The Dialogue
Inform Engage Ideate

Towards A Regulated Data Economy: Getting the Implementation Right

POST ROUNDTABLE REPORT

SUMMARY

- The Dialogue, in association with ESC and CUTS International organized a stakeholder consultation 'Towards A Regulated Data Economy: Getting The Implementation Right' on 26 September 2018 at Electronics and Computer Software Export Promotion Council (ESC), New Delhi.
- This was a roundtable discussion to gather stakeholder inputs on the Personal Data Protection Bill, 2018.
- The discussion focused on key issues under the Bill, namely the consent architecture; Grievance redressal mechanism; Enhanced personal entitlements; The role and functionalities of Data Protection Authority; Data privacy; Data localization; and more.

OVERVIEW

The Personal Data Protection Bill, 2018 proposes a framework to secure the informational privacy of citizens of India. The areas covered by the draft bill include consent, what comprises personal data including sensitive personal data, exemptions which can be granted, grounds for processing data, storage restrictions for personal data, individual rights and right to be forgotten. The draft of Personal Data Protection Bill, 2018 restricts and imposes conditions on the cross-border transfer of personal data and suggests setting up of Data Protection Authority of India to prevent any misuse of personal information.

The Dialogue
Inform Engage Ideate

ABOUT ROUNDTABLE CONFERENCE

The stakeholder consultation was divided into two sessions:

- Session 1: Rights & Responsibilities of Data Principal, Obligations of Data Fiduciary, User Rights
- Session 2: Regulatory Architecture & Institutional Uncertainties

The roundtable featured speakers that ranged from law enforcement, government stakeholders, internet companies, public policy think tanks and global business strategy firms. Speakers included Mr. Varun Kapoor IPS, (ADGP) Director, PRTS Indore, Mr. Amol Kulkarni and Ms. Swati Punia from CUTS International, Hike's Gautam Vohra, Kazim Rizvi and Madhav Sharma from The Dialogue, Adnan Ansari - Associate Principal, Albright Stonebridge Group, Charu Chadha from Facebook, Pranav Mehra - Snapdeal, Divya Dwivedi - Policy Head, UKIBC, Tridivesh Singh Maini - Assistant Professor, Jindal University, Anubhuti Bhrany, Govt Relations Head - HP, DK Sarin from ESC India, Rahul Sharma - IAPP. In addition to this, Mr. Deepak Maheshwari, Govt. Affairs Director, Symantec, shared his inputs offline.

The Roundtable discussed and discerned the fundamentals of data driven ecosystem, intent and aspirations of the stakeholders' vis-a-vie the proposed legal framework, regulatory and institutional architecture, and implementability thereof. It invited views and suggestions from multi-stakeholder community and will submit them for consideration by the Government in building the Indian data protection law and process of reforms in the interest of development of a strong and contextually relevant data protection framework.

The first session *"Rights & Responsibilities of Data Principal, Obligations of Data Fiduciary, User Rights"* moderated by Swati Punia, CUTS International focused on three key areas:

- Consent architecture
- Grievance redressal mechanism
- Enhanced personal entitlements - User rights

The second session *"Regulatory architecture & Institutional uncertainties"* moderated by Kazim Rizvi, The Dialogue focused on these major areas:

- Data Protection Authority/ Data audits/ Data Protection Officer
- Governance and surveillance
- Data Ethics- A marriage of Privacy and Data Protection
- Data Localization

The Personal Data Protection Bill 2018 (hereinafter referred to as the "Bill") is the first step towards securing the data of Indian citizens by strengthening the privacy laws. The sharing of

personal data is currently being governed by the Sensitive Personal Data And Information (SPD) rules 2011, which are now insufficient, such as, under SPD the rules apply to person, corporate bodies located in India but the Bill expands its gamut to cover parties that are even in foreign nations. The whole bill rotates around the idea of consent. The idea of consent was introduced to safeguard the user data.

All the speakers gave insightful observations related to their industry. There were interesting questions raised as well. For example, at what level will the consent be required from the data principals in a logistics chain company? Who will borne the cost of maintaining the data infrastructure - data principals or fiduciaries?

Session 1: Rights & Responsibilities of Data Principal, Obligations of Data Fiduciary, User Rights

"Moving away from the oil economy to a data economy, emerging technologies presents newer challenges that will impact Bill", said DK Sarin, ESC India.

Newer emerging technologies such as Blockchain and AI presents newer challenges. Realities and facets are ever changing. With this, the consumer's perception on data economy and digital economy will also change. A framework needs to be developed that incorporates such dynamic changes. The bill must have provisions to deal with these flexibilities - newer technological challenges and emerging realities.

Session 2: Regulatory architecture & Institutional uncertainties

The roundtable discussions outlined and discussed the functionalities of The Data Protection Authority of India and how government will ensure its transparency. Should the DPA act as a consumer forum platform or should it encompass the framework of handling criminal offences?

On security and Aadhaar, Chapter XV of the Bill on Miscellaneous provisions - Section 98(1) allows the Central Government to issue "such directions" to the Data Protection Authority ("DPA"), "as it may think necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order". Such directions on questions of policy then bind the DPA.

OUTCOMES AND SUGGESTIONS

1. Consent Architecture

Touching upon the consent architecture, an important question that was raised is as follows:

"Can the duties emanating from the rights bestowed upon the consumer overburden them? Does the consent framework (elaborate, granular & multi-level) balance the rights and duties of the stakeholders?".

Mr. Gautam Vohra from Hike rightly raised the point of taking consent at the right stage as important - whether it's at data collection stage or before processing data. He indicated that there was lack of clarity on the scope of processing as it encapsulated collection in language present in the Bill. The important point raised by the moderator was data fiduciaries' onus and responsibilities in ensuring rights of consumers be safeguarded and elaborate framework for an informed consent be implemented.

How EU-GDPR deals with consent (specifically, explicit consent)

Consent is one of the six conditions for the lawfulness of processing personal data as stipulated in Article 6 of the GDPR text. The new GDPR consent guidelines among others tackle the topic of explicit consent, the focus of this particular discussions.

Explicit consent is not strictly part of the definition of consent as you can read it in Article 4 (Definitions) of the General Data Protection Regulation text, according to which consent of the data subject regarding personal data means any:

- freely given,
- specific,
- informed and
- unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Explicit consent matters regarding the higher levels of control and data protection a data subject has in the case of special categories of personal data and special types/circumstances of personal data processing.

Explicit consent mainly comes into the picture in three 'consent' circumstances:

1. Explicit consent and the processing of special categories of data
2. Explicit consent and automated individual decision-making, including profiling

3. Explicit consent and derogations in international data transfers

The EU-GPDR also emphasizes on Two stage verification for explicit consent. Two stage verification can be a way to make sure explicit consent is valid. For example, a data subject receives an email notifying them of the controller's intent to process a record containing medical data. The controller explains in the email that he asks for consent for the use of a specific set of information for a specific purpose.

Therefore, **Bill must have a clear and unambiguous text highlighting explicit consent and at what stage taking consent is right**. There is also a requirement to mandate consenting. Is there a need to take consent at the data collection stage or consent should be taken only when the user data is processed?

Suggestion: Therefore, it's **important to engage the user in a way that is easy for them to traverse through the consent forms and understand what they are signing up for**. A mechanism that involves notice-based data collection at first and then commission consent taking process could be looked at.

At Facebook, Charu Chadha outlined how consent forms are designed keeping user's interface and user experience in mind. "Facebook has incorporated graphical presentation to walk through privacy settings that allows new users to access the consent document. Language of privacy setting is simplified and comes from how we understand data". There is also a multidimensional facet to consent. Determining when to ask a user for consent and to whom do you ask for consent is imperative.

For a product, the language of privacy setting must be simplified and should come from how the data is understood by the data fiduciary.

The implications of equating consent forms with a Product as the liability, an important aspect of The Bill, of the data fiduciary thereof might raising the cost of services was also discussed. "Product liability in the Bill does not clearly distinct between provider of services and provider of product", said Pranav Mehra from Snapdeal.

Rahul Sharma, Founder, The Perspective spoke about consent and product liability. "Focus of consent taking should not be shifted to user, if the technology overburdens the user, they give it up". "Organizations should be more open and transparent with their policies. Bill should be in vernacular languages and vernacular consent taking catering to different kind of consumers."

Another important detail that came out from the discussions were consent throughout the user's interaction with a product or service. For example, let's take a case of a typical user journey to purchase an item from an ecommerce website. First, they might choose to type their preference in a search engine which takes them to the website of their liking. After scanning through the items, they choose to select the ones they like and click on "Buy Now". The ecommerce website then redirects the user to a payment portal after which the user is redirected back to the website. In this process, there is also an access of the logistic chain partner.

Therefore, it is mandatory to clearly define consent throughout this entire process of chain. For a data fiduciary, there should be a clear outline on how many features and third-parties are built in to create a new product. There must also be an interplay between the partners and the governments. An organization should be more open and transparent with their policies. User should be also be notified of and be active of any further data analytics usage by the organization. The whole consent taking activity is futile unless privacy and consent is crucial and tied with organization's policies and mission. An organization should induce transparency and visibility - when is the product/service using a user's consent services.

Product Liability

The Bill states that product liability norms should be incorporated into consent forms. This means that the data fiduciary will continue to have liability for any harm caused to the data principal on account of the data being given to him, despite having obtained consent. This further means that greater liability is imposed on the data fiduciaries for ensuring that consent is properly obtained. The presence of pre-ticked boxes, non-appearance of the notice at the required time, or the use of the data for purposes not reasonably expected by the data principals are some of the harms outlined by the bill. These clauses definitely impose a much higher burden on the data fiduciaries.

This will not only increase the cost on the business, but also the user. In addition to the costs, data fiduciaries must also take the responsibility to generate awareness among its users about consent, product liabilities and privacy.

The discourse led to an interesting observation on whether a product liability is limited only to a "product" or will it also be applicable on "services". This will also lead to deliberation on a clear distinction between a provider of service and a provider of product.

2. Grievance redressal mechanism

For individuals to exercise their rights, the Bill provides three primary means by which a user can exercise your rights. First, there is a set of 'data principal rights', second, a grievance redressal mechanism, and third like with many other laws, there is an enforcement mechanism, which provides for penalties, compensation and criminal offences. Data fiduciaries must maintain grievance redressal mechanisms for complaints about violations. Where this doesn't work, a complaint can be made to the adjudicating officer appointed under the data protection authority to be established under the bill.

The role of grievance redressal mechanism is to address any deficiencies in consent services. Does a user have a right to represent themselves instead of going the lawyer route?

Like Grahak Suvidha Kendra of Department of Consumer Services, a process needs to be identified that lessens the burdens on consumer courts. A consumer can approach the Kendra which can make them aware about their rights and grievances hence leading to an efficient grievance redressal.

A grievance redressal mechanism should be accessible to people. Helpline numbers, chatbots, emails being few examples. Citizen will view a tech product with suspicion because they feel they are not users, they are the product and the data is being sold.

The roundtable was joined by Mr. Varun Kapoor IPS, (ADGP) Director, PRTS Indore. "Grievance redressal system should be accessible to people. A correct mechanism and process pipeline has to be identified. Helpline numbers, chatbots, emails are some of the ways by which efficient grievances redressal mechanism can be put in place. Only after then comes the criminal enforcement part."

"Citizens view tech products with suspicion. They feel they are not the 'users of the product', they are the 'product' and that their data is being sold. Proper grievance redressal will increase trust factor", he said. It was pointed out that some inspiration could be taken from the mechanisms under the Consumer Protection Act, wherein consumer courts have the rights of civil courts but are not necessarily bound by their procedures.

3. Enhanced personal entitlements - User rights

Personal data is any data about or relating to a natural person who can be directly or indirectly identified by such data. This 'identifiability' could be with respect to any

characteristic, trait, attribute or other feature of the identity of a person, or any combination of such features and other information.

The data principal rights include the right to confirm that a data fiduciary has their personal data, to access, and correct / update your data. It also includes the right to data portability – allowing a user to transfer data between service providers, and to restrict continuing disclosure of your personal data in certain cases, i.e. the right to be forgotten.

There is also a cost (data processing cost) involved while commissioning user rights. The users' right entails a cost on the data fiduciary, which can be a small-scale marginal enterprise. Therefore, a discourse needs to be initiated on whether the cost will be borne by the data fiduciary or the onus of the cost be shifted to a user.

4. Data Protection Authority/ Data audits/ Data Protection Officer

Many concerns were raised as to whether a DPA in India would ensure equal representation of different stakeholders, in order to ensure its independence. The Bill establishes a Data Protection Authority of India, consisting of one chairperson and 6 whole time members. The DPA members are to be appointed by the Central Government, based on the recommendations of a body that will consist of the Chief Justice of India, the Cabinet secretary and one CJI nominated expert. The Bill specifies the qualifications and expertise of the persons to be appointed.

Monitoring cross-border transfer of personal data is one of the functions of the proposed Data Protection Authority of India (DPA). Such monitoring of cross-border transfers of personal data in digital form would only be possible if communication networks are specifically monitored by the DPA. In this regard, the roles and responsibilities of the Data Protection Officers (or equivalent thereof) to be appointed by the data fiduciaries were discussed. Lack of clarity on accountability of such DPOs was highlighted. Concerns with data audits and data trust scores were also pointed out. It was mentioned that such scores could remain subjective and unclear and might not be the best mechanism to inform users of the data protection tools employed by data fiduciaries.

The Singapore government has announced the Data Protection Trustmark (DPTM) scheme, under which Singapore-based firms will be able to get officially certified for their data protection measures. The certification will assure clients or consumers that their personal data is being securely handled. The company will be judged based on four principles developed by the Personal Data Protection Commission (PDPC): governance

and transparency, management of personal data, care of personal data, and individuals' rights. Discussions on whether this can be worked in a country like India which has a diversifying demographics. The challenges of having a trust score based system were also discussed.

Outcome from these discussions also entailed that a significant DPA must have a presiding Data Protection Officer(DPO). The data fiduciaries should also participate in ensuring that a DPO is working in his/her parameter – preventing breaches etc.

The Bill must also clarify the role and responsibilities of DPO. It is different than the law envisages. The DPO, as per the bill, reports directly to the board and are not in the hierarchy of a typical organizational structure. Just like in EU-GDPR, the role of a DPO should be segregated from a compliance officer. The DPO should act as a facilitator between a data fiduciary, the DPAI and most importantly, the end consumer/user.

From the discussions, a salient debate on whether the body of DPO will be mandated or not. A professional or a compliance body like company secretaries, it's only natural to think that there is a possibility that the body DPOs will be developed into a professional body, like what happened in the case of insolvency officers. An important question the needs to be addressed now is should the body of DPO be an independent body?

5. Localization

One of the related implications of this vast jurisdiction are the data localization rules to be imposed under Section 40, which confirm the data localization reports that arose some time ago. Under these, one copy of all personal data to which the law applies are to be kept in a server within India. Further, certain categories of data, which are to be specified by the government as critical personal data are to be stored in India alone. Additionally, requirements for cross-border transfer of data are also imposed. Divya Dwivedi, UKIBC raised the issue of equivalence between EU GDPR and the the Bill and highlighted the need understand the points of divergences and similarities between the two legislations.

On Data Localization, Tridivesh Singh Maini - Assistant Professor, Jindal University spoke, "A bottom up approach makes sense instead of going top bottom. For example, Telangana has an opposing view of data localization. Allow the states, districts, SMEs and startups decide the data localization requirements. Cooperative federalism not only in domestic issues but also foreign issues and policies. Identifying important local stakeholders is key."

Even if the data is localized and stored within the domestic territories, they would be an issue of access. First, with differentiation between the laws in a country (for example, USA) and India. This issue has to be further clarified by the Bill.

Although, there are data investigation processes already in place, vital data that pertains to the security of life and property to the citizens may be stored locally, but the costs will be significant that may be borne by the user. Other data (data not vital to national importance) should have applicable access by the governments, whether through a mutual legal assistance treaty (MLATS) or an association of countries participating in free-flow of data.