TAXMANN

www.taxmann.com
• Direct Tax Laws • Corporate Laws • Service Tax
• International Taxation

[2023] 153 taxmann.com 572 (Article)

Revamping Internal procedures in the wake of The Digital Personal Data Protection Act, 2023

CS PUZHANKARA SIVAKUMAR

Managing Partner, SEP & Associates Company Secretaries

CS SYAM KUMAR R

Senior Partner, SEP & Associates Company Secretaries

These days most of the services that an individual avails of are transacted online and this necessitates sharing of personal data online. While sharing of data was necessitated even before the digital revolution, online sharing and digital storing of data causes concerns of data theft and unauthorized processing of data. One often wonders when he gets an unsolicited call from some marketing agencies, how they got his personal details and who shared the details with them. We are left wondering whether there is some action we can take against the businesses with which we share data. Hence, a legislation that aims at protecting the data, while at the same time recognizing that sharing of data is inevitable in this digital world is the need of the hour. To this end, the Digital Personal Data Protection Bill, 2023 was passed by both houses of the Parliament during the recently concluded monsoon session and received President's assent on 12.08.2023. This Act aims at protecting digital personal data and also provides for the procedures for utilization of such digital data.

Now, let us acquaint ourselves with some of the terms used in the Act, before we proceed further to discuss the implications of the Act. 'Personal Data' refers to such data about an individual that enable identifying an individual, 'Data Principal' refers to the individual to whom the personal data relates to and 'Data Fiduciary' refers to the persons processing such personal data. The law is applicable to the processing of digital personal data within India if the data is collected in digital form or is collected in other manner but is digitized later. It also applies to such processing outside India if it is in connection with the provision of goods and services to Data Principals in India. There is a Data Protection Board ('the Board') established under the Act, inter alia, to hear complaints from Data Principals.

'Data Fiduciaries' can process data only in accordance with the Act and for a lawful purpose with the consent of such individuals or for legitimate uses. What is a legitimate use is also given under the Act. This includes, among others, the specified purpose for which the Data Principal has voluntarily shared the data, processing by the State for providing subsidies, benefits, licences, etc., by the State for protecting the sovereignty and integrity of India, for fulfilling legal obligations, for compliance with judgment or decree

and for responding to a medical emergency. It is notable that it can also be used for safeguarding the employer from corporate espionage and protection of trade secrets.

The purpose of processing data, the rights available to the Data Principal, the manner of making complaint to the Board must be specified before obtaining the consent. The consent has to be unambiguous and give clear positive affirmation to use the data for the specified purposes. It shall be limited to the personal data that as is necessary for the specified purpose. Hence, providing e-mail ID or mobile number, may not necessarily mean the giving consent to receive push notifications unless it was specified in the consent. It should be noted that, on a plain reading, affirmative consent is not needed for certain legitimate uses as described above. Further, the consent can be withdrawn at any point of time by the Data Principal. On such withdrawal, the Data Fiduciary shall cease to process such data within a reasonable time. The Data Principal may give and manage her consent through a Consent Manager registered with the Board.

Any Data Fiduciary, be it businesses, professionals or any person handling personal digital data of their customers or other stakeholders, are required to protect such information against data breach and put in place such measures to ensure compliance with the Act. Data Fiduciaries using the service of Data Processors shall also ensure protection of data handled by such Data Processors. The Data Principal has the right to access the personal data that is being processed by the Data Fiduciary and the right to correction, completion, or erasure of such data and have readily available means of grievance redressal.

Any breach of personal data shall be reported to the Board constituted under the Act and the individual to whom the data pertains. Most notably, the Act imposes penalty for data breach, which extend up to Rs 250 crores. The Board is empowered to give appropriate direction to mitigate the risk in relation to such breaches and also to investigate and give appropriate orders in this regard. It also has the power to refer such instances to Mediation between the parties for a settlement.The Act has empowered Central government to issue Rules for implementation of the Act.

Corporates particularly in the service sector are dependent on the personal data of customers to provide services and they should establish clear process and procedures for obtaining and updation of personal digital data of its customers. The consent from Data Principals should be drafted in a manner fair to both the Data Principal and the Data Fiduciary and in a manner that achieves the purpose of the Act. This may be best achieved by seeking professional advice. With the advent of the new Legislation, the Data Fiduciaries have to revisit their Policies and procedures dealing with Customer digital data and shall be ready for implementation as soon as the implementation date will be announced by the Government. Data Fiduciary shall implement appropriate organizational and technical capabilities to ensure that the obligations under the Act are complied with. They will have to identify and report Data breach instances if any, and that too within the applicable timelines. This is more important from the fact that the penalties prescribed under the Act is enormous which cannot be affordable for any type of Corporates. Regarding penalties, clarity is required in cases of multiple breaches, whether the prescribed penalties will be in multiples etc. which will hopefully evolve from the subordinate legislations and further proceedings of the Board.

There are some notable elements in the way in which the law is drafted. In the entire Act, instead of the pronouns, "he", "his", "him", the pronouns "she", "her" is used to refer to individuals irrespective of gender. Further, the Act is drafted in a relatively simpler language with examples paving the way for laws that are more user-friendly. Some ambiguities are there which will hopefully be ruled out in the form of subordinate legislation or legislative amendments. As we await the detailed Rules and Regulations for implementation of the Act, the present norms dealing with data privacy under the Information Technology Act, 2000 and the Rules thereunder will continue and it is likely that the new Act will replace the said provisions. The

compliance cost for the Data Fiduciaries will be on the up at least for a short term till the processes and procedures stabilize over a period of time.

As quoted by Alvin Tofler: "*The illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn and relearn*" and similarly with the advent of this Act, without an element of doubt we can consider that the professionals not having knowledge of Data Protection Regulations will invariably be an illiterate.

■■