International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 2, February 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Data Protection Bill 2019: Participative Role of General Public

N Parmesh

Student, Sastra Deemed University, Thanjavur, Tamil Nadu, India

ABSTRACT

Protection of data privacy is a very crutial aspect considering the advent of technology in every Sphere of human life. It directly depends of how privacy is understood and the legal framework present behind that to protect ones privacy in the way it is meant to be understood. Data protection bill would let us understand the variety of rights and obligation when the question is about protection of ones privacy. At the same time, non- invasion into the privacy of others is also quintessential. The research article would elucidate in detail the matter crux of Data protection bill considering the practical implications of the rules therein mentioned. The author would also deal with the suggestions would help, safeguarding the privacy at the very ground level.

KEYWORDS: *Data, Breach, GDPR, European*

How to cite this paper: N Parmesh "Data Protection Bill 2019: Participative Role of General Public" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-2, February 2020, pp.1101-1103, URL: www.ijtsrd.com/papers/ijtsrd30250.pdf

IJTSRD30250

Copyright © 2019 by author(s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

Meaning of Personal Data breach in legal parlance

According to the definition of the Data Protection bill, personal data breach means any unauthorised or accidental revealing of, acquisition of, sharing of, use of, alteration of, destruction of, loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal.

Although the PDP Bill does not expressly state this, it is likely to be believed that the violation occurred due to the data fidu ciary's inability to comply with the law and to safeguard the Personal data kept by the data fiduciary or by a data process or reporting to the data fiduciary.

Limitation for reporting to the authority for data breach

Subclause (3) of section 25 of the PDP Bill provides that the notice referred to in subsection (1) shall be given by the data a fiduciary to the Authority as soon as possible within the period specified by the regulations laid down by the Authority under the PDP Bill after accounting for any period of time that may be required to take any urgent measures to remedy the situation. After the PDP Bill comes into effect, we expect the government to frame regulations under this section to specify the time period within which the Authority has to be notified by the data fiduciary after a personal data breach takes place. Irrespective of such a time limit, the data fiduciary is obliged to notify the Authority as soon as possible after a breach has occurred.

The Requistites of a notice to be sent to the authority

The Data fiduciary has to send the requistite details which should inculde the following details

A. nature and the kind of personal data which is the subject matter of the breach,
B. details of the data principals who were affected
C. The direct repurcussions of the breach
D. The positive act of the data fiduciary to prevent the data breach

It is very pertinent to note that Sub-clause (6) of section 25 of the PDP Bill states that the Authority may also instruct the data fiduciary to take suitable remedial action immediate and to evidently post the details of the personal data breach on its website. In any event, each data fiduciary is under an obligation to take all conceivable steps after any personal data breach that occurs.

The role of the authority to prevent further data breach

Once the notice is received, the Authority shall check whether such breach should be reported by the data fiduciary to the data principal, considering the nature of the harm that may be possibly caused to the related data principal or if some positive action is to be initiated by the data principal to lessen its effect.

The Authority may direct the data fiduciary to submit the information relating to the personal data breach on the data appropriate website of data fiduciary. The Authority has got the discretion to upload the information relating to the data fiduciary's personal data.

After the authority is brought to the notice regarding the presumed data breach, the reasons for the violation will mostly be evaluated and a positive action will be commenced against the data fiduciary with respect to the applicable laws for any infringement of such laws and the rules concerned.

As said earlier, it is noted that any breach of data of the fiduciary will bring a presumption that the data fiduciary, or any data processor reporting to the data fiduciary, did not succeed to comply with the law and rules concerned and the safeguard the personal data that was held by the data fiduciary or the data processor, as the case may be. The data fiduciary would have to overcome that presumption by providing the Authority with sufficient information to convince the Authority that the infringement of personal data occurred without the data fiduciary, or any data processor reporting to the data fiduciary, in violation of any applicable law or regulation.

Breach of Personal data and failure in reporting it

Pursuant to section 57(1)(a) of the PDP Bill, in the event that The data fiduciary contravenes its obligation to take timely and appropriate action in response to an infringement of data security under section 25 of the PDP Act, such data fiduciary is liable to a penalty which may amount to Rs. 50,000,000 (Rupees fifty million) or 2% (two percent) of its total worldwi de turnover.

Section 57 of the PDP Bill clarifies that the expression "*total worldwide turnover*" can be explained as the gross amount of revenue available in the profit and loss account or any other equivalent statemen from the Distribution, supply and sale of goods or services with refernce to services given, or both, and where such revenue is generated within India and outside India. It further denotes that the total worldwide turnover with respect to data fiduciary would be considered as the total worldwide turnover of the data fiduciary and the total worldwide turnover of any group entity of the data fiduciary wherein such turnover of a group entity evolves as a conseqence of the processing functionalites of the data fiduciary, considering the criterias mentioned below:

Summation of the overall economic interests of the data fiduciary and the group entity; The relationship between the data fiduciary and the group entity conscientiously with respect to the processing activity undertaken by the data fiduciary; or he amount of control exercised by the group entity over the data fiduciary or vice versa, as the case may be.

Comparison with GDPR

Analysing section 33 of the General Data Protection Regulation brings so much value to the subject of privacy. It is noted the section 33 of GDPR is almost similar to section 25 of the PDP Bill. Article 33 of GDPR explains that any breach to be reported without undue and unreasonable delay and where accountable, within 72 (seventy two) hours getting the acknowledgement about it. The point of difference between the provisions of PDP bill and GDPR in this regard it that PDP does not state that the clock will start ticking once the data fiduciary become aware of the breach. Section 25 of the PDP Bill brings a condition that the data fiduciary to notify the Authority as soon as possible after a breach has occurred. The words "as soon as possible" would indiate that the data fiduciary should have gained knowledge of the breach. However, the last deadline (that will be possibly mentioned in the rules to be created) is not subject to the data fiduciary's knowledge. It is possible that the rules to be created will start the timer for the last date from the time the data fiduciary acknowledges the data breach.

Moreover, Article 34 of the GDPR deals with the disclosure of infringement of personal data to the data subject and specifies that, where the infringement of personal data is likely to result in a high risk to the rights and freedoms of natural persons, the controller is obliged to inform the data subject of the infringement of personal data without unnecessary delay. There is no parallel provision in the PDP Bill that mandates the data fiduciary to directly inform a personal data breach to the data principal. The communication that is necessary to be informed directly to the data subject under Article 34 of the GDPR should include the same kind of data information as is required to be reported to the supervisory authority under Article 33 of the GDPR. But Article 34 of the GDPR also says that the communication to the data subject under Article 34 is not mandatory under the following conditions:

A. the controller has executed the most fitting technical and organisational protection methods, and those measures were used to the personal data affected by the personal data breach, with respect to those that make the personal data unintelligible to any person who is not having the permission to access it, it includes encryption;
B. the controller has taken subsequent and successive measures which should confirm that the higher risks which were existnt before are no longer material or
C. if it would include disproportionate effort. During the situation of the communication involves disproportionate effort, Article 34 of the GDPR clearly indicates that there should instead be a public acknowledgement of the information or any other appropirate similar measure whereby the data subjects are effectively informed about the matter.

However, like the PDP Bill, Article 34(4) of the GDPR provide s that where the controller has not already communicated th e violation of personal data to the data subject pursuant to A rticle 34 of the GDPR, the supervisory authority may request that the controller do so.

Under Article 58(2) of the GDPR, the supervisory authority h as, inter alia, the power to issue reprimands to a controller o r processor where the processing operations have infringed t he GDPR provisions and to order the controller or processor to comply with the GDPR provisions, where appropriate, in a specified manner and within a specified time limit.

However, with the provisions of GDPR the supervisory authority does not have the authority to either order the controller to post details of the personal data breach on the controller's website or to post details of the breach on its own website.

Does the GDPR mandate the reporting of data breach

The Information Commissioners Office ("**ICO**"), who is an independent authority set up in the United Kingdom to preserve the information rights in the public interest, encouraging openness by public bodies and data privacy for individuals, on its website provides clarity on what data breaches are required to be disclosed. The website provides the details in the form as mentioned below.

What kinds of breaches to be reported to the Information Commsioners Office?

During the occurrence of ones personal data breach, he/she needs to present the likelihood and seriousness of the risk

that is caused to the rihgts and freedom of the people concerned. Even if there is any possiblity of adverse effect of an act of an individual, the same has to be reported the ICO. If a person decides that he isnt going to report the breach, even for that he need to justify in writing, why does he considers the breach not to be material to be reported.

Article 85 of GDPR reads as follows:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

The below mentioned examples would elucidate in details the repurcussions of privacy breaches by big gaints in their respective industries.

British Airways

The case is relating to customer details of 50000 members of British airways whose personal data was compromised. The details of the incident is reported below.

The case was first brought to light on September 6, 2018. British Airways had informed that 380,000 (three hundred eighty thousand) transactions and the concerned details were revealed but the data did not include passport or visa details. The ICO noticed that a variety of personal data was "compromised" by british airways's poor security features and other administrative lacunas. The revealing of data included payment details, log in and transactionsal details which were alos part of sensitive personal data. The ICO had also clarified that British Airways had been assertive about the improvements and they were very cooperative with the investigation that was conducted by the authority. BA was Fined a penalty of 1.5% (one point five percent) out of its worldwide turnover in 2017 amounting to approximately GBP 183,390,000 (British Pound Sterling one hundred eighty three million three hundred ninety thousand).

Google

Interesting case study about google would reveal the importance of intricate concepts relating to regulation of privacy legislation. When it came to light that Google Inc.'s smart speaker was unintentionally recording and storing user information including converstaions, the data protection commission had scrutinized the reports of a potential violation of its privacy clauses to check for personal data breach at Google Inc. ("**Google**"). Google, as per the guidelines, prepared the breach notification.

Google was ordered to pay 50 millon euros on the basis of complaints from an Austrian organisation and a French non-governmental organisation on May 25, 2018, and May 28, 2018. The same was regarding creation of accounts during the time of configuration process involved in android mobile initiation. Insufficient information and transperancy regarding the data that is stored led to the payment of such huge penalty. The aforementioned fine of € 50,000,000 (Euros fifty million) is the highest fine ever imposed any data protection authority under GDPR till date.

Conclusion

Though there are variety of improvements over technology. It is always found that even ones at the top of its market take undue advantage in either deciphering the privacy details of other companies to improve its own or to compromise the data security system of its own users. Practical application of the rules mentioned in GDPR to avoid the lacunas to produce a discrete framework of law is the need of the hour. Once the shift of therotical application of law into practical parlance would reduce the violations that happen with privact concerns.