Computer & Communications Industry Association
Tech Advocacy Since 1972

Computer & Communications Industry Association (CCIA) Comments to India Ministry of Electronics and Information Technology Draft Digital Personal Data Protection Bill, 2022

17 December 2022

The Computer & Communications Industry Association (CCIA) submitted the following comments to the Ministry of Electronics and Information Technology (MeitY) regarding the Draft Digital Personal Data Protection Bill, 2022 (hereinafter "Draft Bill"). [1]

CCIA appreciates the continued work of the Government of India to develop national privacy legislation that will protect the privacy interests of users while enabling growth in the digital economy. The Digital Personal Data Protection Bill, 2022[2] is a marked improvement from prior iterations of national privacy legislation, and CCIA encourages policymakers to continue to consult with all relevant stakeholders as this legislation progresses to ensure regulatory coherence and provide direction on how this framework intends to interact with other proposed digital measures in upcoming months.

These comments detail concerns regarding some provisions in the Bill that, if enacted, could present significant compliance burdens and challenges to businesses operating in India.

A. General Comments on Enforcement Timeline

To provide adequate time for affected companies to comply, there should be an implementation timeline guidance that is consistent with international norms and allows for enforcement of these rules no earlier than 24 months after the Bill is enacted. While a provision on timeline was included in prior iterations of privacy legislation, it is absent from the 2022 Draft Bill.

A clear legislative timeline is important given that many areas of the Draft Bill direct the Central Government of India and/or regulators to prescribe implementing rules or frameworks for

[1] Via online submission at: https://innovateindia.mygov.in/digital-data-protection/.
[2] https://www.meity.gov.in/content/digital-personal-data-protection-bill-2022

processing personal data. Companies should be afforded adequate time following the issuance of these clarification and implementation guidance to set up compliance models.

B. Deemed Consent Grounds for Processing

Generally, regulators should promote a responsible data protection regime that provides for effective protection by requiring data fiduciaries to take reasonable, affirmative steps to reduce risks to users' privacy. This includes evidence-driven assessment frameworks, limitations on collection of sensitive data, and adoption of privacy-enhancing measures.

The Draft Bill details grounds for legal processing and prescribes categories of consent. However, there is a growing consensus that requirements for explicit consent for data processing are becoming less effective in advanced data protection regimes.[3] While it is important for individuals to understand how a company may use or collect information as a condition of offering services and have the clear ability to opt-out where reasonable or decline specific terms, frequent consent notices can have diminishing returns as users are less likely to read notices and may divert attention from more important choices.

The Draft Bill details grounds for legal processing and prescribes categories of 'deemed consent'. It is important that the interpretation of the designated categories are aligned with global norms to ensure consistency and predictability for industry.

Clause 8(9) enables personal data to be processed "for any fair and reasonable purpose as may be prescribed". This should include the grounds of contractual necessity. Data fiduciaries should be able to process the personal data of data principals to fulfill their contractual obligations without obtaining consent every time their data has to be processed. The inclusion of these grounds will not only help data principals avoid consent fatigue but will also ensure that the Draft Bill is consistent with global norms.

In addition, 'legitimate interest' should either be considered to be valid within the construction of deemed consent, or included as an independent ground for processing personal data in keeping with international practice. 'Legitimate interest' is the most commonly used ground for processing by data fiduciaries in advanced data protection legislation, and is helping in pursuing purposes such as preventing fraud, spam detection, and addressing security concerns, and which often

[3] *See* https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html.

involve third parties—all which cannot be exhaustively listed in legislation. The Data Fiduciaries should be allowed to self-determine what constitutes legitimate interests. Legitimate interests should also not be limited to prescribed purposes or have to outweigh "any" adverse effect, as stated in Section 8(9). It is instead important that adverse effects are not disproportionate in comparison to the legitimate interest pursued. CCIA suggests removing the stated limitations to ensure the provision does not lose its utility.

Clause 4(3) of the Draft Bill should be modified to include an exception for de-identified data. This would incentivize further innovation around privacy-enhancing technologies and other similar tools used to anonymize personal data.

C. Obligations Regarding Processing of Personal Data of Children

CCIA and its members share the goals of India to ensure that the online environment is one in which children are both empowered and protected, and that the Internet and ICT-enabled services can continue to provide learning and education opportunities. This is also important as digital services create more pathways and job opportunities in ICT-intensive careers.

The Draft Bill defines a child for purposes of the processing as an individual below the age of 18 years. CCIA recommends that the age of consent be revised to be consistent with international standards, which ranges from 13 to 16 years.[4]

The Draft Bill requires 'verifiable parental consent' for the processing of personal data of children in Clause 10. When devising the parameters for verification, the Central Government should look to existing industry practices and tested mechanisms through which verifiable consent can be obtained after accounting for the intricacies and nuances involved in the operation of various online services. Additional clarification will also help confirm whether this requirement is technically feasible for companies across a range of services in a manner that still protects the privacy of children online. Both parental consent and deemed parental consent should be available for processing of children's personal data. A strict parental consent requirement may be overly restrictive and prevent processing where consent is not viable or cannot be timely obtained, such as in cases of fraud prevention etc.

[4] *See* https://tile.loc.gov/storage-services/service/ll/llglrd/2021680641/2021680641.pdf.

In addition, even the general prohibition on all data fiduciaries from tracking and behaviorally monitoring children and directing targeted advertisements at them should be reconsidered. This is because it rests on the unfair presumption that all tracking and monitoring activities and targeted advertising are detrimental to children, even though the same are often carried out keeping in mind the best interests of children and specifically to protect them, including adherence to India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021.[5]

The Draft Bill also vaguely prohibits data processing of children that is 'likely to cause harm'. A more appropriate rule to limit harm would be to borrow from concepts of the widely-accepted UN Convention on the Rights of the Child and direct data fiduciaries not to process personal data which is contrary to the 'best interests of children'. [6]

D. Mechanism for Enabling Cross-border Data-Flows

Clause 17 directs the Central Government to assess instances where personal data may be transferred outside the country, effectively creating a 'white list' of approved countries (and implicitly prohibiting transfers to all other destinations). CCIA supports various mechanisms to enable transfers, as cross-border data flows remain essential to global commerce today. While the adequacy decision model to allow for transfer of data outside a country is common in many countries it has proven cumbersome to implement,[7] and this model is usually accompanied with other legal avenues for data transfers such as contracts or binding corporate rules or international certifications.[8] The Central Government should ensure that such alternatives are available and consider these avenues when assessing cross-border data transfers.

It will be essential that as this legislation progresses, additional clarity is provided to avoid regulatory uncertainty on how the Central Government intends to implement this type of adequacy regime including what factors it deems 'necessary' as well as specifying the terms and conditions that will govern cross-border data transfers. Absent further information on what these

---

[5] *See* https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf at 33 ("Every publisher of online curated content providing access to online curated content which has an "A" rating shall take all efforts to restrict access to such content by a child through the implementation of appropriate access control measures.").

[6] https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

[7] For example, in the 27 years since the EU passed its original Data Protection Directive, it has only reached adequacy determinations on 14 countries.

[8] For example, regulators may look to the Global Cross-Border Privacy Rules Forum as a means to govern international data transfers (in addition to white lists as contemplated by the Draft Bill). *See* https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

terms and conditions will entail, companies are unable to plan their compliances and calibrate their existing data transfer operations. Moreover, the exemptions to the adequacy requirement of Section 18 are too limited and should include consent from the data principal (Section 7) and deemed consent options (Section 8).

There should be a reasonable transfer period following the passage of the Draft Bill to allow for data transfers until the Central Government has instituted alternative transfer mechanisms and identified the countries where companies can transfer data per this provision.

Additionally, to the extent that the Draft Bill creates a presumption against cross-border transfers upon passage, it would likely implicate India's international trade obligations. Implementation of the provision should be consistent with India's commitments including those under the World Trade Organization's General Agreement on Trade in Services. Therefore, it is essential that the Government of India publish the 'whitelist' well before the Bill comes into force to avoid potentially halting cross-border transfers of data.

Under the GATS, India undertook commitments to allow all WTO Members to offer the cross-border supply of services in a number of sectors that would, typically, involve personal information. For example, India must allow foreign firms to offer re-insurance services to Indian customers, a service that invariably involves personal information. Similarly, India committed to allow foreign firms to offer the cross-border supply of a range of value-added telecommunications services including electronic mail, voice mail, on-line information and database retrieval, enhanced/value- added facsimile services and on-line information and/or data processing—-all of which typically involve personal information. The inability of a company that is deemed a data fiduciary under the Draft Bill from a WTO Member to supply such services absent inclusion on a 'white list' departs from international standards and would put such a supplier at a competitive disadvantage. Such a measure would likely be inconsistent with India's commitment to offer national treatment and Most Favored Nation (MFN) treatment.

E. Data Breach Notification.

Clause 9(5) of the DPDP Bill directs data fiduciaries and data processors to notify the Data Protection Board, as well as the concerned data principal, in case a personal data breach occurs. Data breach notification requirements should reflect international norms with respect to timeline of notification, thresholds of parties affected, and responsibilities of the data fiduciary.

Given the definition of 'personal data breach' in the Draft Bill, this provision may require all kinds of breaches to be reported, irrespective of the threshold, impact, or nature of the harm caused. This can unduly burden the Data Protection Board with non-critical information and amount to undue regulatory burdens on data fiduciaries. Similarly, data principals ideally ought to be notified of a breach only if the same impacts them adversely. The Draft Bill also does not acknowledge the dual reporting obligations, as entities have to report personal data breaches or leaks to the Indian Computer Emergency Response Team as well.

Clause 9(4) of the Draft Bill needs to offer further guidance around what constitutes reasonable security, especially given the penalties for non-compliance.

Officials can assist companies in their implementation of appropriate data security measures by adopting a risk-based approach to security. Officials can look at existing frameworks, such as the NIST Cybersecurity that are flexible, voluntary, and stakeholder-driven.[9] This guidance has helped organizations manage and respond to cybersecurity risk, and created a collaborative environment between the business community and government. This has helped ensure the frameworks remain effective for proper data security practices across products and services, and the timely sharing of information in the event of a major breach or cyber incident/attack.

F. Exemption for Central Government.

Clause 18 of the Draft Bill provides for broad exceptions for the Central Government and any instrumentality of the State, allowing state actors not to uphold privacy protections detailed in the legislation.

It is concerning that the exceptions, as drafted, are quite broad, allowing for the Central Government to act in an unregulated manner that could undermine the privacy interests of its citizens without adequate oversight and transparency. This, in turn, may make citizens less likely to utilize the full benefits of digital technologies in fear that these protections may not extend to government processing and use of personal data. Trust is essential for technology firms to continue offering services in new markets and absent clear rules on how personal data is used by both private and public entities, companies may be less incentivized from investing in new markets.

[9] Cybersecurity Framework 1.0, Nat'l Inst. of Standards and Tech. (April 2018) https://www.nist.gov/cyberframework.

G. Additional Responsibilities for Significant Data Fiduciaries.

Clauses 11(2) of the Bill imposes additional obligations and reporting requirements for firms designated as 'significant data fiduciaries'. CCIA recommends that this provision be removed.

These obligations include appointing a data protection officer based in India. However, many 'significant data fiduciaries' often already appoint a single data protection officer for all jurisdictions in which they operate. In other cases, companies have implemented effective grievance redress mechanisms without local presence, such as the case with the Consumer Protection (E-Commerce) Rules, 2020 ("E-Commerce Rules"), where there is no requirement for the grievance officer to be based in India. Moreover, the appointment of an Independent Data Auditor should be done away with, given that Section 11(2)(d) already requires Significant Data Fiduciaries to conduct periodic audits. It may not be practicable to require companies to allow independent auditors for multiple reasons including commercial and business secrets that may not be possible to disclose.

Also, the obligation to conduct periodic audits should be done away with. Imposing such obligations on the significant data fiduciary entails a very high risk of data leaks and increases the unwarranted burden on the company. The objective of risk mitigation through independent audits can be achieved through DPIAs. Audits can be conducted as part of the investigations by the Data Protection Board.

H. Other Key Issues.

The requirement to access data in 22 languages in addition to English, as per Section 3 and 6(3) is hard to implement in practice and will increase compliance burden. This may be removed or made optional as in Section 7(3).

Further, a seven day timeline has been provided for grievance redressal under Section 14(2). This is a very short timeline to investigate grievances and if maintained, will generate a high volume of complaints to the Board that do not need the Board's intervention. The timeline must therefore be increased to at least 30 days.

Conclusion

CCIA again appreciates the efforts of MeiTY in developing comprehensive and robust rules for privacy within domestic law and encouraging innovation. As the Central Government works through the details of this legislation, industry encourages policymakers to continue consultation with stakeholders.