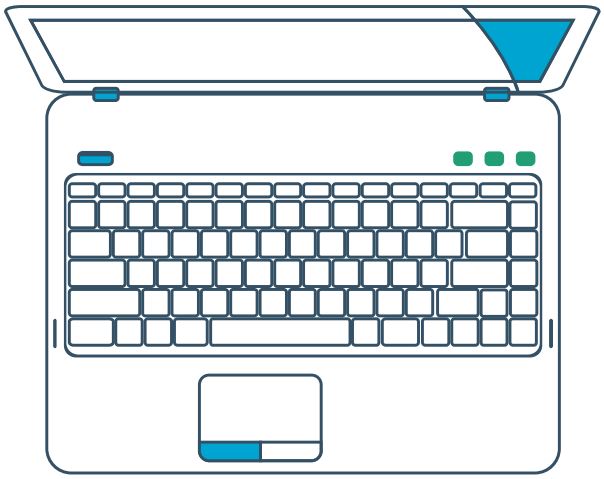
Deloitte.

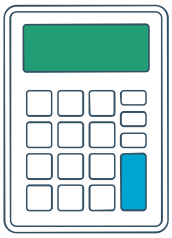
The Personal Data Protection Bill, 2018

Private and confidential

2018

Forensic





The Personal Data Protection Bill, 2018 (the "Bill"), showcases India's growing concern for data privacy. The objective of the Bill is broadly to protect the autonomy of individuals by safeguarding their personal data and giving them the power to allow or deny use of their personal information. The Bill covers diverse aspects of data protection including collection, processing, and analysis of personal data. It also lays emphasis on protection of personal and sensitive data, including that of children.

Most organizations today allow company issued computers, laptops and other IT assets ("Company's IT Assets") to be used by their employees for employment and it is observed that such Company's IT Assets are sometimes subject to the incidental personal use by employees. Therefore, it is likely that the user's personal data could reside on such assets.

Some thoughts on the impact of the propositions made under the Bill, as it stands currently in the context of fraud risk management/investigations:

#1 Obtaining consent prior to accessing data: A formal consent letter stating the purpose of data collection, types of data required and the party requesting for data access must be obtained. Failure to do this may also attract penalties.

- Consent on use of selected employee data would be necessary prior to an investigative/ fact finding exercise. Further, should third parties be carrying out these activities on behalf of the organization, the consent letter issued by organizations and signed by employees must specifically mention this.
- Employee data cannot be monitored as part of prevailing routine controls in the organization such as encryption, and data leakage prevention, among other measures without consent. Even in cases where the organization explicitly prohibits personal usage of office owned systems, written consent from employees is preferable as monitoring the actions of individuals may be considered a privacy infringement.

#2 Limited employee personal data access is permitted: Data access that can enable employment or termination of a data principal by a data fiduciary; employment benefit sought by the data principal who is an employee of the data fiduciary; and any activity relating to assessing the performance of the data principal who is an employee of the data fiduciary, is permissible. However, use of data provided for purposes other than intended will require consent.

- Personal identifiers and sensitive personal information on company owned devices/ servers/ systems/ applications etc. such as bank statements, credit card bills, insurance documentation, pay slips, Form 16s etc. cannot be disclosed to third parties as part of an independent verification/due diligence or fact finding exercise commissioned by the organization without consent of the employee.

#3 Cross border data transfer and processing is not permitted unless approved by data protection authorities and the government.

- Investigations, fact finding reviews, and performance reviews among other activities for which personal data is being analyzed must be conducted within the jurisdictional boundaries of India subject to the applicable provisions of the Bill. In case of outsourcing this to agencies outside India, approval from the Data Authority and consent from the data principal/custodian would be required again.
- The employee's personal data which is not critical as referred in the Bill, sought by the organization, such as educational qualifications cannot reside on a server outside the country, without approval by the data protection authority.

#4 Outsourcing of data processing must be governed by a clear and explicit agreement. Third party data processors will not initiate or commence personal data collection and processing unless specifically permitted by the Bill and provided there is a valid contract.

- Data fiduciaries (clients/employers) must have a valid contract with third party data processors before engaging them for any services which may involve any kind of data processing on behalf of the data principal to the extent specifically permitted by the Bill. Data Processing by the third party data processor shall be subject to the provisions of the Bill.

#5 Collected personal data may have to be erased as per the data principal's "right to be forgotten"

- Data fiduciaries (clients/employers) will have to demonstrate adequate efforts in case a data principal requests for his/her personal data to be erased. This can include
  - Physical documents stored with finance or HR teams; these will need to be shredded or appropriately destroyed;
  - Forensic images of data principals' company issued laptop/desktops as acquired by a data processor; the entire forensic image will have to be securely wiped and a report of the same will serve as evidence.
  - Personal data of data principals residing within system applications may also be considered and therefore data fiduciaries will be required to remove any identified personal data as requested by the data principal.

For more information, please contact the following people:

Nikhil Bedi
Partner | Leader – Forensic
Financial Advisory
Deloitte India
T: +91 9769371571
E: nikhilbedi@deloitte.com

Jayant Saran
Partner – Forensic
Financial Advisory
Deloitte India
T: +91 9810042303
E: jsaran@deloitte.com

Sachin J. Yadav
Partner - Forensic
Financial Advisory
Deloitte India
T: +91 9867306790
E: sachyadav@deloitte.com

Deloitte.