CCAOI™

Representing the ecosystem of Internet -Bharat Model

CCAOI Feedback on the Draft Personal Data Protection Bill

Submitted by: Amrita Choudhury
Director, CCAOI, India
amritachoudhury@ccaoi.in

At the outset, we wish to thank MeitY for giving Indian stakeholders the opportunity to submit our feedback on the Draft Personal Data Protection Bill.

It is a welcome step that a framework for Data Protection is being laid out in India, which is much needed as we are moving towards a digital world. In an age when each individual is generating an enormous amount of data and with instances of data breaches, it has become very important that the privacy and security of personal data are given utmost priority.

While we appreciate the bill in terms of recognizing that privacy is a fundamental right, consent being essential for processing any data, purpose limitation and collection limitation of data, privacy by design, right of data portability and setting up data protection authority in India, please find below our comments on the certain aspects of the paper that need a relook.

1. **Ownership of Data**:

   The complete ownership rights of data should reside with the data principals which is not the case currently.

   Further, the data principal should be informed by the data fiduciary or have access to know when and for what purpose their personal data is being processed. This would help to build trust and transparency in the system.

   Though withdrawal of consent is mentioned in Sec 8(1)(d) and 12(2)(e) it must be recognized as a separate right under this chapter so that it can be enforced

2. **Grounds of Processing Personal Data**:

   (a) Processing of sensitive personal data by the State:

   There should be checks and balances to ensure states do not abuse the power vested on them under section 13 to process personal data "for the exercise of any function of the state" even without consent. There should be more legislative and judicial oversight over the exemptions given to the state, with clearly defined circumstances

when the state can exercise their right to provide a service or benefit to the individual without consent.

(b) Processing of sensitive personal data by Employer

Exemption offered to all employers in India to process data for " the purpose related to employment" seems quite broad in nature and lacks clarity. This should not be allowed as there may be chances of abuse of individual rights and privacy by employers.

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

a. Age of a Child

Today when in many social platforms the digital identity starts developing at around 13 years, the suggested age benchmark of 18 years is considered too high. Even in the EU, the GDPR has defined the age competency between 13-16 years. Also, procedure to verify age of minors is not sufficient and could be misused. There needs to be a well defined, robust mechanism to verify the age of the children while using different online services so as to restrict them to services that require the user to be an adult.

b. Consent of Adults

In a country with poor literacy, including digital literacy levels among parents, lack of understanding of technology, english language, limitations to access devices, there are chances of parents ingnot be adequately aware of what they are consenting to on behalf of their child.

For ensuring parents can make an informed decision on behalf of their children, it is important to promote digital literacy, safe browsing, educate and build capacity among parents, ensure the information is posted in easy simple language and in local languages along with pictorial depictions.

4. **Transfer of personal data outside India**

The privacy and security of the data of each data principal should be at the core of the privacy bill. The Redressal process should be fast and easy for data principals. The concerns of privacy of personal data should go hand in hand with security and should not be an either or situation.

We believe storing at least one serving copy of personal data within India, that has been proposed under section 40(1) may necessarily not be a solution to resolve the threats to the data as stated in the bill. Rather, rules must be framed such that data fiduciaries cannot allow any form of surveillance over the data by any third party organisations or nation, either within India or overseas, as has happened in the past. Provisions should be made such that law enforcement authorities in India gets faster response or access to data under proper judicial and legislative oversight with a well laid out process to get faster redressal for legitimate queries.

5. **Personal Data Breach**

In case of personal data breach, it should be mandatory for the data fiduciary to inform the data principal of the data breach and not left to DPA to decide whether the data breach incident needs to be informed to the individual. It should be an obligation for Data Fiduciaries to inform data principals if there has been any breach of their data immediately.

6. **Composition of DPA**

The DPA should comprise of members coming from different stakeholder communities (government, business, civil society, technical) and multi disciplines. There should not only be members from the techno legal background, but also human rights, law enforcement, financial and social sciences background in order to get a holistic understanding of how to manage and enforce and effective data protection regime

Lastly, it would be important to ensure that the enforcement of what is drafted as a Privacy bill is well implemented and enforced to ensure its success.

Thanking you and looking forward for favorable consideration of suggestions in the interest of growth of internet in the country.