The Dialogue™
INFORM ENGAGE IDEATE

RESEARCH PAPER

THE INSTITUTIONALISATION OF INDIA'S DATA PROTECTION AUTHORITY

Authors : Kamesh Shekar | Karthik Venkatesh | Shefali Mehta

THE INSTITUTIONALISATION OF INDIA'S DATA PROTECTION AUTHORITY

Copyright ©2022

Published on 19th October, 2022

by The Dialogue™

Authored By

Kamesh Shekar[1]

Karthik Venkatesh[2]

Shefali Mehta[3]

Edited By

Kazim Rizvi[4]

Kriti Singh[5]

Designed By

Diksha Kumari

The authors would like to thank Ms. Beni Chugh (Dvara Research), Mr. Sreyan Chatterjee (The Dialogue) and Mr. Venkatesh Krishnamoorthy for their expert comments and peer review of the paper. The experts provided their inputs in their personal capacity and all errors and omissions remain those of the authors.

[1] Kamesh Shekar is a Programme Manager - Privacy and Data Governance at The Dialogue. Corresponding author's Email ID: kamesh@thedialogue.co.

[2] The author is a J.D. Candidate at Villanova Law and an alumnus of The Dialogue

[3] The author is a student at The Fletcher School at Tufts University and an alumnus of The Dialogue

[4] Founding Director, The Dialogue

[5] Chief of Staff, The Dialogue

FOREWORD

The COVID-19 pandemic has accelerated the internet penetration rate in India as people moved toward the digital ecosystem to stay connected and avail services. About 23% more users started to consume the internet in 2020 compared to 2019 (pre-pandemic), and information technology spending is expected to increase by 7% in 2022 compared to 2021.

These digital technologies use data as the backbone for hastening service delivery while realising the economic value of data. However, it is also essential to ensure that this data collection is done in a privacy-respecting and secure manner, especially since the right to informational privacy has been recognised by the Supreme Court of India as a facet of our fundamental right to life and personal liberty and fundamental right to freedom of speech.

Intrinsic to India's long-drawn transition towards chartering a privacy-safe environment, in December 2019, the Personal Data Protection Bill 2019 (PDP Bill) was introduced in the parliament by the Minister of Electronics and Information Technology. This bill was referred to the Joint Parliamentary Committee (JPC), where I was privileged to be a member. After two years of deliberation over the PDP bill, the JPC chairperson tabled the report on behalf of members and draft the Data Protection Bill 2021 in the 2021 winter session of the Parliament.

The proposed Data Protection Authority (DPA) in the bill would have been the cornerstone of India's data governance endeavours. It must function as the independent supervisory authority for all relevant stakeholders - including the Government. In its present form, questions are being raised about its independence and capacity due to specific foundational and structural issues. I have also written extensively on this issue.

I want to congratulate The Dialogue™ for this timely paper on 'The Institutionalisation of the Data Protection Authority', which discusses the critical structural and functional issues with the DPA. The paper very well captures the issues with the DPA structuring, starting from composition of authority, inappropriate accountability framework, lack of separation of power etc. It also discusses various roadblocks to DPA as it comes into force, starting from capacity issues, lack of coordination, functional independence, and enforcement capacity.

Some strategies discussed within the paper advised by international best practices for DPA to become a robust data protection regulator are well thought out and steps in the right direction. I believe this paper will be a great value addition to the process of building a robust DPA in the future within the context of India's tech policy ecosystem.

As we expect the new form of the Data Protection Bill to be introduced in Parliament soon this year, we hope these aspects are pondered upon and taken into consideration while building India's first data regulator.

Dr. Amar Patnaik,
Member of Parliament (Rajya Sabha)
Member of the Joint Parliamentary Committee on Personal Data Protection Bill, 2019

EXECUTIVE SUMMARY

India is witnessing tremendous growth in digitalisation efforts, where technology is making a footprint across various sectors. These technological developments are increasingly moving toward data-driven business models that aim to value data in economic terms. The concomitant effect of this development has brought privacy risks and concerns to the forefront, where businesses have created a privacy void. In an attempt to protect user rights in the wake of the commercialisation of data, States have tried to enact robust data production regulations. The Indian government, similar to other jurisdictions, will enact a data protection regime to secure informational privacy to fix the privacy void.

In December 2019, the Personal Data Protection Bill 2019 (PDP Bill) was introduced in the Indian Parliament by the Minister of Electronics and Information Technology. It was referred to the Joint Parliamentary Committee (JPC) for fine-tuning through consultation with various stakeholders. The objective and reason for enacting this Bill dates to August 24, 2017, when the Supreme Court of India delivered its judgment on *Justice K.S Puttaswamy and Others vs Union of India*, declaring privacy as a fundamental right under the Indian Constitution. The judgment also directed the Government of India to bring in a robust data protection regime for the country.

As the PDP Bill was withdrawn from the Parliament during the monsoon session of 2022 to introduce the new comprehensive data protection bill, through this paper, we will highlight the concerns with the envisioned Data Protection Authority within the previous versions of the Bill to, in turn, inform the new bill. The PDP Bill provided a contour for setting up a DPA that will protect the interest of the data principal, formulate rules, functions, penalties and boundaries for data fiduciary and processor, supervise compliance with the bill, and perform an adjudicatory role in matters of informational privacy. This future regulator must be made through greater regulatory synergy, capacity, financial independence, coordination between the regulators and state governments, and responsive policymaking. But the envisioned DPA, as it stands now, has various issues in terms of structural and functional aspects, which need urgent attention as we move forward. To bring a robust DPA for India, in this policy paper, we suggest means and strategies advised by international best practices and other legacy regulators in India that would aid in the process of building DPA, keeping regulatory synergy, capacity, accountability, independence etc., as core values.

In section 2 of this paper, we discuss various structural issues with the DPA starting from its foundation, i.e., the constitution and composition of the authority, institutional design, financial independence etc. This section tries to analyze the existing structure proposed within the bill and its various limitations. Analyzing the gaps in the proposed structure, this section tries to juxtapose best practices followed by other jurisdictions as an alternative model. Best practices for appointment, removal and composition of authority discussed in this section are advised by the model followed by African countries like South Africa, Kenya, and European countries like Italy, and France, in addition to Japan, Brazil, and Australia. This section discusses how EU GDPR

ensures the financial independence of the DPA as a best practice. Also, this section discusses the institutional design followed by the DPA in Germany and Brazil to advise India's DPA.

Despite getting the structural foundation straight, envisioned DPA in the previous versions of the bill may hit various roadblocks as it comes into force because technology evolves faster than the regulations. Section 3 of the paper discusses how building capacity, agility, cooperation, co-ordination, and function independently is still a problem within the envisioned DPA which would hinder the seamless functioning of the DPA. This section analyses the nitty-gritty of the rulemaking function of the DPA and discusses the best practices in terms of a participatory approach, impact assessment and enforcement functions advised by other sectoral regulators of India. In addition, this section also deep dives into the coordination function of the DPA with other legacy regulators and discusses some of the best practices in terms of building regulatory synergy.

Finally, in section 4, we provide recommendations to weed out some of the structural and functional issues and bottlenecks of DPA to help serve its purpose. This section proposes an alteration to the appointment process of the authority, which is more balanced than the one that is executive drive. Similarly, we propose a removal procedure that is more balanced. We recommend a tiered structure for DPA with various building blocks like the Board of DPA, Advisory expert council, Research wing and office of DPA, which works in a coordinated manner. To smoothen the tension between the centre and states within the constitutional quasi-federal structure, we suggest a model state-level DPA which can work in tandem with central-level DPA through the distribution of functions. Also, in this section, we recommend various facets of revenue streams for the DPA at different levels to enhance financial independence.

Moving to the functional aspect, in sub-section 2 of the final section, we provide recommendations for making the operations of DPA smoother and more proactive by solving some of the concerns with its functions. The paper proposes setting up a data protection board to have coordinated and uniform enforcement of the data protection framework. The board will act as a high-level coordination body comprising regulators (including DPA), policymakers (both executive and legislator) and the judiciary. To move toward responsive regulation, the paper suggests a two-prong approach - (a) creating a coordinated sandbox mechanism to understand innovations and (b) conducting a prevalence-based complaint audit to understand the regulatory gaps. The paper also suggests a calibrated hierarchical grievance redressal mechanism with horizontal and vertical coordination (between different elements of the system) and agility proofing. The proposed calibrated grievance redressal mechanism involves Interactive voice response (IVR) Interactive voice response (IVR), Online Dispute Resolution (ODR) systems, etc., and traditional systems like appellate tribunals and entities' grievance management systems.

As the envisioned DPA will have an influential and crucial role in this digital age, it is essential to iron out the structural and functional issues, and bottlenecks discussed in the paper using the strategies and recommendations provided within the new comprehensive bill, which is been drafted currently.

CONTENTS

1. INTRODUCTION

Internet penetration worldwide is witnessing tremendous growth, where the COVID-19 pandemic accelerated the same as people moved toward digital set-up to stay connected and avail contactless services. With individuals increasingly moving towards digital set-ups and the internet, the call for securing informational privacy is becoming exigent - as a heap of information sharing happens daily for availing services and other kinds. For instance, the pandemic lockdowns led to increased online learning where schools moved towards using learning platforms.[6] While these technological developments are making their footprint into various sectors and positively impacting society by enabling innovation in business models, providing better service/welfare delivery methods, and helping in crisis management and connectivity, it has also created gaps in the regulatory perimeter.

The age of information further complicated this issue. Regulating and curbing access to data is a tremendously challenging task because data often moves too fast to control or regulate. Data has become an invaluable resource cutting across industries. With India moving towards a "data-rich" nation by 2025,[7] where both public and private players hold significant data, protecting individuals' informational privacy has become pertinent. With a fast-growing, mobile-first population, there is immense scope to regulate and harness data to uphold individual privacy in tandem with harnessing the economic value of that data, albeit in a privacy-respecting manner.

India's data protection landscape has evolved considerably since the Supreme Court declared privacy as a fundamental right under the Indian Constitution in the Puttaswamy judgement I (2017).[8] The judgement also vested a positive obligation[9] over the government to protect the informational privacy[10] of individuals. At the executive and legislative layers, too, there has been recognition of gaps left by the pace of evolution of the technological landscape. Instances of the executive action can be seen in the changes in the IT Rules, 2021,[11] as well as the raft of policy measures announced under the National Digital Health Mission[12] etc. A crucial legislative intervention is the introduction of the Personal Data Protection Bill 2019 (PDP Bill). This Bill was drafted by the Ministry of Electronics and Information Technology in 2019, based on the Justice Sri Krishna Committee Report.[13] Ultimately, the Bill introduced by the Ministry, i.e. the PDP Bill, travelled to the Joint Parliamentary Committee by reference, whose report[14] was tabled in Parliament in December 2021. The draft Bill has currently been withdrawn and will be re-introduced, but this provides an opportunity to voice the concerns with the envisioned DPA structure and functions within Personal Data Protection Bill, 2019 and in the JPC's recommended Draft Data Protection Bill, 2021.

[6] Sarma, A. (2021). The rise of the platform economy and access to educational resources. Retrieved from Observer Research Foundation: https://www.orfonline.org/expert-speak/the-rise-of-the-platform-economy-and-access-to-educational-resource
[7] *'India will transform from data poor to data rich in 5 years'*. (2020, February 16). The Indian Express. Retrieved April 23, 2022, from https://indianexpress.com/article/technology/tech-news-technology/india-will-transform-from-data-poor-to-data-rich-in-5-years-railtel-chairman-6270226/
[8] Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors. AIR 2017 SC 4161
[9] Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors. AIR 2017 SC 4161 (Para 158)
[10] Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors. AIR 2017 SC 4161 (Para 81)
[11] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. (2021). Retrieved from MeitY: https://www.MeitY.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf
[12] Ayushman Bharat Digital Mission. (2021). Retrieved from National Health Authority: https://abdm.gov.in/
[13] A Free and Fair Digital Economy Protecting Privacy, Empowering Indians Committee of Experts under the Chairmanship of Justice B. (2018). Retrieved from MeitY: https://www.MeitY.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
[14] Report of the Joint Parliamentary Committee on the PDP Bill, 2019. (2021). Retrieved from Lok Sabha: http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

The Data Protection Authority (DPA), as envisaged under the Personal Data Protection Bill, 2019 and in the JPC's recommended Draft Data Protection Bill, 2021, will be responsible for regulating domestic and cross-border data flows, and approving data portability requests, among several other crucial duties. The DPA will play an essential role in determining relationships with other sectoral regulators that may have overlapping jurisdictions, such as the Reserve Bank of India (RBI), the Telecom Regulatory Authority of India (TRAI), etc. Nevertheless, establishing a DPA is essential for constituting India's data protection standards to secure individuals' informational privacy. But the envisioned DPA, under the PDP Bill, has various issues in terms of structural and functional aspects, which need attention as we move toward the revised Bill.

Therefore, to bring off a robust DPA for India, in this policy paper, we suggest means and strategies advised by international best practices and other legacy regulators in India that would aid in the process of building DPA, keeping regulatory synergy, capacity, accountability, independence etc., as core values.

Section 2 of this paper discusses various structural issues with the DPA starting from its foundation, i.e., the constitution and composition of the authority, institutional design, financial independence, etc. Section 3 of the paper discusses how building capacity, agility, cooperation, coordination, and functions independently is still a problem within the envisioned DPA which would hinder the seamless functioning of the DPA if retained in the upcoming Bill. Finally, in section 4, we provide recommendations to weed out some of the structural and functional issues and bottlenecks to help serve its purpose, as mentioned in the Personal Data Protection bill, 2019.

2. STRUCTURAL CONCERNS WITH ENVISIONED DATA PROTECTION AUTHORITY

There are certain issues with the DPA structure starting from the foundation, i.e., the composition of authority. The envisioned DPA will have not more than six members and a chairperson, which would be inadequate to handle the enormous duty vested over the DPA in diverse and populated countries like India. Additionally, the provisions don't elaborate on the members' diversity and representation of technical experts within the board. It is essential that envisioned DPA consider the pluralistic aspect of the data principal/fiduciary, covering for diversity in data principal/fiduciary and contextual heterogeneity in the issues.

The legislative and judiciary (or any other stakeholders) wing merely has representation in the selection committee of chairperson and DPA members. Besides, the DPA is accountable to the central government (which comes under the preview of the DPA for actions related to data protection[15]) for their performance. There is also an absence of any disclosure requirements for the central government regarding the selection process by the committee.

Similarly, there is a crack in another vital foundational block, i.e., the funding structure of the DPA. As it stands now, the central government will decide the means and ways through which DPA can generate revenue in addition to its grants, which hampers financial independence.

While acknowledging that the central government has a crucial role in setting up the DPA, as we move forward, it is essential to answer how to keep their interference at arm's length in terms of constituting the crucial foundations of DPA like composition, finance etc.

Besides, the structural foundations of the DPA in its current form lack a robust & transparency framework for itself and the central government, a mechanism to separate powers and means to act financially independent. The below table maps the issues against the provisions in the PDP bill and JPC's recommended Draft Data Protection Bill, 2021 pertaining to DPA structuring. Followed by it, we discuss the critical and first-order structural issues tabulated in detail.

Table 1: Mapping the concerns with DPA Structuring

Structural aspects	Provisions in PDP Bill	Provisions in the JPC recommended Data Protection Bill, 2021	Issues
Composition	Clause 42(1) – DPA comprises a chairperson and not more than six members Clause 42(4) – the six members of the Data Protection Authority (DPA) must be qualified in the fields of "data protection, information technology, data management, data science, data security, cyber and internet laws, public administration, national security.	N/A	Not more than seven people (6 members + chairperson) would be inadequate to handle the enormous duty vested over the DPA. This clause doesn't mention or incorporate efforts to enhance the members' diversity and representation of technical experts within the board.

[15] Unless they are exempted under Clause 35 or Clause 36 in the PDP Bill

Structural aspects	Provisions in PDP Bill	Provisions in the JPC recommended Data Protection Bill, 2021	Issues
Appointment and removal process	Clause 42(2) – Chairperson and members of the authority will be appointed by the central government on the recommendation made by the selection committee	Along with the existing members prescribed in the earlier iteration, the Committee has recommended the composition of the Selection Committee be expanded to include the Attorney General and three other members nominated by the Central Government (an independent expert from relevant fields, Director of an IIM and the Director of an IIT)	This clause vests powers in the hand of the central government in terms of appointing the chairperson and members of DPA without any consultation with the legislative or judiciary wing (or any other stakeholders) as the selection committee is represented almost only by the executive.
	Clause 47 – A change or a vacancy in the composition will not impact the decision or functioning of the authority in any manner	N/A	Aspects such as the prescription of rules and procedures regarding the transaction of business at selection committee meetings, which include important matters like the quorum at such meetings, have been left to be prescribed at a later date may prove to be problematic.
	Clause 44 – The central government can terminate any member or chairperson of the authority	N/A	These clauses hamper the DPA's independence as they are accountable to the central government, which comes within the DPA supervision in terms of data protection. While conditions for removal of the Chairperson or any member of the Authority are similar to other jurisdictions. However, the inclusion of the condition - "abused their position as to render their continuation in office detrimental to the public interest," which employs the use of overbroad criteria of "public interest", is concerning.
	Clause 62 - Central government will prescribe the list of Adjudicating Officers	N/A	While the central government can be part of the process, it is important to involve the judiciary in this aspect.
Institutional design	Clause 41 (3) & (4) – Envisioned DPA is a single central authority with the opportunity for the Central Government to establish offices in different places in India.	N/A	This clause doesn't account for the pluralistic aspect of the data principal/fiduciary, where a single central authority can't cover for diversity in data principal/fiduciary and contextual heterogeneity in the issues.
Financial independence	Clause 43(2) – The salary, allowance and terms and conditions of the members and chairperson of the authority will be prescribed	N/A	As per the powers vested in the central government, they retain control over the means and ways for generating revenue in

Structural aspects	Provisions in PDP Bill	Provisions in the JPC recommended Data Protection Bill, 2021	Issues
	Clause 78 – Central government will provide grants to the authority Clause 79(1)(b) – Central government will decide from which other sources DPA can generate revenue Clause 80 – DPA to furnish returns and statements (including enforcement data) along with programmes for promotion and development of personal data protection with the Central Government in a time-to-time manner on the requirement		addition to its grants; the question is how to keep the central government at arm's length from DPA.

2.1. CONCERNS WITH THE COMPOSITION OF THE AUTHORITY

The DPA must have diversity and incorporation of technical experts with its board to deliver a wide range of functions starting from standard-setting and compliance management to adjudication.[16]

The prescribed structure, under the PDP Bill 2019, states that one individual will be a law expert; as for the others, it mentions ten years of experience in fields such as data protection, cyber security, and allied fields as the criteria. It is essential that envisioned DPA consider the pluralistic aspect of the data principal/fiduciary, covering for diversity in data principal/fiduciary and contextual heterogeneity in the issues. Adding to this, currently, India doesn't have an overarching administrative law like what we have in the US[17] and in some form in the UK.[18] This hampers overarching process accountability and oversight, which streamlines rulemaking procedures for the DPA. Besides, the structure envisioned within the PDP Bill provided excessive delegation to DPA in rule-making without any prescription for any form of engagement (consultation, workshop, etc.) with technical experts and stakeholders to have responsive subordinate legislation.

In terms of members, there is a complete absence of a prescription for non-executive members (in the form of part-time members) to be part of the Authority. Regulators in India[19] and globally have non-executive members[20] to provide nonpartisan inputs and oversight in the functioning of a DPA.[21] In the absence of part-time members, the authority is precluded from the opportunity to involve experts as a part of the authority itself.[22] Moreover, the Financial Sector Legislative Reforms Commission

[16] Rai, S. (2018, February 9). *A Pragmatic Approach to Data Protection*. The Leap Blog. Retrieved April 27, 2022, from https://blog.theleapjournal.org/2018/02/a-pragmatic-approach-to-data-protection.html

[17] US Administrative Procedure Act, 1946

[18] UK FSMA 2000

[19] *Insurance Regulatory & Development Authority*. (n.d.). Department of Financial Services. Retrieved April 27, 2022, from https://financialservices.gov.in/insurance-divisions/Insurance-Regulatory-&-Development-Authority; *TRAI - Section 3: Establishment and incorporation of Authority*. (n.d.). India Code. Retrieved April 27, 2022, from https://www.indiacode.nic.in/show-data?actid=AC_CEN_37_58_00002_199724_1517807323214&sectionId=16703&sectionno=3&orderno=3

[20] Lalitkomon, N., Chanpanich, T., & Mahakunkitchareon, G. (2022, January 20). *Thailand Establishes Personal Data Protection Commission - Privacy - Thailand*. Mondaq. Retrieved April 27, 2022, from https://www.mondaq.com/data-protection/1152268/thailand-establishes-personal-data-protection-commission

[21] Burman, A. (2020, March 9). *Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?* Carnegie India. Retrieved April 27, 2022, from https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217

[22] *Our submission to the Joint Committee of Members of the Indian Parliament on the Personal Data Protection Bill, dated 25 February 2020*. (2020, February 25). Dvara Research Blog. Retrieved April 27, 2022, from https://www.dvara.com/research/blog/2020/03/04/our-submission-to-the-joint-committee-of-members-of-the-indian-parliament-on-the-personal-data-protection-bill-dated-25-february-2020/

report[23] notes that appointing non-executive members who are experts in their respective fields on part-time bases brings in (a) an element of a neutral observer of the regulator's functions as they are not full-time employees (b) information and expertise related to the sector to the table of the regulator. Though the PDP Bill empowered the DPA to engage consultants, these consultants do not serve as a part of the authority itself. They can merely provide counsel without actively participating in the decision-making aspect of the authority.

Besides, the absence of any requirements of prior judicial experience is also of concern. The Data Protection Authority is to exercise judicial functions (like adjudication), and the regulator's capacity to perform these functions is crucial. Moreover, as DPA will be exercising executive powers in terms of supervision and enforcement, it is important to balance this act with having members with judicial expertise perform a quasi-judicial function such that the actions of the DPA are within the legal framework.

2.1.1. BEST PRACTICES FROM OTHER JURISDICTIONS: COMPOSITION

As discussed below, the composition of the DPA prescribed in certain jurisdictions aptly tackles technical capacity issues and diversity concerns and introduces independence in decision-making.

A. DIVISION OF MEMBERS AND THEIR EXPERTISE: SOUTH AFRICAN CASE

The South African regulator comprises a chairperson and four other ordinary members. The legislation envisions that these members must be appropriately qualified, fit and proper persons. Among these members, one member must have experience as a practising advocate/attorney or a professor of law at a university to ensure that the regulator possesses legal expertise, whereas the other's qualifications, expertise and experience must be in line with expressly stated objectives of the regulator.

It also distinguishes ordinary members who will serve in a full-time capacity, i.e. individuals who may not perform or undertake any other remunerative work during this period and mandates the presence of at least two full-time members. Regarding the other two ordinary members, there is an option to appoint them in a part-time capacity.

[23] *Report of the Financial Sector Legislative Reforms Commission*. (2013, March). Department of Economic Affairs. Retrieved May 21, 2022, from https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf

B. CRITERIA FOR APPOINTMENT: KENYA CASE

In terms of appointment, the law[24] lays down criteria for appointment of holding a degree from a University recognised in Kenya in the fields of data science, law, information technology and other related fields. It lays down that their knowledge and relevant experience must be ten years or over; in addition to that, they must hold a master's degree. No members are eligible for re-appointment.

C. INCLUSIVITY AND DIVERSITY IN MEMBERS COMPOSITION: FRANCE CASE

The Commission nationale de l'informatique et des libertés (CNIL)[25] comprises 18 members in total. The qualifications of the commission members are inclusive, where there is a representation of parliamentarians, the judiciary, members of relevant councils and public figures related to the subject. The CNIL requires the following in terms of representation[26]:

- 01 representative of the Commission of Access to Administrative Documents
- 06 representatives of High Jurisdictions (02 Council of State, 02 Court of Auditors, 02 Court of Cassation)
- 04 Members of the Parliament (02 National Assembly and 02 Senate)
- 05 Qualified Personalities
- 02 Members of the Economic, Social and Environmental Council

The diversity of members essentially aids independence and enhances the technical and legal expertise of the authority. It facilitates accountability and reduces any aspect of executive bias despite having members from the executive by providing a healthy balance. The commissioners' mandate is for five years, or, for Parliamentarians, as long as the duration of their mandate.

D. Technical and Legal Expertise of the Authority: Brazil case

The Brazilian Data Protection Authority (ANPD) comprises 05 (five) directors, including the CEO.[27] In addition, the members of the Board of Directors shall be chosen from Brazilians who have an "unblemished reputation, a superior level of education and a high degree in the speciality field of the positions to which they will be appointed." Beyond this, the structure or design of the authority greatly aids the technical and legal expertise of the authority by creating various institutions that aid the highest governing council, i.e. the Board of Directors.

In addition to ANPD, the National Council for Personal Data Protection and Privacy is established, comprising 23 members that ANDP appoints. This council has representation across the spectrum, i.e. executive, senate (upper house), house of representatives (lower house), other national councils like justice and public prosecutor, Brazilian internet steering committee, civil society, technological and innovative institutions, trade union confederation, and the labour and business sector. This enhances

[24] Section 7 (1) , Kenya Data Protection Act, 2019
[25] Appointed via Act No. 78-17 on Information Technology, Data Files and Civil Liberties dated 6 January 1978, as amended by Act No. 2018-493 dated 20 June 2018
[26] https://www.cnil.fr/en/node/287
[27] Section 55 D, Brazilian Data Protection Act, 2018

innovative institutions, trade union confederation, and the labour and business sector. It will also enhance the technical expertise of authority and establishes the capacity to deal with a myriad of issues across a host of sectors.

Moreover, in Brazil, as per the Brazilian General Data Protection Law, 2018, the National Data Protection Authority (ANPD) has a tiered structure with various components. The ANPD is composed of the following components:[28]

a. Board of Directors, the highest governing body;

b. National Council for Personal Data Protection and Privacy;

c. Internal Affairs;

d. Ombudsman;

e. Its own legal advisory body; and

f. administrative units and specialised units necessary for the application of the provisions of this Law.

Adopting such a structure that divides responsibilities into specialised bodies under the larger ambit and control of the Board of Directors of the National Data Protection Authority *(ANPD)* helps Brazil tackle issues at scale. It also aids in enforcing its legislation and helps to enhance the technical or legal capacity of the regulator. The development of this regimental structure of the ANPD was vested in the hands of the Board of Directors.

Moreover, legislation[29] held that "*until the date of entry into force of its regimental structure, the ANPD shall receive technical and administrative support from the Civil House of the Presidency of the Republic for the exercise of its activities and The Directing Council shall provide for the internal regulations of the ANPD*" in a bid to handle affairs until the authority was fully established and functional.

E. PERMANENT STAFF RECRUITMENT PROCESS: ITALY CASE

In addition to the Panel of Commissioners, the *Garante* (Italian DPA) also comprises the Office.[30] As per Section 156 of the Personal Data Protection Code of Italy, The Office of the *Garante* shall be under the authority of a secretary-general, who shall be appointed out of individuals with proven high-level qualifications. The position covered and the objectives to be achieved may be selected from the ranks of the judiciary, including administrative courts and courts of auditors, Avvocati di Stato [State lawyers defending public bodies and employees in administrative law proceedings, full professors in law and economics, and senior heads of departments in public bodies].

The permanent staff of the Office or Bureau shall include 100 positions.[31] The list of permanent staff may only be joined following a competitive public examination. This is helpful with a view to ensuring cost-effectiveness and efficiency of administrative activities and fostering the recruitment of more

[28] Section 55 C, Brazilian Data Protection Act, 2018
[29] Section 55 G, Brazilian Data Protection Act, 2018
[30] Under Section 155, the Office of the Garante shall implement the principles concerning appointment and tasks of officials in charge of the individual cases, separation between guidance and supervisory tasks as conferred on the highest authorities and managerial tasks as committed to executive staff.
[31] Section 156 (2), Italian Data Protection Code

experienced staff. The *Garante* may reserve no more than fifty per cent of the vacancies to be filled through such procedures to the permanent staff of public administrative bodies that have been recruited via competitive public examinations and have held their positions for at least three years. The duties of the staff thus employed shall be laid down by the *Garante* by its regulations that must be published in the Official Journal.

F. PART-TIME MEMBERS IN THE AUTHORITY: JAPAN CASE

As per the Protection of Personal Information Act[32], the Commission thus established comprises a chairperson and eight commissioners. It provides for four of the eight commissioners to serve part-time.[33] Additionally, it provides the opportunity to employ a "specialist commissioner" to investigate any specialised matter or particular point of contention. The Commission may post a specialist commissioner that is to be appointed by the Prime Minister based on a proposal made by the Commission, who is relieved of their part-time service upon completion of the said specialised matter.[34]

2.2. CONCERNS WITH EXECUTIVE DRIVEN APPOINTMENT AND REMOVAL PROCESS

As witnessed in Table 1, various versions of envisioned data protection regimes,[35] place the entire responsibility or vest the entire power of appointing a DPA in the hand of the central government. All members of the selection committee are either members of the executive themselves or are executive appointees.[36] The introduction of the four new members by the recommendations of the Joint Parliamentary Committee (in their version of the Data Protection Bill, 2021) in a bid to enhance independence in the appointment process fails to achieve its purpose.[37] The Attorney General of India remains an executive appointee, and the executive also chooses the three other members.[38] The same is being carried out without any consultation with the legislative or judicial intervention (or any other stakeholders) as the selection committee is represented only by the executive. Additionally, the criteria for membership in the Select Committee may be considered vague compared to other regulators.[39] Besides, there is an absence of any disclosure requirements for the central government regarding the selection process by the committee.

This is a matter of concern as the Government may soon be one of the biggest data fiduciaries in India. Keeping in mind the aggressive push of the Government towards the adoption of digital measures, also witnessed in the Finance Bill, 2022 and the speech of the Hon'ble Finance Minister,[40] the need for the authority to function independently and in a supervisory capacity with regards to the Government's handling of data will be critical. Purely executive-driven appointments will bring into question the ability

---

[32] Section 63 (1), Personal Information Protection Act, 2020 https://www.ppc.go.jp/files/pdf/APPI_english.pdf

[33] Section 63 (2), Personal Information Protection Act, 2020 https://www.ppc.go.jp/files/pdf/APPI_english.pdf [34] Section 69 , Personal Information Protection Act, 2020 https://www.ppc.go.jp/files/pdf/APPI_english.pdf

[35] Directly PDP Bill and indirectly JPC's version of Data Protection Bill, 2021

[36] Shefali M., et. al., (December 2021), Preliminary Analysis: Report of The Joint Parliamentary Committee (JPC) On The PDP Bill, 2019, New Delhi, The Dialogue and DeepStrat. Retrieved April 27, 2022, from https://thedialogue.co/wp-content/uploads/2021/12/Final-Preliminary-Analysis-_-JPC-Report-on-PDP-Bill-2019.pdf

[37] Shekar, K. (2022, March). *Virtual Stakeholder Consultation Report: Implementing India's Data Protection Regime*. The Dialogue. https://thedialogue.co/wp-content/uploads/2022/04/Implementing-India%E2%80%99s-Data-Protection-Regime.pdf

[38] Ibid

[39] See Section 9, Competition Act; Sections 4(4), SEBI Act; Section 4, TRAI Act; Section 3, IRDA Act.

[40] Sangani, P. (2022, February 1). Budget 2022: *Govt's digital push to drive big business for startups and tech firms*. The Economic Times. Retrieved April 27, 2022, from https://economictimes.indiatimes.com/tech/technology/govts-digital-push-to-drive-big-business-for-startups-and-tech-firms/articleshow/89283553.cms

of such an authority to perform as an independent arbitrator in cases involving the Government.

The selection process of the Authority requires improvements, including more judicial involvement. Justice Sri Krishna Committee report had also recommended including judicial members within the Selection Committee.[41] The authority's independence, which is mainly dependent on its appointment process, is also required from an international perspective.

Without such a separate and independent body, India's chance to be considered adequate for the essential purposes of cross-border transfer of data by other jurisdictions may be reduced, impacting India's position in the global digital economy.[42] Though the PDP Bill handed over its adjudicatory function to adjudicatory officers, the manner and terms of appointment are prescribed by the Central Government. India's qualifying adequacy test of jurisdictions is crucial as businesses indulge in cross-border data transfer, exchange, port and transmit data to a third party or other business units for various business purposes like processing, research and development, marketing, storage etc. In addition, businesses do cross-border data transfer in case of data portability requests by consumers.

In addition, the power of removal and the prescription of salaries/allowances/conditions for members and the Chairperson has vested with the Central Government. This includes the power to terminate any member or chairperson of the authority, which impacts the authority's functional independence. But in the case of some of the other existing regulators, functional independence is secured.[43] For instance, in the case of the Right to Information (Section 14), the Chief Information Commissioner and Information Commissioner can be removed from office only by the President of India, advised by the inquiry done by the supreme court.

Therefore, this heavy-headed executive involvement in the process of DPA appointment from previous versions of the bill would likely hamper the authority's independence in regulating/supervising the Government's data practices and result in weaker enforcement of the law.[44]

2.2.1. BEST PRACTICES FROM OTHER JURISDICTIONS: APPOINTMENT AND REMOVAL PROCESS

Globally, various authorities have adopted different methods of appointment and removal of members of the authority. However, some stand out when it comes to facilitating independence, as discussed below.

---

[41] *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians Committee of Experts under the Chairmanship of Justice B.* (2018, July 27). MeitY. Retrieved April 27, 2022, from https://www.MeitY.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf [42] Rizvi, K. (2021, November 12). *Towards a progressive data protection regime*. Times of India. Retrieved April 27, 2022, from https://timesofindia.indiatimes.com/blogs/voices/towards-a-progressive-data-protection-regime/

[43] For instance, Palmer, D., Berlin, M. M., & Das, D. K. (2018). *Legal Accountability of the Police in India Centre for Law and Policy Research*. CLPR. Retrieved April 27, 2022, from https://clpr.org.in/wp-content/uploads/2018/09/Police-Accountability-CLPR.pdf

[44] Shekar, K. (2022, March). *Virtual Stakeholder Consultation Report: Implementing India's Data Protection Regime*. The Dialogue. https://thedialogue.co/wp-content/uploads/2022/04/Implementing-India%E2%80%99s-Data-Protection-Regime.pdf; Shefali M., et. al., (December 2021), Preliminary Analysis: Report of The Joint Parliamentary Committee (JPC) On The PDP Bill, 2019, New Delhi, The Dialogue and DeepStrat. Retrieved April 27, 2022, from https://thedialogue.co/wp-content/uploads/2021/12/Final-Preliminary-Analysis-_-JPC-Report-on-PDP-Bill-2019.pdf

A. PARLIAMENTARY APPROVAL FOR APPOINTMENT AND REMOVAL: SOUTH AFRICAN CASE

In South Africa, under the Protection of Personal Information Act, the Data Protection Authority gives effect to the right to privacy. It seeks to balance it against other essential rights like access to information. The bill establishes its information regulator as a juristic person focusing on independence and subject only to the Constitution. Though the South African data protection authority has fewer maximum members with a lack of technical diversity, the process of member selection is independent of executive capture. In terms of the appointment, though the President appoints the Chairperson and members, it is on the recommendation of the National Assembly, i.e. the lower house (including indicating differences between which members are appointed in a full-time or part-time capacity). These recommendations by the National Assembly are made by a committee composed of members of parties represented in the Committee and then approved via a resolution adopted through a majority vote of the members of the Assembly.

In terms of removal, though the power lies with the President de jure (with the power to suspend once a motion for removal has been placed in the assembly), it is de facto undertaken only by resolution of the National Assembly, calling for removal on the grounds of misconduct, incapacity or incompetence. This process remains utterly independent of pure executive appointment and removal.

B. PRESIDENTIAL DECREE AND JUDICIAL APPOINTMENT PROCESS: FRANCE CASE

In France, the DPA or the Commission Nationale de l'informatique et des libertés is appointed by the decree of the President of the Republic. Further, the assemblies and the judiciary appoint the 17 members of the commission. This procedure guarantees independence in terms of appointment, which is also followed by various other European Union countries that establish their DPAs according to EU GDPR guidance.

C. PARLIAMENTARY PROCESS FOR APPOINTMENT AND REMOVAL: ITALY CASE

As per Section 153 of the Personal Data Protection Code of Italy, the Panel of Commissioners include four members, two elected by the Chamber of Deputies and two by the Senate through a particular voting procedure.[45] The members are elected following a procedure[46] wherein candidates apply to a selection procedure that is published by a notice posted on the websites of the Chamber of Deputies, the Senate and the *Garante*. The applications received and the relevant CVs shall be transparently published on the aforesaid websites. Further, the applicants shall be persons ensuring independence with proven experience in the field of personal data protection with particular regard to law or computer science.[47] As for decisions pertaining to the President of the Garante, the members vote amongst themselves to appoint the president who holds the right to have a casting vote where votes are equal.[48]

[45] Section 153 (2), Italian Personal Data Protection Code, Legislative Decree no. 196 of 30 June 2003
[46] Panetta, Rocco. Analysis: Italy's GDPR implementation law, IAPP.org, September 2018
[47] Section 153 (2), Italian Personal Data Protection Code, Legislative Decree no. 196 of 30 June 2003
[48] Section 153 (3), Italian Personal Data Protection Code, Legislative Decree no. 196 of 30 June 2003

D. COMMISSION-LED APPOINTMENT AND STATUTORY REMOVAL: JAPAN CASE

The Personal Information Protection Commission (PPC), which functions as per the Protection of Personal Information Act[49], is one of the highly independent regulators or organs in the Japanese legal landscape. The Commission is composed of the chairperson and eight Commission members, appointed by the Prime Minister with the consent of both Houses of the Diet (from those with "high character and deep insight").[50] Further qualifications in detail are mentioned in subsequent sections. Thus, once again, the prime minister makes the de facto appointment; however, the de jure power lies with the Houses of the Japanese Parliament. In terms of removal, the terms have been laid down in Article 65, titled "Guarantee of Status", they include the commencement of bankruptcy proceedings, being punished under this Act or the Numbers Use Act[51], when punished by imprisonment, or when recognised to be incapable of carrying out their duties owing to physical or mental incapacity and may only be removed by the Prime Minister when these specific, clearly worded instances.[52]

E. PUBLIC SERVICE COMMISSION LED APPOINTMENT AND REMOVAL: KENYA CASE

The Office of DPA in Kenya is designated as a State Office.[53] The Public Service Commission[54] initiates the recruitment process. The process thus adopted includes the call for applications which is followed by shortlisting and interview process.[55] The Public Service Commission nominates 3 persons for the role of the Data Commissioner. Ultimately, the President appoints the Data Commissioner upon receiving the approval of the National Assembly.

In terms of removal, a person who desires removal of the data commissioner on any ground specified in Act[56] may present a complaint to the Public Service Commission that sets out the alleged facts. The grounds for removal include death, resignation, a conviction of offences (with jail term exceeding 6 months), and grounds of inability to perform functions from mental or physical incapacity, non-compliance with disqualification norms of the Constitution, and bankruptcy incompetence or gross misconduct. Under Article 47 of the Kenyan Constitution, the Public Service Commission shall consider the complaint, investigate, and recommend the Cabinet Secretary initiate the removal. However, the commissioner shall be given an opportunity to present his/her defence against any such allegation. The de jure power of removal remains with the constitutional body, i.e. the Public Service Commission.

[49] Protection of Personal Information Act, 2020, https://www.ppc.go.jp/files/pdf/APPI_english.pdf
[50] Section 62 (3), Protection of Personal Information Act, 2020 (Japan), Supra No. 34
[51] The Japanese government enacted the My Number Act, which took effect in January 2016. It assigned a unique 12-digit number, called My Number, or the Social Benefits and Tax Number or Individual Number, to every resident of Japan, whether Japanese or foreign.
[52] Section 66, Protection of Personal Information Act, 2020 (Japan), Supra No. 3 [53] Section 5, Kenya Data Protection Act, 2019
[54] https://www.publicservice.go.ke/
[55] Section 6, Kenya Data Protection Act, 2019
[56] Section 11 (d), Kenya Data Protection Act, 2019

F. PRESIDENTIAL APPOINTMENT AND REMOVAL PROCESS: BRAZIL CASE

In Brazil, as per the Brazilian General Data Protection Law, 2018, the board of directors of the National Data Protection Authority *(ANPD)* is appointed by the President of the Republic of Brazil. However, unlike in India, where DPA is formed by the selection committee, which is executive driven, in Brazil, the President appoints members of ANPD after approval by the Federal Senate (upper house of the Brazil Parliament) in line with Item III of Article 52 of the federal constitution of Brazil. In terms of decision-making, autonomy is assured to the ANPD.[57] Brazil also follows the involvement of the Parliament in their appointment process, with explicit mention of decision-making autonomy. In terms of removal of members, it may occur only on the grounds of resignation, final court conviction or penalty of dismissal arising from administrative disciplinary proceedings.[58] To initiate any proceedings under the removal provisions, the Chief Minister of the Civil House of the Presidency of the Republic may institute administrative disciplinary proceedings, and then they will be conducted by a special commission composed of stable federal civil servants.[59] This is ultimately then carried out by the President on the recommendation of the commission, as mentioned earlier.[60]

G. GOVERNOR-GENERAL LED APPOINTMENT AND REMOVAL PROCESS: AUSTRALIA CASE

The Office of Australian Information Commissioner[61] is the independent national regulator for privacy and freedom of information. The Office of the Australian Information Commissioner is established as an independent statutory agency within the Attorney-General Department's portfolio.[62] The Australian Information Commissioner is to be appointed by the Governor-General by written instrument.[63]

2.3. Concerns with Centralised Institutional Design of the DPA

Keeping in mind the size of the population, the centralised institutional design of the DPA covering a broad ambit of functions may pose a roadblock[64] as discussed below.

Quasi-federalism debate: The proposed authority within PDP Bill had to bear the onus of penalising both central and state governments in its role as a regulator. Therefore, it is imperative to reconsider the centralised structure of the DPA and provide adequate representation to the states, in line with India's quasi-federal structure. At present, the structure fails to meet the requirements of the separation of powers between Union and State as envisaged under the Constitution of India.[65] For instance, maintaining "public order", which appears in the PDP bill, is the subject of the State List (item 1) in the seventh schedule of the Indian Constitution.

---

[57] Section 55 B, Brazilian Data Protection Law, 2018
[58] Section 55 E, Brazi
[59] Section 55 E (Para 1), Brazilian Data Protection Law, 2018
[60] Section 55 E (Para 2)
[61] Section5 (1) , Australian Information Commissioner Act, 2010, https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/84651/94328/F352296725/AUS84651.pdf
[62] Section 5 (3) Australian Information Commissioner, 2010
[63] Section 14, Australian Information Commissioner Act, 2010
[64] Bhardwaj, D. (2021, September 27). *Need state-level data protection authorities: Joint parliamentary committee MP Amar Patnaik | Latest News India*. Hindustan Times. Retrieved April 27, 2022, from https://www.hindustantimes.com/india-news/need-state-level-data-protection-authorities-joint-parliamentary-committee-mp-amar-patnaik-101632679181340.html
[65] *Indian Constitution*. (n.d.). Seventh Schedule. Retrieved April 27, 2022, from https://www.mea.gov.in/Images/pdf1/S7.pdf

Repercussions of neglecting India's Quasi federal governmental structure while framing the institutional design of DPA will be felt during the implementation phase, where trust in the DPA will erode if there is no room for state-level representation.[66] Moreover, preserving quasi-federalism is the heart of our constitutional scheme, and it would also provide certain independence from the central government.

States collect data through different laws passed by the legislative assembly thus, it is not ideal for the central authority to decide on the data standards for the state collected data and its functionality. Besides, the current structure poses the question that if both centre and state can legislate the 'information' under Right To Information (RTI), how could data be only legislated by the centre? Therefore, the current structure of the central DPA will have statutory backing but lack constitutional backing while safeguarding constitutional rights.

Concerns with horizontal structuring: The institutional design of the DPA envisioned within the previous version of the bills raised the concern of effective delivery of the breadth of tasks assigned to it. The DPA is tasked with the onus of function as the regulator, along with responsibilities like standard-setting and non-regulatory missions like awareness building. Some non-regulatory tasks require horizontal structuring by delegating responsibilities to state-level bodies. For instance, requiring agencies within proximity is crucial for delivering one of the critical non-regulatory tasks, i.e., awareness building.[67]Therefore, the lack of provisions for horizontal structuring would dilute the awareness creating function of the DPA.

Lack of agility: Decentralised state-level DPA is crucial for tackling the issue of agility. Telangana's experience in tackling the issue of piracy[68], emphasise the need for the state-level body to respond to the crisis with agility and reduce the harm (loss). For instance, a health data breach would need quick action from an authority, for which decentralisation would be an ideal way forward.

Capacity concerns: The centralised institutional design of DPA, as provided within the previous versions of the bill with a broad ambit of tasks with narrow capacity, gives it a start on the wrong footing, which would become a difficult problem to be solved at a later stage.[69] Due to the diversity and vastness of the country, it is not ideal to have a single DPA for the entire country. A single DPA at the central level will be overwhelmed and would lack the capacity to deliver its board of tasks. For instance, tackling complaints from state-level data principals in real-time for a heavily populated country like India would be a laborious task, which calls for state-level DPAs with delegated responsibilities.

---

[66] Shekar, K. (2022, March). *Virtual Stakeholder Consultation Report: Implementing India's Data Protection Regime*. The Dialogue. https://thedialogue.co/wp-content/uploads/2022/04/Implementing-India%E2%80%99s-Data-Protection-Regime.pdf

[67] Carrigan, C., & Poole, L. (2015). *Structuring Regulators: The Effects of Organizational Design on Regulatory Behavior and Performance*. University of Pennsylvania Law School. Retrieved April 30, 2022, from https://www.law.upenn.edu/live/files/4707-carriganpoole-ppr-researchpaper062015pdf

[68] Government realising the direct leakage of revenue through piracy in the movie industry, Telangana adopted the UK model for protecting Intellectual Property Rights. Instituting a body at the state level, the government collaborated with the film industry. The industry would share clips of the film in the body; the government would search the entire web to find out if those exact matches appear on any other website using sophisticated technologies.

[69] Rai, S. (2018, February 9). *A Pragmatic Approach to Data Protection*. The Leap Blog. Retrieved May 1, 2022, from https://blog.theleapjournal.org/2018/02/a-pragmatic-approach-to-data-protection.html

2.3.1. BEST PRACTICES FROM OTHER JURISDICTIONS: INSTITUTIONAL DESIGN

Due to the diversity and vastness of the country, it is not ideal to have a single DPA for the entire country. There are various best practices from other jurisdictions on decentralisation of the DPA, and also some of our Indian regulators have a decentralised institutional design, as discussed in this section.

A. STATE-LEVEL DPAS MODEL: GERMANY CASE

Germany doesn't have a single central Data Protection Authority; instead, it has several different Authorities for each of the 16 German states responsible for ensuring that data protection laws and regulations have been complied with across the nation. At the helm, is "The Federal Commissioner", which functions as the German Federal supervisory authority, in compliance with Article 51 of the EU GDPR and also responsible for all federal authorities and organisations.

The state-level authorities govern all aspects of the private sector and public sector in their respective States, except the telecommunication and postal services in the private sector. The responsibility of supervisory authority over telecommunications and postal services lies with the Federal Government.[70]

However, in the Indian context, while the overarching framework or data protection regulation must come from the national level, some of the functions like grievance redressal and awareness building etc., must be delegated to state-level bodies as discussed in Section 4.1.5.

B. EXISTING STATE-LEVEL AUTHORITIES IN INDIA

In India, Under section 5(1) of the RTI Act, every administrative unit and office (except the scheduled two[71] units) is mandated to designate a separate central and state public information officer depending on the state and central list. Further, section 5(2) of the RTI Act also mandates public authority to appoint an officer as central and state assistant public information officers at every sub-divisional and sub-district level.

Besides, while the consumer protection authority of India is established at the central level, the Consumer Protection Act mandates the establishment of the consumer protection council and consumer dispute redressal commission at all three levels, i.e., central, state, and district.

2.4. Lack of Financial Independence of DPA

By not vesting the control over raising funds from other sources and relying solely on Government approval, the financial independence of the DPA can be limited. If the Central government decides the means and ways for generating revenue in addition to its grants and all other sources of income. All such income will be transferred to the Data Protection Authority fund for the use of the Authority as per the Government's directions. However, having enforcement and fundraising functions within DPA could cause moral hazards due to lack of separation of power, at the same time, completely restricting DPA from determining revenue sources which will be disproportionate.

[70] Ibid
[71] Refer to section 24 of RTI Act, 2005

Financial independence is key as the Authority functions as an independent arbitrator between all stakeholders, including the Government, which reinforces the need for authority that is not to be entirely or heavily dependent on the Government for its financial needs.[72] The complexity of the competing interests between the data principals (both users and providers), the government, the community, and the state[73] reinforces the need for financial independence, which in turn facilitates functional independence. The first step toward establishing financial independence is to keep the sole power of the central government at an arm's length distance from deciding financial matters of DPA.

2.4.1. BEST PRACTICES FROM OTHER JURISDICTIONS: FINANCIAL INDEPENDENCE

As a fourth branch regulator, the functional and financial independence of the DPA is a cruciale element. Some of the jurisdictions have made financial independence an integral element of the effective function of DPA, as discussed below.

A. INDEPENDENT ANNUAL BUDGET OF DPA: EU CASE

Article 52[74] of the EU GDPR encourages financial autonomy and promotes the independence of any data protection authority established. Article 52(6) and Recital 120[75] specifically outlines the need for every member state to "*ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget*." The independence of DPAs is also increased by ensuring that they are involved in all aspects of the budgetary preparations, assessing the amount needed in a detailed proposal, and being consulted throughout the decision-making process.[76] For instance, the Polish DPA drafts its own budget, which is then presented to Parliament by the government. The government cannot introduce any changes to the proposal, and the only institution that decides is Parliament.[77] Similarly, the Italian DPA's budgetary proposal is submitted by the DPA to the government and included directly in the State Budget – which is to be approved by Parliament, however the DPA interfaces with Parliament with regard to all issues relating to the final budgetary apportionment.[78]

Though the EU encourages financial autonomy, this is not entirely binding on the Member States; however, in the case of the *European Commission v Republic of Austria*, the CJEU expressed concern that in instances where the budgetary competence of the DPA falls within a specific ministerial department CJEU stated that "the attribution of the necessary equipment and staff to such authorities must not prevent them from acting 'with complete independence' in exercising the functions entrusted to them."[79] Thus, the CJEU effectively encourages the Member States to adopt maximum financial autonomy measures.

---

[72] Patnaik, A. (2020, July 24). *Who controls citizens' data? Personal Data Protection Bill must empower an independent and robust Data Protection Authority. Times of India*. Retrieved April 27, 2022, from https://timesofindia.indiatimes.com/blogs/toi-edit-page/who-controls-citizens-data-personal-data-protection-bill-must-empower-an-independent-and-robust-data-protection-authority/

[73] *Elements of independence of data protection authorities in the EU*. (1997, June 13). FRA. Retrieved April 27, 2022, from https://www.asktheeu.org/en/request/2398/response/9765/attach/3/21.FRA%20Focus%20Data%20protection%20authorities%20independence%20funding%20and%20staffing%20ATTACHMENT%20FRA%202013%20Focus%20DPA.pdf

[74] EU General Data Protection Regulation, https://gdpr-info.eu/

[75] Recital 120 deals with Features of Supervisory Authorities under the EU GDPR,

[76] Ibid

[77] Supra at 67

[78] European Union Agency for Fundamental Rights, Elements of independence of data protection authorities in the EU, Page 12

[79] CJEU, C-614/10, Commission v. Republic of Austria, 16 October 2012, para. 58.

B. DIVERSIFICATION OF FINANCIAL PORTFOLIO: UNITED KINGDOM CASE

In the United Kingdom, apart from the budgetary allocation and Government aid provided, the Information Commissioner's Office (ICO) can collect data protection fees from all entities (except those explicitly exempted) that process data.[80] As per Information Commissioner's Annual Report and Financial Statements 2017-18[81], the ICO received a grant in aid from the Government of 5195 pounds sterling, along with a 1400 pounds sterling[82] grant in aid specifically for the preparation of the GDPR implementation in the year 2018. Besides, ICO also earned 21,300 sterling from collecting data protection fees, i.e., a certain amount of money collected from entities that handle personal information to ensure the regulator is appropriately resourced. This is indicative of the ICO's ability to sustain itself independently financially.

[80] https://ico.org.uk/for-organisations/data-protection-fee/
[81] https://ico.org.uk/media/about-the-ico/documents/2259463/annual-report-201718.pdf
[82] Ibid

3. FUNCTIONAL ROADBLOCKS WITH THE DATA PROTECTION AUTHORITY

Despite getting the structural foundation straight, still, DPA may hit various roadblocks as it comes to force because technology evolves faster than the regulations, and how the authority keeps up the pace through building capacity, agility, cooperation, and coordination is a crucial question.

In India, the implementation of the privacy regime will be a fresh start for regulators and domestic industries. The range of entities covered by DPA will be immensely vast, starting from big tech to MSMEs to government agencies. While a one-size-fits-all approach towards data protection regulation might bring in compliance (at a cost) amongst the horizontally (within the sectors) and vertically (across various sectors) diverse range of data fiduciaries, it might not bring cooperation.

While building cooperation is crucial, having coordination amongst the regulators should also be the priority to avoid regulatory arbitrage. As JPC deliberated on the PDP Bill, various data regulations and governance frameworks at different capacities have been floated in India in a disjointed ad-hoc manner. While the withdrawn PDP Bill did talk about coordination amongst the functioning regulators and governments, still harmonising technology regulations to have a uniform data protection framework for the country will be a significant task for the DPA.

In addition to the above-discussed central government interferences, some of the provisions in the PDP Bill empowered the central government to issue binding orders in the form of directions without any due process to be followed. This once again reiterates the importance of keeping the central government at arm's length, as it can hamper the functional independence of the DPA.

Besides, DPA was not empowered to decide on its internal regulations and processes, regulatory strategies, or selection of issues to be addressed as part of its functions without central government interference. The below table maps the issues against the provisions in the PDP bill and JPC's recommended Draft Data Protection Bill, 2021 in terms of DPA's functions. Followed by it, we discuss the critical and first-order functional issues tabulated in detail.

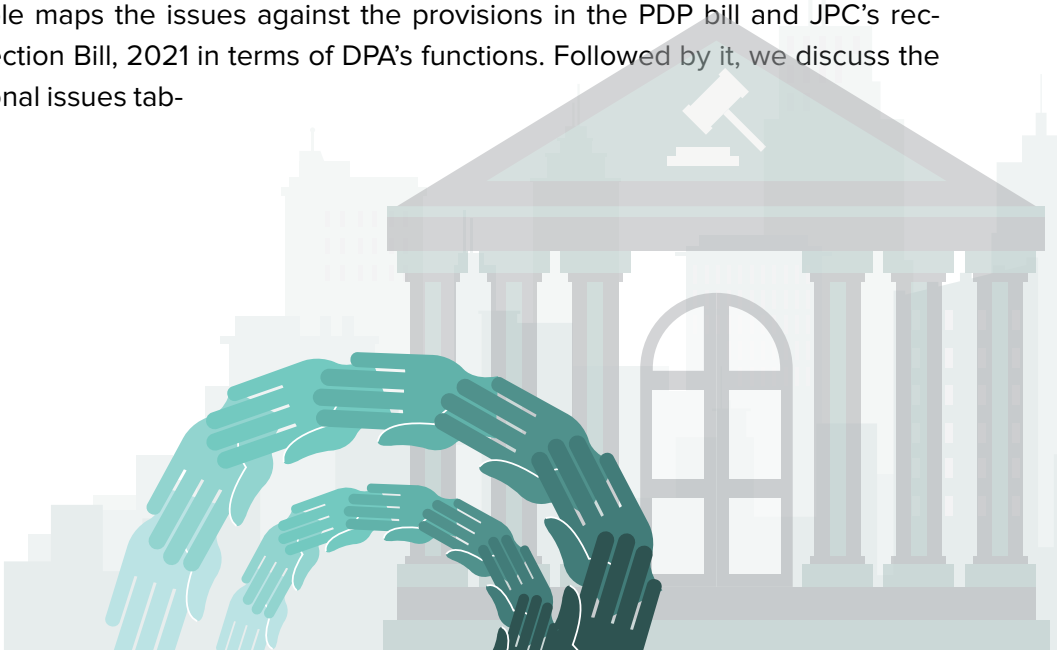


Table 2: Functional issues with DPA

Roadblocks to functions of DPA	Provisions in PDP Bill	Provisions in the JPC recommended Data Protection Bill, 2021	Issues
Issues with rulemaking	Clauses 50 - DPA must set the standards and codes of practice for data handle/ use	N/A	Technology often evolves faster than the regulation itself, however, this clause does not envision or make suggestions on how the DPA intends to be up to date or make preemptive measures. Besides, the wide range of entities is likely to be covered by DPA, starting from big tech to MSMEs to government agencies. This is owing to the wide definition of "data fiduciary" under the PDP Bill, but the clause hints toward a one-rule fits all approach which might not be appropriate for these varying entities.
Discretionary power to DPA	Clause 52(1) - DPA is empowered to issue, without prejudice to any other provisions of these Acts, a call for information required *reasonably* to discharge its functions[83] from any data fiduciary or data processors. Clause 53 - In case of dispute, DPA will form an inquiry officer (who is an employee of DPA) who will investigate and report to the board Clause 55 - The inquiry officer can order the seizure of information through a police officer or any officer of the Central Government, provided there are reasonable grounds to believe that information being sought is likely to be tampered with, altered, manufactured or falsified.	N/A	The main issue is the use of overbroad language and the scope for discretion provided to the authority. These clauses must be thought through in terms of the separation of functions as it seems that same authority (DPA) will be entrusted to undertake rulemaking and rule implementation.
Coordination with government and sectoral regulators	Clause 50(2) – Authority may approve any code of practice submitted by any sectoral regulator or statutory authority, or any departments or ministries of the central or state government (as well as industry) Clause 56 – Establishing coordination between authority and other regulators	N/A	Though these clauses deal with coordination amongst the functioning regulators and governments, still, harmonisation of technology regulations to have a uniform data protection framework will be a significant task for the DPA.

[83] Clause 49 of the PDP Bill, 2019 and DPB Bill, 2021 as recommended by the JPC

3.1. ISSUES WITH RULE-MAKING

The Bill laid down the extensive potential for rule-making. However, it failed to prescribe mechanisms that promote participatory policy-making and accountability, such as public consultation, notice and comment period, responses to comments received, regulatory impact assessment (cost-benefit analysis) and harmonisation of other existing rules.

In light of prior experience, even when regulators follow notice-and-comment procedures, the follow-through with responses and incorporation of the comments in the drafts is low.[84] A perusal of official websites indicates that the Securities Exchange Board[85] of India and Reserve Bank of India[86] fail to publish comments that they received in most cases.

Unfortunately, in India, Regulatory Impact Assessment (RIA) is not a practice/procedure adopted by regulatory bodies in India.[87] There is a limited acceptance of RIA by the Government as a pre-policy measure. Even prior to the inclusion of localisation provisions within the PDP Bill, there was no form of cost-benefit analysis or RIA conducted by the Ministry.

The PDP 2019 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.[88] This would include, for example, a draft bill on DNA technology, health data retention and management etc.[89] Given that the upcoming data protection bill will prevail over other existing and proposed laws in case of inconsistency, this jurisdictional precedence is easier said than implemented in the Indian regulatory landscape.[90]

3.1.1. BEST PRACTICES FROM OTHER LEGACY REGULATORS OF INDIA

Various Indian regulators follow a participatory approach to rule-making. They diligently engage with the stakeholders through the consultation process, mechanise robust citizen feedback procedures, and dedicate time for notice and comment periods, as discussed below:

A. CONSULTATIVE PROCESS

Many regulatory bodies are mandated through statute to include consultations in the process of regulation-making. For instance, the Telecom Regulatory Authority of India (TRAI) and the Airports Economic Regulatory Authority of India are bodies mandated to conduct consultative processes. The level of consultation mandated is subject to variation, respectively.

---

[84] Zaveri, B. (2016, January 17). *Participatory governance in regulation making: How to make it work?* The Leap Blog. Retrieved April 27, 2022, from https://blog.theleapjournal.org/2016/01/participatory-governance-in-regulation.html
[85] https://www.sebi.gov.in/
[86] https://www.rbi.org.in/
[87] *Institutionalising Regulatory Impact Assessment in India*. (n.d.). Cuts CCIER. Retrieved April 28, 2022, from https://cuts-ccier.org/pdf/BP-Institutionalising_Regulatory_Impact_Assessment_in_India.pdf
[88] Shekar, K., Bahl, V. S., & Singh, A. (2022). *DPB 2021: The Data Protection Authority And Coordination With Sectoral Regulators*. The Dialogue - NASSCOM. Retrieved July 19, 2022, from https://thedialogue.co/wp-content/uploads/2022/07/DPB-2021-The-Data-Protection-Authority-and-Coordination-with-Sectoral-Regulators.pdf
[89] Shekar, K. (2022, April). *Building Effective and Harmonised Data Protection Authority: Strategies for Structural Design and Implementation*. The Dialogue. https://thedialogue.co/wp-content/uploads/2022/04/Building-Effective-and-Harmonised-Data-Protection-Authority-Strategies-for-Structural-Design-and-Implementation.pdf
[90] Shekar, K., Bahl, V. S., & Singh, A. (2022). DPB 2021: *The Data Protection Authority And Coordination With Sectoral Regulators*. The Dialogue - NASSCOM. Retrieved July 19, 2022, from https://thedialogue.co/wp-content/uploads/2022/07/DPB-2021-The-Data-Protection-Authority-and-Coordination-with-Sectoral-Regulators.pdf
[91] https://carnegieindia.org/2019/04/02/measuring-regulatory-responsiveness-in-india-framework-for-empirical-assessment-pub-78871

B. PARTICIPATORY POLICY MAKING

While consultation is sub-set, overarchingly, DPA must adopt a participatory policymaking approach. Among India's many regulatory bodies, TRAI has robust citizen feedback procedures. TRAI has shown continuous efforts to include comments from consumer groups. However, consumer participation is usually low in these meetings, with service providers attending these meetings and benefitting from discussions in these meetings.[92] Some of the best practices for benchmarks are as follows:

a. more than two mechanisms like town halls, call for comments etc. for seeking public input into planning,

b. clear time frame for decisions,

c. clear time frames for consultation, and

d. accountability for incorporation of inputs received through public engagement.

While TRAI is a legacy regulator, newer regulators, such as the Unmanned Aircraft Systems Promotion Council under the Drone Rules, 2021, explicitly mention collaborating with industry experts and academic institutions for policy advice within the statute.

C. NOTICE AND COMMENT PERIODS

Regulatory bodies in India have notice and comment periods, but days vary accordingly. Taking the examples of IRDAI, RBI, FSSAI, and TRAI, the average number of days provided to respond to drafts lies in the range of 17-41 days.[93] It has to be noted that bodies like SEBI and RBI rarely publish explanatory documents before issuing regulations.[94] Besides, some of these regulators find a way around a participatory approach mandated in statute through language usage. For instance, RBI calls its subordinate regulations mostly "notification", which doesn't necessarily need comments from the stakeholders. On the contrary, countries like the United States of America (USA) and Portugal have mandatory notice and comment procedures that are legally backed, while Canada is driven by policy directives.[95] In the Indian context, TRAI is the only regulatory body that publishes its comments and furnishes responses to them.[96]

D. REGULATORY IMPACT ASSESSMENT (RIA)

In spirit, the public consultations and invitation of comments are a step to include stakeholders in regulation-making. The Pre-Legislative Consultation Policy by the Government of India acknowledges the importance of gauging the impact of legislation on its stakeholders. In terms of official recommendation, NITI Aayog had suggested that RIA be incorporated into the regulation-making process through the Regulatory Reform Bill.[97]

E. CROSS-REFERENCE REGULATION

Sectoral or domain-specific regulators could work with the DPA to create regulations that cross-

[92] http://www.cogitasia.com/release-proposed-regulation-in-india-with-cost-benefit-analysis-input-from-stakeholders/
[93] https://www.bloombergquint.com/law-and-policy/how-responsive-are-indias-regulators
[94] https://www.oecd.org/mena/governance/36785341.pdf
[95] https://www.bloombergquint.com/law-and-policy/how-responsive-are-indias-regulators
[96] https://niti.gov.in/planningcommission.gov.in/docs/aboutus/committee/wrkgrp12/wg_brf2103.pdf
[97] https://carnegieindia.org/2019/04/02/measuring-regulatory-responsiveness-in-india-framework-for-empirical-assessment-pub-78871

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.[98] This could be useful in areas such as cybersecurity, where the DPA 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 the upcoming bill 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.

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 sectors.[99] 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 upcoming data protection bill and the various existing and proposed laws.

3.2. DISCRETIONARY POWER TO DPA

Along with the wide scope for inquiry and seizure of information, there is also a concern regarding misuse or abuse of this discretion by the authority that is not entirely independent in its foundation. Recently, the protection of commercially sensitive information submitted during investigations[100] and inquiries has been a priority for companies in digital markets. In the recent past, we have witnessed various companies approach the courts to seek redressal against leaks of sensitive information, which includes the recent investigations by the Competition Commission of India.[101] Keeping in mind the vacuum created by the absence of a trade secrets law in the Indian jurisdiction;[102] it becomes especially imperative that relevant safeguards for data fiduciaries are in place.

3.2.1. ANTICIPATED BEST PRACTICES

In the past, confidentiality regimes of other Indian regulators like the CCI, have suffered from fragilities, necessitating authorities to go back to the drawing board. In the context of the DPA, we hope that either separate regulations that pertain to the maintenance of confidentiality are formulated in due time, or its general regulations focus on this aspect, consequently providing robust confidentiality safeguards.

3.3. COORDINATION WITH GOVERNMENT AND SECTORAL REGULATORS

As India's digital economy develops, the legal and regulatory framework that governs it is still being finalised to strike a balance between consumers' rights, innovation, and states' legitimate needs. This

[98] 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/

[99] *See,* Ministry of Finance, *Report of the Financial Sector Legislative Reforms Commission – Volume 1*, (2014), available at https://dea.gov.in/sites/default/files/fslrc_report_vol1_1.pdf

[100] Clause 49(3) of the Bill provides that the DPA shall not disclose any confidential information that is treated as confidential by the fiduciary; except where the DPA is required to do so under any law or to carry out its functions.

[101] Kalra, A., & Roy, A. (2021, September 24). *Google, India antitrust watchdog tussle in court over probe leak*. Reuters. Retrieved April 28, 2022, from https://www.reuters.com/world/india/google-india-antitrust-watchdog-tussle-court-over-probe-leak-2021-09-24/

[102] Raina, C. (2015). Trade Secret Protection in India: The Policy Debate. Centre for WTO Studies. Retrieved April 28, 2022, from http://wtocentre.iift.ac.in/workingpaper/Trade%20Secret%20Protection%20in%20India-%20The%20policy%20debate.pdf

could lead to a lot of overlap between various regulatory authorities and laws - which is yet to be adequately addressed.[103]

For instance, two key policy frameworks that will be the backbone for promoting innovation and privacy protection would be the Competition Act and the upcoming Data Protection Regime. There are concerns about jurisdictional conflict between the DPA and other regulators, including the Competition Commission of India (CCI)[104], especially over data privacy and protection questions. It is imperative to ensure coordination between DPA and other regulators like the CCI to prevent regulatory burden, and uncertainty for stakeholders within digital markets,[105] primarily as India seeks to position itself as a favourable market in this space.

3.3.1. BEST PRACTICES

A. CROSS-REGULATOR CONSULTATION PROCESS

In India, The National Competition Policy and Allied Matters, 2011, constituted by the Ministry of Corporate Affairs, proposed a mandatory consultation process recognising that sectoral regulators have domain experts in their relevant sectors.

Other jurisdictions, such as Argentina, France and Turkey, have a legal requirement for mandatory consultations between competition agencies and sector regulators.

B. SINGLE ENFORCEMENT AUTHORITY MODEL: USA CASE

The United States doesn't have an overarching federal-level data protection regulation. Still, there are various related privacy and data protection regulations and legislations catering to an issue, population, sector and state. These buckets of regulations have different enforcement authorities and agencies. But in terms of cross-border data flows, the European Union had recognised the Federal Trade Commission (FTC) as the central enforcement authority for data protection in the case of the EU-US Privacy Shield. While EU-US Privacy Shield was struck down in Schrems I and II case by the Court of Justice of the European Union for a different reason when it was functioning, the United States effectively implemented the same in the data protection landscape, which is subjected to multiplicity of laws.

C. FORUM OF DIGITAL PLATFORM REGULATORS: AUSTRALIA CASE

Australia follows a co-regulatory mechanism. Australia recently constituted a forum of digital platform regulators[106] that includes all of the regulators in Australia that regulate digital platforms, forming a collective of diverse regulatory options. 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.

---

[103] Shekar, K. (2022, April). *Building Effective and Harmonised Data Protection Authority: Strategies for Structural Design and Implementation*. The Dialogue. https://thedialogue.co/wp-content/uploads/2022/04/Building-Effective-and-Harmonised-Data-Protection-Authority-Strategies-for-Structural-Design-and-Implementation.pdf

[104] In a report published by CCI on the telecom sector (Market Study On The Telecom Sector In India, 2021) in January 2021, the Commission analysed the synergy between competition and privacy in a non-price competition market. The report notes that abuse of dominance can be in the form of lower privacy protection for consumers, as sub-optimal privacy standards can impact consumer welfare. 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)

[105] Shekar, K. (2022, April). *Building Effective and Harmonised Data Protection Authority: Strategies for Structural Design and Implementation*. The Dialogue. https://thedialogue.co/wp-content/uploads/2022/04/Building-Effective-and-Harmonised-Data-Protection-Authority-Strategies-for-Structural-Design-and-Implementation.pdf

[106] *Agencies form Digital Platform Regulators Forum* | ACCC. (2022, March 11). Australian Competition and Consumer Commission. Retrieved May 22, 2022, from https://www.accc.gov.au/media-release/agencies-form-digital-platform-regulators-forum

4. RECOMMENDATIONS

As the envisioned DPA will have an influential and crucial role in this digital age, in this section, we provide recommendations to weed out some of the structural and functional issues and bottlenecks (discussed above) to help serve its purpose, as mentioned in the Personal Data Protection bill, 2019.

The below-discussed recommendations are advised by some of the international best practices, processes followed by some of the legacy regulators and suggestions provided by various committees formed by the Indian government. While these recommendations would act as a means to alleviate the concerns with DPA structuring and function, however, we also propose government to consider any other recommendations and strategies suggested by the experts and stakeholders to have a robust foundation for India's envisioned Data Protection Authority while revisiting the Bill.

4.1. STRUCTURAL ASPECTS

There are various issues in DPA structuring, as envisioned under the PDP Bill 2019, starting from appointment, removal, the composition of authority, inappropriate accountability framework, lack of separation of power, transparency, and financial independence. In this sub-section, we provide recommendations for making the foundations of the DPA strong by solving some of the structural concerns.

4.1.1. ALTERATION OF THE APPOINTMENT PROCESS

The selection procedure for members and chairpersons of the DPA should be independent. To achieve this, the upcoming data protection bill must provide that the President of India appoints the DPA's members and chairperson as followed in many jurisdictions like Brazil, France etc., as per the advice of the selection committee.

As the independence of authority partially depends upon the selection committee, it is important to have a combination of the judiciary, executive and legislative within the committee to ensure independence.[107] The selection committee currently is heavily executive driven; alternatively, we recommend that the selection committee should comprise the following members to ensure independence:

- **Judiciary:** Representation of retired/sitting apex court judge, practising lawyers, etc.
- **Legislature:** Opposition Party Leader (similar to RTI Act), chairperson of Standing Parliamentary Committee on Information Technology, other relevant standing committee chairpersons, members elected from both lower and upper houses of the parliament (Similar to the structure followed in France).
- **Executive:** Cabinet Secretary, Secretary of MeitY, Legal affairs etc. (similar to PDP Bill 2019).
- **Independent members:** Academicians, civil society members, business representatives, industry experts etc.

[107] Roy, S., Shah, A., Srikrishna, B.N., & Sundaresan, S. (2018, July 10). *Building State capacity for regulation in India*. Macro/Finance Group at NIPFP. Retrieved May 1, 2022, from https://macrofinance.nipfp.org.in/PDF/RSSS_building-state-capacity.pdf

4.1.2. POWER AND PROCEDURE OF REMOVAL

The removal procedure should be of high standards, limiting the leveraging power of the executive to drive the functions of DPA. The current removal procedure is subjected to the central government's discretion which doesn't give tenure security to the authority to act independently. For instance, under Section 11 of the Reserve Bank of India Act, 1934 central government can remove the governor at their discretion which impacts it's independence.[108]

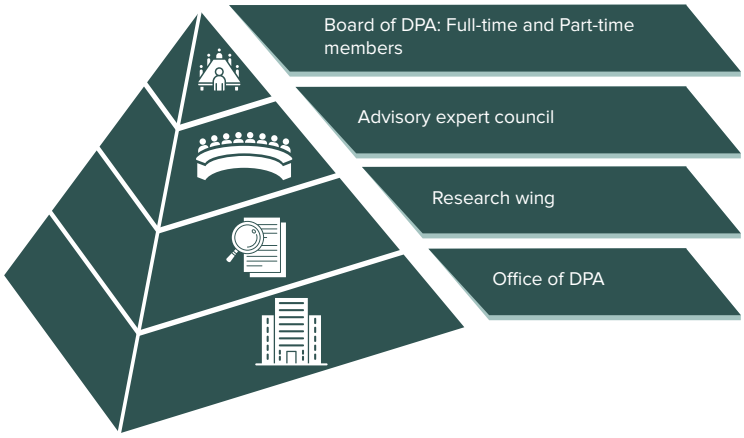
The President of India must command the removal order of the chairperson, and members of the DPA after both houses of Parliament support the motion by a majority or on the ground of misbehaviour after the Supreme Court's investigation and verdict. A similar model is followed in the removal procedure[109] of the Public Service Commission, which fares well as an independent body.[110] Besides, the removal motion should be initiated on the below grounds (advised other jurisdictions[111]) if the members and chairs are:

- Punished/sentenced to prison under India Penal Code.
- Incapacitated in delivering the duties owning to physical and mental ointments.
- Bankruptcy.
- Misconduct and disciplinary allegations (like sexual harassment) during the tenure.
- Lack of performance evaluated using a robust mechanism by an independent commission.

4.1.3. TIERED COMPOSITION MODEL

To enhance the capacity of the Data Protection Authority, we propose a tiered structural design for enforcing data protection and privacy, as illustrated below. The tiered approach proposed is a combination of models followed by other jurisdictions like Brazil, Japan, South Africa and other Indian regulators, and our research on structuring DPA. We believe the suggested tiered model would bring clarity to structuring the DPA using a bottom-up approach where tasks and responsibilities are mapped and partially calibrated.

Figure 1: Tiered Structure



[108] Sridhar, G. N. (n.d.). *How independent is the Reserve Bank Governor?* The Hindu BusinessLine. https://www.thehindubusinessline.com/money-and-banking/how-independent-is-the-reserve-bank-governor/article7503967.ece
[109] Article 317 of Indian Constitution
[110] Bhalerao, C. N. (1958). THE UNION PUBLIC SERVICE COMMISSION (INDIA) AND THE U. S. CIVIL SERVICE COMMISSION. *The Indian Journal of Political Science, 19*(3), 263–270. http://www.jstor.org/stable/42743611
[111] Refer to Section 2.2.1
[112] Refer to Section 2.3.1.2
[113] Refer to Section 2.1.1.6
[114] Refer to Section 2.1.1.1

Board of DPA: In addition to the chairperson, the five-member board must be expanded significantly to include full-time and part-time members like other regulators in India to deliver its functions.

- **Full-time members:** The full-time members must bring in diversity in terms of representation, including law expertise, technology knowledge, cyber security expertise, industry expertise, legal enforcement expertise, and economic, cultural and sociological expertise.
- **Part-time members:** Provision for having part-time members will allow DPA to engage with a diverse range of experts on a short-time basis depending upon the needs. The part-time members' provision is followed by various jurisdictions like Japan, South Africa etc. Therefore, qualifications of the part-time members must be kept broad such that DPA can extract much out of this – where it can also include sitting parliamentarians, business representatives, industry experts, researchers, civil society members etc.

Advisory expert council: Similar to Brazil's National Council for Personal Data Protection and Privacy, DPA must have an advisory expert council comprising parliamentarians, judges, members of the parliamentary standing committees, regulators, civil society members, researchers, academicians, trade union confederation, business associations and the labour and business sector representatives etc.

The council must aid the board (a) in the constitutional data protection regulations, guidelines, standard-setting, and policies, (b) evaluate the performance of the regulations and policies (c) conduct various knowledge management and dissemination work.

Research wing: Like CAFRAL[115] – an independent research institution promoted by the Reserve Bank of India, DPA must also have a research wing that aids the advisory expert council with its functions.

Office of DPA: DPA must also have sufficient permanent and temporary office staff to aid the functions of the tiered model proposed (like in the case of Italian DPA). To have qualified staff, DPA can borrow learnings from the Italian style of competitive public examination to fill the positions, where DPA can also adopt a civil servant recruitment model. Currently, in India, the intake of civil service officers happens through the Civil Service Exam (UPSC), where DPA can have competitive exams for staff (similar to Italy). Besides, recently India instituted the lateral entry model, which the DPA can also explore. In addition to administrative wings, the office of DPA must also comprise the following:

- **Dispute Resolution wing (DR):** There has to be a dispute resolution wing - a mediated litigant dispute resolution framework facilitated through online/offline platforms. DR must be extensively used to resolve disputes as this is more efficient, quick turnaround and cost-effective. DPA must mechanise the DR framework in order to reduce its adjudicatory burden.
- **IVR wing[116]:** The first step in the grievance redressal process is to find the designated portal for lodging a dispute. In many cases, navigating the grievance management system for both consumers and entities is arduous, making it difficult to reach the designated portal.[117] Therefore, we propose to have an Interactive Voice Response (IVR) wing as part of DPA's office. This automated voice response system (through call) will navigate consumers (or entities) to reach the appropriate grievance portal, i.e., the data fiduciary's grievance redressal system or dispute resolution wing of DPA.

---

[115] https://www.cafral.org.in/

[116] Shekar, K. (2022, April). *Building Effective and Harmonised Data Protection Authority: Strategies for Structural Design and Implementation*. The Dialogue. https://thedialogue.co/wp-content/uploads/2022/04/Building-Effective-and-Harmonised-Data-Protection-Authority-Strategies-for-Structural-Design-and-Implementation.pdf

[117] Chivukula, C. (2021, February 18). *Consumer Grievance Redress in Financial Disputes in India. Dvara Research*. Retrieved May 22, 2022, from https://www.dvara.com/research/blog/2021/02/18/consumer-grievance-redress-in-financial-disputes-in-india/

4.1.4. FINANCIAL STRUCTURE OF DPA

As a fourth branch regulator, the financial independence of the DPA is a crucial element. The DPA would need a steady and sustainable flow of revenue to keep its operations (a) seamless, (b) financially and functionally independent (c) safe from data fiduciaries lobbying and state capture. To achieve these goals, we propose various facets of revenue streams (advised by portfolio diversification[118]) for the DPA at different levels, advised by other jurisdictions' experience, which let the operations move without dependence on one source of income.

Union Budget: While the central government will be providing grants to DPA, we propose a transparent budgetary structure like the one followed in Hungary. The DPA's funding must be guaranteed through a separate budgetary appropriation line within the upcoming Bill.[119] The budget of the DPA must constitute an independent title within the budgetary chapter of Parliament for approval. Besides borrowing inferences from Polish model, we propose that the Board of DPA must be consulted during the drafting of the budget for DPA.

Data Protection fees: In the United Kingdom, the Information Commissioner's Office (UK's DPA) raises about 85% to 90% of the funding requirement by imposing data protection fees on organisations that use and process data. Drawing inferences from the UK model, we recommend DPA to have slabbed data protection fees depending upon the market share, profits and nature of businesses.

Selling & Leasing rights: In Brazil, the DPA can generate its revenue through selling or leasing movable and immovable assets of the authority, resources derived from agreements, contracts or similar instruments held with entities, bodies, or companies and by selling publications, technical matters, data, information etc. Similar rights for selling and leasing assets must be provided to India's DPA. Moreover, while the Indian government had recently launched asset monetisation plans,[120] in terms of regulators, who has the ownership rights of the public assets is unclear. Moreover, the regulator's capacity in terms of maintenance of assets,[121] enforcing a contract while leasing etc.[122] has to be enhanced to have fruitful revenue from this source.

Plaintiff and defendant contribution: DPA shall levy a nominal fee for providing dispute resolution to both plaintiff and defendant. This nominal fee should be an operational cost in addition to a small margin. This should also have exemptions where the cost of approaching DPA must not hamper individuals from receiving grievance redressal.

Other means and ways: We suggest that the DPA be provided independence to decide on other means and ways to generate revenue without hampering the functions as will to be envisioned in the Bill with appropriate checks and balances to weed out moral hazards.

---

[118] Jain, P. (2022, February 18). *Your Money: Five benefits of a diversified portfolio*. The Financial Express. Retrieved May 1, 2022, from https://www.financialexpress.com/money/your-money-five-benefits-of-a-diversified-portfolio/2437206/

[119] In addition to the grant-in-aid from the government

[120] *NATIONAL MONETISATION PIPELINE*. (2021, August 23). NITI Aayog. Retrieved May 21, 2022, from https://www.niti.gov.in/sites/default/files/2021-08/Vol_I_NATIONAL_MONETISATION_PIPELINE_23_Aug_2021.pdf

[121] Lahiri, A. (2021, November 29). *India's asset monetisation plan*. Ideas for India. Retrieved May 21, 2022, from https://www.ideasforindia.in/topics/macroeconomics/india-s-asset-monetisation-plan.html

[122] J., P. P. (2021, September). *Is monetising public assets a good idea?* The Hindu. https://www.thehindu.com/opinion/op-ed/is-monetising-public-assets-a-good-idea/article62105542.ece

4.1.5. QUASI-FEDERAL INSTITUTIONAL DESIGN

Due to the diversity and vastness of the country, it is not ideal to have a single DPA for the entire country for the reasons discussed above. For instance, Germany doesn't have a single central Data Protection Authority; instead, it has several different Authorities for each of the 16 German states responsible for ensuring that data protection laws and regulations have been complied with.

Similarly, in India, Under section 5(1) of the RTI Act, every administrative unit and office (except the scheduled two[123] units) is mandated to designate a separate central and state public information officer depending upon the state and central list. Further, section 5(2) of the RTI Act also mandates public authority to appoint an officer at every sub-divisional and sub-district level as central and state assistant public information officers, respectively. Besides, while the consumer protection authority of India is established at the central level, the Consumer Protection Act mandates the establishment of the consumer protection council and consumer dispute redressal commission at all three levels, i.e., central, state, and district.

Therefore, the DPA must branch out into various state-level authorities such that the quasi-federalist model of Indian Democracy is maintained, where (a) states have authority over the data collected under state laws and (b) also build trust through bringing democratic legitimacy in terms of proximity. Besides, a state-level body should aid in capacity issues in terms of adjunction function like in the case of RTI[124], where the state-level authorities, i.e., the State Information Commission, are empowered to dispose of complaints within their state and shall have the same power vested in a civil court under the Code of Civil Procedure, 1908. Besides, while we move toward decentralised DPA, it is also essential to adopt an institutional design that ensures maximum coordination between the central level and state level to avoid regulatory arbitrage and confusion. Moreover, the grievance redressal function of the state-level DPA should have a simplified and progressive structure adopting some features discussed in The Right Of Citizens For Time Bound Delivery Of Goods And Services And Redressal Of Their Grievances Bill, 2011.[125] Besides, grievance redressal mechanisms must give importance to the local context and scenarios.

Also, as a single DPA at the centre will dilute the awareness-creating function of the DPA, this function must be delegated to state-level DPA to make people or data principals aware of the value of the data through various exercises. Therefore, it would be ideal to branch out the DPA to the central and state-level where a couple of officers at the state level can deal with functions like awareness creation.

4.2. Functional Aspects

Despite getting the structural foundation straight, still, DPA will hit various roadblocks as it comes into force because technology evolves faster than the regulations. How the authority keeps up the pace through building capacity, agility, cooperation, coordination, and functional independence is still a crucial question. In this sub-section, we provide recommendations for making the operations of DPA smoothen and proactive by solving some of the functional concerns.

[123] Refer to section 24 of RTI Act, 2005
[124] Refer section 18(1) of RTI Act, 2005
[125] *The Right Of Citizens For Time Bound Delivery Of Goods And Services And Redressal Of Their Grievances Bill, 2011.* (2011, December 19). PRS India. Retrieved May 22, 2022, from https://prsindia.org/files/bills_acts/bills_parliament/2011/Right_of_Citizens_for_Time_Bound_Delivery_of_Goods_and_Services_and_Redressal_of_their_Grievances_Bil,_2011.pdf

4.2.1. DATA PROTECTION BOARD: A COORDINATING BODY[126]

High-level coordination amongst the regulators, including DPA and policymakers, is necessary to implement data protection regulation. While there are provisions for coordination and harmonisation in some of the legislation and data sharing & transfer framework and policy, including the PDP bill, they stand disjointed and unclear. For instance, the provision on MoUs within the PDP Bill only considers regulators/authorities constituted under a Union or State law, precluding non-statutory regulators or authorities with a potential jurisdictional overlap like the National Health Authority.[127]

While considering fleshing out elements of MOU and having interlocking directorates like other regulatory systems in India. 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.[128] However, there are limitations to these approaches.[129]

Therefore, there is merit in exploring the establishment of a formal body, such as a data protection board,[130] similar to the European Data Protection Board, the Indian government (in association with legislators and the judiciary) may constitute a Data Protection Board (DPB).

The EU's Data Protection Board model does fit our case because it was formed for harmonisation.[131] Also, various countries use this mechanism to enhance inter-regulatory coordination like Australia[132], the United Kingdom[133], Brazil[134] etc. Besides, similar to this 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,[135] whose primary mandate is to enhance inter-regulatory coordination.

DPB, as an independent body, must look into the consistent application of uniform data protection. This board should comprise regulators (including DPA), policymakers (both executive and legislator) and the judiciary. The DPB must promote cooperation amongst the regulators/policymakers and DPA, provide guidance and clarifications on the data protection framework, and provide opinions to various regulators/policymakers in cases related to data protection in the form of advice.

---

[126] Shekar, K. (2022, April). *Building Effective and Harmonised Data Protection Authority: Strategies for Structural Design and Implementation*. The Dialogue. https://thedialogue.co/wp-content/uploads/2022/04/Building-Effective-and-Harmonised-Data-Protection-Authority-Strategies-for-Structural-Design-and-Implementation.pdf

[127] Shekar, K., Bahl, V. S., & Singh, A. (2022). DPB 2021: *The Data Protection Authority And Coordination With Sectoral Regulators*. The Dialogue - NASSCOM. Retrieved July 19, 2022, from https://thedialogue.co/wp-content/uploads/2022/07/DPB-2021-The-Data-Protection-Authority-and-Coordination-with-Sectoral-Regulators.pdf

[128] Section 189, The Insolvency and Bankruptcy Code, 2016.

[129] Shekar, K., Bahl, V. S., & Singh, A. (2022). DPB 2021: T*he Data Protection Authority And Coordination With Sectoral Regulators*. The Dialogue - NASSCOM. Retrieved July 19, 2022, from https://thedialogue.co/wp-content/uploads/2022/07/DPB-2021-The-Data-Protection-Authority-and-Coordination-with-Sectoral-Regulators.pdf

[130] EDPB is an EU body in charge of the application of the General Data Protection Regulation (GDPR)

[131] While GDPR is regulation (the term regulation in EU refers to binding for the members countries to follow), still, it provides flexibility for member countries to have their own data protection framework and authority

[132] *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.

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

[134] 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/*.

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

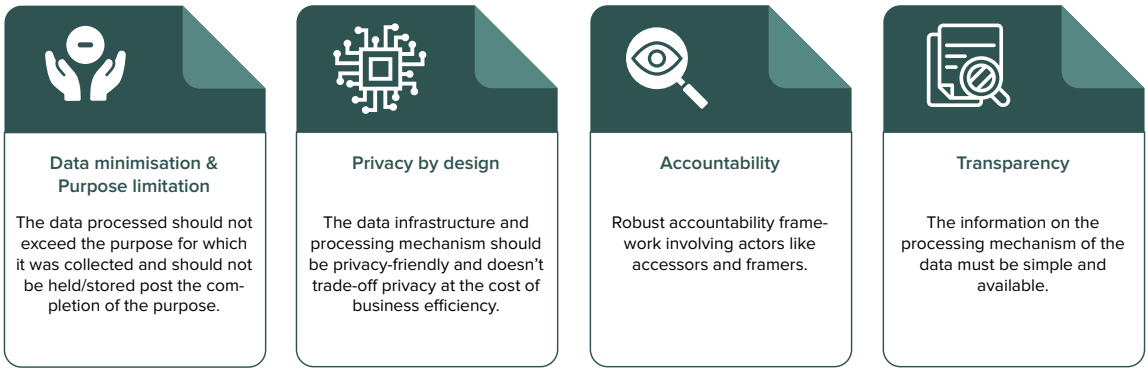
4.2.2. PRINCIPLE-BASED SANDBOX MECHANISM: A COOPERATION APPROACH

One of the fundamental critiques of the PDP Bill is that it is taking too long to take effect and is expected to continue with its withdrawal, and such a delay may render it obsolete given the fast pace of technological advancement as the subject matter of the Bill may need changes and updates over time it comes into effect. The Bill focuses on the responsibility of data fiduciaries; however, with the rapidly changing landscape of technology, data fiduciaries (defined in the Bill) may not be the only data handlers, and instead, will be increasingly replaced by new technologies and players, which doesn't currently fall under the definition like data brokers. While Indian legislators and regulators may sometimes brush off newer technologies that they don't understand yet for fear of insidious intent and hidden features they may miss, it is not a very business-friendly and cooperative approach.

As policymakers and regulators are overwhelmed by the pace of technological advancement, therefore, to aid regulators in moving towards a cooperative approach, we propose a sandbox mechanism where the data fiduciaries can test their innovation against the set principles notified by the regulator taking cognisance of the interests of other sectoral regulators. While PDP Bill provided for a sandbox mechanism, some key principles regarding technology and data protection (illustrated below) need to be part of the framework.

Besides, the sandbox mechanism effectively introduces new technology to lawmakers and regulators to prevent a fear-based reactionary ban and instead seek exemptions for the new technology rather than ad hoc legislation. While technology can be dynamic, changing legislation can be time-consuming and strenuous, so we suggest giving exemptions based on principles. Therefore, the sandbox would bring in an accommodative stand towards a new technology as long as it ticks all the principles.

Figure 2: Principles to be a part of the Sandbox



While the PDP Bill, 2019[136] envisioned a sandbox mechanism, central, and state governments and regulatory bodies in India already use the sandbox mechanism for testing innovations. For instance, the RBI introduced the Regulatory Sandbox in 2019. This sandbox aims to bring innovation to financial services by allowing businesses to live test their solutions in a controlled regulatory environment.[137] Since 2019,

[136] The Clause 40 PDP Bill (JPC has suggested a new version titled Data Protection Bill, 2021) provides for a sandbox mechanism where new technology can be tested by the innovators under the scrutiny of the regulator

[137] Enabling Framework for Regulatory Sandbox. (2019, August 13). Reserve Bank of India. Retrieved January 21, 2022, from https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=938

RBI has hosted four regulatory sandbox cohorts on retail payments[138] (six entities successfully exited), cross border payments[139], MSME lending[140] and prevention and mitigation of financial fraud.[141] At the state level, one such initiative is the establishment of the Karnataka Innovation Authority and the mechanisation of the sandbox mechanism under it.[142] The authority through this has enabled start-ups and businesses to test their innovations without legal barriers. The sandbox aims to bring innovative businesses and emerging technologies under legal perimeter through testing until the existing legal framework evolves to the pace of technological development. However, operating distributed and parallel sandboxing mechanisms by different regulators would create complexities for businesses seeking to explore new technologies and create gaps in the holistic examination of the risks posed by innovation.

As some of these technological innovations fall within the regulatory perimeter of sectoral regulations, state policies and the upcoming new comprehensive data protection bill, it is essential to harmonise the sandbox mechanisms. Therefore, there is a need to examine whether the DPA can collaborate with different regulators and authorities to run integrated sandboxes[143] that allow innovations to be evaluated collaboratively through MoUs. In practice, this could involve entities proposing innovation classified as data fiduciaries being tested against a horizontal set of principles (consolidated from PDP 2021) and by an additional framework developed by the DPA in coordination with other sectoral regulators.

4.2.3. CALIBRATED GRIEVANCE MANAGEMENT SYSTEM[144]

Two significant problems with the existing grievance management system are (a) lack of coordination horizontally (in terms of various coexisting systems and mandates) and (b) lack of agility in terms of resolution. It is useful here to note the observations of the Task Force on a Financial Redress Agency (**TFFRA**). Their report provides a step-by-step implementation plan to operationalise a redress forum for retail financial consumers.[145] Here, for now, we note that there is value in exploring a more calibrated approach to grievance redressal.[146]

Therefore, we suggest a calibrated hierarchical grievance redressal mechanism with horizontal and vertical coordination (between different elements of the system) and agility proofing. Borrowing inference from the responsive regulation framework[147], the below infographic illustrates the suggested calibrated grievance management system.[148]

---

[138] Regulatory Sandbox (RS): First Cohort on 'Retail Payments' – Exit. (2021, September 13). Reserve Bank of India. Retrieved January 21, 2022, from https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52217

[139] Regulatory Sandbox (RS): Second Cohort on Cross Border Payments – Test Phase. (2021, September 13). Reserve Bank of India. Retrieved January 21, 2022, from https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52218

[140] Reserve Bank Announces Opening of Third Cohort under the Regulatory Sandbox. (2021, September 13). Reserve Bank of India. Retrieved January 21, 2022, from https://www.rbi.org.in/scripts/FS_PressRelease.aspx?prid=52219&fn=9

[141] RBI's fourth regulatory sandbox cohort is on the prevention of financial frauds. (2021, October 9). Business Standard. Retrieved January 21, 2022, from https://www.business-standard.com/article/finance/rbi-s-fourth-regulatory-sandbox-cohort-is-on-prevention-of-financial-frauds-121100900048_1.html

[142] Joshi, B. (2020, February 24). *Karnataka government eyes innovation push through Innovation Authority Bill*. Deccan Herald. Retrieved April 11, 2022, from https://www.deccanherald.com/state/top-karnataka-stories/karnataka-government-eyes-innovation-push-through-innovation-authority-bill-807509.html

[143] *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

[144] Shekar, K. (2022, April). *Building Effective and Harmonised Data Protection Authority: Strategies for Structural Design and Implementation*. The Dialogue. https://thedialogue.co/wp-content/uploads/2022/04/Building-Effective-and-Harmonised-Data-Protection-Authority-Strategies-for-Structural-Design-and-Implementation.pdf

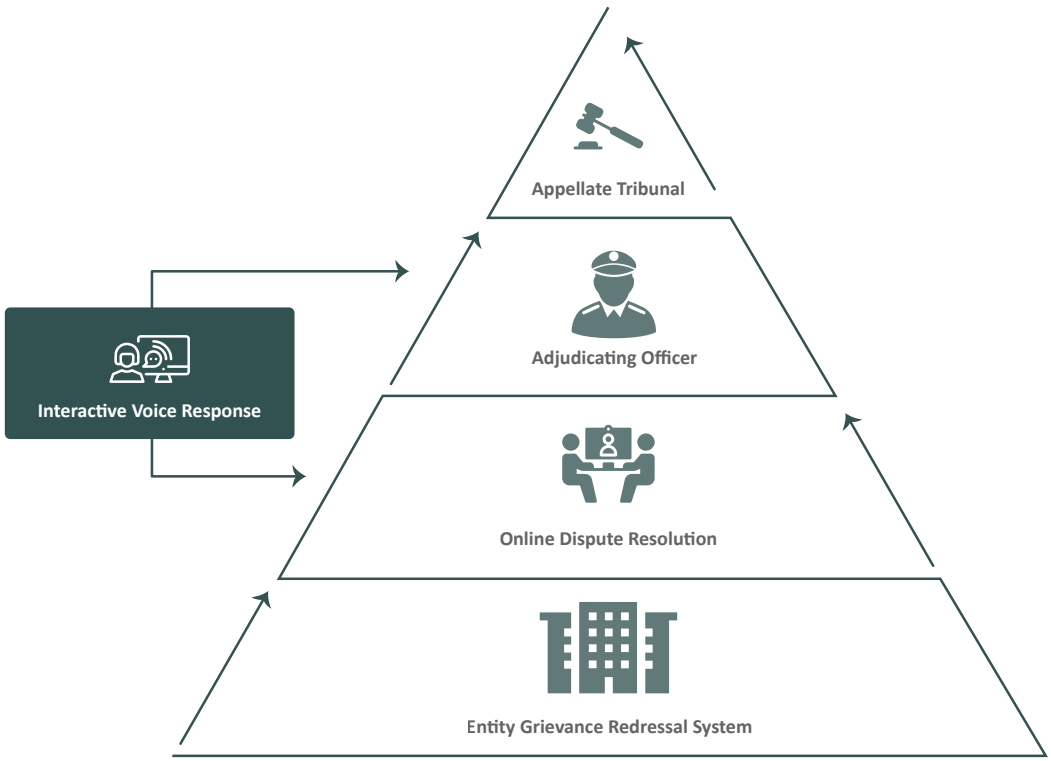
[145] *See* Department of Economic Affairs, *Report of the Task Force on Financial Redress Agency*, (2016) available at: https://dea.gov.in/sites/default/files/Report_TaskForce_FRA_26122016.pdf

[146] 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

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

[148] To implement this system, it is important to amend clause 32 of the PDP Bill

Figure 3: Pyramid eliciting calibrated grievance management system



Interactive voice response: The zero-step of the proposed grievance management system should involve the Interactive Voice Response (IVR) wing discussed in section 1.3 of the recommendations. This automated voice response system (through call) will navigate consumers (or entities) to reach step 1, i.e. to the entity's grievance redressal system or to step 2, i.e. online dispute resolution, if step 1 is already complete.

Entity's grievance redressal system[149]: While various legislations and data sharing/transfer policies mandate entities to set up a grievance mechanism, it is important to harmonise those mandates in terms of point of contact and timeline for resolution. Therefore, step one of the proposed grievance management system is to get the dispute redressed by reporting it to the entity itself.

Online dispute resolution: Online Dispute Resolution (ODR) is a mediated litigant dispute resolution framework facilitated through online platforms. ODR has been extensively used by courts and entities to resolve disputes as this is more efficient, quick turnaround and cost-effective. The ODR framework must be mechanised by DPA, keeping core principles intact (with room for flexibility) in order to reduce its adjudicatory burden. The ODR platform must assign a mediator for every dispute depending on the nature of the case. Therefore, step 2 of the proposed grievance management system is to reach out to ODR[150] if step 1 fails. In case of step 2 failure, the ODR platform must escalate the dispute to step 3, i.e. moving to the Adjudicating Officer by automatically filing a complaint with all the negotiation details.

[149] It is worth considering a board-based grievance redressal mechanism than a single-point-of-contact based system.
[150] Central government is planning to introduce a bill on mediation in winter session 2021 (Ahmed, 2021).

Adjudicating officer: The PDP Bill placed 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.[151] Therefore, next in the pipeline is to approach the Adjudicating Officer. In case individuals aggrieved by an order made by the Adjudicating Officer can approach/ appeal to Appellate Tribunal.

Appellate tribunal: Appellate tribunal was planned to be set up under the PDP Bill (chapter XI), to hear and dispose of any appeal from an order of the adjudicating officer therefore, next in the pipeline is the approach of the Appellate tribunal. We propose a system where the data protection appellate tribunal is horizontally coordinated, where benches formed under Clause 71 of the PDP Bill must comprise other tribunals (regulators if it deems them) according to the nature of the dispute. Therefore, step 3 of the proposed grievance management system is the appellate tribunal's verdict if step 2 fails.

4.2.4. PREVALENCE-BASED COMPLAINT AUDIT TO UNDERSTAND THE GAPS: A PROACTIVE APPROACH[152]

A feedback mechanism based on analysing the prevalence of complaints received by the DPA, DPB (refer to section 4.2.1), and calibrated grievance management system (refer to section 4.2.3) is one way of identifying gaps in current regulation, making the DPA proactive. For instance, after receiving negative feedback following its takedown, Facebook reinstated the award-winning image of a naked girl fleeing napalm bombs during the Vietnam War. While Facebook received this feedback through newspapers and civic movements, this event still shows that aggregating grievances can provide feedback on policies and actions.[153]

The United States Federal Trade Commission (FTC)[154] and Consumer Financial Protection Bureau (CFPB)[155] adopt a similar approach. They periodically publish and maintain a complaints database, to highlight systemic issues.

If all the complaints received by regulatory bodies were to be analysed for prevalence, patterns would emerge to reflect where the mechanism has formed a void or lacks seamlessness. These complaints could flag the proportion of problems in different laws for pre-existing technologies and signal any new technological trends that aren't covered by regulation yet. Once this audit of complaints is conducted and data patterns emerge, the problem areas become more apparent and easier to solve. Newer technologies can then be studied, understood, and regulated, recurring problems can be addressed with alternative solutions, and any blockages in redressal mechanisms can be eased.

---

[151] *See* clauses 32, 62, 65, 69, PDP 2019.

[152] Shekar, K. (2022, April). *Building Effective and Harmonised Data Protection Authority: Strategies for Structural Design and Implementation*. The Dialogue. https://thedialogue.co/wp-content/uploads/2022/04/Building-Effective-and-Harmonised-Data-Protection-Authority-Strategies-for-Structural-Design-and-Implementation.pdf

[153] Shekar, K. (2021). How to Fight Electoral Fake News on Social Media. Retrieved from Freedom Gazette: https://www.freedomgazette.in/2021/02/how-to-fight-electoral-fake-news-on-social-media/

[154] *Consumer Sentinel Network Data Book 2020*. (2021, February 4). Federal Trade Commission. Retrieved February 23, 2022, from https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2020

[155] *Consumer Complaint Database*. (n.d.). Consumer Financial Protection Bureau. Retrieved February 23, 2022, from https://www.consumerfinance.gov/data-research/consumer-complaints/

4.2.5. MARKET MECHANISMS FOR COMPLIANCE: EFFECTIVE USE OF CAPACITY

In India, implementing the privacy regime is a fresh start for regulators and domestic industries. The range of entities covered by the Bill will be immensely vast, starting from big tech to MSMEs to government agencies. While a one-size-fits-all approach towards data protection regulation might bring in compliance (at a cost) amongst the horizontally (within the sectors) and vertically (across various sectors) diverse range of data fiduciaries, it might not bring cooperation. Therefore, the DPA must operationalise various market mechanisms to build a healthy relationship and cooperation with the data fiduciaries and processors with a limited capacity for disposal.

In addition to the direct supervision and enforcement, the DPA must follow normative theories of regulation[156] and institute market mechanisms such as (a) audit of data-driven features used by data fiduciaries and (b) market for principles-based accreditation, enabling a competitive edge for platforms. While an independent auditing agency must perform the audit, the DPA or authorised entity must perform the accreditation process at a nominal cost based on defined principles. The accreditation process must have a well-laid process and procedure that balances transparency and safeguards to protect intellectual and proprietary information. Besides, the accreditation process must be aspirational such that it pushes the data fiduciaries toward performing better on the user outcome aspect, i.e., securing informational privacy through better data protection standards.

[156] Hertog, J. d. (n.d.). *Encyclopedia of Law & Economics - 5000 General Theories Of Regulation | FindLaw*. Legal Reference Material. Retrieved May 1, 2022, from https://reference.findlaw.com/lawandeconomics/5000-general-theories-of-regulation.pdf

https://thedialogue.co

Recommended Citation : *Shekar, K., Venkatesh, K., & Mehta, S. (2022). The Institutionalisation of India's Data Protection Authority. 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.