SUGGESTIONS ON DRAFT PERSONAL DATA PROTECTION BILL

A&A DUKAAN FINANCIAL SERVICES PRIVATE LIMITED

(BANKBAZAAR.COM)

September 2018

September 27, 2018

The Joint Secretary,
Ministry of Electronics and Information Technology ("**MeitY**")
Room No. 4016, Electronics Niketan,
6 CGO Complex, CGO Complex,
Lodhi Road, New Delhi – 110 003

Dear Sir,

We thank you for providing us the opportunity to present our suggestions to the Personal Data Protection Bill, 2018.

BankBazaar.com is a neutral online marketplace helping its customers compare and choose financial products such as loans, insurance, credit cards, fixed deposits, saving accounts, mutual funds etc., over its platform. We are headquartered in Chennai and also have our presence in Bangalore, Mumbai, Delhi, Singapore and Malaysia. We are also members of fintech committees of Internet & Mobile Association of India, The Confederation of Indian Industry etc.

Being a law - abiding corporate citizen and being a prominent player in cutting edge fin-tech domain, we treat the privacy and data protection of our customers with paramount importance. BankBazaar is ISO/IEC 27001:2013 certified under certificate number IND17.0322/U. We have also implemented the ISO/IEC 27001: 2013 standard for all processes supporting the development and delivery of services by BankBazaar. We also author many digital reform white papers with Niti Aayog from time to time and have even presented before the Household finance committee of Reserve Bank of India under the chairmanship of Dr. Prof Tarun Ramadorai. We were also invited to put forward our views before the Prime Minister of India at the *'Champions of Change'* Initiative on the theme 'Reforms in the Financial Sector' organized by Niti Ayog on August 21, 2017. We were also a part of the 7th Pre-Budget consultation meeting group with the Ministry of Finance and Corporate Affairs chaired by Mr. Arun Jaitley on December, 2017.

The scope of our suggestions has been limited in terms of the areas of activity and operations in which BankBazaar is involved in. We have put forth our suggestions based on our conjoint reading of the Bill and the Report. Our suggestions are primarily based on the following limbs:

(a)Grounds of Processing of Data; (b) applicability of Bill; (c) purpose limitation; (d) impact of Bill on product and digital innovation; (e) data localisation requirements; (f) right to be forgotten; (g) removal of “Financial Data” from the definition of sensitive personal data; (h) strengthening the autonomy of Data Protection Authority; and (i) allied laws.

Our suggestions mostly revolve around the concept that data protection regulations should complement innovation. New age customers want the convenience of digital finance on smartphones, and government is also working towards greater financial inclusion by encouraging a transparent digital ecosystem. However, restricting the usage of financial data by financial institutions or fintech firms will have an impact on financial inclusion and ability by Financial Institutions to provide life stage based financial product mapping. We request the hon’ble Ministry to acknowledge the anticipated innovations in digital finance domain and consider our suggestions to the Draft Personal Data Protection Bill, 2018 before tabling the Bill before the Parliament.

For A&A Dukaan Financial Services Private Limited

_____

Parag Mathur
General Counsel and Head of Compliance

FEEDBACK/SUGGESTION ON PERSONAL DATA PROTECTION BILL AND REPORT ON A FREE AND FAIR DIGITAL ECONOMY PROTECTING PRIVACY, EMPOWERING INDIANS

S. No.	CHAPTER	SECTION/ HEADING	ISSUES/CHALLENGES	SUGGESTIONS/FEEDBACK
1.	1	3(8) – Definition- Biometric Data	The definition of "**Biometric Data**" includes behavioural characteristics within its ambit. In addition to fingerprints, iris scans, facial images, biometric data has been defined to include "behavioral characteristics". The said term is not defined in the Bill.	We are of the view that inclusion of "behavorial characteristics" will have far reaching consequences. By means of an example, it may affect certain functions dependent on data analytics of behavioral patterns, such as targeted advertisements, recommendations on search engines and other similar services. We recommend removal of 'behavioral characteristics' from the said definition.
2.	1	3(19) Definition – Financial Data	The Bill classifies all financial data as "sensitive personal data". Categorising financial information as sensitive data may have an affect on financial inclusion as well act as a catalyst in the India's pursuit to provide easy access to financial products to all its	Sensitive personal data is the most intimate class of data associated with individuals in data protection laws globally. 67 out of 68 countries studied by the Data Security Council of India do not categorize their financial data as "sensitive" in the Report. This is partly because such an interpretation can stymie innovation by restricting usage. In India's case,

			citizens and become a truly digital economy.	financial innovation such as credit-scoring based on financial data can enhance key objectives like financial inclusion. Private agencies and organisations often have a legitimate interest in an individual's financial information, for example, in relation to providing loans to an individual. Such information is necessary to the functions and activities of agencies and organisations in order to protect the interests of all parties to transactions. Therefore, we suggest that further deliberation is required before taking final decision on inclusion of "financial data" under the ambit of Sensitive Personal Data.
3.		Retrospective Applicability	The Report titled "*A Free and Fair Digital Economy Protecting Privacy, Empowering Indians"* drafted by Committee of Experts under the Chairmanship of Justice B.N. Srikrishna ("**Report**") recommends that the Draft Bill will not	We request the hon'ble Ministry to provide clarity on the aspect of continued processing activities of data sets which were obtained with or without consent prior to the Bill.

			apply to any processing activity completed prior to the law coming into effect. The Bill however is silent on the aspect of such data sets which are applicable under the Bill but would not have historically been collected with consent of a data principal. Thus, for any continued processing, fresh consents may be required to be obtained again from the data principal. This may mean renegotiation of previously concluded contracts. Requesting consent from data principals again at every juncture will result in lengthier notices, disclaimers and formats for ticks or checks, leading to friction and drop-off's midway.	
4.	II	5(2) – Purpose Limitation	The Bill states that personal data of a data principal shall be processed only for	We request the Ministry to envisage the test for determining the "incidental purposes" for which the data

			purposes specified or for any other "incidental purpose" that the data principal would reasonably expect the personal data to be used for, having regard to the specified purposes, and the context and circumstances in which the personal data was collected. The Bill, however does not provide clarity on the incidental purposes for which data fiduciaries may reasonably process or collect the data of a data principal.	fiduciaries may reasonably process or collect the data of a data principal for specified purposes in the Draft Bill. New age customers want the convenience of services on smartphones and policymakers are also working towards greater financial inclusion by encouraging a transparent digital ecosystem. However, restricting the processing of financial data by financial institutions or fintech firms will impact financial inclusion and its ability to provide life stage-based product mapping as the nature of financial products are complex and awareness regarding them is currently low. We also suggest that purpose limitation could create friction and hinder financial institutions in their process to analyse and propose the right product to its customers at the right age.
5.	II	8(1) - Notice	Section 8(1) of the Bill envisages a broad set of information which a data fiduciary is required to	In the Bill when the interest of data principal is adequately protected, the right to revoke consent is available at any

			provide to a data principal at the time of collection of their data.	stage of transaction. Therefore, single consent for multiple transactions or purposes should be allowed if it is explicitly obtained with due notice to the data principal. The criteria mentioned in the Section should not end up in one-standard-fits-all models.
6.	II	9 (1) – Data Quality	Section 9(1) of the Bill states that data fiduciary should take reasonable steps to ensure that personal data processed of a data principal is accurate, not misleading and updated. Making data fiduciary accountable on the accuracy of the data principal's data is onerous since there are few authenticate sources of information available for data fiduciaries to verify a data principal's information provided to them.	The Bill should make the data principle equally responsible and liable for any incorrect data provided by them to a data fiduciary. The Bill already provides "*Right to Correction*" to a data principal (S.25) which will allow them to rectify or update any of their incorrect or outdated information shared with a data fiduciary.

7.	II	Section 10 – Data Storage Limitation	The Bill states that the data fiduciary shall retain personal data as long as may be reasonably necessary to satisfy the purpose for which it is processed	We note that record retention guidelines mentioned under e-authentication guidelines for eSign- Online Electronic Signature Service issued under Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 mandates the minimum retention period for the records provided is 7 (seven) years. [1] We note that the said guidelines are not mentioned in the allied laws section of the Report. We request the Ministry to provide clarity on the said regulations. We also request the Ministry to harmoniously construct the data storage provisions with purpose limitation. This will enable businesses to offer a life cycle based solutions to its customers basis the data which they share, to help them access the right financial product at various stages of life to mitigate financial risk and optimum planning.
8.	VI	Section 25 – Right to	Section 25 of the Bill provides a data principal	The above obligations seem quite onerous on the Data

[1] Rule 2.6(2) of the eSign- Online Electronic Signature Service, Version 1.4 issued on 22 June 2018.

		Correction, etc.	with the right to request a data fiduciary to correct their inaccurate or misleading data. The Bill also places an additional obligation on the data fiduciary "to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion or updating, particularly where such action would have an impact on the rights and interests of the data principal".	Fiduciary as they will be required to bear the burden of communication to the other Data Fiduciaries who may also have an independent relationship with the Data Principal. This information may not be immediately accessible to most Data Fiduciaries, and an industry solution to share such information may have to be developed.
9.	VI	Section 27 - Right to be Forgotten	Section 27 of the Bill also provides Right to be Forgotten to a data principal which shall be determined by the Adjudicating officer basis the request made by them. The Bill does not provide exception on the Right to be Forgotten for investigation purposes. Moreover, Regulation 46 of RBI KYC Master	The Bill should carve out specific exceptions where a data principal cannot exercise their Right to be Forgotten. For example: data is required by investigating agencies for financial frauds which happens days after data sets is collected from a data principal. For example, Regulation 46 of RBI KYC Master Direction, 2016 mandates all Regulated Entities to maintain necessary

			Direction, 2016 mandates each Regulated Entity ("**RE**") to maintain all necessary records of transactions between the RE and the customer, both domestic and international, for at least 5 (five) years from the date of transaction.	records of transactions between the Regulated Entity and the customer for at least 5 (five) years from the date of transaction.
10.	Chapter VIII	Section 40 - Restrictions on Cross-Border Transfer of Personal Data.	Section 40 of the Bill states that a data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data. Each organisation is now required to create an additional layer of infra for maintaining servers in India. Please find our recommendations on the said requirement in the Bill set forth below. The impact of data localisation not only causes higher cost in establishing data centres but also calls for a re-architecture of global based	We request the Ministry to remove data localisation obligation on a data fiduciary since the cost for implementing the same will hamper innovations in digital economy.

			systems which can impact the performance and quality of products and services. In the past, localisation measures have also caused certain companies to leave the market in few jurisdictions. For data localization purposes, an additional category of information is identified, i.e. “critical personal data”, however, this term has not been defined at this stage. We can only comment on the same once we get a clarity from the same.	

----------*----------**