EMPOWER DATA PRINCIPALS

Data Principals should be empowered to challenge the unnecessary data collection by Data Fiduciaries.

December 11, 2022

Prepared by:
Poruri Sai Rahul

Empower Data Principals

Data Principals should be empowered to challenge unnecessary data collection by Data Fiduciaries.

The Digital Personal Data Protection Act 2022 (DPDPA 2022) requires Data Fiduciaries to provide Data Principals an itemised notice of personal data sought for collection and the purpose of processing of such data in Section 6 (1).

In Section 7 (8), Data Fiduciaries are prevented from denying service to Data Principals if Data Principals refuse to consent to additional data collection not necessary to a concluded contract.

In addition to these two clauses, we would like the Data Principals to be able to challenge unnecessary personal data collected by Data Fiduciaries in such cases where the data is not necessary for the product or service delivery.

Illustration: 'A' opens a Digital Bank Account with 'X'. Along with the necessary KYC documents, 'X' requests access to 'Phone', 'Contacts', 'Location' and other information from 'A'. 'A' should be able to challenge this additional data collection as unnecessary to the underlying bank account and not provide such information.

Illustration: 'B' requests a personal loan from 'Z'. Along with KYC documents, 'Z' requests additional personal data like 'Messages', 'Location'. 'Z' notifies 'B' that this additional personal information might help them provide a higher loan amount, to which 'B' consents.

For convenience, Data Fiduciaries can categorize personal data into essential and non-essential. This enables the users to opt-in to additional digital personal data collection if it interests them.

Justify digital data collection

Data Fiduciaries should justify why the digital personal data being collected In essential to the service.

In the Notice (See Section 6 of DPDPA 2022) the Data Fiduciaries provide to Data Principals, the Data Fiduciaries should justify, in clear and concise terms, why the digital personal data being collected is essential to the service.

Illustration: 'A' retains the services of an Ambulance Operator 'W'. 'W' requests access to the live location of 'A'. This ensures that 'W' can reach 'A' even when 'A' is unable to guide them to their location.

Illustration: 'B' opens a bank account with neo-bank 'Y'. 'Y' requests access to the Camera on 'B' mobile phone as the Video KYC necessary to open a bank account is done via the 'Y' app. 'B' can optionally choose to remove access to 'Camera' after the Video KYC formalities are complete, if they don't wish to use other 'Camera'-specific functions in 'Y'.

Challenge digital data collection

Data Principals should be able to question why the Data Fiduciaries collect certain digital personal data.

If Data Fiduciaries are unable to justify the digital personal data being collected as essential to provide goods and services, the Data Principal should be able to contact the Data Protection Officer or any other person authorized by the Data Fiduciary for such communication. (See Section 14 on Right of Grievance Redressal).

Problem: Unnecessary digital personal data collection

The industry tends to collect more personal data than necessary for the delivery of goods and services. The purpose of processing of such personal data is an afterthought.

"We have, for instance, seen that some service providers ask for information that they do not need for the main purpose of the service they offer," says Lothar Fritsch, researcher in IT-security at Karlstad University. "They may ask for details while assuring the user that these will not be shown publicly or are protected by a user policy. These details are then used to find out as much as possible about users to enhance their business opportunities, something which is not mentioned in any agreements."

"Data saturation is everywhere. We've often had the belief that more is better; however, that actually isn't true in the case of data. The rapid rise in our ability to collect data hasn't been matched by our ability to support, filter and manage the data. … Too much data with not enough structure in place to manage the data and not enough meaningful application."

"The FTC filed a complaint against Rockyou, Inc., alleging that the company violated numerous statutes by collecting users' email addresses and passwords and storing them in clear text. According to the FTC, Rockyou had no legitimate business need for that information."

Problem: Unnecessary digital personal data collection

"… consumers are becoming increasingly intentional about what types of data they share—and with whom. They are far more likely to share personal data that are a necessary part of their interactions with organizations. … That lack of trust is understandable given the recent history of high-profile consumer-data breaches. Respondents were aware of such breaches, … The great majority of respondents—87 percent—said they would not do business with a company if they had concerns about its security practices. Seventy-one percent said they would stop doing business with a company if it gave away sensitive data without permission."

The industry tends to collect more personal data than necessary for the delivery of goods and services. The purpose of processing of such personal data is an afterthought.

Solution: Unnecessary digital personal data collection

The industry tends to collect more personal data than necessary for the delivery of goods and services. The purpose of processing of such personal data is an afterthought.

The Government could enforce Data Fiduciaries to categorize their personal data collection into necessary and add-on. The notice can contain information about how the add-on data processing will benefit the Data Principal. The Data Principals can then provide consent separately for the necessary and the add-on digital personal data.

For convenience, the Government can choose to exempt certain Data Fiduciaries, depending on how little digital personal data they process, from categorizing their personal data collection.

The Government must enforce all Significant Data Fiduciaries to categorize their digital personal data collection.

Illustration: 'A' makes a dinner reservation at restaurant 'Z'. 'Z' can request digital personal data without categorizing it as necessary and add-on. If 'A' is unhappy, she can choose a different restaurant.

Illustration: 'B' opens a bank account with a major national bank 'Y'. As a Significant Data Fiduciary, 'Y' must categorize the digital personal data they collect into necessary and add-on. 'B' chooses opts-in to the add-on data collection in addition to the necessary data collection.

Outcomes

"Hackers can't steal what you don't have."

Cyber Security is a matter of national importance. Given the involvement of state actors, data breaches should not just be considered a hypothetical. They are in fact inevitable. Efforts to reduce the amount of digital personal data collected by Data Fiduciaries can lead to a significant reduction in risk when a data breach eventually occurs. This is especially relevant in the case of Significant Data Fiduciaries. (See Section 11 of DPDPA 2022).

Reduction in costs to Data Fiduciaries

We expect the categorization of digital personal data as necessary and add-on will lead to a reduction in the amount of digital personal data collected by the Indian Industry. This will directly lead to a reduction in the costs that the Indian Industry bears to maintain the relevant digital infrastructure to store, update, retrieve and operate upon the digital personal data.

Trade-Offs

Increased burden on the Data Protection Board (Board)

Because the proposed alternative allows Data Principals to register a complaint with the Board, the burden on the Board increases. The Board needs to have the relevant expertise to be able to differentiate digital personal data into the necessary and add-on categories for a wide range of applications.

Rulings made by the board on mis-categorization of digital personal data opens a potential avenue for appeals by the Data Fiduciary.

Increased cost to Data Fiduciaries

The need to categorize digital personal data collection into necessary and add-on categories increases the cost of doing business to the Data Fiduciaries.

The reduction of cost due to reduction in data storage should be taken into account when looking at the increased cost of compliance.

Better compliance, while a cost in the short term, might lead to better business opportunities for the Indian Industry in the long term.