

NASSCOM®

NASSCOM-DSCI STATEMENT ON PERSONAL DATA PROTECTION BILL 2019

To deliberate on the recently tabled Personal Data Protection Bill, NASSCOM-DSCI held an industry consultation with its members today. **Debjani Ghosh, President NASSCOM**, said, “A robust data protection law is critical for India’s success in the data economy and we are very happy that the Government is taking the necessary steps to pass the law at the earliest. Am also happy that the voice of the industry has been heard and that this version has incorporated several of the recommendations made. There are a few areas where we still need further clarity and NASSCOM will continue to work with the Government to ensure the bill is a win -win for India and the Industry.”

The notable positive changes in the draft of the Bill include:

- **Removal of Restrictions on Cross-Border Transfer of Personal Data** – The earlier draft of the Bill required one copy of personal data to be stored within the territory of India, for transfers of Personal Data to take place. Further, such transfers could only take place on the basis of standard contractual clauses, intra-group transfer schemes or adequacy decisions. These restrictions have now been removed.
- **Removal of Passwords from the indicative list of Sensitive Personal Data** – Passwords have been removed from the indicative list of Sensitive Personal Data under Clause 2(36) of the Bill.
- **Certain Offences Removed from the Bill** – The earlier draft of the Bill listed the obtaining, transferring or selling of personal and sensitive personal data in a manner contrary to the Act, as an offence. These provisions have now been removed.
- **Relaxations on Cross-Border Transfer of Critical Data** – It has been explicitly clarified in the Bill, that personal data which is notified by the Central Government as critical data, may be transferred outside the territory of India in certain limited circumstances – i.e. (i) prompt action for the provision health services or emergency services; and (ii) where the transfer is to a territory where the Central Government allows the transfer of critical data.
- **Creation of sandbox to encourage innovation** – The Data Protection Authority (DPA) shall create a sandbox for encouraging development of artificial intelligence, machine learning or any emerging technology in public interest.
- **Due Process Requirements for Investigating Offences** – The power granted to police officers above the rank of Inspector to investigate offences under the Bill have been removed. Any investigation has to happen on the basis of a complaint by the DPA, and subsequent to a court order issued on the basis of such complaint.

The key areas of concern for the industry however, are:

- **Power to Exempt certain Data Processors** – Central Government has the power to exempt data processors, that process personal data of data principals who are outside the territory of India. While this was included in the earlier draft of the Bill as a miscellaneous provision, this has now been included under the Chapter on exemptions under the Bill. However, no material changes have been made to the text. The industry, in particular the IT-BPM and GCC industries will need greater certainty on the scope and issuance of the exemption.
- **Inclusion of Provisions Dealing with Non-Personal Data** – The Bill empowers the Central Government to direct data fiduciaries or data processors to share anonymised data or non-

personal data for the purpose of enabling better targeting for delivery of services or for the formulation of evidence based policies by the Central Government. The Central Government has to make annual disclosures of the directions issued under this provision. However, no safeguards have been provided for protecting IP rights, or other business sensitive non-personal data.

- **Categories of Sensitive Personal Data**- The Bill retains “financial data” as a category of sensitive personal data. Further, “financial data” continues to be defined broadly under the Bill. This is an area of concern, especially with reference to employee data processing for operations such as payroll services, that requires processing of financial data. Given that explicit consent is the only ground for processing sensitive personal data, the classification of “financial data” as sensitive personal data poses potential problems for other business operations such as risk management, fraud detection, among others.

Lastly, there are some areas where we will be seeking further clarity. For instance, while the classification of data has been designed in the same manner, personal data now covers inferences drawn for the purposes of profiling, we will be studying this closely to assess its impact. Other areas where clarity will be sought includes:

- **Classification of Significant Data Fiduciaries** – The Bill provides certain factors that need to be considered by the DPA while classifying certain data fiduciaries as “significant data fiduciaries”. It needs to be made abundantly clear that these factors will be assessed cumulatively, instead of individually, by the DPA.
- **Classification of certain Personal Data as Critical Data** – The Central Government retains the power to notify any personal data as critical data. However, the Bill still does not provide any definition for critical data, or provide any guidelines for the determination of what may be notified as critical data. This is an area that needs further clarity to create business predictability from an operational standpoint.
- **Cross-Border Transfer of Sensitive Personal Data** – The Bill requires continued storage of sensitive personal data in India, in instances where a cross-border transfer of sensitive personal data is affected. It is unclear as to what this requirement entails vis-à-vis manner of storage.
- **Removal of Transitional Provisions** – The Bill excludes transitional provisions provided in the earlier draft. Upon enactment, the industry will need sufficient time to implement changes in their business models. Accordingly, there is a need for further clarity from the Central Government on the manner in which various provisions will be brought into force, so that the industry is able to achieve meaningful compliance.

We will continue working with government stakeholders and seek more discussions on this issue.”