Data Protection and Privacy : Relevance in an Increasingly Digitalised World- Policy Issues[1]

If one were to name the single factor that has driven the most rewarding advancements and technologies during last decade, it will undoubtedly be 'data' – the new global currency. With multi-exponential growth of use and misuse of data, sourced from and targeted at individuals, it will not be an overstatement to say that human beings may almost be reduced to mere datasets in days to come. As data manipulation with human and artificial intelligence assumes the sophistication of genetic engineering-equivalence in a socio-economic milieu, human dignity may be at risk unless looked over. The term 'dignity' is generally associated with human beings, and never with data (unless the 'data dignity' economic model is reckoned). As per the historic 2017 ruling of Hon'ble Supreme Court of India, while 'privacy' was treated as a 'fundamental right' under Indian Constitution, it also recognized 'privacy' as the constitutional core of dignity. This philosophical mooring will be helpful to appreciate dimensions of the subject and nuances of our own Digital Personal Data Protection Act, 2023 (DPDPA). After all, the concept of 'privacy' is said to have been introduced by great philosopher Aristotle in BC era and interestingly, no law so far, GDPR and DPDPA included, has given a precise definition of 'data privacy'. As per a study, there are a total of 157 countries with data privacy laws at the end of 2022, meaning that two thirds (67%) of the world's 232 independent jurisdictions have such laws. If there is a 'privacy' tilt in my remarks today, call it 'imminence bias' in the foreground of DPDPA.

Increasing Relevance of Data Protection and Privacy

2. Often used interchangeably, better understanding of both the terms is required to stabilize the dependence on one at the cost of the other. Conceptually, Security and Privacy are parts of overarching concept of Data Protection, which additionally ensures data availability, immutability, preservation, destruction covering management of the entire lifecycle of data and information. In terms of high-level characteristics, data protection is more technical, process-focused and privacy is more policy/ regulation-focused; having one does not guarantee the other. In terms of sequencing,

[1] Keynote Address by Shri Jayant Kumar Dash, Executive Director, Reserve Bank of India in CAFRAL Program on Data Protection, Data Privacy and Data Localization on September 11, 2023

privacy standards need to be answered first before data protection bulwark can be drawn up– that frontloads the challenges for the data security experts when the privacy laws make a late entry. The responsibility of data protection lies with the banks as institutions, and the privacy responsibility often rests with the users, generally.

3. The relevance of data protection and data privacy is not far to seek in an ever-pervading digital world. As the specie of *homo digitalis*[2] grow and spread, their protection can be only through data protection. The contemporary digital transition can be essentially described as a relationship between digitalization and the economy. When it comes to banking services, they were among earliest adopters of digital transformation. From policy perspectives, security and privacy, as parts of data protection, exist in substantive forms in most of the systems used by them - some are internally driven, and some regulator-enforced. Incidentally, RBI first introduced 'customer confidentiality obligations' on banks in May 2004. However, the notification of DPDPA may need shifts in approach and design, ranging between basic to radical, in the digital systems and channels used. Again, at a philosophical level, the impact of DPDPA may bring profound behavioral changes in the platforms and rails that have been built as part of existing business model. The legislation on data privacy will prove to be more an enabler of business rather than a constraint.

Policy Issues around Data Protection and Privacy

4. Policy issues on data protection and data privacy for banks are multi-faceted, complex and developing - driven by rapid & pauseless advancements in technology, changes in digital consumer expectations, and updates in laws & regulations. Further, the policy issues around data protection and privacy need to be robust, must not be solely regulation dependent for entities in digital financial service business. It bears mentioning that regulatory compliance is always a base line. Many banks have had data breaches despite following 'in compliance' status. Banks must prioritize data privacy and protection to maintain customer trust.

5. That said, policy issues are rarely seen in isolation, without reference to the existing technological legacy and constraints vis-à-vis what the data privacy regime orders.

[2] *Homo Sapiens* usually connote human being connected to each other and things through digital devices after emergence of BigTech, IoT, AI etc; also referred to as post-humans by some.

Hence, for management of banks, it would be appropriate to identify and approach the policy issues in a methodical manner while carving out buffer zones for potential future requirements. I am tempted to preface the policy issues with a gentle judgment that if the significant players in financial service space have not yet done the gap analysis with the provisions of DPDPA and not prepared the 'bill of material' equivalent of all the data assets in the organization through a comprehensive data discovery process, they are already lagging. Many banks could still have a number of disparate, often siloed data sources in their systems without an identifiable data principal. This would also greatly help at consultation stage before rules and notifications are issued.

6. The principle-based regulations has an aura of maturity attached but comes with a long tail. The banks have to be in reediness for having good clarity on many aspects before signing off the policy issues. Personal data, as experts say, could include biographical information or current living situation, looks / appearance/ behavior, workplace or education details, and other private & subjective data. Name by itself is not personal data in some jurisdictions. However, when combined with any other information, it assumes the attributes of personal data. It requires cautious treading in the context of treatment of financial data, the mainstay of banks, as personal or otherwise. The context in which data is discussed and the types that are becoming more prominent have evolved with advances in technology, especially in areas like big data, AI, and the IoT such as metadata, sensor data, contextual data, etc. Segregating personally identifiable information (PII) therefrom needs deep comprehension. Data Fiduciary (DF) will bear the primary responsibility even when processing is done by an agent, thereby signifying availability of a compliant contract. Peer sharing between DFs too would be subject to the provisions of the Act. Who will be treated as Significant data Fiduciary (SDF) among regulated financial service providers is still an open topic. Data flows/ sharing under various regulated activities involving CICs/Information Utilities/ CKYCR etc. or in the context of co-lending or cross-marketing / outsourcing of technology service etc. will need to be seen in light of the rules under DPDPA that is awaited. Possibility of double jeopardy in levy of penalty or treatment of consent taken prior to notification will be other typical areas which may require disambiguation.

Governance and Compliance

7. As for a discrete **Privacy Governance Model**, most of the large banks and NBFCs may already have some kind of IT governance structure - mostly regulator prompted or driven by industry standards. Choosing the right and commensurate privacy governance model is a first policy issue for the management of banks/ NBFCs to address. The key building blocks of the model include developing privacy vision & mission statement, crafting a privacy strategy, evolving relevant policies & standards, developing processes & procedures, positioning the privacy team, choosing the tools & technologies, defining roles and responsibilities, and cultivating right culture & awareness while lending constant management tone and support. These can typically fit into a Three Lines Model consisting of Governance Layer at the head, Monitoring and Control Layer in the middle, and Operational Layer at the ground. However, the exact suitability of any model would be relative to scale, architecture, and complexity of data processing. Generally, centralized authority command and control privacy organization structure seems to be a popular adoption.

8. Under DPDPA, a **Data Protection Officer (DPO)** has been mandated for SDFs, who for all intents and purposes will be figuratively the neck of the SDF under DPDPA. The Act specifies that the DPO would be responsible to the Board of Director, like many control/assurances functional heads as specified by RBI, implying its independence. While Indian law is not as much prescriptive, GDPR outlines some granular aspects to avoid conflict of interest, such as minimum tenure i.e not being an employee on short or fixed term; managing own budget, authority to investigate etc. Hence, positioning her/him in an existing assurance / control vertical, IT or otherwise, would require some strategic thoughts. The DPDPA does not provide for the rule making or qualification criteria for DPOs. However, there are provisions in the Act, such as its responsibility to the board which will ensure that they function in interest of the data principals. It's a priority for DFs to do everything they can, including having a good DPO, to be able to discharge their obligations.

9. Presuming that most banks already have a reasonable **Data Protection Policy**, it will be timely to emphasize on a global **Data Usage and Privacy Policy** to complement and comply. This needs a careful and unhurried refresh and must be treated as a living document for regular updating. For entities having presence in or

multiple data-residency jurisdictions, it may pay to craft the policy in a manner it adopts the more stringent of requirements. Banking groups may also consider the need to align the privacy policy across all the group entities. It must be borne in mind that relevant financial sector regulators have been enabled to build on regulatory requirements on the floor of DPDPA in certain aspects. Inaccurate statement/s of entities about its data processing activities in its Privacy Statements has attracted costly penal action globally. From the DPDPA requirement of the consent given by the Data Principal being free, specific, informed, unconditional and unambiguous, the clarity / simplicity in the privacy policy for intended users gain paramount importance. The DPDPA has practiced it by using simple English without legalese and giving illustration to most of its provisions, not usual with many contemporary statutes.

10. The challenges of **ongoing Privacy Compliance** need to be better assimilated upfront. In the context of a typical organigramme, the 'what's are generally answered by Privacy, Risk and Legal resources while the 'how's are by Compliance, Security and Business resources. A textbook approach to capability maturity model of a privacy compliance program could grow though development of essentially three capabilities viz. foundational, scaling and evolving. At a foundational level, the key components may include data discovery, data classification/enrichment, risk mapping, data record keeping and data retention. The maintenance level of data privacy could cover privacy measurement and reporting framework, data mapping, privacy audit automation, automated impact assessment, incidence response, data residency etc. As the frameworks evolve, adoption of increasing data masking / tokenization, data life cycle governance, analytics and business intelligence, data end-of-life controls might drive a bank / NBFC up in the maturity curve. In the absence of a full-fledged data protection regulator i.e DPB's role essentially being that for post-breach adjudication, the compliance program must be tightly self-driven.

11. From the perspective of a utilitarian approach to privacy compliance, it is important to see the **cost of compliance** relative to the cost of non-compliance. A data breach can cost organizations a king's ransom in business disruptions, productivity loss, revenue loss, penalty and settlement costs etc. apart from potential customer flights. To aggravate, if a bank is breached, it may now face intense regulatory penalties from an array of agencies. The per-breach penalty of ₹250 crore under DPDPA, as profit-at

risk measure may prove to be material even for SDFs of medium size. For banks, the dominant parameters for determining significance as data fiduciary may be the volume of personal data processed and risks to the privacy rights of the customers.

12. To be compliant, the **specific cost overheads** for financial service industry could cover both capital expenses such as investment in data processing systems, specialized tools and technology infrastructure and recurring costs such as policy developments, privacy audits / assessments, incidence response ecosystem, grievance redressal, staff training/ certification, customer communication and awareness etc. A private benchmark study in Europe in December 2017, i e after the GDPR was legislated, found that financial service industry bore the highest cost of compliance among 13 top industry samples. It was also seen that higher the number of employees, the cost has been higher. Techno-legal in nature, the complex data privacy compliance may face the additional challenge with resource deficit in the market due to bunching of hiring. Requirement of consent (even for additional purposes) is built into architecture of the law. The banking industry may have to explore digital tools to reduce technical and financial overload in seeking consent. Consent architecture through consent manager can modularize and ease these exercises.

13. To add to the **complexity of compliance landscape**, DPDPA treats all forms of digital personal data uniformly and is described as horizontal in nature i,e it will work in consonance with other present and future laws and regulations. The untested concept of 'certain legitimate use' (defined under Sec.7) and the reinforced right to withdraw consent assume significant implications for organisations collecting data which bring opportunities as well as challenges. Certain exceptions where consent may not be sought for data processing include investigating offences, schemes of compromise or merger or amalgamation and detection of financial frauds. Data protection regimes for financial service industry in India were generally governed by provisions of IT Act, 2000 and SPDI Rules, 2011 and specifically as per instructions of sectoral regulators. The sensitive personal data included passwords, bank account details, debit/credit card details, biometric data etc. A new right is the right to nomination (Sec 14 of DPDPA) is a pioneering international standard with respect to the rights of individuals in the digital space. The nomination process can be initiated at any time on registration on a platform and can also be changed at any point.

Children and adults with disabilities are clubbed together and special intervention in their consent for platforms and rules will define them granularities.

Technology

14. Privacy by Design (PbD) is an approach that involves originally integrating privacy and data protection principles into the development lifecycle and digital data processing ecosystem rather than adopting a bolt-on or retro-fitting approach. It ensures that the most privacy-friendly settings are applied as the default configuration. While DPDPA has not specifically mentioned about PbD, the major principles of Fair Information Practices (FIPs) such as purpose specification, collection limitation, data minimization and use, retention & disclosure limitations are already weaved into DPDPA. Hence, the future of data privacy compliance lies in conforming to seven foundational principles[3] borrowed from GDPR. These aspects need to be borne in mind for all DevOps. Confidentiality, Integrity and Availability, also known as the CIA triad, is a classic but dated model designed to guide policies for information security within an organization. It may be necessary to marry traditional CIA triad with 'Distributed, Immutable, Ephemeral' (DIE) strategy to encourage security by design and minimize risk, as experts say. With greater dependence technology and automation – CISO's role will assume elevated importance under post-DPDPA time.

15. **Effective security control** would include fine grained access controls, adoption of zero trust security strategy, regular testing and evaluation and continuous improvement. Balancing performance, security with usability is the challenge that must be met. This may typically involve data base exploration, encryption and key management, performance / network engineering, DR/BC. Protection of personal data becomes difficult when co-mingled with non-personal data, as in certain legacy database designs. The importance of discovering data security vulnerability in real time; securing all vulnerabilities to prevent catastrophic breach, bringing in cost efficiency vis-à-vis data protection efficiency in terms of both primary and secondary costs assume significance for banks. Privacy management tools often help banks conduct privacy impact assessments, test processing activities against requirements

[3] (1. Proactive, not reactive; preventive, 2. Privacy as defaults setting, 3. Privacy embedded into design, 4. Full Functionality 5. End-to-end security, 6. Visibility and transparency, Respect for user privacy)

from privacy angles/ regulations, and track incidents leading unauthorized disclosures of personal data. Analysis and documentation of data flows of personal information (e.g nature, processing purpose, data controller etc.), help authoring and of privacy policies distribution and user awareness tracking are some of the functionalities of such tools. Unlike common data-at-rest security controls, **privacy enhancing computation** (PEC) protects data in motion. Privacy enhancing computation techniques for data processing in untrusted environment and multi-party data sharing is emphasized. As per a recent Gartner study, about 40% of privacy compliance technology will rely in AI in next couple of years.

16. In an age progressively adopting Banking as a Service (BaaS) operating model, the **third-party relationship** may undergo redefinition under the intents of the DPDPA as regulations for BaaS evolve. Banks often share customer data with third-party service providers for the purpose of processing. Privacy policy needs to establish rules governing data sharing and ensure that these third parties comply with data protection standards and regulations. DPDPA framework, complemented by Data Empowerment and Protection Architecture (DEPA) of India, where the digital consent is embedded, may add compliance levers the third-party relationship, particularly on platforms.

17. Cross border data flow is another area where the privacy laws play their parts. For banks operating across borders or acquiring customers from across borders, the challenge of compliance with varying data protection laws is enormous. While macro policy tenets would revolve around harmonizing international data transfer rules and agreements, the banks would have to deal with the differences. The DPDPA provisions of cross-border data does not appear to be limiting the application of existing law/ regulation in India that offers greater protection or restraints on transfer of personal data by a data fiduciary outside India.

18. It noteworthy that while the core definition of data remains same, **technological advancements / emerging technologies** have led to new perspectives on how data is generated, collected, processed, and utilized across various domains and use cases. Absence of any specific provisions to govern the emerging technology and tools in DPDPA is unmissable. Generally, AI systems process data that are fed as it is and unless programmed, there would not be clear distinction between processing personal

and non-personal data. The Generative AI does put out disclaimer about not ensuring data privacy. Some banks already use third party conversational messaging platform which uses all types of data. The pervasiveness of AI models and the necessity to train them is the latest addition to privacy concerns. A Gartner study last year showed that 40 % of the organizations had an AI privacy breach and only 25 % breaches were malicious. Usable to improve processes and policies to safeguard privacy, AI can also be misused to breach privacy rights and data protection. Little wonder that the creators of AI are advocating separate regulation for AI.

19. But it is not all gloom and doom. The capability of AI in helping strengthen data anonymization, that protect individuals' privacy by removing PII from datasets, can minimize the risk of re-identification. AI may help develop and improve privacy-enhancing technologies such as encryption, secure protocols, and privacy-preserving algorithms. AI algorithms can also be used to analyze and summarize privacy policies to help individuals understand how their data will be used, shared, and protected. In a privacy-preserving approach called federated learning, model machine training occurs locally on decentralized devices or servers without the need to share raw data. This helps protect sensitive data while benefiting from aggregated insights. With the use of algorithms and AI, concerns about algorithmic bias and discrimination have arisen. As AI and machine learning algorithms are increasingly used to make decisions based on personal data, there's a growing demand for transparency and explainability. Individuals want to understand how decisions that affect them are being made, especially when automated systems are involved.

Users and Customers (Data Principal) Interface

20. The ecosystem of **Customer Consent / Preference Management and Control** under DPDPA will take time to fully develop and evolve. DPDPA explains Consent Manager to be a person registered with the DPB in such manner and subject to such technical, operational, financial and other conditions as may be prescribed. DPB acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform. Streamlined consent processes will be a key factor to alleviate administrative burdens and improve efficiency. The principles of fairness, transparency and accountability

enshrined in the DPDPA should the lodestar for data collection practices. The consent record should ideally be stored and be linked to individual for whom it is obtained. The Consent Manager is accountable to the Data Principal and shall act on her behalf in such manner and subject to such obligations as may be prescribed. More clarity needs to emerge on a data principal's choice of consent manager vis-à-vis those linked to a data fiduciary. The scenario of mid-stream consent withdrawal will have to be tested as well. Section 11 (1) of DPDPA allows the Data Principal the right to request information from a Data Fiduciary, to whom they have previously given consent for personal data processing. These subject rights requests are also referred to as data subject requests (DSRs), data subject access requests (DSARs), or consumer rights requests.

21. It is said, user privacy vs user experience are two sides of the same coin (as long as non-digital), not ends of a single spectrum. Increased consumer awareness of subject rights and transparency expectations would suggest a **centralized privacy user experience** (UX). Bringing together 360 degree of the privacy UX — notices, cookies, consent management and subject rights requests (SRR) handling — into one self-service portal could be a forward-looking approach. By 2023, Gartner predicts, 30% of consumer-facing organizations will offer a self-service transparency portal to provide for preference and consent management. A fully functional privacy center as a central hub can also take care of all complex aspects, have built-in logic to dynamically adapt to privacy regulations, and provides backend orchestration and integration with data systems or app. Though not a legal requirement, they help organize the data privacy protocols and make the user experience simpler and consistent. Data Principal rights require readily available means of **grievance redressal** provided by a Data Fiduciary or Consent Manager in respect of any act or omission regarding the performance of its obligations.

22. The DPDPA promotes the practice of **data minimisation and purpose limitation**, where financial service providers should collect only the necessary data for specific purposes. This helps mitigate the risk of misuse and reduces the potential impact of data breaches. "Specified purpose" means the purpose mentioned in the notice given by the Data Fiduciary to the Data Principal in accordance with the provisions of the Act and the rules made.

23. **Data Retention and Destruction Policy** sets out principles that guide how a bank, employees, and parties interact; how data is captured, stored, or removed. A data retention and destruction policy template determine the data retention period and what happens to that data post retention period. Most data management systems have capability that collect, sort, archive, and delete data based on rules. Automation of data retention and destruction may be the next level. However, more clarity has to emerge vis-à-vis maintenance of records policy of banks guided by RBI regulations, PMLA, under Income Tax Act, Limitation Laws etc. It may still be an open question as to determining when the purpose gets over. System should be able to identify if a datum qualifies to be PII and label it so and recording the purpose for which it is acquired. Consent-based vs. legitimate use basis of data processing may need distinction. While GDPR prescribes record of processing activities, DPDPA has not.

24. The obligations for **incidence response, reporting, notifying** is and will continue to be an onerous responsibility under DPDPA. Compliance with extant instructions (e.g for RBI or CERT-IN) as well as that under DPDPA may require some amount of clarity and work reengineering. Notification to user for data change is a norm in certain jurisdictions.

25. It is said, human errors create levels of vulnerabilities too complex to be managed by machines. Hence **training and awareness** measure for of both employees and customers would be of help. Hybrid engagement models of employees, both the opportunity and desire for increased tracking, monitoring and other personal data processing activities rise, and privacy risk becomes paramount.

Conclusion

26. Any view around privacy is essentially a cultural subject. Until now, the putative data economy was built around a “digital veil” designed to obscure the data-use practices from the customers as well as the law. All the data monetization model of doing business may need a restructure. Data Protection Law is a necessary enabler for the growth, adoption, and acceptance of an inclusive resilient digital ecosystem. Technology has been one of the main differentiators so far among banks in India. It is said that data privacy could be the shape of competitive edge in financial service industry in the next stage, particularly in post DPDPA scene. The trade-off between

personalized service / or customer targeting with data-abundance i.e combining identity data with behavioral data and the principle of data minimization will need fine balancing. The important policy challenges that need to be answered may involve embedding data privacy on the face of increasing scale of data, proliferating end-points, loose data culture, increasing maintenance costs and dealing with evolving regulations / case laws while gaining better visibility into the entire data spectrum. How expensive the exercise for additional personal data or taking consent may become depend on the tools used, though DPDPA does not indicate any specific technology. Compliance for micro finance entity may be a challenge. There would be deep behavioral changes in the way data is processed by data fiduciaries keeping in view the best interest of the citizens. At this stage the preparatory steps that need to be taken by banks /NBFCs are data identification/ classification/ labeling/ purpose-tagging; implementing data retention policy, implementing/ reviewing data disposal policy, performing secure erasure, ensuring compliance with third party vendors and giving due importance to transparency with data principals. Even, an accidental disclosure of data will pose a big risk. For compliance with data privacy laws, it is better to err on the side of caution even after better clarity emerges.

Thank you and wish the seminar a day full of secured deliberations, not necessarily private.

xxxxx