Data Protection Journal of India

No: 3/2021: 30th July **2021**

THE VALUE OF DATA

Journal published For

Foundation of Data Protection Professionals in India
[Not for Profit, Section 8 Company limited by guarantees: CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK first Stage, Second Block, Bangalore 560050
Web: www.fdppi.in: E Mail fdppi@fdppi.in: Ph: 08026603490: Mob: +91 8310314516

Publisher: Na.Vijayashankar

(g) the manner for submission of privacy by design policy under sub-section (2) of section 22."

It must be noted that it is regulations to be made and not the rules, meaning that such matters (auditors, privacy by design and DTS) should be directly controlled and monitored by the Authority. The Authority may, by notification, make regulations consistent with this Act and rules to implement the DTS provisions.

Evaluation of fiduciary by Data Auditor

As per Section 29 of the bill, a significant data fiduciary shall get its policies and the conduct of its processing of personal data, audited annually by an independent data auditor. Further the Authority6 have powers vested with them to direct any data fiduciary to get an audit carried out by an appointed data auditor, if they are of the view that the data fiduciary is processing personal data in such manner that is likely to cause harm to a data principal. Therefore we can deduce that it is mandatory for all significant fiduciary to get audited annually and for others, it is the on the performance of fiduciary as observed by the Authority. However such proposals should normally be through written directions that could be part of the regulation.

The parameters to be used by a data auditor to evaluate the compliance of a data fiduciary includes, "(a) clarity and effectiveness of notices under section 7; (b) effectiveness of measures adopted under section 22; (c) transparency in relation to processing activities under section 23; (d) security safeguards adopted pursuant to section 24; (e) instances of personal data breach and response of the data fiduciary, including the promptness of notice to the Authority under section 25; (f) timely implementation of processes and effective adherence to obligations under sub-section (3) of section 28; and (g) any other matter as may be specified by regulations." As this is an inclusive provision similar parameters could be added in the form of regulations, within the principal framework of the bill. It is the responsibility of the Authority to, not only notify the forms and procedures for conducting audits but also appoint persons with expertise in the area of information technology, computer systems, data science, data protection or privacy, possessing such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as it may be specified by regulations, as data auditors under the Act. This provision leads to formation of a new stream of auditors specialised in privacy law and appropriate technology, after due entrance examination and personality tests that could be formulated under the regulations. This is one of the most critical aspects in effective implementation of privacy laws as such auditors are to exercise the responsibilities of compliance audit, followed by assigning DT score of the registered fiduciaries. Now we shall examine each of the above prescribed factors to explore the ways to compute the principles in the proposed DTS.

Issue of notice to principal

We shall examine each of the factors prescribed in Section 29 of the bill to explore the ways to compute the principles in the proposed a fair and justifiable Data Trust Score. Every data fiduciary shall issue a notice to the data principal before the collection or processing of personal data and the contents contained in such form is one of the factors to be considered

to evaluate the trust score. Some factors indicated in section 7(1) of the bill, among others, include the following which are relevant for the present discussions.

"(k) the procedure for grievance redressal under section 32;

(l) the existence of a right to file complaints to the Authority;

(m) where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary under sub-section (5) of section 29; and

(n) any other information as may be specified by the regulations".

From the above it is to be noted that (i) having a grievance redressal as prescribed in section 32; (ii) principal's right to file complaints to Authority and (iii) intimating the data trust score assigned under section 29(5) to the data principal, are the important factors to be considered by the auditor to evaluate the trust score of a fiduciary. To enable higher rating of DTS, it is important for the fiduciary to have a dynamic grievance redressal mechanism in place. At the same time it is the responsibility of the Authority to provide a tool to lodge complaints by the principal and to suitably redress them.

Redressal of grievances of principal

As mandated under section 32 of the bill, every data fiduciary should provide an effective mechanism for redressal of grievances of the data principals. The facility for lodging a complaint by the principal for any contravention of the provisions that has caused or is likely to cause harm to her/him is an essential responsibility of the fiduciary. Such a facility must be managed by the data protection officer or designated officer of the entity. Complaints received have to be resolved by the data fiduciary in an expeditious manner, within 30 days of receipt of the complaint. If such complaints are rejected or not resolved within the time frame, or if the principal is not satisfied with the manner of disposal, the data principal may file a complaint with the Authority. Therefore the Authority is expected to host a separate facility for receiving complaints from principal against such unattended grievances.

As the volumes of transactions are expected to be high, it is expected that these services to the principal could be built by the fiduciary and the Authority together in digital mode. For this development of a central digital facility by the Authority in association with the entities are preferred, as it eases the complaint filing mechanism to the principal, and further monitoring, disposal as well as recording of the entire process could be automated. The quantum of transactions and timelines followed in redressal process could be used as a realistic data source to measure the trust score in respect of each of the fiduciary at one place.

However it is interesting to note that there is no mechanism inbuilt in the bill to obtain feedbacks of the principal.

Privacy by design policy

The second factor to be considered for awarding the score by the auditor is the effectiveness of measures adopted under 'Privacy by design' policy as mandated under section 22 of the bill. The Bill mandates that a data fiduciary is required to formulate policy that (a) ensures

Managerial, organizational, business practices and technical systems designed in a manner to anticipate, identify, and avoid harm to the data principal, (b) meets the listed obligations towards protection of personal data, (c) uses the technology in accordance with commercially accepted or certified standards, (d) protects the legitimate interests of businesses including any innovation is achieved without compromising privacy,(e) protection of privacy throughout the processing, from the point of collection to deletion of personal data, (f) processing of data in a transparent manner and (g) interest of the data principal at every stage of processing of personal data. The data fiduciaries should submit the policy so prepared to the Authority for certification within the prescribed period. The Authority after due verifications of the information and compliance having been provided as prescribed under Section 22(1), shall certify the same. The said information need to be published in the official websites of the Authority and of the fiduciary concerned. This entire process could be built on a digital platform and the emerging data could be used to gauge the trust score.

Transparency and security measures

Transparency in relation to processing activities under Section 23 is the third factor that needs to be considered in awarding the data score. The fiduciary should make available, in prescribed form and manner, the information namely, "(a) the manner and categories of personal data generally collected; (b) the purposes for processing the personal data; (c) any probable risk of significant harm in such processes; (d) the facilities available for the data principal to exercise rights regarding access, correction, erasure, portability and such other rights vested under law; (e) the right of data principal to file complaint against the data fiduciary to the Authority; (f) where applicable, any rating in the form of a data trust score accorded to the data fiduciary under section 29(5); (g) where applicable, information regarding cross-border transfers of personal data that the data fiduciary generally carries out; and (h) any other information as may be specified by regulations."

The fourth factor that needs to be considered is the security safeguards adopted by such entity pursuant to section 24 of the bill. Every data fiduciary and the data processor shall implement and review periodically the necessary security safeguards, such as, "(a) the use of methods such as de-identification and encryption; (b) steps necessary to protect the integrity of personal data; and (c) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data". These could be verified by the auditor who can list out the gaps to arrive at the data score relating to the fiduciary. Similarly the instances of personal data breach and timely response of the data fiduciary, including the promptness of notice to the Authority under section 25, timely implementation of processes and effective adherence to obligations under section 28(3), being the fifth and sixth factors, that could be verified by the auditor to draw fair conclusions.

In this concluding part we shall deliberate on the fair means to use of the mandated principles within the scope of the objectives and the proposed legal framework, to arrive at the possible data score methodology. The author is not inclined to propose a definitive scoring pattern as the bill in hand is still a legislation in the making and more changes are expected before it becomes the law of the land. Once the legislation gets the nod of both the houses, carrying

out such an exercise will be more realistic and useful. Therefore the discussions are limited to the components that should be part of the DTS system.

Objectives of the bill

The Preamble part of the bill declares the purpose of the legislation as, "to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data". It further vouches (i) to protect the rights of individuals whose personal data are processed, (ii) to create a framework for organisational and technical measures in processing of data, (iii) laying down norms for accountability of entities processing personal data,(iv) remedies for unauthorised and harmful processing, and (v) to establish a Data Protection Authority of India for the said purposes. The honourable Supreme Court in the case of Justice K.S. Puttaswamy7 v/s Union of India has held that right to privacy is a fundamental right and therefore it is necessary to protect the personal data as an essential facet of informational privacy. At the same time it is necessary to create a collective culture that fosters a free and fair digital economy, ensuring empowerment, progress and innovation through digital governance. No doubt that the data is the lifeblood of any digital business, but on its abuse, the ultimate losers are the consumers, who may receive an irreversible shock on their private life.

Obligations of the fiduciary

The privacy rights of an individual has to be accomplished for which the data fiduciaries are expected to follow certain obligations stipulated under section 4 to section 11 of the bill. The Bill allows the processing of data by Fiduciaries only after the due consent is obtained from the individual / Principal. For obtaining the consent of a Principal for collection or processing of personal data there is need of issue of a notice by the fiduciary to such person, stating the reasons in clear, concise and easily comprehensible terms. The procedure for issue of notice to the principal, at the time of collection of data8, for obtaining the consent is elaborate and due care to be taken to devise digital tools for meeting the requirements. In the notice the Principal should be informed about the purpose, nature and categories data being collected. The identity and contact details of the data Fiduciary and the contact details of the data protection officer are also to be informed to the Principal. Such Principal should be informed of the procedure to withdraw his consent in the mandated way. Further a personal data can be processed only for specific, clear and lawful purposes. The Data Fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it was processed and shall delete the personal data at the end of processing. The personal data may be retained for a longer period only after the data fiduciary gets necessary consent from the Data Principal. During the compliance audit, it is for the data auditor to comment on each one of these parameters followed by the fiduciary, before proceeding for the quantification of DTS score. The measure so made should indicate the trust factor of the fiduciary in handling the personal data of the principals.

It is pertinent to mention here that the relationship between the principal and fiduciary enshrined in the bill are of special and unique nature. Here the fiduciary should extend a breach-proof mechanism to the personal data owner / principal which are equivalent to safeguarding the fundamental rights of the principal. Therefore the measure applied to score the 'trust-worthiness' needs to be rational and realistic. Efforts should be made to measure directly or indirectly all the stipulated obligations, compliances and functions of the fiduciary, and by using digital tools, wherever possible to meet the meet the requirement of law.

Voice of principal needs recognition

From the above deliberations we find that there are compliances mechanisms and complaint mechanism in place but the crucial element of feedback mechanism is missing in the entire framework under consideration. As stated in the earlier part, the major stake holder or the beneficiary in this entire bill is the principal, but her/his observations about the services rendered by the fiduciary are not provided due place in scoring the credentials of the fiduciary. Further any personal data breach that takes place at the fiduciary's location, through the dark nets may land in the hands of the cyber criminals, who could exploit the data to cause injury to the principal. The safeguards taken by the fiduciary to eliminate personal data breaches protects the principal from being a victim of cyber crime. The satisfaction of the principal about the protection layer provided by the service providing fiduciary is an important element in measurement of trust score. The DTS is supposed to express the trust of the principal as to the level of protection the fiduciary has extended. Therefore the principal's feedback about the satisfaction in the services provided by the fiduciary will be one of the best indicators of mutual trust, the author feels.

Finding fault or gap in services should not be based on the mere observations of the auditor or on sheer outcomes of the complaint mechanism in place. The principal's voice should be heard which deserves a place in formulating the score for the fiduciary. Therefore a feedback system should be legislated wherein the fiduciary should be asked to obtain responses from their principal whenever they provide them with any service. This will also adds value to the review mechanism of the fiduciary.

As per the above deliberations it is clear that there is no provision made in the law for a principal to offer the feedback about the services extended by a fiduciary. This needs to be used as a positive aspect to draw the trust scores, the author observes. A suitable section could be inserted prescribing an effective feedback mechanism and using them to determine the scoring of the data trust.

Authority to be well equipped

Further in a Democratic society like Bharat, to take up the huge responsibility of implementation of this law and the disproportionate issues that could emerge, the Authority concerned should be well equipped in terms of skilful techno-legal manpower along with robust digital platform to be used as e-governance vehicle. As per section 49 of the bill, "It shall be the duty of the Authority to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of this Act, and promote awareness about data protection" which a huge responsibility to be discharged. Further the

responsibilities Authority include, (i) taking prompt and appropriate action in response to personal data breach (ii) maintaining a database and the data trust score on the web, (iii) classification of data fiduciaries, (iv) monitoring technological developments and commercial practices that may affect protection of personal data,(v) receiving and inquiring complaints, (vi) selection of auditors,(vii) prescribing the design by policy and DTS measures, together with registration and regulations of various provisions relating to safeguard the interest of the principals are going to be matters of great concern.

As the task involved is around safeguarding the fundamental rights of a citizen, it becomes all the more important as the Supreme Court and high courts could be directly approached for reliefs. Added to this the technological advancements are on an accelerated mode, so also the information exchanges and communications as well as the cyber crimes. Unless the officials are proportionately equipped with techno-legal skills, the implementation of law may leave huge scar in governing of citizens. The Authority must select officials with requisite technical and legal qualifications only. Such executives are to be suitable trained which is going to be the most critical element for the successful implementation of this new regime.

The section 49(3) requires the Authority to be treated like any other fiduciary as far as the processing of the personal data is concerned. It expressly mandates that, “it shall be construed as the data fiduciary or the data processor in relation to such personal data as applicable, and where the Authority comes into possession of any information that is treated as confidential by the data fiduciary or data processor, it shall not disclose such information unless required under any law to do so, or where it is required to carry out its function under this section”. This is a crucial aspect of the bill that deserves special attention. Further all the central government departments are following the standards prescribed under Service Quality Management System as per IS 15700- SEVOTTAM, which should be made applicable the Authority.

Conclusions

The computation of DTS by the auditor to be fair and justifiable may consist of the following major components:

(1) Outputs from the measurable components like (a) dynamic grievance redressal mechanism; (b) online periodical compliance by fiduciary; (c) reported breaches and remedial action taken along with time frame. etc.,

(2) Outputs from the verification report drawn by the data auditor on subjective issues such as obligations met by the fiduciary, appreciations and deficiencies noticed during the audit etc.,. and

(3) Feedbacks from the principal about the quality of the services provided as against the mandated obligations and the trust she/he could recommend.

(4) The Observations by the executives who are implementing these provisions.

The suggested weightage to obtain the consolidated DTS score form the above four components could be, for first three components, 30% each and 10% for the last. The author welcomes any additional suggestions and ways to measure the trust score so that it becomes the forerunner in the cyber society and the best practices to ensure privacy of the individual.

1 sec. 22(5), PDP bill

2 sec. 7(1) (m), ibid

3 sec. 23(1) (f), ibid

4 sec. 49(2) (c), ibid

5Sec. 29 (7), ibid

6 Sec. 29(7), ibid

7 (2015) 8 S.C.C. 735 (India)

8 Sec.7, PDP bill

Q & A

Here are a few questions that FDPPI has come across recently and some view points from FDPPI team:

Q 1: As per the current legal provisions, who is competent person to provide 'consent' for PII processing of an adult who is mentally challenged/lunatic/person in vegetative physical and mental status.

A: Consent is a contract and the person in a mentally incapacitated state has to be represented by the guardian. Guardian can be a natural guardian or a Court appointed guardian. In case of a natural guardian, it is preferable to obtain a medical certificate about the incapacity.

Q2: What do consider your biggest risk when it comes to data?

a) Hackers

b) Sloppy Third Parties

C) Internal Bad Actors

d) Outdated Policies and Procedures

A: Since penalties for non compliance of Data Protection laws can arise from one or multiple reasons, it is not necessary to rate the different types of risks. All risks are equally important and equally damaging.

Q3: The PDP Bill fends only for economic aspects of Privacy but does not provide for any rights against the state despite it being a fundamental right. How can Government be incentivised to incorporate rights against the State?

A: This is not a correct perception. PDPB2019 includes Government bodies as data fiduciaries. There are however some exemptions under reasonable exceptions provided for fundamental rights under Article 19(2) of the constitution.

Further the heads of departments are liable like CEOs of companies for vicarious liability subject to due diligence protection.

Q 4: Do You foresee any conflict between RTI act and PDP Bill?

A: It is natural. However Right to Information is also a right that is important for individuals in a democracy. It is also required for security reasons of the individual. PDPB 2019 expects that the person responsible for release of information under RTI will conduct a “Harm Audit” and decide if the information may be released.

Q 5: Since the Court hearings are now online and open hearing is the part of the rule of law, how do we balance the right to privacy of the parties against this? Is there a need for specific law to deal with the privacy of judicial data?

A: Privacy is not an absolute Right. It has to survive with other various rights. Citizen has a right to know if our Judiciary which is the key pillar of our democracy is fair and is functioning properly. Online hearing per-se may allow only the litigants and the counsels attend and hence there is no privacy issue..

The move to hold some sessions online with public access is different. It is like a public hearing as compared to an "In-camera" hearing. This is a great move which has to be appreciated. It is educative for the public to know how the Courts are functioning. It will also place the counsels and Judges under public scrutiny. It will perhaps reduce arbitrariness of the Courts and even corruption. Hence it is a move to be appreciated and welcome.