 18 months from the notified date.

In order to provide more certainty for data fiduciaries and data processors that will have to dedicate sufficient time and resources in preparing for compliance with the law, the Draft Bill should specify more clearly when the "notified" date will commence following enactment of the law. A "notified" date of 6 months from enactment versus 1 week from enactment makes a huge difference to organisations. The Draft Bill should also specify the timeline for the DPA to be fully functional. This is currently uncertain and could be interpreted to be 12 months after the notified date once it has completed its codes of practice and specified the list of activities of reasonable purposes or it could be interpreted to be on the day the law comes into full effect or some other standard. A DPA that is fully functioning in advance of the law's provisions applying to organisations provides an opportunity for organisations to ask questions and seek insights on specific compliance preparations and efforts through constructive engagement with the DPA.

To be compliant, companies will need to become familiar with the provisions of the new law, understand how it may be interpreted by regulators and practically applied, and take appropriate measures internally. This is particularly difficult where no previous comprehensive privacy law existed. A reasonable timeframe would be at least 3 years from the enactment date or preferably 3 years from 12 months after the notified date as organisations, under the current timeframe, will potentially have only 6 months to define in detail all internal processes and build a consistent compliance program in line with the requirements created by the DPA as laid out in its codes of practice (which can be completed by the DPA as late as 12 months after the notified date).

Organisations had 2 years to implement the EU GDPR in countries that have already had comprehensive data privacy laws in effect for many years with many of the same features as the GDPR and even then 2 years was not sufficient for many organisations. In addition, several international companies which had not reached the requisite level of compliance by 25 May 2018 shut down their service in Europe.[45] Experience has shown that it takes a long time to ensure legacy IT systems and existing uses of data are fully brought into compliance with new rules. Furthermore, policies and procedures may have to be updated, organisational changes may need to occur and, most importantly, organisations will need adequate resources to carry out and implement any significant changes, which typically have to be budgeted several fiscal cycles in advance. Organisations will need sufficient time to allocate the necessary resources and then undertake long and complex internal processes to implement the new legal requirements across their organisations. Therefore, we encourage lawmakers to review this timeline in order to ensure a clearer and more predictable enforcement timeline and allocate organisations enough time to prepare.

Finally, with respect to data collected prior to the law entering into full effect, organisations should not be required to re-obtain consent for the continued processing of such data if the purposes for which the data was initially collected remain the same. This would facilitate and

[45] See "Startups, Media Companies Block European Users in Wake of New Privacy Laws", Janko Roettgers, 25 May 2018, available at https://variety.com/2018/digital/news/gdrp-sites-blocked-1202822432/.

assist organisations as they transition to the new law and a similar approach was adopted by Singapore when the PDPA was enacted.[46]

**Conclusion**

We hope the above recommendations provide useful input into finalising the Draft Personal Data Protection Bill 2018. We look forward to further opportunities to comment on and provide input into this process. If you have any questions or would like additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; or Sam Grogan, sgrogan@huntonAK.com.

[46] See Section 19 PDPA (Personal data collected before appointed day), available at https://sso.agc.gov.sg/Act/PDPA2012.