Comments of BSA | The Software Alliance on "The Personal Data Protection Bill, 2018"

September 28, 2018

BSA | The Software Alliance ("BSA") appreciates this opportunity to comment on the draft Personal Data Protection Bill ("the Bill") prepared by the Committee of Experts on Data Protection ("Committee"). BSA and its member companies are global organisations that provide data-driven services that support innovation and economic growth across the world while maintaining high levels of data protection.[1] Robust data protections are an important part of the global digital economy, as they ensure respect for individuals' fundamental rights and strengthen the trust that is necessary to promote full participation in digital society. At the same time, data protection laws that provide sufficient flexibility, reasonable obligations, and consistency with different data protection frameworks are critically important in this global environment. Data protection laws that strike an appropriate balance of these different factors can help advance the goal of providing strong protections for personal data, in part by leveraging the data protection programs in which BSA members have already made substantial investments.

Although many aspects of the Bill would lay a strong foundation for a robust data protection framework in India, several requirements would pose substantial challenges to BSA members and other organisations that operate globally, and are disproportionate to the objectives of the Bill.[2] These comments identify BSA's most significant concerns and, as appropriate, suggest alternatives for the Ministry of Electronics and Information Technology ("MeitY") to consider. Although the issues discussed below do not account for all of BSA's concerns about the Bill, they highlight the provisions that, in BSA's view, would create the greatest difficulties for businesses that process personal data as part of a dynamic, innovative, and global digital economy, without furthering data protection or privacy in any meaningful way.

At the outset, we highlight certain conceptual issues in the Bill that are of primary concern to us and inform our comments throughout this document. We find that the Bill builds on other jurisdictions' experience, like the European Union's General Data Protection Regulation ("GDPR"), but lacks the conceptual clarity and consistency that would enable the Indian digital economy to be integrated with the globalized data economy.

Issues relating to the classification and categorization of data and the attendant regulation of data practices and activities, which are at the core of any data protection framework, are not clearly established in the Bill. For example, the Bill creates a new category of personal data called "critical personal data," which would be subject to local data processing requirements and prohibitions from any movement across the border. However, neither the Bill nor the Committee's report provides any objective criteria for such classification by the Central Government. Further, even though the Bill exempts "anonymized data" from its purview, it does not adapt legal requirements in circumstances where other

[1] BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, and Workday.

[2] Unless otherwise noted, these comments cite specific provisions of the Bill by referring simply to the relevant section(s) in the Committee's draft.

Le-Meridien
15th Floor, Room 1529
Windsor Place, Janpath
New Delhi 110001
India

P (91 11) 4978 9066
W bsa.org

de-identification techniques are used to mitigate privacy risks, including with respect to data breach notification obligations and risk assessments, which would encourage use of these practices. Other data categories, like "non-personal data" and "community data," are mentioned in passing, but are neither adequately discussed nor explained in the report or the Bill.

The Bill also does not adopt a pragmatic approach with respect to supervisory and enforcement functions. The Bill establishes an independent regulator called the Data Protection Authority ("DPA"), but its current formulation would make it ineffective. While the report recognizes the lack of regulatory capacity and expertise in India to carry out the DPA's proposed functions, the Bill continues to burden the DPA with such functions, including wide discretionary powers that could disrupt business operations in India. There is also no clarity on whether the Bill adopts a collaborative approach to rule-making, wherein industry stakeholders will have an opportunity to participate in the formulation of codes, standards and regulations.

The lack of clarity in the Bill on these underlying principles, which lie at the core of any data protection framework, creates an environment of uncertainty for businesses, which could have a spillover effect on commercial operations, R&D activities, and future investments in India. Further, the unpredictability of rules – as several provisions will be determined after the enactment of the Bill - impinge on the ability of organisations to define appropriate privacy and data protection programs, policies, and practices.

Moreover, MeitY should evaluate the Bill not only to assess whether strong privacy protections are sufficiently implemented, but also with the objective of helping Indian individuals and firms access the global digital economy and to empower citizens and businesses alike. With these dual objectives in mind, the conceptual underpinnings of the Bill should allow for seamless integration of India's proposed data protection law with global legal frameworks and domestic infrastructure with global internet infrastructure. As such, any provisions in the Bill that create artificial barriers should be eliminated, in the interests of promoting technical and operational efficiency and to optimize the growth of the digital economy. Therefore, it may be appropriate for MeitY to consider an integrated approach to personal data protection, in part by leveraging existing data protection frameworks and practices from around the world, rather than for India to adopt a strategy that would isolate it from global markets.

With these considerations in mind, our comments emphasize that:

1. Restrictions on the cross-border transfer of personal data in the form of data localisation requirements do not advance data protection goals. Instead, they disrupt companies' operations and make it costlier to provide services in India, even as an unintended consequence.

2. An adequacy requirement and other conditions on cross-border data transfers, if imposed, should maximize consistency with existing mechanisms under other data protection frameworks.

3. Effective penalties and remedies are important elements of a data protection framework, but imposing criminal penalties and individual liability is disproportionate to the risk of harm addressed in this context, inconsistent with international best practices, and likely to chill legitimate data processing activities. Moreover, India already has a substantial body of penal laws to deal with any *mala fide* acts that can be invoked to address actual criminal conduct that occurs.

4. Specifying grounds for processing can provide certainty to data fiduciaries, but the Bill should also provide flexibility for fiduciaries to determine such purposes.

5. Accountability measures are a foundation of many global data protection programs, and the Bill should support companies' use of such measures, rather than shifting them to regulatory requirements administered by a data protection authority ("DPA").

6. It is essential that the DPA operates in a manner that is fair, transparent, and predictable; and MeitY should consider providing the DPA with more limited discretion on issues concerning implementation of the Bill as well as the conduct of investigations.

7. Security safeguards should be flexible, risk-based, and founded on internationally recognized standards. Personal data breach notification requirements should focus on helping data principals avoid harm and should not interfere with businesses' responses to security incidents. In addition, the law should provide positive incentives, e.g. exemption from breach notification requirements if the data fiduciary has taken adequate organizational and technical measures (such as strong encryption) to make the data unusable.

8. The Bill should establish a clear, default allocation of liability between data fiduciaries and data processors, while allowing them to reallocate liability through contracts.

9. Children deserve heightened data protections, but setting the threshold for those additional protections at the age of 18 is inconsistent with other global approaches to ensuring children's privacy.

As MeitY, together with the rest of the Government of India, considers revisions to the Bill and further steps toward enacting legislation, BSA urges due consideration of the issues raised in these comments. BSA would gladly provide further input on the Bill, or future revisions, if MeitY seeks additional feedback from stakeholders. BSA shares India's interest in a strong data protection framework that protects the rights of its citizens while also positioning India to thrive in the digital economy. We would be pleased to serve as a resource for MeitY going forward.

1. Restrictions on Cross-Border Transfer of Personal Data (Data Localisation)

A. Impact of Data Localisation Requirements

The introduction of any server or data localisation requirements would have a negative impact on India's digital ecosystem and curtail its ability to participate effectively in the global digital economy. Specifically, Prime Minister Shri Narendra Modi's ambitious "Digital India" program[3] and the IT Minister Ravi Shankar Prasad's plans to develop a "Roadmap for $1 Trillion Digital Economy" in India depend on the growth of innovative technologies like artificial intelligence ("AI"), cloud computing, and the Internet of Things ("IoT").[4] As we have discussed in our previous submissions to the Committee, MeitY, and other stakeholders, innovation in such technologies would be severely impacted by a legal mandate to process data only in India.[5]

---

[3] *See* "Digital India – A programme to transform India into digital empowered society and knowledge economy," http://pib.nic.in/newsite/PrintRelease.aspx?relid=108926.

[4] *See "Sh. Ravi Shankar Prasad Meets the Industry Leaders to Develop a Roadmap for US$1 Trillion Digital Economy," available at:* http://pib.nic.in/newsite/PrintRelease.aspx?relid=165697.

[5] *See* Responses of BSA | The Software Alliance to the White Paper of the Committee of Experts on a Data Protection Framework for India, at 8-9 (Jan. 29, 2018), http://www.bsa.org/~/media/Files/Policy/Data/012918BSAResponseofWhitePaperDataPortectionFrameworkIndia.pdf ("BSA White Paper"). *See also* BSA's response to the Department of Telecommunications on the Draft National Digital Communications Policy, 2018 (May 2018).

The Bill requires that data fiduciaries store in India "at least one serving copy" of personal data subject to the Bill.[6] Very few countries have adopted such data localisation requirements, and for good reason: Data localisation requirements do not serve on their own to improve data protection and, indeed, may undermine efforts to do so. Instead, they severely disrupt operations of both fiduciaries and processors and result in a range of negative economic consequences, discussed further below.

The Bill also would allow the Central Government to designate categories of personal data as "critical personal data" that can only be processed in India.[7] However, neither the report nor the Bill draws clear boundaries on the scope of such a mandate. The Bill does not define the term "critical personal data," while the Committee's report only indicates that "critical personal data" is any personal data that is "critical to India's national interests" and could include, among other things, health data, infrastructure data, and transport data. The absence of any clear criteria for classification of personal data as 'critical personal data' creates an environment of uncertainty for businesses, which could have a spillover effect on commercial operations, R&D activities, and future investments in India.

A requirement to store data in India – if not conducting processing exclusively in India – is the default rule under the current Bill. Although the Bill would allow the Central Government to exempt certain categories of data from the data localisation requirement, the standard for making such designations is rather narrow, and it is unclear whether and under what circumstances the Government would grant such exceptions.[8] Moreover, such exceptions would not apply to "sensitive personal data" like financial and health data, which are vital to India's digital ecosystem and necessary for the provision of essential services and applications, such as medical diagnosis and peer-to-peer digital payments. [9]

1. Negative Impact on Key Economic Growth Indicators

As the Committee's initial White Paper recognized, data localisation measures have a negative economic impact on GDP.[10] For example, one study estimates that data localisation measures could have an -.8% impact on GDP in India, and an estimated -1.7% in Vietnam.[11] The study also concludes that data localisation measures negatively affect exports for several countries, resulting in a -1.7% export loss in both Indonesia and China.[12] According to Gartner, public cloud services in India are projected to grow at 38% this year to total USD $1.81 billion. Data localisation requirements could impede this national economic growth, as they often impose significant costs on the countries that adopt them.

2. Increased Cost and Impact on SMEs

Data localisation requirements also raise the cost of providing services in the country to which the requirements apply, potentially increasing costs for end consumers as well. Data localisation requirements may also put a dent on the ambitious "Start Up India" campaign of the Government of India, as such burdensome regulatory requirements disproportionately impact small- and medium-sized enterprises (SMEs) that may not have the necessary resources to ensure compliance when they leverage global services. Further, data localisation may prevent local start-ups from choosing and using services at affordable rates, leaving them with fewer and more expensive choices resulting from a lack of effective

[6] Section 40(1).
[7] Section 40(2).
[8] *See* section 40(3) (authorizing the Central Government to grant exceptions "on the grounds of necessity or strategic interests of the State").
[9] Section 40(4).
[10] *See* White Paper of the Committee of Experts on a Data Protection Framework for India, at 70.
[11] European Centre for International Political Economy, *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, at 6 (2014), *available at* http://ecipe.org/publications/dataloc/.
[12] *Id.* At 9.

competition. Studies also indicate that local companies would be required to pay 30-60% more for their computing needs in such cases.[13]

3. Negative Impact on Competition and Choice

As referenced above, data localisation requirements would also inhibit competition and the choice of technology available to end-users and procuring entities, including start-ups and government agencies. Any legal mandate that requires data to be hosted within India would eliminate many data storage options from those available in the global market. It is simply not practical for providers to have all of their services and functionality available in every country, since part of the cost savings and efficiencies that cloud service providers are able to offer result from economies of scale, which often require data be stored in multiple locations. Even where a particular provider has hosting facilities in India, because of how such platforms are configured, it is likely that some features or functionality will require certain data to be stored outside of India. In many cases, it is not possible to process all data locally with the same quality of service as could otherwise be achieved – for example, with respect to certain fraud detection services. Moreover, the trend toward relying on micro-services, *i.e.*, a service architecture that increases distribution of data processing, means that introducing such restrictions is likely to result in companies choosing not to serve businesses and individuals in India or instead significantly reducing functionality of their services.

Keeping in mind the need for a vibrant and competitive digital ecosystem in India, it is important to formulate policies that promote access to digital products and services, such as cloud applications and other edge services, at competitive prices. This would enable Indian businesses and start-ups to participate in global supply chains and directly access customers in foreign markets.

4. Undermining Cybersecurity Efforts

Moreover, disrupting global data flows through localisation can also undermine cybersecurity significantly. Data security is ultimately not dependent on the physical location of the data or the location of the infrastructure supporting it. Security is instead a function of the quality and effectiveness of the mechanisms and the controls maintained to protect the data in question. Companies consider many factors when deciding where to locate digital infrastructure, for example in optimizing Internet speed and access, developing redundancy and backup capabilities, and the deployment of state-of-the-art security solutions. The Bill restricts the ability of companies to make decisions based on such considerations.

Effective cybersecurity defenses also rely on having timely access to global sources of ongoing threat information and the ability to synthesize the collected information into actionable intelligence for security products and services. The undue restrictions on the flow of data will limit the types of information that can be drawn on for analysis and correlation and leave end users more vulnerable to new attacks that continue to surface on a daily basis. In particular, if global cyber threat analysis centers are unable to evaluate relevant cybersecurity threat activity occurring in India, the visibility and ability to detect and mitigate against emerging cyber threats in India will be severely reduced.

Further, centrally stored information can provide an attractive target to malicious actors, who understand that breaching systems of localised data could yield complete sets of data. By contrast, using cloud systems to distribute data storage globally improves the ability to compartmentalize data sets, improving the chances that a breach in one location will not lead to access to the entirety of any data set. Moreover, data localisation requirements can create additional points of security failure or privacy non-compliance by restricting businesses' ability to optimize their data governance and control practices, including by using or establishing data centers in strategic locations around the world or by selecting

[13] *See id.* at 73 (citing Erica Fraser, *Data Localisation and the Balkanisation of the Internet*, 13(3) SCRIPTed 359 (December 2016)).

cloud computing providers with established track records for security, availability, resilience, and other key performance characteristics.

In sum, it is clear that keeping a copy of all Indian data in country is neither necessary nor scalable.

B. Data Localisation Requirement Lacks Adequate Justification

As explained in the Report, the Committee's objective in introducing data localisation requirements is dual: to ensure effective enforcement and to secure the critical interests of the nation. Applying the Committee's own standard, it does not appear necessary and proportionate that all types of personal data processed by all data fiduciaries should at all times be stored in India with all the costs, data governance, and other complications explained below that this entails, in order to ensure that Indian data protection law applies and to secure the critical interests of the nation. As mentioned in the Report, with respect to data localisation, the White Paper recognised "the need for treating different types of personal data differently and a one-size-fits-all model was not considered appropriate." Despite this recognition, Section 40(1) of the Bill adopts a one-size-fits-all approach whereby all types of personal data must be stored in India. The Committee enumerates four distinct reasons to justify a restriction on cross-border transfer of personal data. However, a closer analysis of these reasons suggests that a data localisation mandate, as proposed in the Bill, is not a suitable method to achieve the stated objectives.

First, the Committee suggests that a data localisation mandate would assist in law enforcement. However, there are more reasonable alternatives to aid law enforcement agencies' access to data, including through bilateral agreements, contractual arrangements between governments and businesses, and MLAT reform.[14]

Second, the report discusses security vulnerabilities that arise by relying on undersea cable networks. As explained earlier in these comments, any mandate to establish digital infrastructure exclusively in India would actually undermine cybersecurity and privacy by creating a centralized target for malicious actors. Moreover, the Draft National Digital Communications Policy, released by the Department of Telecommunications earlier this year, itself highlights the need for additional International Cable Landing stations to 'improve international connectivity.'[15]

Third, the Committee's report states that the growth of the AI ecosystem depends on harnessing data, which would require "processing of data within [India], using local infrastructure". BSA's members are actively engaged in the development and use of cutting-edge AI technologies worldwide.[16] Cross-border data transfers are integral to every stage of the AI life cycle, from the development of predictive models to the deployment and use of AI systems. Therefore, any mandate to localise data would severely impact the development and use of AI-based systems to provide insights, including, for example, to farmers in India, by recommending real-time adjustments that improve crop yields while lowering the costs and environmental effects of farming.[17] The "National Strategy for Artificial Intelligence" released by

---

[14] *See* Bedavyasa Mohanty and Madhulika Srikumar, "Data localisation is no solution," (August 2018) *available at* https://www.orfonline.org/research/42990-data-localisation-is-no-solution/.
[15] *See* Section 1.1(e) of the Draft National Digital Communications Policy, 2018, *available at* https://innovate.mygov.in/wp-content/uploads/2018/05/Draft-NDCP-2018.pdf.
[16] *See* "Artificial Intelligence Maximizing the Benefits" (March 2018), *available at* https://software.org/wp-content/uploads/AI_Report.pdf.
[17] *See* "Spurring AI Innovation with Sound Data Policy" (May 2018) *available at* https://www.bsa.org/~/media/Files/Policy/BSA_2018_AI_DataPolicy.pdf.

NITI Aayog also discusses such use cases, including applications developed by our member companies, and highlights the need for an enabling data ecosystem based on international standards.[18]

Lastly, the Committee's report suggests that the processing of data exclusively in India would help prevent foreign surveillance. The report specifically mentions the "PATRIOT Act amendments to FISA" as an example. BSA supports the right of governments to protect personal and confidential information they hold, as well as individual citizens' right to secure the privacy of their personal information.[19] However, the proposal for a data localisation mandate, as contained in the Bill, is not an appropriate solution to address the issue of foreign surveillance. Instead, MeitY should explore other alternatives referenced in the Committee's report, including bilateral discussions and technical solutions, such as encryption.

Recommendations:

- Section 40 of the Bill should be deleted in its entirety. In this regard, we invite MeitY's attention to the dissent notes submitted to the Chairman of the Committee, on record, by Ms. Rama Vedashree and Prof. Rishikesha T Krishnan, the industry and academic representatives on the Committee respectively, who have categorically opposed the Committee's recommendations on data localisation contained in the Bill.

- MeitY should also recognize the role of private contractual arrangements, for example, between data fiduciaries and processors, in strengthening accountability mechanisms and to promote cross-border data flows. Creating a general obligation for processors and fiduciaries to be accountable – as is the case under Canada's Personal Information Protection and Electronic Documents Act – is a more effective way to achieve MeitY's data protection goals.[20] As discussed elsewhere in these comments, the Bill contains strong accountability requirements, and BSA recommends relying on these requirements to provide the assurances that section 40 is intended to address.

2. Conditions for Cross-Border Transfer of Personal Data

The seamless transfer of data across international borders is critical to cloud computing, data analytics, and other modern and emerging technologies and services that underpin global economic growth.[21] Global data flows enable multinational companies to scale global operations, start-ups to use cloud services to obtain digital infrastructure at lower costs, and small- and medium-sized enterprises to use digital platforms to find customers and suppliers abroad. As noted above, cross-border data flows are particularly important in the area of cybersecurity, enabling distributed and compartmentalized data storage, as well as allowing correlation of threat data for more effective cybersecurity defense. BSA understands that new government policies on cloud computing may require entire distributed systems to be located only in India. As mentioned early on in this submission, any such requirements would severely curtail India's ability to integrate its domestic infrastructure with global internet architecture. This lack of integration could result in loss of efficiency and functionality for end-users, as well as restrictions on market access for Indian firms and citizens. Therefore, to accelerate the growth of the digital economy

[18] *See* "Discussion Paper – National Strategy on Artificial Intelligence," NITI Aayog at 8 (June 2018) *available at* http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf.
[19] *See* "Encryption Principles" available at http://encryption.bsa.org/downloads/BSA_encryptionprinciples.pdf.
[20] *See Personal Information Protection and Electronic Documents Act, Principle 1 and Schedule 1, § 4.1, available at http://*laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html.
[21] *See* BSA White Paper at 8-9.

and to digitally empower citizens, MeitY should eliminate any provisions from the Bill that create artificial barriers to cross-border data flows.

Cross-border data flows also fuel data analytics, which can deliver socially and economically beneficial results in situations ranging from digital commerce to responses to natural disasters. For example, in 2015, researchers around the world conducted a real-time analysis of mobile phone patterns to assist in disaster relief efforts in the wake of the devastating earthquake in Nepal.

BSA therefore has strong concerns about the limits that the Bill would impose on personal data transfers outside of India.[22] Although the Bill provides various grounds to effectuate international data transfers, including (1) standard contractual clauses; (2) adequacy determinations; (3) intra-group schemes; and (4) reasons of necessity,[23] it does not include certain additional grounds like certifications, which are incorporated in other global data protection frameworks to promote cross-border data flows, including the EU's GDPR and Brazil's newly enacted data protection law.

Further, the linchpin for international data transfers in the Bill remains an adequacy determination by the Central Government.[24] As the Committee recognized in its report, adequacy requirements have proven to be cumbersome in practice.[25] In fact, the Committee states that adequacy-based models should be looked at "cautiously" as it places undue burden on the proposed DPA.[26] However, despite recognizing the regulatory burden and lack of capacity in India to deal with such determinations, the Bill retains the adequacy approach to cross-border data transfers.

The adequacy approach may substantially harm countries that impose them. For instance, a World Bank study found that restrictions on data flows "can reduce GDP by up to 1.7 percent, investments up to 4.2 percent, and exports by 1.7 percent."[27] In fact, India has been perhaps the largest beneficiary of cross-border data transfers, making it the pre-eminent outsourcing destination globally and in earning USD $135 billion by way of IT and IT-enabled services export.[28]

On the other hand, policies that promote cross-border data flows are expected to unlock opportunities for the digital economy in a variety of ways, including $39 billion of export opportunities for India by 2022,[29] and growth of the Big Data analytics sector in India to $16 billion by 2025.[30] Globally, the value of data flows amounted to USD $2.8 trillion in 2014 alone, thereby contributing significantly to overall trade and GDP.[31]

Instead of an adequacy approach, the Bill should focus on alternative models that are more effective in protecting data and promoting the responsible use of personal data. Specifically, the Bill instead should focus on accountability for cross-border data flows. Under the accountability model, organisations that process personal data remain responsible for its protection, no matter where or by

---

[22] Section 41(1).
[23] *See* section 41(1).
[24] *See* section 41(2).
[25] *See* Committee of Experts Under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (July 2018) (the "Report").
[26] *See* Committee's Report at 85-86.
[27] *See* http://www.bsa.org/~/media/Files/Policy/BSA_2017CrossBorderDataFlows.
[28] https://www.thenewsminute.com/article/nasscom-pegs-it-exports-growth-7-9-cent-2018-19-76744.
[29] *See* https://economictimes.indiatimes.com/news/economy/foreign-trade/rising-digitalisation-offers-39-billion-export-opportunity-for-indian-business-by-2022-report/articleshow/65057061.cms.
[30] *See* https://economictimes.indiatimes.com/tech/ites/big-data-analytics-to-become-16-billion-industry-by-2025/articleshow/59410695.cms.
[31] *See* https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

whom the data is processed. As such, any organisations transferring personal data must take steps to ensure that any obligations – in law, guidance, or commitments made in privacy policies – will be met. To incorporate these frameworks into the Bill, MeitY should study the accountability model under the OECD framework as well as the Asia-Pacific Economic Cooperation's ("APEC's") Cross-Border Privacy Rules.

Lastly, sensitive personal data would be subject to even more stringent conditions.[32] Given that sensitive personal data is broadly defined and includes financial data and passwords, as well as health and other broad categories of data, the Bill would place unreasonable restrictions on cross-border data flows that could hurt key industries, including the digital payments and healthcare industry in India.

Recommendations:

- MeitY should reconsider its support for an adequacy requirement.
- To the extent that MeitY continues to support an adequacy requirement and specific data transfer mechanisms as part of its proposed data protection framework, it should consider:
    - leveraging existing international mechanisms, such as the APEC's Cross-Border Privacy Rules,[33] standard contractual clauses recognized by the European Commission,[34] and binding corporate rules (recognized under the EU's GDPR[35] and also by Israel), rather than creating national versions of these same mechanisms;
    - allowing consent to be one basis for cross-border transfers without including consent as an additional requirement when other legal mechanisms for cross-border transfers are invoked;
    - permitting transfers based on codes of practice, by explicitly including such codes of practice as a ground for cross-border transfer of personal data under section 41 and ensuring that the requirements for industry consultations and procedural transparency, as set out in section 61, are strictly followed, and to ensure that no preferential market access is afforded to any particular technology or service; and
    - permitting transfers based on "reasonable purposes" established as a basis for processing personal data, including cybersecurity and fraud prevention. The parameters for specifying such reasonable purposes should be revised as discussed in Section 4 below.

3. Penalties and Remedies

Effective remedies in a data protection framework are important to ensuring that data principals' rights are sufficiently protected and fiduciaries are deterred from violating their obligations under the law.

---

[32] *See* section 41(3) (limiting transfers of sensitive personal data to (1) strict necessity for prompt action in connection with health services and (2) necessity for specific fiduciaries or principles provided that the transfer "does not hamper the effective enforcement" of the Bill's other provisions).

[33] *See* Cross Border Privacy Rules System, http://www.cbprs.org/ (last visited Aug. 21, 2018).

[34] *See* European Comm'n, Model contracts for the transfer of personal data to third countries, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en (last visited Aug. 21, 2018).

[35] *See* European Comm'n, Binding Corporate Rules, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en (last visited Aug. 21, 2018).

Providing monetary relief to compensate data principals for any economic harm they suffer and imposing appropriately tailored conduct relief to prevent future violations are both useful tools within a broader system of data protection enforcement.

A. Fines and Remedies

Notably, the Bill introduces high penalties as a means to deter violations of personal data protection rules. Although the Bill borrows heavily from the EU's GDPR in relation to these provisions and the level of the fines foreseen, it adopts a stricter approach, without justification, and fails to take into account the manner in which those penalties under the GDPR are intended to apply. The fines under the GDPR are set out with the condition that their imposition "in each individual case" should be "effective, proportionate and dissuasive." Further guidelines on these provisions explain that the imposition of fines should be a last resort, taking into account a list of mitigating or aggravating factors.

The Bill's stricter treatment of this issue could result in a penalty structure that is disproportionate to potential law violations. Importantly, the current draft does acknowledge the role of accountable approaches by organisations as a tool for risk mitigation and, in fact, lists transparency and accountability among the factors to determine a penalty. We encourage further emphasis on these mechanisms as the whole ecosystem, from start-ups, to SMEs, to large corporations, would be incentivized to put in place appropriate measures to minimize privacy and data protection risks. To that end, the list of mitigating or aggravating factors should explicitly include the degree of cooperation with the DPA to remedy or otherwise mitigate the possible adverse effects of the infringement. This is an important incentive for cooperation that can help substantially reduce the harm to data principals.

In addition, the existing system for grievance redressal and dispute resolution under the Bill places an undue burden on the DPA and may not serve as an effective means for individuals to obtain remedies. For instance, rather than establishing separate entities to deal with enforcement and adjudication, the Bill bestows all powers and functions within the DPA, under separate wings, despite its limited capacity (as recognized in the Committee's report). Instead, the Bill should empower data fiduciaries and processors to implement their own grievance redressal systems that can be adapted to the specific context, including the type of remedy sought and the risk of harm to the individual. A flexible grievance redressal system, that does not depend on onerous regulatory interventions by the DPA, is more likely to achieve the objectives of ensuring quick and efficient grievance redressal for individuals.

B. Criminal Penalties

In addition, several of the Bill's penalties and remedies would go much further than necessary to compensate data principals for any harm they suffer and to deter violations of the law. Indeed, some of the Bill's penalties and remedies go far beyond other data protection frameworks. Criminal penalties and individual liability are the cause of greatest concern to BSA.

Criminal penalties simply do not have a useful role to play in data protection law and, while present in some jurisdictions, are far outside of international best practices. Tellingly, the Committee's report offers no principled justification for criminal liability and only mentions in passing that some commenters on the Committee's November 2017 white paper supported criminal penalties.[36] This falls far short of a rationale for imposing severe criminal penalties for data protection law violations, and it does not explain how other penalties and remedies fail to provide sufficient protections. Moreover, the remedy is disproportionate to the risks addressed in a data protection framework.

In BSA's view, the substantive requirements of a data protection law, combined with monetary relief and conduct remedies provided through administrative or civil judicial processes, are sufficient to

[36] *See* Report, *supra* note 12, at 163.

protect individuals' privacy interests. In contrast, the specter and risk of criminal liability – even if limited to knowing, intentional, or reckless violations[37] – can chill beneficial and harmless data practices, as illustrated in the following section of this submission.

Moreover, the Bill's imposition of individual liability for "every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company" is even more concerning.[38] Establishing liability for "every person" is unrealistic given the nature of data governance and data management practices. For example, if the offence consists of the violation of the obligation "to undertake a data protection impact assessment by a significant data fiduciary under section 33," the number of persons that may be involved in this violation can be very large – across functions and potentially geographies – and implicate people with little culpability. This is one of the reasons why liability for such offences lies with the company. The high fines for the company and other non-compliance risks, including reputation damage and loss of business, deter employees from violating policies that the company needs to establish in order to ensure compliance.

Furthermore, to avoid being deemed guilty, such individuals would need to prove that they had no knowledge of the violation or "exercise all due diligence to prevent the commission of such offence."[39] Individuals acting in their official capacities for a fiduciary or processor should not be subject to such a presumption of individual liability. Moreover, the offences set out in Chapter XIII of the Bill are "cognizable and non-bailable,"[40] which would imply that individuals alleged to have committed offences under this Chapter can be arrested without a warrant, and further, there is wide discretion in the hands of the court to grant bail to such individuals.[41] As previously stated, the provisions relating to accountability already contained in the Bill would adequately protect individuals' privacy. Therefore, the inclusion of criminal liability provisions would be disproportionate to the objectives of a data protection framework as identified by MeitY and would have a chilling effect on innovation and ease of doing business in India.

Recommendation:

- MeitY should eliminate the possibility of criminal liability for violations of the Bill, and eliminate or narrow the circumstances for individual liability to situations in which it is proven that the relevant individual possesses an appropriate level of culpability for alleged violations.

4. Grounds for Processing

Providing several grounds for lawful data processing is an important and helpful feature of the Bill.[42] For example, the Bill appropriately recognizes that processing personal data may be necessary to respond to medical emergencies or to ensure public safety.[43] Providing a ground for processing personal data for employment purposes is also useful and recognizes the distinct application of privacy and data protection principles in that sphere. Indeed, affording flexibility in the grounds for processing – either through a generally formulated standard or several enumerated grounds – has strong foundations in other data protection frameworks. As the Committee's report recognizes, "[t]here is a need for a residuary ground for processing activities which are not covered by other grounds like consent, compliance with

[37] *See* sections 90-92.
[38] *See* section 95(1).
[39] Section 95(2).
[40] *See* Section 93.
[41] *See* Code of Criminal Procedure, 1973.
[42] *See* sections 12-17 (specifying grounds for processing: consent, functions of the State; compliance with law or court order; taking "prompt action" (e.g., responding to a medical emergency); necessity for employment purposes; and reasonable purposes).
[43] *See* sections 15(a) and (c).

law, prompt action and public function but are still useful to society."[44] BSA strongly supports this approach as a way to address the overarching challenge of balancing certainty and flexibility in establishing lawful grounds of processing.

In its current formulation, however, the Bill's reasonable purpose ground does not provide sufficient flexibility, creates uncertainty, and could inhibit beneficial data processing. For example, the Bill could affect the processing of personal data in the course of preparing industry reports and watch lists, product development and troubleshooting, web traffic analytics for crime prevention, service personalization, direct marketing, and regulatory compliance.[45] It is impossible to predict and enumerate all the different types of purposes to which such exceptions should apply. Further, the storage limitation provision prevents businesses from carrying out necessary processes to improve their services by preventing them from retaining personal data beyond the period necessary for the purpose for which it was collected. Therefore, the current provisions of the Bill should be amended to provide adequate flexibility.

As an initial matter, MeitY should clarify that section 17(1) permits data fiduciaries to specify reasonable purposes for processing personal data, and that the reference to the DPA role in section 17(2) is to provide further guidance and certainty with respect to additional non-exhaustive reasonable purposes. If MeitY fails to clarify this point, and the Bill is interpreted as requiring the DPA to recognize specific reasonable purposes before any such purposes can be the basis for processing, section 17 will lack sufficient flexibility in at least three ways.[46]

First, depending on the DPA's specification of reasonable purposes is at odds with the notion of flexibility. Data fiduciaries are in the best position to understand the benefits and risks of their data processing activities. These benefits and risks may vary considerably from one firm to the next, particularly where innovative forms of data processing – which data protection law should encourage – are involved.[47] Other elements of the Bill, including the comprehensive safeguards that data fiduciaries must provide, would provide robust protections for the interests of data principals. Similarly, the purpose limitation, which operates over and above the grounds for processing in its current form does not account

---

[44] Report at 117.

[45] *See* "Examples of Legitimate Interest Grounds for Processing of Personal Data," Centre for Information Policy Leadership" (16 March 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_16_march_2017.pdf.

[46] It is also plausible to read section 17 to permit data fiduciaries to specify reasonable purposes. Under this reading, subsection (1) is a source of authority for data fiduciaries as well as the DPA to specify reasonable purposes, after taking the factors in clauses (a)-(e) into account. Subsections (2) and (3) then apply only DPA specifications, with subsection (2) enumerating a non-exhaustive list of purposes that the DPA "may specify" as reasonable, and subsection (3) instructing the DPA to establish safeguards and take notice considerations into account before specifying reasonable purposes. BSA recognizes that the Report criticizes the GDPR's legitimate interest ground of processing as a "freely constituted residuary ground" that is "too capacious" and expresses an intent to "circumscribe[e] the ambit of the provision" by making the DPA responsible for specifying reasonable purposes. *See* Report at 118. Still, subsection (1) does not appear to preclude the possibility that data fiduciaries may specify reasonable purposes. Moreover, the legitimate interest ground for processing is a well-established feature of data protection frameworks that aim to facilitate the use of personal data for innovative purposes while also ensuring that the risks to individual rights and freedoms of data principals are appropriately taken into account. This approach recognizes that the person or entity processing the data is best positioned to assess the risk of processing in the first instance, and that accountability measures, such as the documentation of safeguards, provide suitable mechanisms to ensure legal compliance if issues arise. MeitY should reconsider the role that a legitimate interest ground for processing could play in India's efforts to achieve its dual goals of protecting personal data and advancing its Digital India initiative.

[47] *See* Report at 3 (stating that "the protection of personal data holds the key to empowerment, progress, and innovation").

for various reasonable purposes that might not be strictly "incidental" to the initial purpose of creation, leading to even greater inflexibility in processing.

Second, DPA approval could be cumbersome in practice. Aside from requiring the DPA to issue notice of which grounds listed in section 17(2) are reasonable within 12 months of the notified date,[48] the Bill does not provide specific timelines for the DPA to act, nor does it provide a procedure through which data fiduciaries may request to have a purpose recognized as reasonable. Ultimately, in this way, DPA approval could pose substantial burdens to both the DPA and to industry.

Third, section 17's requirement to consider the reasonableness of obtaining consent in connection with specifying a reasonable purpose is unnecessary. Although consent is an important component of data protection frameworks, part of the reason to include a reasonable purpose ground is that consent is infeasible in some settings. For example, it may be impractical for companies that collect personal data from sensors and other IoT devices to satisfy the Bill's consent requirements. Companies that understand how their systems are deployed, and what data they are collecting and using, are well-positioned to recognize these difficulties. Requiring the DPA to make its own assessment of the reasonableness of consent can only lead to second-guessing data fiduciaries' business and technical decisions. Further, by requiring the DPA to determine the "reasonableness" of obtaining consent, along with other factors such as the "reasonable expectations" of the data principal, the Bill appears to infringe on the contractual freedom between parties and unreasonably interferes in the special relationship between the data fiduciary and the data principal, to which the DPA is an external third party.

As a final matter, we note that the regulatory burden imposed on the DPA and lack of capacity will result in inefficiencies and failure to realize the Bill's objectives. Section 17 of the Bill places undue burden on the DPA by requiring it to "specify" reasonable purposes based on a variety of factors, not all of which are relevant to such determination, and which could impact the ability of businesses to innovate. Further, assuming that data fiduciaries will have to rely on the DPA's prior determination before proceeding under this exception, BSA submits that such *ex-ante* regulation is antithetical to the goal of promoting a "free and fair digital economy" as stated in the report and the Preamble to the Bill. In fact, another analogous statute, the Competition Act, 2002 provides limited *ex-ante* regulatory powers to the Competition Commission of India (i.e. only for "merger reviews"), based on the understanding that such regulatory assessments are subjective by nature and requires specialized knowledge and understanding of emerging practices and developments in the industry.[49] By the Committee's own admission, the DPA is unlikely to have the necessary capacity to make such technical and business determinations, at least initially, which would unreasonably curtail the legitimate research and business activities of entities in India and hamper the growth of the digital economy.

Recommendations:

- MeitY should clarify that data fiduciaries may specify reasonable purposes. Specifically, the Bill should permit data fiduciaries to process data for purposes that they determine to be reasonable under the factors listed in subsection (1), except that MeitY should eliminate the requirement to consider the reasonableness of obtaining consent as a factor. MeitY could also consider adding a requirement to conduct a risk assessment. The considerations in subsection (1), combined with

[48] *See* section 97(5) ("The Authority, shall, no later than twelve months from the notified date, notify the grounds of processing personal data in respect of the activities listed in sub-section (2) of section 17."); section 1(3) (requiring the Central Government to provide notification of a date on which certain transitional provisions of the Bill will go into effect).

[49] *See* K.K. Sharma, "Ex-Ante' and 'Ex-Post' Regulation," (October 2010) *available at* https://www.cci.gov.in/sites/default/files/presentation_document/COMPATCLBAConference19Oct2010.pdf?download=1.

the accountability requirements in the rest of the Bill, would provide strong protections for data principals' rights while fulfilling the goal of providing appropriate flexibility in data processing.

- MeitY could also consider revising the Bill to declare some of the purposes currently listed in subsection 17(2) to be generally, *per se* reasonable. For example, the purposes of preventing and detecting fraud and protecting the security of a data fiduciary's networks and systems are beneficial to data principals, data fiduciaries, and society as a whole. Moreover, processing for these purposes poses little risk to data principals' rights. Further, even in certain instances where sensitive data is involved, there are circumstances that warrant explicit recognition that purposes for processing personal data are reasonable, such as compliance with Know-Your-Customer and anti-money laundering laws. The Bill should explicitly authorize processing for these purposes, rather than leaving them to the discretion of the DPA. Moreover, the fact that this determination would be made after the enactment of the bill would likely create uncertainty for organisations that are shaping their internal policies, processes, and practices.

- MeitY should consider recognizing not only the legitimate interests pursued by the data fiduciary but also those of a third party, similar to the legitimate interest ground for processing provided under Article 6(1)(f) of the GDPR. For example, in addition to processing data to protect the security of data fiduciaries' own networks, BSA member companies and several others collect and process cyber security threat intelligence to serve the legitimate interests of 'third parties"—all of their customers and users.

- Relatedly, the Bill should recognize that processing that is necessary to perform a contract to which a data principal is a party is a reasonable purpose under essentially all circumstances. In practice, this ground for processing is routinely used in day-to-day business transactions and, for that reason, has been explicitly recognized in the GDPR and other frameworks.[50] Such frameworks also recognize consent as an important legal ground for processing personal data, but that recognition does not supersede the existence of a separate legal ground for processing that is based on the performance of a contract.

- Finally, the Bill should require the DPA to solicit and incorporate input from stakeholders as part of any process to specify reasonable purposes. The factors in subsection 17(1) necessarily implicate the interests and perspectives of data fiduciaries and data principals. Fully considering these perspectives is necessary to inform the DPA's decisions about which purposes are reasonable under the law.

5. Transparency and Accountability Measures

Accountability is important to ensuring that data fiduciaries establish and maintain compliance with relevant data protection laws.[51] Procedural requirements that take into account the wide variations in data fiduciaries' size and sophistication, as well as the scope of their data processing operations, are appropriate for this purpose. The Bill contains several measures that are helpful in protecting the rights of data principals, including privacy by design[52] and security safeguards.[53] However, some of the accountability requirements in Chapter VII of the Bill could give rise to significant uncertainty and would

[50] *See, e.g.,* GDPR art. 6(1)(b).

[51] *See, e.g.*, GDPR art. 5(2); OECD Principles at 14-15 (recommending that a "data controller should be accountable for complying with measures which give effect to the principles" and outlining elements of a data protection program that could be used to demonstrate compliance).

[52] *See* section 29.

[53] *See* section 31.

be onerous to implement. Of particular concern to BSA are (A) the designation of significant data fiduciaries; (B) data protection impact assessments ("DPIAs"); (C) data audits; and (D) data protection officers ("DPOs").[54]

A. Designation of Significant Data Fiduciaries

Although it may be appropriate to impose heightened obligations on data principals that engage in processing that creates significant risks of harm to data principals, section 38's grant of authority to classify specific fiduciaries, or classes of fiduciaries, could distract from this goal and is both under-inclusive and over-inclusive when it comes to promoting the underlying goal of accountability.

Section 38 is potentially over-inclusive because it appears to focus on the data fiduciary as an *entity*, rather than specific data processing *activities* that may warrant heightened accountability measures. The obligations that the DPA may impose on significant data fiduciaries appear to apply to the entity that receives such a designation.[55] Thus, even if data processing – let alone data processing that poses a significant risk of harm to data principals – constitutes a small portion of data fiduciary's overall activities, being designated as a significant data fiduciary would seem to inappropriately affect the entity as a whole. Section 38 also requires the DPA to take into account factors that may bear little relation to risk of harm in making significant data fiduciary classifications. For example, the "turnover of the data fiduciary" may provide little information about risk, particularly if data processing is a small portion of an entity's overall business. Similarly, the "use of new technologies for processing" does not have a clear relationship with heightened data processing risks.

Conversely, Section 38 is also potentially under-inclusive. Data fiduciaries that have not been designated as significant could engage in processing that creates significant risk without being subject to the requirements of a significant data fiduciary. Although Section 38(4) provides that the DPA may impose some of the section's obligations on other data fiduciaries if it is determines that "any processing activity undertaken by such data fiduciary . . . carries a risk of significant harm to data principals," this provision would create operational challenges, as it depends on the DPA to identify high-risk processing after it has already begun.

Recommendations:

- As an alternative to significant data fiduciary classifications, the Bill should focus instead on accountability. This approach would put the strongest focus of accountability on activities that create the greatest risks – and only those activities.

- If MeitY maintains its interest in significant data fiduciary classifications, it should look strictly to the significant risk of harm as the basis for making classification decisions.

B. DPIAs

BSA is also concerned about the potential for DPIAs to become tools of precautionary regulation, rather than an element of a broader accountability-based approach. To be sure, DPIAs are an important part of data protection programs. However, subsections 33(4) and 33(5) would require data fiduciaries to submit DPIAs to the DPA and authorize the DPA to order the data fiduciary to cease or modify the relevant data processing activities if the DPA "has reason to believe that the processing is likely to cause harm to the data principals." In the first instance, it is unclear what benefit would result from a DPA's review of such a large number of documents, and the review of these materials would significantly delay

[54] *See* sections 38, 33, 35, and 36 respectively.
[55] *See* section 38(3).

the delivery of innovative products and services. In addition, the resources required by the DPA to review these voluminous materials would be immense, diverting resources away from other important enforcement efforts. Moreover, these provisions conflict with the notion of accountability and the data protection goals of the Bill as a whole in two significant ways.

First, section 33 appears to provide the DPA with summary power to stop or alter data fiduciaries' operations. The Bill is unclear, at best, as to whether any of the procedural safeguards governing the DPA's authority to conduct inquiries,[56] issue directions,[57] or otherwise take action with the powers enumerated in the Bill[58] apply to DPA actions taken pursuant to section 33(5).

Second, the standard that governs the DPA's determination that provides a basis for taking such drastic action is remarkably loose and generally unmoored from the rest of the Bill. The DPA only needs "reason to believe" that harm to data principals is "likely," a relatively low standard to meet.[59] Moreover, subsection 33(5) only requires the DPA to find that data processing is "likely to cause harm," without regard to the significance of the processing, any offsetting benefits, or the extent to which data principals might exercise their own autonomy in connection with the processing – by providing consent, for example.

Recommendation:

- Consistent with the notion that the DPIAs are first and foremost an accountability tool, the Bill should be revised to require data fiduciaries to keep their DPIAs on record and provide them to the DPA on request.

C. Data Audits

The Bill's data audit provisions could also lead to inflexible, burdensome regulatory obligations without necessarily advancing the goal of accountability or increasing the level of effective personal data protection for data principals. Accountability and risk-based approaches are better suited for data protection laws.

Audits are best used as an investigative tool; in contrast, a requirement for significant data fiduciaries and any other data fiduciary that the DPA finds "likely to cause harm to a data principal" to obtain annual audits[60] would add a significant new and burdensome element to fiduciaries' global data protection programs, which typically do not include routine audits. Moreover, audits under the Bill would have a broad scope, including, among other things, an assessment of a data fiduciary's privacy-by-design processes and its security safeguards, as well as other matters prescribed by the DPA.

The Bill's provisions relating to a "data trust score" derived from data audits raises two separate concerns.[61] First, a data trust score would necessarily condense a highly complex set of data processing considerations into a single rating.[62] Compressing so much information into a single score is unlikely to be useful to a data fiduciary's efforts to maintain ongoing compliance with the Bill's substantive

---

[56] *See* section 64.
[57] *See* section 62.
[58] *See* section 60 (articulating powers and functions of the DPA).
[59] *See* Section 33(5).
[60] *See* sections 35(1), (5); *see also* section 35(2) (prescribing elements of a data audit).
[61] *See* section 35(5) ("A data auditor may assign a rating in the form of a data trust score to the data fiduciary pursuant to a data audit conducted under this section."); Sections 8(1)(m) (requiring disclosure "any rating in the form of a data trust score that may be assigned[]to the data fiduciary under section 35").
[62] *See* Section 35(5) (referring in the singular to "a rating" that forms the basis for a data trust score).

obligations. The identification of shortcomings in a data protection program and specific recommendations for improvements would be far more useful.

Second, public disclosure of a data trust score is unlikely to provide useful information to data principals and could create misleading impressions about the trustworthiness of fiduciaries. It would be difficult to convey to data principals the factors that go into a data trust score or the method for calculating the score. Indeed, providing this information would only add to the challenge of providing data principals with information that "alleviates, as best as is possible, the problems of opacity, uncertainty, lack of clarity, and lack of accountability because of which privacy harms are caused."[63] A data trust score, on its own, is likely to be opaque to data principals; but providing an explanation of the score would necessarily involve asking data principals to digest more information about data processing.

Recommendations:

- Instead of requiring annual data audits – even if the requirement is restricted to significant data fiduciaries and others designated by the DPA – the Bill should authorize the DPA to conduct data audits under appropriate circumstances.

- A data trust score is unlikely to advance the interests of data principals or data fiduciaries and should be eliminated from the Bill.

D. DPOs

DPOs are now an established part of global data protection programs and can play a valuable role in helping businesses maintain compliance with their data protection obligations.[64] However, companies vary in size, complexity, and volume of personal data processing and, therefore, should maintain flexibility to determine how they will ensure compliance with a data protection law. To the extent the DPO requirement is mandated by law, MeitY should consider other ways to provide flexibility, such as allowing a single DPO for a group of undertakings, as is provided under the Article 37(2) of the GDPR. In addition, MeitY should address the significant operational challenges that the bill would create by requiring that data fiduciaries retain DPOs who are based in India.[65] This requirement would not only impose unnecessary expense, it would undermine companies' global compliance efforts by designating officials with this important role in India who are not otherwise part of more centralized efforts to address global privacy issues.

Recommendation:

- The Bill should not require a data fiduciary to retain a DPO who is located in India, but rather allow each company the possibility to choose its organizational structure based on business needs.

[63] Report at 58.
[64] *See, e.g.*, GDPR arts. 37-39 (specifying circumstances under which it is necessary to appoint a data protection officer and specifying the officer's duties).
[65] Section 36(4).

6. Data Protection Authority of India

BSA recognizes the importance of effective enforcement by a data protection authority that operates fairly, transparently, and predictably to the achievement of the Bill's data protection goals. Several of the Bill's provisions relating to the structure of the DPA would serve these ends. For example, the multi-member structure,[66] requirements that the DPA's members possess relevant expertise,[67] and protection from arbitrary removal[68] would all help establish an expert, independent body.

However, in its current formulation, the Bill fails to recommend an institutional framework for enforcement that would promote the goals of efficiency, predictability and proportionality. Moreover, the timeline for the establishment of the DPA and the broad number of key provisions to define after the enactment would add further complexity for organisations to plan and appropriately structure internal programs, processes, and policies. The myriad concerns regarding the framework for enforcement are described in further detail below.

First, as mentioned earlier in this submission, the Bill burdens the DPA with several functions, while at the same time acknowledging its lack of capacity and expertise to make appropriate determinations (e.g., relating to adequacy), which could disrupt business operations in India. As one example, the Bill recognizes the value that the use of personal data can provide for research purposes and appropriately provides a research exception from most of the Bill's requirements. However, the Bill requires fiduciaries and processors to pre-clear research with the DPA to avail themselves of the exception. In so doing, the Bill creates unnecessary administrative burdens that not only cause delay but also fail to provide significant benefits, as the expertise for reviewing such research would not likely reside with the DPA. *Second*, the wide discretionary powers granted to the DPA – for example, to specify "reasonable purposes" and approve standard contractual clauses – creates an environment of uncertainty for businesses, which could have a spillover effect on commercial operations, R&D activities, and future investments in India and could stand in the way of fair, transparent, and predictable operation in practice. In addition to authorizing the DPA to make decisions with major regulatory consequences for fiduciaries, as discussed above,[69] the Bill would grant the DPA excessively vast powers to implement substantive provisions and to investigate and adjudicate alleged violations. *Third*, the regulatory burden and lack of expertise would also severely impact the goal of promoting quick and efficient grievance redressal for individuals.

A. Specification of Additional Sensitive Personal Data Categories

As referenced above, the DPA's wide latitude to implement key provisions raises concerns. In particular, BSA is concerned about the level of discretion afforded to the DPA to create new categories of sensitive personal data. In this regard, the Bill's definition of sensitive personal data already includes an overly expansive set of categories,[70] and yet, section 22(3) would permit the DPA to specify additional sensitive categories based on "repeated, continuous or systematic collection for the purposes of profiling"

---

[66] *See* section 50(1).
[67] *See* section 50(4).
[68] *See* section 52.
[69] These comments do not discuss all of the DPA's authorities set forth in section 60(2).
[70] *See* section 3(35). BSA also recommends limiting sensitive personal data to categories of data that carry special risks in relation to discrimination and abuse of fundamental rights. Data routinely processed by fiduciaries and processors, such as passwords, while important should not qualify as sensitive. Just like a key protects the physical valuables, a password protects the virtual valuables, including sensitive personal data, but it, alone, is not sensitive. The limited grounds for processing sensitive personal data compound the difficulty of managing the Bill's broad definition of sensitive personal data.

and "additional safeguards or restrictions" for the processing of such data.[71] This authority would depart from the risk-based approach that the Bill otherwise takes to defining sensitive personal data, as well as other provisions for adding sensitive personal data categories.[72] In other words, section 22(3) unjustifiably enables the DPA to expand the definition of sensitive personal data solely on the basis of repeated processing.

The relationship of such processing, on its own, to any risk of harm to data principals is unclear at best. Instead, the Bill's broad definition of harm and general provisions for adding categories of sensitive personal data should apply to profiling.

Recommendation:

- MeitY should delete section 22(3) from the Bill.

B. Investigative Authority

Consistent with BSA's strong concerns about the Bill's criminal penalty provisions, BSA is similarly concerned with the DPA's authority under section 66 to execute searches and seizures. Although part of the justification to grant search and seizure appears to be a concern for the destruction of evidence, section 66(1)(c) includes a catch-all predicate for "a contravention of any provision of this Act has been committed or is likely to be committed by a data fiduciary."[73] This ground for ordering a search or seizure, which can be conducted by forcing entry to physical premises or "access[ing] *any* computer, computer resource, or any other device containing or suspected to be containing data,"[74] appears to unjustifiably allow the DPA to treat any data processing inquiry as a criminal inquiry.

The mere existence of this investigative authority, along with the severe criminal and civil penalties that the Bill would impose, is almost certain to chill legitimate and beneficial data processing activities. Rather than risk such activities, BSA strongly recommends that MeitY consider whether other provisions of the Bill otherwise would assure that the DPA can preserve and obtain evidence to aid its inquiries without resorting to such draconian grants of investigative authority.

Given that the focus appears to be related to the destruction of evidence, MeitY should consider more reasonable mechanisms to achieve the same objectives, for example by relying on data retention requirements, either under the Bill or other statutes that have provisions to this effect, such as Section 67C of the Information Technology Act, 2000 ("IT Act") which allows the government to notify rules requiring service providers to "preserve and retain such information as may be specified for such duration and in such manner and format" as may be specified.[75] Further, an analysis of the Criminal Procedure Code as well as the Indian Evidence Act should be undertaken in this context, and appropriate amendments or rules may be made.

Recommendation:

- MeitY should reconsider the scope of the DPA's search and seizure powers, including the elimination of the search and seizure predicate in section 66(1).

---

[71] *See* section 22(3).
[72] *See* section 22(2) (authorizing the DPA to add categories of sensitive personal information based on, among other things, "the risk of significant harm that may be caused to the data principal by the processing of such category of personal data"); Section 3(21) (defining "harm").
[73] *See* section 66(1) (specifying grounds for authorizing a search or seizure).
[74] *See* sections 66(1)(i)-(v) (emphasis added).
[75] See Section 67-C of the Information Technology Act, 2000.

- Consider alternative mechanisms to achieve the same objectives, for example by notifying rules relating to data preservation and retention under the IT Act.

7. Security Safeguards and Personal Data Breach

A. Security Safeguards

BSA and its member companies take safeguarding personal data seriously. Data security is integral to many BSA members' business models and how they protect personal data. Indeed, BSA members are industry leaders in the development and adoption of security-by-design and privacy-by-design solutions and secure software development lifecycle processes, and have played key roles in developing and adopting international standards and best practices. In addition, BSA members are at the forefront of using cloud computing, data analytics, and AI to improve cybersecurity for their customers and the businesses and individuals they serve. To take into account the wide range of security risks that companies face, the rapidly changing nature of security threats, and the complexity of developing security standards, data security requirements should be based on internationally recognized standards that are flexible, risk-based, technology-neutral, and outcome-focused.

On the whole, the security safeguards requirements in section 31 would accommodate this approach, but other provisions of the Bill would seriously undermine a flexible, standards-driven approach to data security. Specifically, section 61(6)(l) authorizes the DPA to issue security codes of practice, and section 97(6)(f) *requires* the DPA to issue these codes within 12 months of the notified date. This mandate not only burdens the DPA with an extremely complex technical undertaking in a very short period of time but also fails to recognize the significant investments that industry and other stakeholders have already made in developing and implementing security standards. It also ignores that flexible, international standards-based approaches to data security result in better security.

Given the wide range of security standards, and the fact that it is a continuously evolving field, a more useful role for the DPA would be to work with data fiduciaries and data processors, including small and medium online businesses in India, to identify existing security standards and best practices, and determine how to apply them in respective context. This kind of process would take advantage of the state-of-the art technology, rather than introducing additional complexity and confusion into an already challenging landscape.

Recommendation:

- MeitY should revise the Bill to (1) direct the DPA to consult with stakeholders to develop guidance as to which internationally recognized, risk-based, technology-neutral, outcome-focused standards apply to processing activities and (2) eliminate the mandate directing the DPA to issue security codes of practice.[76]

B. Personal Data Breach

From the state level in the United States to the GDPR in the EU, breach notification requirements are now a fixture of data protection frameworks, and BSA supports reasonable and appropriate personal breach notification requirements harmonized with global best practices to provide incentives to ensure robust protection for personal data and to enable data principals to take protective actions in the event their data is compromised. To achieve these goals – and to avoid the pitfalls of over-notifying individuals

[76] *See* section 97(6)(f).

– it is critically important to set the correct threshold for reporting breaches based on risk to data principals, to allow sufficient time for data fiduciaries to report, and to provide appropriate exceptions.

BSA is concerned about several aspects of the Bill's approach to breach notification. First, the Bill neglects to define the term "breach" and sets the reporting trigger – "likely to cause harm to any data principal" – too low, creating a substantial risk of over-notification, particularly in light of the expansive definition of harm.[77] The Bill would also require reporting "as soon as possible" and, in any event within a time period specified by the DPA,[78] potentially leading to unrealistic and inflexible timelines. Breaches may be subtle and carried out by highly sophisticated and well-resourced actors, or they may occur in the systems of third parties, such as data processors. These considerations make it impractical to start the timeline for notification with the occurrence of the breach. Moreover, it means that notifying data principals before all relevant facts have been ascertained can create confusion and lead to the need for follow-up notifications. Finally, the Bill lacks sufficient exceptions (*e.g.*, the data at issue is encrypted) to relieve data fiduciaries of the obligation to report in circumstances involving little or no risk to data principals.

Recommendations:

- The Bill's definition of "personal data breach" at section 3(30) in relation to "loss of access" to data should refer to permanent loss of data and not a temporary loss of access to data by data principals (otherwise every time a system undergoes maintenance or is offline for other reasons would constitute a breach).

- A breach should be reportable to the DPA only if it creates a significant risk of material harm to principals.

- The Bill should create positive incentives to data fiduciaries to adopt robust data protection. For example, data that has been rendered unusable or illegible (e.g., through the use of encryption) should be exempt from the reporting requirements.

- Instead of relying on the DPA to set an explicit deadline for notification, the Bill should require notification "as soon as practicable" or "without undue delay." Moreover, the timeline for notification should only begin when the responsible team within the fiduciary is aware of the breach (not when the breach occurs) and has had sufficient time to assess its potential impact on data principals.

- Regardless of the DPA's power to determine whether a breach is notifiable to data principals, fiduciaries should have the right to voluntarily notify data principals prior or in parallel to notification of the DPA in order to minimize the impact of a breach.

8. Relationship Between Data Processors and Data Fiduciaries and Allocation of Liability

In most instances, the Bill appropriately recognizes that the relationship between data processors and data fiduciaries should be governed by contract. However, section 37(2) imposes a requirement that would obligate data processors to obtain data fiduciaries' prior authorization before engaging sub-processors. Although other laws recognize a role for notification and clearance in these instances, they

[77] Section 32(1).
[78] Section 32(3).

apply a more flexible standard and do not require an affirmative, explicit prior authorization. For example, Article 28(2) of the GDPR permits a general written authorization in which a processor may inform the fiduciary of any intended changes regarding the addition or replacement of other processors and allow the fiduciary to object. Such an arrangement provides the requisite flexibility to the data processor while offering a reasonable opportunity for the data fiduciary to object to the proposed substitution.

Further, BSA supports the separation of obligations on data fiduciaries and data processors, and the Bill appropriately imposes most obligations directly on data fiduciaries. The Bill, however, muddies what should be a clear separation between fiduciaries' and processors' responsibilities by creating a confusing structure for compensating data principals who seek compensation pursuant to section 75.

Specifically, section 75(5) would potentially make data processors liable for any harm arising from any violation of the Bill to the extent that the data processor is involved in "the same processing activity" that caused the harm. Section 75(6) would leave it to data processors and fiduciaries to engage in a potentially adversarial process after compensation is awarded to determine whether any of the processors and fiduciaries involved owe compensation to another. This kind of liability is likely to undermine the relationships between data fiduciaries and data processors. It could also have a negative impact on investments in data processing and outsourcing services. Moreover, it is unnecessary, as processors and fiduciaries best can address liability and indemnification related to data protection issues through private contract before any compensation is awarded.

The draft bill further allows a court to order data processors to pay the entire compensation to data fiduciaries and recover from the data fiduciaries or other processors as per the harm caused by each, which creates unnecessary exposure for processors, who may not have access to the data principal or other data processors. This could potentially create significant negative consequences to the data processing industry in India, the largest contributor to the Indian IT sector revenues.

Further, the "explanation" in section 75 extends liability to processors not only in instances where they act outside of the instructions from the controller or fail to provide security safeguards, but also in the case of negligence. Given that processors do not have control over the decisions regarding the processing of data or visibility into the data that is stored or processed using their services, the extension of liability to circumstances outside of the processor's role or control is impractical and lacks sufficient justification.

Recommendation:

- MeitY should clarify that the authorization referenced in Section 37(2) may be a general notification by the processor with an opportunity for the data fiduciary to object, rather than requiring an affirmative, explicit authorization by the data fiduciary.

- MeitY should revise the Bill to clarify that data fiduciaries are responsible for any violation that relates to an obligation that the Bill imposes directly on them, but that fiduciaries and processors may enter into contracts that allocate financial responsibilities differently. This change would better correspond with typical commercial arrangements, avoid the need to reform existing contracts, and lead to greater efficiency overall in making compensation under section 75. Further, the bill should be revised to reflect that the data fiduciary may pay the entire compensation and then recover from data processors pursuant to its valid contractual relationship.

- MeitY should revise the "explanation" in section 75 to remove the reference to imposing liability on data processors for negligence and limit it to circumstances where the processor acts contrary to the data fiduciary's instructions or fails to provide adequate security safeguards.

9. Personal and Sensitive Personal Data of Children

Consistent with the EU's GDPR and the United States' Children's Online Privacy Protection Act ("COPPA"),[79] BSA supports considering the personal data of children to be sensitive and providing heightened data protections for their data.

Such protections, however, should be better harmonized with other data protection frameworks, including the GDPR and COPPA. In this regard, the Bill's upper age limit of 18 clashes with other standards for protecting children's data.[80] For example, COPPA applies to children under 13 years old, providing appropriate protections to individuals at the most vulnerable ages. The GDPR sets the upper age limit of children to 16 and allows EU member states to lower the age to 13.[81] The Bill's lack of harmonization with COPPA and the GDPR could increase the cost of providing services and prevent some children – particularly middle and older teenagers – from accessing services that will be beneficial to them. In BSA's view, defining children to be individuals under 13 provides sufficient protections for this class of data principals.

Recommendation

- To promote harmonization with other data protection laws, MeitY should revise the definition of "child" to mean a data principal under the age of 13.

* * * * *

BSA appreciates MeitY's solicitation of feedback on the Bill and would be pleased to serve as a resource as development of the Bill continues.

Regards,

Venkatesh Krishnamoorthy
Country Manager - India
BSA | The Software Alliance
venkateshk@bsa.org

[79] *See generally* 15 U.S.C. § 6501 *et seq.* and 16 C.F.R. Part 314.
[80] Section 3(9).
[81] *See* GDPR art. 8(1).