The Dialogue™
INFORM ENGAGE IDEATE

NASSCOM®

DPB 2021: THE DATA PROTECTION AUTHORITY AND COORDINATION WITH SECTORAL REGULATORS

THE DIALOGUE - NASSCOM POLICY BRIEF SERIES ON DATA PROTECTION BILL 2021

VOLUME 1 | ISSUE 1

JULY 2022

Authors
Kamesh Shekar, Varun Sen Bahl and Apurva Singh[1]

Design
Diksha Kumari

ABOUT THE POLICY BRIEF

For the past five years, Indian policymakers have been on a path to create a comprehensive data protection law, which will regulate personal data collection, handling, sharing, and processing. Today, these activities are ubiquitous and are engaged in by both public and private sector organisations. They underpin citizens' interactions with data-driven technologies that are commonplace in daily life. It is easy to see, therefore, how such a law, once passed, will significantly reshape both the technology and regulatory landscape in India. There have been three significant efforts to formulate a bill so far, with the most recent one being the (Draft) Data Protection Bill of 2021 (DPB 2021) proposed by the Joint Parliamentary Committee.[2] For stakeholders like data fiduciaries, data processors, data principals and other policy actors, DPB 2021 currently serves as the base for deliberating upon what the final version should look like. There is merit, therefore, in examining its different components, identifying potential bottlenecks, and exploring ways to ease them. To this end, The Dialogue and NASSCOM have come together to author a series of policy briefs analysing specific aspects of the DPB 2021. This policy brief is the first in that series. It focuses on the provisions of inter-sectoral regulation and coordination in the DPB 2021.

TABLE OF CONTENTS

INTRODUCTION

A central component of the DPB 2021 will be establishing the Data Protection Authority of India (DPAI) to enforce the new data protection regime.[3] Given that the effective protection of personal data is necessary for realising the fundamental right to privacy, the DPAI will, in effect, have to act as a new 'fourth branch institution' in India.[4]

This will be a challenging role for the DPAI as it will have to design and enforce standards aimed at realising a fundamental right across a wide range of contexts and sectors – essentially wherever the activities of collecting, using, handling, storing or disclosing personal data take place. These are ubiquitous and high-frequency activities engaged in by both private and public sector entities at an economy-wide and State-wide level, constituting a vast regulated space. When we juxtapose the legacy of low state capacity in India against this role envisaged for the DPAI, it becomes clear that setting up the DPAI will be one of the most significant exercises of establishing a new regulatory system undertaken in India so far.[5]

A major aspect of this exercise will be contending with inter-regulatory harmonisation and coordination problems.[6] In this policy brief, we identify four specific challenges of inter-regulatory harmonisation and cooperation and discuss why they will arise, how they are presently being dealt with under the DPB 2021, and what gaps in the current approach are likely to arise and will need to be addressed going forward. The four challenges in focus are:

1. *Harmonising Existing and Proposed Allied Laws*
2. *Cooperating on Jurisdictional Overlaps and Enforcement Actions*
3. *Ensuring a Uniform and Holistic Appreciation of New Technologies*
4. *Integrating Grievance Redressal Mechanisms*

CHALLENGE 1: HARMONISING EXISTING AND PROPOSED ALLIED LAWS

The DPB 2021 is not India's first effort to regulate personal data. There are various laws and regulations that directly or indirectly apply to the handling of personal data in India. The Committee of Experts on Data Protection Framework for India under the chairmanship of Justice B.N. Srikrishna (**Srikrishna Committee**) had, in their report, identified fifty *allied laws* meriting assessment for complimentary amendments.[7]

Several parallel policymaking exercises that have sought to formulate new frameworks with elements concerning the processing and protection of personal data have been undertaken since the publication of that report. If concluded before the passage of the DPB 2021, they would also add to the above list. This would include, for example, a draft bill on DNA technology,[8] draft policies on health data retention and management,[9] draft policies on open government data,[10] or consent management for collecting personal data.[11]

Given that it will be a special law on personal data protection, the DPB 2021 will prevail in case of any inconsistencies between itself and any of these existing (or proposed) laws. This is easy to say in theory. In practice, however, this could become a complex issue:

- Out of the list of fifty laws, the report of the Srikrishna Committee only analysed the amendments that would be needed to the Aadhaar Act of 2016 and the Right to Information Act of 2005.[12] Both the Aadhaar Act and the DPB 2021 have been modified since that report was published, so the analysis therein would need to be revisited.

- To amend the other allied laws, line ministries would first have to arrive at a common understanding of the DPB 2021 and weed out the overlapping and conflicting scopes and bring them to congruence with a single framework of data protection while enforced in a coordinated way. Different ministries could follow their timelines to complete these processes, creating a scenario where, in different sectors, existing laws could coexist with the more advanced requirements under the DPB 2021; regulated entities may find it challenging to meet both simultaneously. Addressing this would demand a coordinated inter-ministerial effort.

- The DPB 2021 will bring in several relatively novel concepts on which there would be limited prior jurisprudence. Line ministries could unintentionally vary on the interpretations of details or granular issues, such as definitions or different processing principles. This could undermine a primary purpose of introducing a comprehensive data protection law – harmonisation at a national level. At the very least, minimising these concerns would require concerted advocacy and awareness effort within various arms of the State.

The process of addressing these harmonisation problems would require the involvement of several public institutions across the Central Government. Currently, the only policy option to address these harmonisation problems is the one set out by the Srikrishna Committee – that line ministries will conduct consultative exercises within their respective domains. However, significant duplication of efforts may occur without planning, coordination, and sharing of expertise and resources between the different line ministries and regulators. Regulatory uncertainty on how data is being regulated across domains may also arise.[13]

There is value in exploring a more structured approach to harmonisation of these various allied laws. As the Srikrishna Committee noted, while no other law may operate in derogating the DPB 2021, other laws that impose a higher standard for protecting personal data may coexist with the DPB 2021. A structured process of harmonisation could also reveal opportunities for synergy and integration, especially a shared approach towards establishing a risk-based framework, where regulators could work together to assess when higher standards are practically required and what specific additional obligations are required to mitigate specific risks.

For example, sectoral or domain-specific regulators could work with the DPAI to create regulations that cross-reference each other, allowing them to contend with issues falling within their regimes and under the data protection regime simultaneously in a manner that would avoid duplication of legal obligations and provide entities with certainty on the different regulatory regimes intersecting with each other.[14] This could be useful in areas such as cybersecurity, where the DPAI could work with sectoral or cybersecurity regulators to create interlocking regulations on data breach reporting. This process could involve updating existing regulations in specific domains and introducing new regulations under the DPB 2021 that would cross-reference each other, making it easier for regulated entities under dual regimes to comply with both and for regulators to enforce them.

How can a structured approach to harmonisation be adopted? To address this, we may look toward the strategies proposed by the Financial Sector Legislative Reforms Commission (FSLRC), which was tasked with consolidating and harmonising a fragmented regulatory architecture in the financial sector.[15] One strategy of relevance to the problem at hand was the setting up of an ‘interim coordination council’ consisting of existing regulators and line ministries to ensure that the transition

to a single unified financial law could take place smoothly. A similar structure could be explored to ensure alignment between the DPB 2021 and the various existing and proposed laws. In Figure 1, we outline a rough blueprint of a process that such a coordination council could follow.[16]

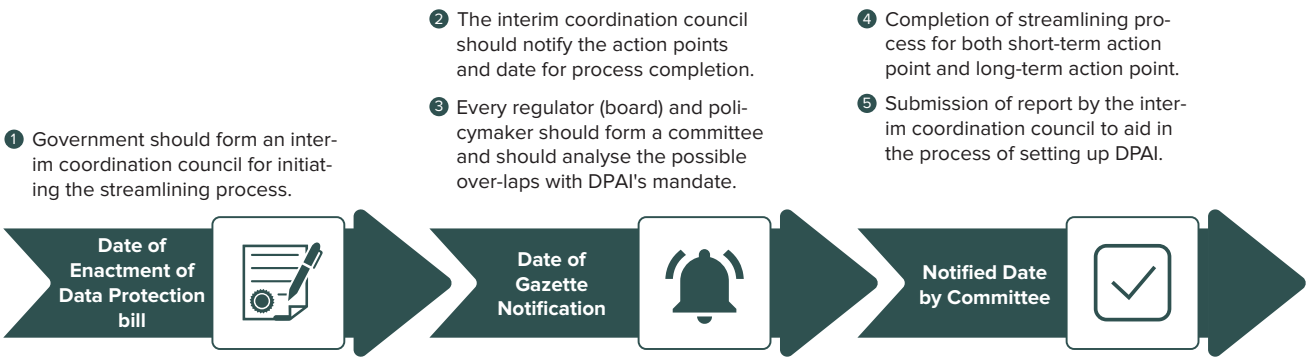

Figure 1: Blueprint for Streamlining Process

The conversation so far has been limited to frameworks at the Central Government. However, State governments and municipal bodies will also have relevant frameworks in place that may have to be amended. For example, some State Governments have policies or laws on protecting personal data, such as under open data policies[17] or whilst delivering electronic services.[18] Municipal governments also process personal data whilst discharging various functions, such as when assessing properties for taxation, collecting payments for taxes, or handling grievances or service requests.[19]

Suppose we are to consider these as well. In that case, the list of 'allied laws' that would be impacted by the DPB 2021 could expand significantly, adding a horizontal dimension to the harmonisation problem. If a structured approach to harmonisation is followed at the Central Government level, this could offer learnings into resolving similar concerns across different levels of government. For this present discussion, we leave the concern of alignment between the DPB 2021 and regulation at the State Government and local government levels out of scope; this issue merits separate examination.

CHALLENGE 2: COOPERATING ON JURISDICTIONAL OVERLAPS AND ENFORCEMENT ACTIONS

Considering that it has been designed as a cross-sectoral regulator, the DPAI will also have to cooperate with several different public institutions regulating different sectors or operating at different levels of government. However, challenges with regulatory cooperation in India have been discussed extensively across multiple domains.[20] One recurring theme has been the need to minimise jurisdictional overlaps between regulators. As has been seen in the past, in some cases, these have often had to be resolved in court or by the Parliament on a case-by-case basis.[21] Examples include conflicts between the Competition Commission of India (CCI) and regulators in the telecommunications and energy sector or between the Securities and Exchange Board of India and the Insurance Regulatory Development Authority of India.[22]

A unique jurisdictional overlap that we can anticipate in the context of personal data protection is its intersection with competition and consumer protection law. We already see scope for overlap between the DPB 2021 and the Consumer Protection Act of 2019.[23] The former includes a general principle that the processing of personal data will be carried out fairly and reasonably, while the latter mentions the unauthorised disclosure of personal data as a type of unfair trade practice explicitly. Similarly, as

regards to the intersection between competition and data protection law, the CCI had, in a report published on the telecom sector in January 2021,[24] analysed the synergy between competition and privacy in a non-price competition market and noted that abuse of dominance could be in the form of lower privacy protection for consumers, leading to sub-optimal privacy standards.[25]

The DPB 2021 does contain a set of frameworks to contend with these challenges:

- **A system of inter-regulatory references:** The DPB 2021 requires the DPAI to consult with any relevant regulator before taking any action. This appears to draw from the Competition Act of 2002, which enables the CCI and other statutory authorities to make references to each other voluntarily.[26] The DPB 2021 goes one step further by mandating that the DPAI consult other statutory regulators before taking any 'action'.

- **A system of memorandums of understanding (MOUs):** The DPB 2021 also states that the DPAI may execute MOUs with other authorities or regulators in areas of concurrent jurisdiction.[27] This concept, which the FSLRC also suggested in the context of coordination between financial sector regulators and the CCI, is a frequently used tool in other countries. For example, the Information Commissioner's Office (ICO) in the United Kingdom has executed different MOUs with both domestic regulators (like those for financial or media markets) and with its foreign counterparts (such as those in the United States, Canada, and Australia).[28]

- **A system for sectoral regulation of 'significant data fiduciaries':** The DPB 2021 also states that *subject to the provisions contained in Clause 56, the significant data fiduciary shall be regulated by such regulations as may be made by the respective sectoral regulators*. This appears to create scope for the DPAI and sectoral regulators to, on a case-to-case basis, use MOUs to designate lead authorities in specific sector to supervise the personal data processing activities of more significant entities.

These frameworks, while useful, are not free from concerns:

- *On inter-regulatory references*, the relevant provision, Clause 56(1), does not define the term 'action', making it difficult to determine when the DPAI will and will not have to consult other regulators. There is also no process for regulators to identify whether or when their jurisdictions overlap in scope or what their jurisdictional boundaries are. Notably, while the DPAI must consult other regulators before taking any action on matters which may also fall within the jurisdictions of the latter set, there is no corresponding obligation on other regulators to consult the DPAI before taking any action concerning personal data protection. The ultimate burden of ensuring harmonisation thus lands on the DPAI without other sectoral regulators having to commit to harmonisation mutually.

- *On MOUs*, the DPB 2021 does not specify what such MOUs will actually contain, or how they may operate, since the current operative phrase – that MOUs shall govern the 'coordination of such actions including economic activities' – is extensive. A second unintended gap is that Clause 56 only considers regulators or authorities constituted under a Union or State law. This appears to preclude the DPAI from entering into MOUs with regulators or authorities not constituted by statute but otherwise potentially seeking to regulate on matters of personal data protection, such as the National Health Authority, which has been created via notification.[29]

- *On sectoral regulation*, as there is no definition of a 'sectoral regulator', it is not clear how this is to be read with Clause 56, which only provides for MOUs with 'statutory' authorities. Further, a system of differentiated regulation within a sector - where the sectoral regulator oversees significant entities while the DPAI focuses on the remaining entities – could create scope for privacy standards to deviate if the regulators are not continuously coordinating.

Across sectors and regulatory domains, these gaps and uncertainties could translate to different regulators following different approaches to understanding privacy risks and concepts of personal data protection, thus creating a fragmented data protection framework.

Though there is undoubtedly often a need for personal data protection to be contextually applied, and for additional safeguards to often be introduced in specific sectors or domains, the DPB 2021 should create frameworks for regulatory coordination and cooperation that can ensure that regulators see the DPB 2021 as an overall standardised and risk-based approach can be followed market-wide. How then can the current frameworks for regulatory coordination be strengthened?

One policy option that has been suggested is to spell out the elements that MOUs under Clause 56 can contain.[30] A review of relevant examples from the United Kingdom suggests that such MOUs usually include the following types of elements that may be considered:

- Information sharing between regulators;
- Cooperation in framing regulations and codes of practice;
- Mechanisms for ensuring inter-regulatory discussions to minimise conflicting supervisory directions and regulations;
- Mechanisms for disclosing and reporting breaches of personal data;
- Processes for inter-regulatory references for sectoral regulations;
- Coordination in conducting awareness-related activities.[31]

A second option, one that has not been contemplated under the DPB 2021, but found in other regulatory systems in India, is that of *interlocking directorates*. Here, representatives from one regulator (including from a ministry or department) sit on the board of other regulators who have connected mandates, thereby serving as a coordination and cooperation mechanism. For example, the governing board of the Insolvency and Bankruptcy Board of India has representatives from the Reserve Bank of India and the Ministries of Corporate Affairs, Finance, and Law & Justice.[32]

The limitation with this approach in the context of the DPAI is that the set of different regulators it would have to coordinate with is very wide, making it difficult to rely exclusively on interlocking directorates. However, the underlying idea,[33] enabling representatives of different regulators to collaborate with each other closely can still be explored.

Different examples of coordination committees have been set up in India today to achieve this purpose. A prominent example is the Financial Stability and Development Council (FSDC), which consists of the Governor of the RBI and representatives from various regulators in the financial sector,[34] whose primary mandate is to enhance inter-regulatory coordination. Another example is the Forum of Indian Regulators, which has been set up by various regulators in the electricity sector and now has representatives from the Telecom Regulatory Authority of India and the CCI involved as well. This body, although registered as a society and with no legal mandate, serves to help participating regulators share best practices and work on common strategies to adapt to new regulatory challenges. There are also several case studies from other jurisdictions to learn from:

- **Europe:** A prominent and relevant example is the European Data Protection Board (EDPB), which was formed for harmonisation.[35] This independent body, comprising of representatives from national data protection regulators and the European Data Protection Supervisor, regularly works on clarifying and promoting a common understanding of European data protection laws, as well as regularly issuing opinions and advisories on complex matters such as adequacy decisions.[36]

- **United Kingdom:** Four regulators – the Competition & Markets Authority, the Information Commissioner's Office (ICO), the Financial Conduct Authority, and the Office of Communications – have also come together and established a Digital Regulation Cooperation Forum (DRCF) to support regulatory coordination and cooperation on online services and digital markets.[37] Every year, they publish detailed work plans and annual reports spelling out how they aim to achieve three goals: regulatory coherence, collaboration, and capacity-building.[38]

- **Australia:** Four regulators – the Australian Competition & Consumer Commission, the Communications and Media Authority, the Information Commissioner, and the eSafety Commissioner, have formed a similar Digital Platform Regulators Forum to drive collaboration on, amongst other matters, consumer protection, online safety, privacy and personal data protection, and their intersection.[39] This forms a collective of diverse regulatory perspectives. This also enables a one-stop-shop for government policymakers to engage with regulators on issues pertaining to digital platforms, ensuring consistency in digital regulation.

- **Brazil:** The National Authority for Data Protection has established a national council comprising experts and representatives of multiple stakeholders, including civil society, academia, and public sector bodies, to provide technical and operational guidance on the application of the Brazilian data protection law.[40]

The above examples suggest that there is merit in exploring the establishment of a formal body, such as a data protection board,[41] that would focus on building a harmonised understanding of data protection laws and encouraging regulatory coordination. Such a body could serve roles similar to those performed by the various coordination bodies that have been set up in the jurisdictions discussed above, such as the DRCF in the UK or the DPRF in Australia, as well as by the expert council system in Brazil.

CHALLENGE 3: ENSURING A UNIFORM AND HOLISTIC APPRECIATION OF NEW TECHNOLOGIES

In recent years, multiple authorities in India have sought to leverage 'regulatory sandboxes' as a valuable tool to determine how to calibrate regulatory systems vis-à-vis technological developments within their domains. We have seen sandboxing frameworks endorsed in India across domains and levels of government. So, for example:

- The International Financial Services Centres Authority (IFSCA) has recently, in 2022, constituted the IFSCA FinTech Regulatory Sandbox for testing FinTech innovations.[42]
- The Reserve Bank of India (RBI) has, since 2019, run a regulatory sandbox regime to allow businesses seeking to introduce new innovations in financial services.[43]
- The Insurance and Regulatory Development Authority of India (IRDAI) runs a regulatory sandbox to encourage innovations that can deepen insurance penetration in India.[44]
- The Securities and Exchange Board of India (SEBI) also runs a regulatory sandbox to promote innovations in the securities market.[45]
- The Karnataka Government has established a new Karnataka Innovation Authority that shall run a sandbox mechanism for start-ups and businesses to test innovations.[46]

We note that the DPB 2021 also envisages the DPAI operating a sandbox mechanism, which shall encourage innovation in *artificial intelligence, machine learning or any other emerging technology in public interest*.[47] This currently poses some challenges:

- The risks and regulatory difficulties with such 'emerging technologies' can only be fully appreciated in the specific context in which they are employed. For example, the risks posed by a machine learning algorithm for a credit scoring system are very different from those posed by one for traffic prediction. Thus, the DPAI may have to source sectoral or context-specific expertise to run a sandbox effectively.
- On the flip side, while the DPAI seeks to evaluate specific innovations viewed through the lens of privacy and data protection, other regulators may also be exploring those innovations through their sectoral or domain-specific lens. This may not be the most efficient approach, due to the risk of duplication of efforts, and would make it more challenging to holistically examine the risks posed by innovation.
- The operation of distributed and parallel sandboxing mechanisms by different regulators would also create complexities for businesses seeking to explore new technologies. They may have to approach different regulators to seek exemptions under distinct regimes for the same new technologies. This could cause roadblocks to start-ups regarding additional cost and hindrance to service/product development. The lack of uniformity in the framework and format of the sandbox mechanism adds to the compliance cost. Also, fragmented approvals of a cross-sectoral innovation could slow down market adoption.

We see value in examining whether the DPAI can collaborate with different regulators and authorities to run *integrated* sandboxes that can allow innovations to be evaluated collaboratively. A similar approach has already been suggested in the context of the financial sector to support fintech innovations.[48] To establish an integrated sandbox with a data protection dimension, the DPAI could enter into specific MOUs with other regulators and adopt a principle-based framework that would guide the operation of the sandbox.[49]

In practice, this could involve innovations being proposed by entities classified as data fiduciaries under the DPB 2021 being tested against a horizontal set of principles (consolidated from DPB 2021) and by an additional framework developed by the DPAI in coordination with other sectoral regulators. Some indicative critical principles regarding technology and data protection to be part of the framework are illustrated below. The principles discussed in the illustration are the key universal and internationally recognised data protection and design principles embedded in various data protection regulations across jurisdictions,[50] including India.[51]

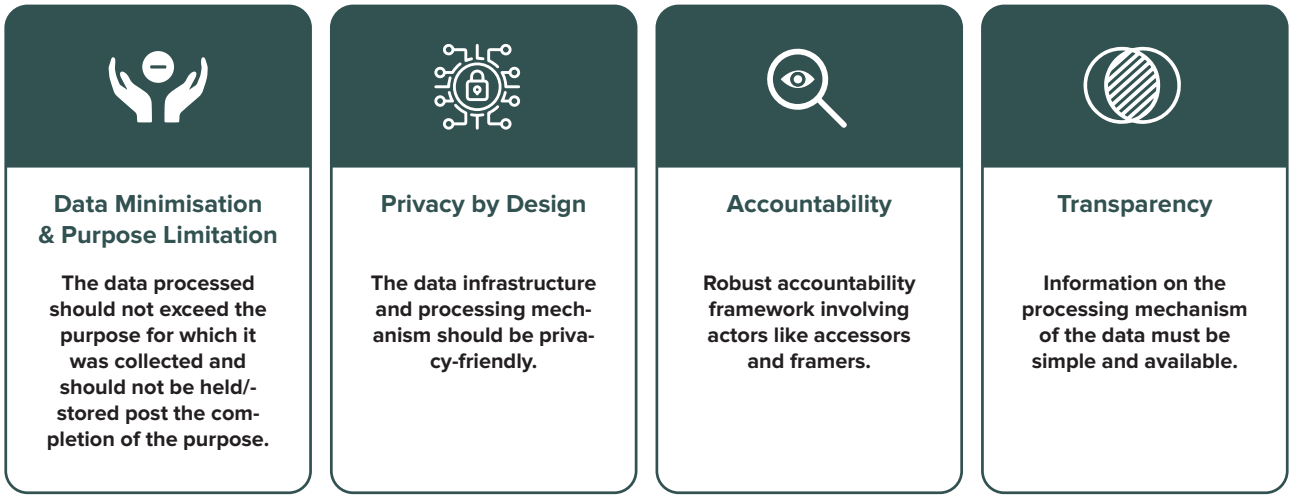

Figure 2: Principles to be a Part of the Sandbox

CHALLENGE 4: INTEGRATION OF GRIEVANCE REDRESSAL MECHANISMS

The DPB 2021 places significant emphasis on grievance redressal and affords the data principal two key rights in this regard. First, is the right to seek redressal against a data fiduciary in cases involving the non-enforcement of the data principals' rights (under Clause 21). Second, is the right to seek compensation by applying to the DPAI (under Clause 65), who then funnels those applications to an Adjudicating Officer (AO) appointed by the DPAI.[52] Finally, under Clause 64 (7), the DPB 2021 provides that any person aggrieved by an order made by the Adjudicating Officer can approach/ appeal to Appellate Tribunal.

These are valuable frameworks. However, there is scope for improvement. Under the DPB 2021, the DPAI is expected to set up AOs to handle penalties or award compensations. We also see that the DPAI will be tasked with other adjudicatory functions – such as hearing complaints from data principals regarding their data subject rights. Within the DPAI structure, this can be streamlined by pooling all adjudicatory functions into the AO system so that AOs act as single points of execution of such functions. This would better secure operational segregation between redress and regulatory functions. It may also lead to better outcomes for consumers, since those with judicial expertise best discharge adjudicatory functions.

We also note that the grievance redressal mechanisms under the DPB 2021 will, once established, co-exist with several other such mechanisms found under other current laws and regulations. For example, intermediaries under the IT Act must appoint a grievance officer and provide a mechanism for users to file complaints;[53] account aggregators[54] or e-commerce entities[55] must appoint a grievance redressal officer and put in place a policy for disposal of customer complaints. The co-existence of these frameworks suggests a strong emphasis on consumer grievance redressal, especially in the context of digital technologies. This is welcomed in principle. However, a fragmented approach can create challenges, including:

- Consumers may find it difficult to determine when to approach one channel over the other. There could also be differences in approach and processes, potentially creating stress for consumers as they navigate multiple mechanisms.

- Entities and regulators operating multiple redressal mechanisms in silos may not be the most efficient approach to resourcing. This can also diminish agility on resolution.[56]

- Without mechanisms for knowledge and experience sharing across systems, different redressal systems could end up working in silos without learning from each other. For example, those handling e-commerce complaints could benefit those handling data principals' grievances.

It is useful here to note the observations of the Task Force on Financial Redress Agency (TFFRA). Their report provides a step-by-step implementation plan to operationalise a redress forum for retail financial consumers.[57] Here, for now, we note that there is value in exploring a more calibrated approach to grievance redressal.[58]

The DPAI could leverage MOUs with other regulators to set up a more integrated grievance redressal mechanism, where the different regulations align in terms of the approach and design. Drawing from the literature on a 'responsive regulation' approach and the recommendations of the TFFRA,[59] we note below some design features that may be considered:

- **Access:** To enable a customer-friendly and accessible approach, grievance redressal mechanisms should incorporate technology-intensive processes and minimise the need for physical hearings. E.g., consumers could be facilitated access to interactive voice response systems available in multiple languages and modes of communication to navigate the grievance redressal mechanism and also to make complaints.

- **Harmonisation at the entity level:** The various obligations imposed on entities to implement grievance redressal systems should be harmonised in terms of point of contact and receipt and redressal timelines. Entities should also be required to provide easily accessible information on how consumers may raise grievances.[60]

- **Online dispute resolution:** The DPAI could, in conjunction with other regulators, operationalise an online dispute resolution (ODR) platform to reduce the overall burden on the redressal system. In any ODR processing, a mediator would be assigned to the dispute, setting up a mediation stage. So, for example, under the DPB 2021, a data principal could reach out to the ODR platform if their complaint was not redressed at the data fiduciary-level. Singapore follows a similar approach under its Personal Data Protection Act of 2012, where under Section 48G, the Singapore Data Protection Commission can refer any complaint by an individual to mediation for resolution if they deem that appropriate. If the dispute would not be resolved even at this platform, then it could be escalated by the ODR platform to the AO. A key mechanism for the platform's success would be its ability to distinguish between low-value simple complaints and relatively complex ones. Creating this mechanism would require a strong feedback loop, trained staff and good use of technology. Such a mechanism could help fast track resolution of most of the complaints. An integrated ODR platform could be operationalised across different regulators, where the ODR platform would be responsible for escalating the complaint to the relevant next stage.[61]

- **Coordination at the regulator-level:** Currently, to handle appeals from disputes regarding grievances raised at the entity level, different regulators set up their own systems.[62] Under the DPB 2021, for example, this would be the job of the AO appointed by the DPAI. Through the MOUs, the DPAI and other regulators could set up processes for these different systems to

speak to each other. So, for example, an AO hearing a dispute involving matters under other laws could coordinate horizontally with the relevant judicial authority responsible for similar functions under those laws (such as a consumer court in the context of e-commerce or an ombudsperson in the context of financial regulation). This could allow for better resolution of disputes that involve complex matters stretching across regulatory frameworks.

We offer a diagrammatic representation[63] of the above suggestions in Figure 3 below.

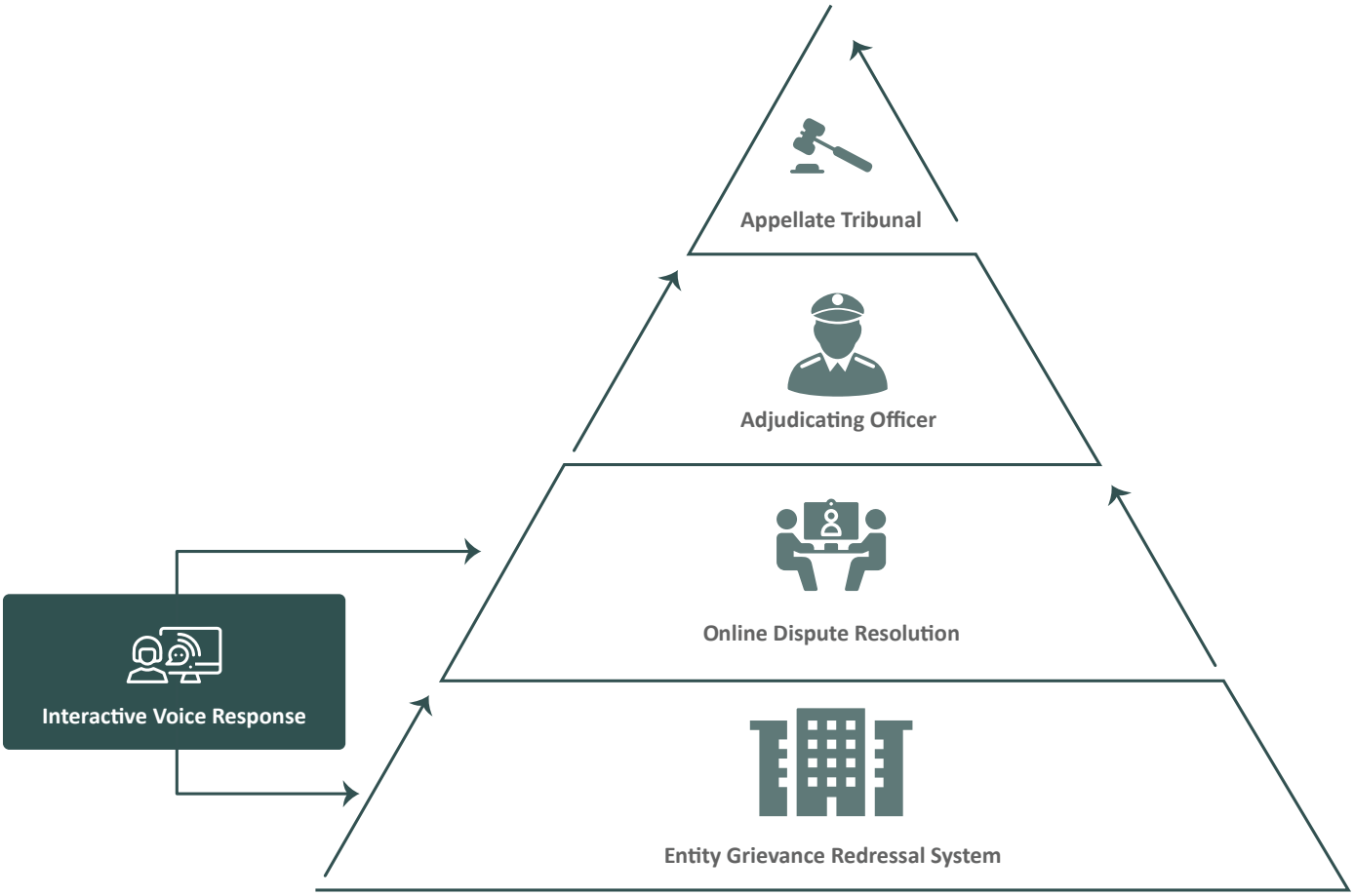

Figure 3: A calibrated Grievance Management System

CONCLUSION

As we are on the cusp of enacting India's Data Protection regime, next in the pipeline is to establish the Data Protection Authority of India.

Since technology cuts across multiple sectors, privacy and data protection are both vertical (across sectors) and horizontal (across the size of the business) in nature. This will be a challenging role for the DPAI as it will have to design and enforce standards aimed at realising a fundamental right across a wide range of contexts and sectors – essentially wherever the activities of collecting, using, handling, storing or disclosing personal data take place. A major aspect of this exercise will be contending with inter-regulatory harmonisation and coordination problems.

In this policy brief, we identified four specific challenges of inter-regulatory harmonisation and cooperation and discuss why they will arise, how they are presently being dealt with under the DPB 2021, and what gaps in the current approach are likely to arise and will need to be addressed going forward. The four challenges focused are *(a) harmonising existing and proposed allied laws (b) cooperating on jurisdictional overlaps and enforcement actions (c) ensuring a uniform and holistic appreciation of new technologies (d) integrating grievance redressal mechanisms*.

Therefore, as the envisioned DPAI is likely to have a crucial role in this digital age, we believe it is essential to address the aforementioned inter-regulatory harmonisation and coordination problems, as well as find solutions for the bottlenecks discussed.

ENDNOTES

1 The Authors are, respectively, Programme Manager – Privacy and Data Governance Vertical at The Dialogue, Manager-Public Policy at NASSCOM and Senior Associate-Public Policy at NASSCOM. We thank Kazim Rizvi and Ashish Aggarwal for their inputs & feedback. Authors can be reached at: kamesh@thedialogue.co; Varun@nasscom.in; Apurva@nasscom.in

2 The DPB 2021 is contained in the Appendix of the Report of the Joint Committee (JPC) on the Personal Data Protection Bill of 2019 (PDP 2019) presented to the Lok Sabha on 16th December 2021 (JPC Report). It builds on the PDP 2019 that had developed by the Ministry of Electronics and Information Technology (MEITY) by modifying the Personal Data Protection Bill of 2018 (PDP 2018), which had prepared by the Committee of Experts under the chairmanship of Justice Sri Krishna (Sri Krishna Committee) and accompanied their Report on a "Free and Fair Digital Economy" (Sri Krishna Report).

3 See clause 49(1), DPB 2021.

4 A fourth-branch regulator is an institution or agency charged with protecting the constitutional democracy through influencing and acting and the other three branches of government (that is, the legislative, the executive and the judiciary). Examples of the existing fourth branch regulators include the Election Commission of India, the National Human Rights Commission, etc. See, Bulmer, E., *Independent Regulatory and Oversight (Fourth-Branch) Institutions*, International IDEA, (2019), available at: https://www.idea.int/publications/catalogue/independent-regulatory-and-oversight-fourth-branch-institutions; Bhatia, G., Fourth Branch Institutions, Indian Constitutional Law and Philosophy, (2021), available at: https://indconlawphil.wordpress.com/category/fourth-branch-institutions/.

5 *See, for example*, L. Panda, *The Weight of Secrets: Assessing the Regulatory Burden for Informational Privacy in India*, INDIAN JOURNAL OF LAW AND TECHNOLOGY, (2019); S. Tyagi and A. Burman, *Banking to groceries — Data Protection Authority has multi-sector role*, but must be efficient, THE PRINT, (2020); S. Rai, *A Pragmatic Approach to Data Protection,* THE LEAP BLOG, (2018).

6 Shekar, K. (2022). Building Effective and Harmonised Data Protection Authority - Strategies for Structural Design and Implementation, THE DIALOGUE, (2022), available at: https://thedialogue.co/wp-content/uploads/2022/04/Building-Effective-and-Harmonised-Data-Protection-Authority-Strategies-for-Structural-Design-and-Implementation.pdf.

7 *See* Annexure C, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, (2018) ('Srikrishna Committee Report').

8 *See* Parliamentary Standing Committee on Science and Technology, Environment, Forests and Climate Change, *Report on the DNA Technology (Use and Application) Regulation Bill, 2019*, 340th Report, (2021).

9 For a discussion on the overlap between these proposals and the DPB 2021, see Shekar, K., & Vaidya, E. (n.d.), *Response to Health Data Management Policy 2.0*, The Dialogue, (2022), available at https://thedialogue.co/wp-content/uploads/2022/05/Health-data-policy-response.pdf; NASSCOM – DSCI, *Feedback to the National Health Authority on the Consultation Paper on the Proposed Health Data Retention Policy*, NASSCOM – DSCI, (2021), available at https://old.abdm.gov.in/assets/uploads/commentsdocs/datapolicy/Varun_NASSCOM42.pdf.

10 For a discussion on the overlaps between the DPB 2021 and such policies, see Shekar, K., & Venkatesh, K. (n.d.), *Our response to Draft India Data Accessibility and Use Policy*, The Dialogue, (2022), available at: https://thedialogue.co/wp-content/uploads/2022/04/Response-to-Draft-India-Data-Accessibility-and-Use-policy.pdf , Bahl, V., Singh, A., & Selvaraj, J., NASSCOM *Feedback on the Draft India Data Accessibility and Use Policy*, NASSCOM, (2022), available at: https://community.nasscom.in/communities/policy-advocacy/nasscom-feedback-draft-india-data-accessibility-and-use-policy; Bahl, V. & Singh, A., NASSCOM-DSCI *Feedback on the Draft National Data Governance Framework Policy*, NASSCOM, (2022), available at: https://community.nasscom.in/index.php/communities/policy-advocacy/nasscom-dsci-feedback-draft-national-data-governance-framework-policy, Shekar, K., & Vaidya, E. (n.d.). *Response to Health Data Management Policy 2.0*. The Dialogue. Retrieved June 9, 2022, from https://thedialogue.co/wp-content/uploads/2022/05/Health-data-policy-response.pdf.

11 *See*, for example, the Draft Non-Personal Data Governance Framework; the Guidelines for democratising the existing geospatial data and maps; NITI Aayog's Data Empowerment & Protection Architecture; the National Digital Health Mission: Health Data Management Policy; The India Digital Ecosystem of Agriculture (**IDEA**); the India Data Accessibility and Use Policy, etc.

12 *See* Srikrishna Committee Report, page 98.

13 *See* Mungan, C., *Seven Costs of Data Regulation Uncertainty*, Data Catalyst, (2019).

14 For a discussion on the concept of regulators cross-referencing regulations, see Perrin, W., Woods, L., *Online Harms – Interlocking Regulation*, Carnegie UK Trust, (2020) available at:https://www.carnegieuktrust.org.uk/blog-posts/online-harms-interlocking-regulation/.

15 *See*, Ministry of Finance,*Report of the Financial Sector Legislative Reforms Commission – Volume I*, (2014), available at https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf.

16 Suprat *Supra* note (vi).

17 *See*, for example, Government of Tamil Nadu, Tamil Nadu Data Policy, (2022).

18 *See*, for example, the Andhra Pradesh Core Digital Data Authority (Effective Delivery of E-Services) Act, 2017.

19 For a discussion on the collection of personal data by urban local bodies in India, see C. Vaishnav et.al., *How Public Should Public Data Be? Privacy & E-Governance in India*, MIT Internet Policy Research Initiative, (2018).

20 *See*, for example, in the context of policies for micro, small and medium enterprises, Ministry of Corporate Affairs, *Report of the Committee for Reforming the Regulatory Environment for Doing Business in India*, (2013), available at: https://www.mca.gov.in/Ministry/annual_reports/DamodaranCommitteeReport.pdf; in the context of financial sector regulation, see Ministry of Finance, *Report of the Financial Sector Legislative Reforms Commission – Volume I*, 93, (2014), available at: https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf.

21 *See* Sen, S., Vivek, S., *The Regulatory Governance Project: An Approach Paper*, NLSIU, (2021).

22 *See* Sahithya, M., Chakraborty, A,."*Sectoral Regulator and Competition Commission: Envisaging a Movement from Turf War to Reconciliation*", NALSAR Student Law Review, (2017).

23 *See* Section 2(47)(ix), Consumer Protection Act of 2019.

24 *See* Competition Commission of India, Market Study on the Telecom Sector in India, (2021), available at: https://www.cci.gov.in/sites/default/files/whats_newdocument/Market-Study-on-the-Telecom-Sector-In-India.pdf.

25 In concurrent with this outlook, the Competition Commission of India filed a suo moto case against WhatsApp concerning its update in terms and conditions and privacy policy (Suo Moto Case No. 01 of 2021).

26 For instance, Section 21 and 21A of the Competition Act, 2002 talk about coordination between CCI and other statutory authorities.

27 *See* Clause 26(4) read with Clause 56, the DPB 2021.

28 *See* Information Commissioner's Office, *Working with other bodies: a list of MOUs*, (2018), available at https://ico.org.uk/about-the-ico/our-information/working-with-other-bodies/.

29 *See* National Health Authority, About NHA, (2019), available at: https://nha.gov.in/NHA.

30 *See* Bailey, R. et. al., *Comments on the draft Personal Data Protection Bill*, 2019, THE LEAP BLOG, (2020).

31 The Information Commissioner's Office in the UK has executed several different MOUs for a variety of purposes and with a wide range of authorities, including the UK's competition authority, the US Federal Trade Commission and various domestic and international law enforcement agencies. See Information Commissioner's Office, *Working with other bodies*, (2021) available at https://ico.org.uk/about-the-ico/our-information/working-with-other-bodies/.

32 *See* Section 189, The Insolvency and Bankruptcy Code, 2016.

33 *See* OECD, *Regulatory Management and Reform in India*, (2010), available at https://www.oecd.org/gov/regulatory-policy/44925979.pdf ; Rajagopalan, S, The trouble with legislation that's difficult to enforce, MINT, (2019) available at https://www.livemint.com/opinion/online-views/opinion-the-trouble-with-legislation-that-s-difficult-to-enforce-1565025977165.html

34 https://m.rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=586.

35 The European Data Protection Board is an independent European body established by Article 68 of the General Data Protection Regulation. The GDPR, though binding on the member countries of the European Union, provides those countries with the flexibility to establish their own data protection authorities and, in introducing the GDPR into their national laws, introduce country-level variations on specific matters (for example, on the age of a child).

36 *See*, Article 68, GDPR; the European Data Protection Board, *who we are*, (2022), available at: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en.

37 *See*, Competition & Markets Authority, *Digital Regulation Cooperation Forum*, (2020), available at: https://www.gov.uk/government/publications/digital-regulation-cooperation-forum.

38 *See* Digital Regulation Cooperation Forum, *Plan of work for 2022 to 2023*, (2022), available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1071501/DRCF_Annual_Workplan.pdf.

39 *See* Australian Competition & Consumer Commission, Agencies form Digital Platform Regulators Forum, (2022), available at: https://www.accc.gov.au/media-release/agencies-form-digital-platform-regulators-forum.

40 Zanfir-Fortuna, G., *The Complex Landscape of Enforcing the LGPD in Brazil: Public Prosecutors, Courts and The National System Of Consumer Defence*, Future of Privacy Forum, (2020) available at: https://fpf.org/blog/the-complex-landscape-of-enforcing-the-lgpd-in-brazil-public-prosecutors-courts-and-the-national-system-of-consumer-defense/; Mari, A., *Brazil announces national data protection council*, ZDNet, (2021), available at: https://www.zdnet.com/article/brazil-announces-national-data-protection-council/.

41 *Supra* note (vi).

42 International Financial Services Centres Authority, *Framework for FinTech Entity in the International Financial Services Centres (IFSCs), (2022)*, available at: https://ifsca.gov.in/Viewer/Index/292.

43 *See*, Reserve Bank of India, *Enabling Framework for Regulatory Sandbox*, (2019), available at: https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=938.

44 *See* Insurance and Regulatory Development Authority of India (Regulatory Sandbox) Regulations, 2019, available at: https://www.irdai.gov.in/ADMINCMS/cms/Uploadedfiles/Regulations/Consolidated/IRDAI%20(Regulatory%20Sandbox)%20 Regulations2019.pdf.

45 *See* Securities and Exchange Board of India, *Revised Framework for Regulatory Sandbox*, (2021), available at: https://nsdl.co.in/downloadables/pdf/2021-0059-Policy-SEBI%20circular%20on%20Revised%20Framework%20for%20Regulatory%20Sandbox.pdf.

46 Joshi, B., *Karnataka government eyes innovation push through Innovation Authority Bill*, DECCAN HERALD, (2020), available at: https://www.deccanherald.com/state/top-karnataka-stories/karnataka-government-eyes-innovation-push-through-innovation-authority-bill-807509.html.

47 Clause 40 of the DPB 2021 provides for a sandbox mechanism where new technology can be tested by the innovators under the scrutiny of the regulator.

48 *See* Ahmed, S., & Chavaly, K, *Blueprint of a - Fintech Regulatory Sandbox Law*, VIDHI CENTRE FOR LEGAL POLICY, (2020) available at https://vidhilegalpolicy.in/wp-content/uploads/2020/03/20200313_Blueprint-of-a-Fintech-Regulatory-Sandbox-Law.pdf.

49 Shekar, K. (2022). Building Effective and Harmonised Data Protection Authority - Strategies for Structural Design and Implementation, THE DIALOGUE, (2022), available at: https://thedialogue.co/wp-content/uploads/2022/04/Building-Effective-and-Harmonised-Data-Protection-Authority-Strategies-for-Structural-Design-and-Implementation.pdf.

50 *See, for example*, the Information Commissioner's Office, *The data protection principles*, (2021), available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/; Healey, R., *Malaysia Personal Data Protection Act of 2019 – 7* Key Principles, (2021), available at https://www.lexology.com/library/detail.aspx?g=ee9444ef-e33e-4716-a920-17df5258267c ; see Francis, M. et al, *An Inventory of International Privacy Principles: A 14 Country Analysis*, (2020), available at: https://scholarspace.manoa.hawaii.edu/handle/10125/64276.

51 *See* Sharma, D., *Personal Data Protection Bill, 2019 – Examined through the Prism of Fundamental Right to Privacy – A Critical Study*, SCC Blog Online, (2020), available at: https://www.scconline.com/blog/post/2020/05/22/personal-data-protection-bill-2019-examined-through-the-prism-of-fundamental-right-to-privacy-a-critical-study/.

52 *See* clauses 32, 62, 65, 69, DPB 2021.

53 *See* Rule 3(2), the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

54 *See* Paragraph 11, Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016.

55 *See* Rule 4(4), the Consumer Protection (E-Commerce) Rules, 2020.

56 Chivukula, C., *Consumer Grievance Redress in Financial Disputes in India*, Dvara Research Blog, (2021), available at: https://www.dvara.com/research/blog/2021/02/18/consumer-grievance-redress-in-financial-disputes-in-india/.

57 *See* Department of Economic Affairs, *Report of the Task Force on Financial Redress Agency*, (2016) available at: https://dea.gov.in/sites/default/files/Report_TaskForce_FRA_26122016.pdf.

58 Shekar, K. (2022). Building Effective and Harmonised Data Protection Authority - Strategies for Structural Design and Implementation. The Dialogue. Retrieved June 27, 2022, from https://thedialogue.co/wp-content/uploads/2022/04/Building-Effective-and-Harmonised-Data-Protection-Authority-Strategies-for-Structural-Design-and-Implementation.pdf.

59 Greenleaf, G., *Asian Data Privacy Laws: Trade & Human Rights Perspectives*, Oxford University Press, (2014).

60 A board-based grievance system rather than a single-point-of-contact based system may be considered.

61 The Central Government has been considering the introduction of a new bill on mediation. *See* Ahmed A., *Centre will introduce new law on mediation: Law Minister Kiren Rijiju, Bar and Bench*, (2021), available at: https://www.barandbench.com/news/law-policy/centre-will-introduce-new-law-on-mediation-law-minister-kiren-rijiju.

62 Shekar, K. (2022). Building Effective and Harmonised Data Protection Authority - Strategies for Structural Design and Implementation. The Dialogue. Retrieved June 27, 2022, from https://thedialogue.co/wp-content/uploads/2022/04/Building-Effective-and-Harmonised-Data-Protection-Authority-Strategies-for-Structural-Design-and-Implementation.pdf.

63 Ibid.

Citation: Shekar, K., Bahl, V. S., & Singh, A. (2022). DPB 2021: The Data Protection Authority and Coordination with Sectoral Regulators. The Dialogue - NASSCOM Policy Brief.

About The Dialogue

The Dialogue™ is a public-policy think- tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think- tanks to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

Twitter ID: @_DialogueIndia | Email ID: info@thedialogue.co

https://thedialogue.co

About NASSCOM

National Association for Software and Service Companies (NASSCOM) is a not-for-profit industry association for the information technology industry in India. Established in 1988, NASSCOM has over 3000 members comprising Indian and foreign organisations.

Twitter ID: @NasscomPolicy | Email ID: policy@nasscom.in

https://nasscom.in/

Publication Date: 18th July, 2022