# Guidelines to Build Robust Security Standards for the Financial Technology Sector in India

*Vipul Kharbanda and Cheshta Arora**

**Abstract** *Given the rapid growth of the fintech sector in India and the lack of any national data protection framework, there is an urgent need to arrive at stop-gap measures to ensure robust information security standards for the sector. Owing to threats such as financial data leakages, malware attacks etc., information security standards are central to ensuring business and operational sanctity. We present a set of minimum guidelines, which privilege a co-regulatory framework for the fintech sector, that should be considered when building a regulatory framework for the fintech entities to ensure adequate data protection as well as the growth of the industry.*



## Introduction

Standards provide a mechanism for institutional coordination to ensure that products and services are safe, sustainable and conform to a basic minimum.

---

* Vipul is a non-resident fellow and Cheshta is a Researcher at the Centre for Internet and Society. Parts of this essay are adapted from the Information Technology (Fintech Security Standards) Rules ("Fintech Rules"), 2019 previously published by the Centre for Internet and Society and authored by Vipul Kharbanda and Prem Sylvester.

While standards are crucial for governance, they may not necessarily be legislated top-down by state actors but be negotiated through a diffused system of industry actors, governments, and civil society, for example, the ISO/IEC standards.[1] Although standards can be classified in varied ways, in the context of this paper, it is important to distinguish between network/technical standards and enforceable standards.[2]

The former refer to those standards that incentivize coordination among actors and their enforcement is generally self-incentivized as the actors using the standards benefit from participation in a certain network. The latter i.e., 'Enforced standards',[3] which are perhaps more relevant for our discussion, refers to standards which are used by parties, not due to their self-interest but rather owing to incentives or demands placed on them via a legal requirement or external pressure.

Regulatory policies often cite multiple information security standards as a baseline that is to be complied with in order to ensure the adequate protection of information systems as well as associated architecture.[4] In the context of the financial industry, information security standards provide consideration to the specific risks and threats that financial institutions may face either owing to their inherent data integrity risks, data leakages or malware attacks or due to collaborations between traditional financial actors and new fintech firms,[5] making information security standards an integral part of the process of ensuring business and operational sanctity.

This interest is amplified considerably due to the policy push towards a 'cashless society'.[6] This recent policy push has in part led to the ubiquitous adoption of technology-centric financial services such as *PayTM, PhonePe, Mobikwik* and others. Thus, there is also an urgent economic interest in

---

1 Wang Ping, 'A Brief History of Standards and Standardization Organizations: A Chinese Perspective' [2011] East-West Center Working Papers <https://www.files.ethz.ch/isn/134857/econwp117.pdf> accessed 7 October 2022.

2 Peter Cihon, 'Standards for AI Governance: International Standards to Enable Global Coordination in AI Research & Development' (University of Oxford 2019) <https://www.fhi.ox.ac.uk/wp-content/uploads/Standards_-FHI-Technical-Report.pdf> accessed 18 October 2022.

3 ibid.

4 Karin Höne and JHP Eloff, 'Information Security Policy — What Do International Information Security Standards Say?' (2002) 21 Computers & Security 402 <https://linkinghub.elsevier.com/retrieve/pii/S0167404802005047> accessed 7 October 2022

5 Khakan Najaf, Md Imtiaz Mostafiz and Rabia Najaf, 'Fintech Firms and Banks Sustainability: Why Cybersecurity Risk Matters?' (2021) 08 International Journal of Financial Engineering 2150019 <https://www.worldscientific.com/doi/abs/10.1142/S2424786321500195> accessed 7 October 2022.

6 RBI, 'Payments Vision 2025' <https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=53886> accessed 7 October 2022.

ensuring robust security of the financial technology sector within the country.[7] In the following essay, we present the guidelines and principles upon which rules pertaining to information security standards for the fintech entities could be based. In the first section, we present an overview of the current information security standards in India and their inadequacy at addressing the needs of different fintech entities constituting the present fintech ecosystem. In the second section, we present a minimum guidelines framework,- privileging a co-regulatory approach, upon which such rules pertaining to information security standards could be based.

## I. Information Security Standards in India: An Overview

The current landscape with respect to security standards for financial institutions in India is multi-pronged with multiple standards in place for companies to implement depending upon the sector in which they operate.[8] There may be an assumption amongst some that all fintech entities are governed by the Reserve Bank of India which has a number of detailed guidelines regarding security standards.[9] However, not all fintech entities come under the jurisdiction of the Reserve Bank of India, which can exercise supervisory jurisdiction only as delineated under various legislations, such as the Reserve Bank of India Act, 1934, Banking Regulation Act, 1949, Payment and Settlement Systems Act, 2007, etc. Similarly, the Securities and Exchange Board of India and the Insurance and Regulatory Development Authority only have powers to regulate entities specific to their sectors as specified by various statutory provisions.

The burden of regulating the security standards of fintech entities which do not fall under the regulations issued by the abovementioned authorities falls on the Information Technology Act, 2000, ("IT Act") and more

---

[7] 'At $29 Bn, Indian Fintech Sector now has 14% Global Funding Share: Report' *The Economic Times* (22 August 2022) <https://economictimes.indiatimes.com/industry/banking/finance/at-29-bn-indian-fintech-sector-now-has-14-global-funding-share-report/articleshow/93715347.cms?from=mdr> accessed 7 October 2022; Ashish Rathi, 'Why Cybersecurity is a Priority for Fintech Firms Today - ETCIO' (*ETCIO.com*, 2022) <https://cio.economictimes.indiatimes.com/news/corporate-news/why-apis-are-so-important-for-fintechs/88747660> accessed 7 October 2022.

[8] Aadya Misra and Mathew Chacko, 'Square Pegs, Round Holes, and Indian Cybersecurity Laws' (2021) 2 International Cybersecurity Law Review 57 <https://doi.org/10.1365/s43439-021-00026-7> accessed 18 October 2022.

[9] Cyber Security Framework in Banks, dated June 2, 2016; Reserve Bank of India (Digital Payment Security Controls) Directions, 2021; Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach, dated December 31, 2019, etc.

specifically on the rules issued pursuant to section 43-A of the IT Act, *viz*. the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011 ("SPDI Rules"). Section 43-A of the IT Act requires body corporates to comply with 'reasonable security practices and procedures' in order to avoid liability for negligence in dealing with data causing wrongful loss or gain.[10] *The explanation to section 43-A states that in the absence of a contract specifying the security practices adopted by the body corporate, reasonable security practices and procedures will be those as specified in the SPDI Rules. Unfortunately, even the SPDI Rules do not lay down any specific security standards or protocols but say that entities would be assumed to have implemented reasonable security practices and procedures if they have undertaken measures that are commensurate with the information assets being protected with the nature of business.*[11]

The only specific standards that the SPDI Rules prescribe or refer to are the ISO27001 (or any other standards developed by an industry body which have been duly notified by the Central government).[12] This means that if a body corporate has implemented the ISO27001 standard it shall be deemed to have complied with reasonable security practices and procedures as long as such standards have been certified or audited on a regular basis.

## Need to develop specific information security standards for the fintech sector

The financial sector in India has to date not developed any sectoral security standards that have been approved by the Central government (as required

---

[10] S 43-A provides as under:

"43-A. *Compensation for failure to protect data.*— Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation .....

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

....."

[11] R 8(1) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[12] R 8(2) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

by the SPDI Rules). Meanwhile, the experience of the industry and more specifically fund strapped fintech start-ups, has been that ISO 27001 is an expensive standard for small businesses to implement.[13] Therefore, there appears to be a need for a set of security standards or guidelines that fintech entities can look to implement which are specific and detailed enough to perhaps form a checklist but easier and more economical to implement than the ISO27001 standard.

The crucial need to have information security standards specified primarily for the fintech industry and not for other entities which deal with sensitive and personal data or information is rooted in the structure of section 43A of the IT Act, which provides for monetary damages due to negligence in dealing with sensitive and personal data.[14] It is assumed that losses due to negligence in dealing with financial data would be easier to quantify in monetary terms, and perhaps would affect users in a more direct manner than other forms of data.[15]

Thus, there is a need to create regulations that can specify a set of security standards for the fintech industry. This will guarantee that user data is handled securely and safely, and that smaller companies in the fintech sector have a specific standard to consider in order to minimize their exposure to any potential breaches. Such regulations could be introduced in the form of delegated legislation under the IT Act similar to how the SPDI Rules were implemented. This approach can help bypass the cumbersome and sluggish process of parliamentary legislation. It is crucial that we introduce regulations specifying the security standards as soon as possible, even if just as a stop-gap measure until the goal of a more comprehensive data protection legislation is finally realized – which could take significant time as the new Digital Personal Data Protection Bill, 2022 issued for public consultation is being perceived in certain sections as being too weak.[16] Concerns have been raised over a number of issues such as increased grounds for collection and processing of data under the concept of deemed consent,[17] non-application

---

[13] Yazan Alshboul and Kevin Streff, 'Analyzing Information Security Model for Small-Medium Sized Businesses' [2015] AMCIS 2015 Proceedings <https://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/26>.

[14] (n 11).

[15] Elisabeth Rhyne, 'Consumer Harm from Data Breaches is a Black Box' (Centre for Financial Inclusion, 18 January 2019) <https://www.centerforfinancialinclusion.org/consumer-harm-from-data-breaches-is-a-black-box> accessed 19 October 2022.

[16] Internet Freedom Foundation, 'IFF's First Read of the Draft Digital Personal Data Protection Bill, 2022' (Internet Freedom Foundation, 18 November 2022) <https://internetfreedom.in/iffs-first-read-of-the-draft-digital-personal-data-protection-bill-2022/> accessed 21 November 2022.

[17] S 8, Digital Personal Data Protection Bill 2022.

to offline data,[18] as well as non-automated processing,[19] absence of the principles of purpose limitation and data minimisation,[20] increased powers to exempt State agencies,[21] etc.

This would suggest that there is a possibility of a long-drawn-out process before a more widely acceptable draft of the Bill is agreed upon and before it passes through the various Committees and debates in Parliament, a process which was fatal for its predecessor, the Personal Data Protection Bill, 2019.[22]

## Defining fintech entities

One of the major stumbling blocks when dealing with the fintech sector is the lack of a universally accepted definition of the term. Fintech is generally understood as an amalgamation of "finance" and "technology," but there is divergence on whether the centre of gravity is the former or the latter.

Those that focus on the financial services offered by fintech entities describe technology as an enabler,[23] with the goal to develop "novel, technology-enabled financial services" with the aim to "transform current financial practices".[24] Others describe fintech in terms of the technological innovations that interact with financial services in a variety of ways — specifically, digital innovations and technology-enabled business model innovations[25] and novel technologies adopted by financial institutions to provide more effective financial products and services that bring the sector into the digital age[26] or to enhance the efficiency of the financial system".[27] Fintech, therefore, has

---

18 S 3(b), Digital Personal Data Protection Bill 2022.

19 S 3(a), Digital Personal Data Protection Bill 2022.

20 Gautam Bhatia, 'Why the New Draft Bill must be Reconsidered', (*Hindustan Times*, 29 November 2022) <https://www.hindustantimes.com/opinion/why-the-new-draft-data-bill-must-be-reconsidered-101669731526700.html> accessed 5 January, 2023.

21 S 18(2), Digital Personal Data Protection Bill 2022.

22 'Govt Withdraws Personal Data Protection Bill 2019, to Present New Bill' (Money control) <https://www.moneycontrol.com/news/india/govt-to-withdraw-personal-data-protection-bill-2021-8946661.html> accessed January 5, 2023.

23 Douglas W Arner, Janos Nathan Barberis and Ross P Buckley, 'The Evolution of Fintech: A New Post-Crisis Paradigm?' [2015] SSRN Electronic Journal <http://www.ssrn.com/abstract=2676553> accessed 20 October 2022.

24 Dávid Varga, 'Fintech, the New Era of Financial Services' (2017) 48 Budapest Management Review 22 <http://unipub.lib.uni-corvinus.hu/3170/> accessed 20 October 2022.

25 Thomas Philippon, 'The FinTech Opportunity' (National Bureau of Economic Research 2016) <http://www.nber.org/papers/w22476.pdf> accessed 20 October 2022.

26 Benedict J Drasch, André Schweizer and Nils Urbach, 'Integrating the "Troublemakers": A Taxonomy for Cooperation between Banks and Fintechs' (2018) 100 Journal of Economics and Business 26 <https://linkinghub.elsevier.com/retrieve/pii/S0148619517301431> accessed 20 October 2022.

27 Daniel McAuley, 'What is FinTech?' (Wharton FinTech, 2 November 2015) <https://medium.com/wharton-fintech/what-is-fintech-77d3d5a3e677> accessed 20 October 2022.

three dimensions: an input (namely the combination of technology, organization and money flow), mechanisms (create or improve or change, disrupt, apply technology to finance, create competition on the market) and an output (creation of new services or products or processes or business models).[28]

While the breadth of approaches in the literature to define fintech offer us a broad range of factors to consider, it also makes it difficult to arrive at a comprehensive definition of the same. We agree with Dorfleitner et al. who note that it is not possible to construct a restrictive definition of "fintech" that applies to all of the entities traditionally associated with the term.[29]

However, for the purpose of laying a foundation for understanding its functions and regulatory responses, we define fintech as a broad range of individuals or entities that develop technology-centred products that enhance the functionality of financial services as were typically offered by incumbent financial institutions (including banks & non-banking financial companies).

We do not incorporate in this definition the form such enhancements may take or the motivations for such enhancements as our objective is to present a minimum set of guidelines that all fintech entities would be required to follow. In the case of fintech entities which have an extremely large number of users, or large turnover, or are extremely data reliant, etc., for whom the generic standards may be considered insufficient, a classification may be made, and larger entities could be mandated to comply with stricter prescribed standards or could be required to comply with ISO27001 or other similar standards.

## II. Minimum guidelines framework: Towards a Co-regulatory approach

Legislative mandates may not always be necessary to regulate certain industries or sectors and in some cases, the goals of the legal mandate may be better achieved through self-regulation rather than state regulation, as has been the case for the countries in the Global North.[30] Self-regulation can take many different forms, but at its most fundamental level, it entails a private organization taking responsibility for its own rules and procedures

[28] Liudmila Zavolokina Mateusz and Gerhard Schwabe, 'FinTech – What's in a Name?' (2016).

[29] Gregor Dorfleitner and others, 'Definition of FinTech and Description of the FinTech Industry' in Gregor Dorfleitner and others, *FinTech in Germany* (Springer International Publishing 2017) <http://link.springer.com/10.1007/978-3-319-54666-7_2> accessed 20 October 2022.

[30] Ping (n 1).

and overseeing their implementation as opposed to a government regulator doing the same under the law. This can be accomplished by each organization tailoring its own code of conduct or by any industry body (such as a trade association) developing a common code or set of principles, and by each individual firm modelling its policies for adopting such a code. Such a model of governance, however, has been criticized due to an overall lack of accountability and transparency, the incomplete realization of the principles promulgated in common codes, and weak oversight and enforcement.[31] Nonetheless, reverting back to a command-and-control regulatory model may not be the most efficient approach for many fledgling industries operating with new technologies as 1) the law would not be able to keep up with the latest developments and 2) excessive regulation could stifle the growth of such industries.

A co-regulatory framework, which involves the government and the industry working together to share the responsibility of drafting and enforcing regulatory standards can offer a middle path between self-regulation and government regulation.[32] This allows the government and the industry body to negotiate proper regulatory goals, collaborate on the drafting of standards, and work in a cooperative manner to enforce the standards against firms which violate them. Furthermore, this approach may be better than the traditional regulatory regimes as it tends to 1) draw on industry knowledge and expertise; 2) yield rules that are more cost-effective, workable, and innovative; 3) create a stronger sense of industry's ownership over rules which can lead to better compliance; 4) lead to rules that are politically viable and efficient.[33] Although the SPDI Rules also provide for a co-regulatory mechanism, there are as yet no standards developed by any industry body which have been notified under the Rules.

A co-regulatory model for information security standards may not depend on a licensing requirement, i.e., fintech entities should not have to comply with the rules as a pre-condition to starting operations. In this regard, they could be like the SPDI Rules, i.e., as a measure to be implemented for fintech entities to absolve themselves of any liability against claims of negligence. This means that there could be no legal obligation on fintech entities

---

[31] Dennis Hirsch, 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?' (2011) 34 Seattle University Law Review 439 <https://digitalcommons.law.seattleu.edu/sulr/vol34/iss2/3>.

[32] Hans-Bredaw-Institut, 'Final Report Study on Co-Regulation Measures in the Media Sector' (University of Hamburg 2006) <https://hans-bredow-institut.de/uploads/media/default/cms/media/cd368d1fee0e0cee4d50061f335e562918461245.pdf> accessed 19 October 2022.

[33] Hirsch (n 31).

to comply with these rules, instead, there would be a commercial rationale to do so given the negative cost of data breaches.[34] Moreover, if a fintech entity adopts and implements the standards prescribed in these guidelines then it can legally absolve itself from liability for damages on the grounds of negligence as specified under section 43A of the IT Act. If not, then the entity leaves itself vulnerable to monetary claims for damages.

Thus, there would be an economic case for fintech entities to implement the standards rather than a legal obligation— which allows us to argue for a co-regulatory approach; this approach should ensure that the data of users is well protected while at the same time ensuring that there is no unnecessary burden on smaller players in the fast-evolving fintech industry. If a fintech entity believes that it is too small or deals with extremely small amounts of data, it can take a commercial decision (risk) on whether to comply with the standards at all or follow its own policies. If it chooses the latter, then in case of a data breach, it will have the obligation to prove in court that its policies comprise reasonable security practices and procedures.

Any regulations prescribing standards for information security would have to take into consideration a number of issues, some of the more significant of which are discussed below:

## A. To include fintech entities not located in India

Due to the very nature of the internet, it has become very easy for entities to offer services to consumers across borders. While the capital controls imposed by the RBI do pose certain restrictions in the Indian context,[35] the advent of Web3.0 and decentralised finance (DeFi) poses fresh challenges to the *status quo*. This was most popularly witnessed in the crypto sector where certain exchanges continued to function despite the (now repealed) restrictions imposed by the RBI in April 2018.[36][37] It is therefore important for any regulation dealing with fintech to include within the ambit not only entities established or located within the territorial borders of India but also those which are not located within India but are offering services within India. However, some filtration mechanisms would have to be used to exclude entities that have a minuscule presence or whose activities are not geared towards

[34] Manas Tripathi and Arunabha Mukhopadhyay, 'Financial Loss Due to a Data Privacy Breach: An Empirical Analysis' (2020) 30 Journal of Organizational Computing and Electronic Commerce 381 <https://doi.org/10.1080/10919392.2020.1818521> accessed 19 October 2022.

[35] See generally the Foreign Exchange Management Act, 1999.

[36] WazirX being the most prominent among them.

[37] RBI Circular No. DBR.No.BP.BC.104 /08.13.102/2017-18 dated April 6, 2018.

India to ensure that compliance does not become a burden to commercial activity. The mechanism used in the EU General Data Protection Regulation and followed to some extent in the Consumer Protection (E-commerce) Rules, 2020 could offer useful guidance in this regard.[38]

### B. Definition of Personal Data

The definition of personal data needs to ensure that all aspects of a person's identity whereby the person could be directly or indirectly identifiable should be covered. Although it may not be possible for the definition to be entirely future-proof, it should at the very least take into account existing technology to ensure its own resilience. To illustrate, a few years ago, anonymization of data was considered an acceptable standard of data protection, however, with the decreasing costs of computing power and increased pervasiveness of big data it is now possible to re-identify individuals from different sets of anonymised data and anonymisation by itself may not be considered an acceptable tool for data protection anymore.[39]

### C. An adequate classification of fintech Entities

While strict standards for privacy and data protection would be laudable aims in themselves when dealing with industry and especially a sunrise sector such as fintech, one must be pragmatic and ensure that we do not throw out the baby with the bathwater. Painting all fintech entities with the same brush and imposing onerous obligations on smaller bootstrapped start-ups just because they are offering services to a few clients in the fintech sector and perhaps not even dealing with very sensitive financial data, would not be beneficial to the growth of the fintech sector. In this context, it may be beneficial to classify entities based on various factors such as the amount of money at risk, the type of data being collected, the number of customers, etc. to calibrate the extent of data protection measures that would need to be implemented by the different fintech entities. The regulation could impose different data protection obligations on fintech entities with the security standards to be implemented getting increasingly stricter and stronger with the increase in the number of customers served, value at risk, the sensitivity of the data, etc. The stricter standards could also include obligations such as periodic security audits and updating of the security practices pursuant

---

[38] Art 3, read with Recital 23 of the Regulation; r 2(2) of the Consumer Protection (E-Commerce) Rules 2020.

[39] Imperial College London., 'Anonymizing Personal Data "not Enough to Protect Privacy," Shows New Study' (*Science Daily*, 23 July 2019) <https://www.sciencedaily.com/releases/2019/07/190723110523.htm> accessed 19 October 2022.

thereto. Such an approach would ensure that the regulatory requirements do not act as an entry barrier for further innovation in the fintech sector. A similar approach was used in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[40]

## D. Minimum Data Protection Requirements

While it's important to distinguish between various fintech entities to find appropriate regulatory standards, there ought to be some fundamental data security and confidentiality rules that would have to be observed by all fintech businesses. These basic requirements should broadly adhere to the privacy principles suggested in the Justice A.P. Shah Committee Report.[41] In brief, these principles are:

*Notice:* Fintech entities should give a simple-to-understand notice of their information practices to all individuals before collecting any personal information.

*Choice and Consent:* Fintech entities should give individuals opt-in and opt-out choices with regard to providing their personal information and take their informed consent for collection of the same.

*Collection Limitation:* Fintech entities should only collect such amount of personal information from consumers as necessary to provide the service.

*Purpose Limitation:* Personal data collected and processed by the fintech entities should be adequate and relevant to the purposes for which it is collected. If there is a change of purpose for usage of the data, this must be notified to the individual. After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures.

*Access and Correction:* Customers should not only have access to the personal information about them held by the fintech entity, but should also be allowed to seek correction, amendments, or deletion of such information where it is inaccurate.

*Disclosure of Information:* Fintech entities should not disclose personal information to third parties, except after providing notice and seeking informed consent from the individual for such disclosure.

---

[40] R 2(1)(w) of The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 which uses the concept of a significant social media intermediary.

[41] *Report of Group of Experts on Privacy* (Planning Commission, Government of India 2021) <http://planningcommission. nic.in/reports/genrep/rep_privacy.pdf>.

*Security:* Fintech entities shall employ reasonable security safeguards to secure users' personal information against loss, unauthorised access, destruction, use, processing, storage, modification, deanonymization, and unauthorized disclosure either accidental or incidental or other reasonably foreseeable risks.

*Accountability:* Fintech entities should be accountable for complying with measures that uphold privacy principles. Such measures may include mechanisms to implement privacy policies including tools, training, and education as well as external and internal audits, etc.

*Openness:* Information regarding the steps taken in order to ensure compliance with the privacy principles shall be made available to all consumers in an intelligible form, using clear and plain language.

### E. Option for Co-regulation

A parallel model that could be considered is the development and certification of industry-led data protection standards. As discussed above, such a model could be especially useful as it enables the fintech entities to take into account the peculiarities and specific context of their business operations, whether in relation to a particular product or service category.[42] Simply put, the fintech industry should have the option to develop its own standards of best practices for data protection. The Central Government may introduce a process of getting such industry-developed standards certified by a competent authority to ensure their adequacy in terms of strictness and resilience. Once such a standard is notified for a particular part of the fintech sector, all entities in that sector would have the option to either follow such industry-developed and notified standards or the standards prescribed in the Rules.

### F. Designation of Data Protection Officers

Fintech entities should be required to designate a specific data protection officer to inform and advise the entity and its employees on data protection issues, monitor the implementation and compliance with data protection standards, supervise updates to the data protection policies as well as act as the nodal person for all data protection issues. To ensure that this obligation does not impose too heavy a cost, smaller fintech entities could allow

---

[42] Maximilian Grafenstein, 'Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the "State of the Art" of Data Protection-by-Design' (18 February 2019) <https://papers.ssrn.com/abstract=3336990> accessed 19 October 2022.

the data protection officer to take up tasks and duties other than merely data protection. A similar approach has also been envisaged under the EU General Data Protection Regulations.[43]

### G. No delay in breach notification to customers

In order to maintain complete transparency with regard to the safety of customer data, there should be an obligation on fintech entities to not only report any breaches to the CERT-In as is required by the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 but also inform the customers in case of any breach of customer data without undue delay.

On a final note, while, there are various sectoral privacy and security regulations e.g., RBI's 2018 data localisation circular, RBI's Master Direction on Digital Payment Security Controls, SEBI's Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants, IRDAI guidelines on Information and Cyber Security, these sectoral legislations are limited to the sectors that they govern. They do not cover other important sectors such as e-commerce, crypto assets, etc. This is why a data protection regulation that transcends sectoral limits is needed.

## Conclusion

With the fast-paced growth of the fintech sector coupled with the Government's push towards a cashless and digital economy, there is an urgent need to strengthen the data protection regime for this critical sector. The withdrawal of the Data Protection Bill, 2019 and criticism of the newly issued Digital Personal Data Protection Bill, 2022 means that the enforcement of a comprehensive data protection regime could still be some time away. In this context, it is imperative to bring about regulations to establish a data protection regime for the growing fintech sector before the lack of strong regulations leads to major consumer disasters. As we have argued, such stop-gap regulations would nonetheless have to take into consideration certain basic aspects of data protection such as the privacy principles, the definition of personal data, the inclusion of non-residential actors, co-regulation, proper classification of entities, etc. in order to strike an ideal balance between providing adequate data protection and ensuring the growth of the industry.

[43] Art 38(6) of the EU-GDPR.