The Dialogue™
INFORM ENGAGE IDEATE

EVENT REPORT

IMPORTANCE OF DATA PROTECTION AUTHORITY TO ENABLE CROSS-BORDER DATA TRANSFERS

EVENT REPORT

IMPORTANCE OF DATA PROTECTION AUTHORITY TO ENABLE CROSS-BORDER DATA TRANSFERS

Authored by Vaishnavi Sharma
Copyedited by Akriti Jayant
Designed by Shivam Kulshrestha

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 DialogueTM 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.

For more information
https://thedialogue.co

Suggested Citation
Sharma, V. (2024). Event Report | Importance of Data Protection Authority to Enable Cross-border Data Transfers. The Dialogue.

Catalogue No
TD/PGD/ER/0124/01

Publication Date
January 9, 2024

CONTENTS

1. INTRODUCTION

On the 1st of December 2023, The Dialogue conducted a virtual roundtable discussion exploring the "Significance of Data Protection Authority in Facilitating Cross-border Data Transfers." The session aimed to assess the potential impact of the Data Protection Board, established under the Digital Personal Data Protection Act, 2023 ("DPDP Act, 2023"), on cross-border data transfers. The discussion, covering diverse themes, offered valuable insights into the role of regulatory authorities and their connection to cross-border data transfers.

Mr. Kamesh Shekar, Senior Programme Lead of the Privacy and Data Governance vertical at The Dialogue, moderated the roundtable discussion. Distinguished panellists who participated in the event included:

- **Dr. Gabriela Zanfir-Fortuna**, Vice President for Global Privacy, Future of Privacy Forum (FPF)
- **Mr. Joseph Whitlock**, Executive Director at Global Data Alliance

Following the roundtable discussion, the participants engaged in a question-and-answer session. It is crucial to note that the roundtable event followed the Chatham House Rules, with this report refraining from attributing any comment or observation to a specific speaker. Moreover, it is pertinent to mention that the views summarised in this report are of a personal nature and do not necessarily reflect the perspectives of the speakers' respective organisations or The Dialogue.

KEY HIGHLIGHTS

The discussions generated clear recommendations likely to benefit policymakers as they continue deliberating on and formulating rules for cross-border data transfers.

To regulate and maintain a seamless cross-border data flow, it is essential to ensure the independence of a data protection authority, such as India's DPB.

Notably, the effectiveness and efficiency of cross-border data flows do not depend on the structure or composition of the data protection authority, as long as it maintains a certain level of independence in its functioning and operations. This independence and autonomy can manifest in various ways, including the power to issue fines and conduct investigations.

Policymakers must pay attention to cautionary tales of data mercantilism and explore ways to restrict cross-border data flows as narrowly as possible.

2. KEY TAKEAWAYS

The evolution of India's data protection law, the DPDP Act, 2023, actively involved significant public and expert consultations and overhauls, showcasing the dynamism of policymaking in the realm of data protection. It underwent a pivotal transition from the initial vision of establishing a Data Protection Authority ("DPA") to the actualization of the Data Protection Board ("DPB") in the enacted version. If materialized, the former would have wielded broader functions, including formulating rules, regulations, and policies, defining a more extensive set of functions, and imposing penalties. In contrast, the current Data Protection Board primarily assumes an adjudicative role, actively focusing on determining non-compliance and imposing penalties. The envisioned authority actively aimed to be a comprehensive body with multifaceted responsibilities, while the present board actively centres on an adjudicatory function. This shift actively reflects a deliberate change in focus from broader functions to a more specialised adjudicatory role, actively marking a unique approach to overseeing data protection in the country. The roundtable discussion actively considered whether the DPB, in its current avatar, could actively impact cross-border data flows.

2.1. NAVIGATING THE VALUE OF INDEPENDENCE OF THE DPB AND ITS RELATIONSHIP WITH CROSS-BORDER DATA FLOWS

This shift from DPA to DPB initiates a nuanced exploration of how India's approach to data protection actively influences its engagements with other jurisdictions. Perspectives on the legal frameworks of the European Union (EU) enrich this exploration, highlighting the intricate dynamics of data protection on the international stage.

The discussion unveils a crucial nexus—the link between DPA independence and international data transfers, particularly apparent in the EU's General Data Protection Regulation (GDPR). The GDPR specifies that jurisdictions receiving data must maintain an independent supervisory authority, a condition mirrored in adequacy requirements globally.

Global variances in the importance ascribed to the independence of data protection authorities add layers to the conversation. The discussion accentuated the EU's legal framework as a point of reference, emphasising that the independence of supervisory authorities (the Data Protection Authorities) is a constitutional imperative. This independence serves as a linchpin for effectively exercising competencies, extending beyond personal data protection to encompass broader fundamental rights.

The EU underscores the integral role of personal data protection as a fundamental right, while examples like Singapore present a contrasting model. In some jurisdictions, data protection authorities operate as part of the executive machinery, with less emphasis placed on independence. The case study of Brazil's legislative evolution serves as a testament to the adaptable nature of DPA independence, initially absent but progressively established through amendments. A key realization is that the link between an independent data protection authority and the aspects of data transfer is not inherently interconnected.

The conversation extends to the importance of independence within the broader context of regulatory authorities. It posits that independence is not only crucial within the realm of data protection but also holds broader significance, resonating with democratic principles. The nuances of appealability and independence become critical considerations within democratic systems, recognizing that the connection between an independent data protection authority and cross-border data transfer isn't inherently interlinked.

Delving deeper into international standards and agreements, the panel referenced the OECD

[1]OECD, Declaration on Government Access to Personal Data Held by Private Sector Entities, OECD/LEGAL/0487
https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

Declaration on Government Access to Personal Data Held by Private Sector Entities.[1] This declaration assumes significance in fostering global trust and aligning with institutional arrangements for cross-border data partnerships. It, among other things, emphasises crucial standards such as democratic principles, transparency, government accountability, non-discrimination, and independence in oversight mechanisms.

Furthermore, the discussion brought to light that gaining insights into data transfer provisions in digital economy agreements provides a comprehensive understanding. Such agreements cover diverse areas, including open government data, cybersecurity, data transfers, and personal data protection. The multifaceted approach highlights the interconnected nature of these provisions, emphasizing that data transfer and localization should not be viewed in isolation.

In the context of cross-border data transfers, India's trajectory has undergone a strategic shift from a stringent data localization approach to a more nuanced regional stance, showcasing the recognition of the socio-economic benefits of cross-border data flows. While the independence of data protection authorities is not a prerequisite for having cross-border data flows, considering trends across the globe, it will be necessary to accord independent functioning, especially when negotiating with the EU legal framework, which calls for the independence of the data protection authorities.

2.2. WHETHER THE DPB IS A "SUPERVISORY BODY/AUTHORITY"

The discussion underscored the paramount nature of the powers and competencies of the regulatory authority, which may encompass the ability to issue fines, conduct investigations, and more. Some data protection authorities globally, such as the California Privacy Protection Agency, possess rule-making powers, allowing them to formulate subordinate legislation.

Conversely, certain data protection authorities, particularly in the EU, possess the authority to issue guidelines. While these guidelines are not legally enforceable, they play a crucial role in outlining how the data protection authorities will enforce the law, determine compliance, and provide guidelines on issuing fines, among other aspects. Notably, in India, the power to issue guidelines is absent, which may not be ideal for data protection authorities.

The panel also stressed the importance of interoperability in the context of cross-border data transfers. Many data protection authorities and trade authorities scrutinize the interoperability of different systems. While countries can maintain essentially equivalent levels of protection, the DPDP Act, 2023, grants the executive the authority to restrict data transfers to specific countries in the future. However, the details around the exercise and implementation of that authority are not explicitly outlined in the law, leaving significant discretion to the government. Although not an issue at the current stage, clarity on this matter in the future is deemed essential.

In India, restrictions would follow a negative list approach. However, if a sweeping restriction is imposed under a negative list, it is crucial to ensure that any blanket restrictions are principles-based and grounded in legal norms.

The discussion highlighted that, among other considerations, privacy stands as the paramount consideration for the DPB in relation to cross-border data transfers. This entails the standards of privacy that India would expect its counterparts to provide concerning the handling of the personal data of Indian citizens. Additionally, it is crucial to ensure that any restrictions on cross-border data transfers are developed accountably, transparently, and without discrimination, and that they are necessary or proportionate to the underlying goals of the restriction. Adequacy norms emerged as crucial benchmarks for international transfers, complemented by recognized safeguards like standard contractual clauses and binding corporate rules.

Lastly, the discussion emphasized that the participation criteria for the Global Privacy Assembly,[2] a global forum for data protection and privacy authorities, could be beneficial for Indian policymakers. Essentially, the criteria require that the concerned authority: (a) is a public entity created by an appropriate legal instrument, (b) has the supervision of the implementation of legislation on the protection of personal data or

[2] GPA membership applications. https://globalprivacyassembly.org/participation-in-the-assembly/become-a-member/

privacy as one of its principal regulatory mandates, (c) operates under legislation compatible with the principal international instruments dealing with data protection or privacy, (d) has an appropriate range of legal powers to perform its functions, and (e) has appropriate autonomy and independence. Indian policymakers could use this as a reference point while forming the DPB and formulating the corresponding rules and regulations

2.3. CROSS-BORDER DATA FLOW: LOOKING TOWARDS INTERNATIONAL PRACTISES

The dialogue set the context by illuminating the interconnected nature of data across sectors, cautioning against overly narrow restrictions. Policymakers globally must align cross-border data transfer policies with fundamental rights, encompassing health, liberty, security, education, and freedom from discrimination. All these considerations are crucial when deliberating and negotiating restrictions on cross-border data transfers.

The discussion also highlighted the cautionary tale of China's experience with data localization, emphasizing the evident adverse impacts on innovation, foreign investment, trade costs, productivity, and overall economic well-being. Policymakers were urged to draw valuable lessons from nations embracing data retention and restrictions. Ensuring an effective and seamless cross-border data transfer is of utmost importance.

Considering India's approach towards blacklisting jurisdictions, although not unprecedented in other domains such as export controls and sanctions, military technology, and use, it represents a unique approach to cross-border data transfers. It is essential that the measures adopted are highly targeted and focused on specific harms, and they must be narrowly tailored to address those harms.

AUTHOR

Vaishnavi Sharma
Research Associate

Vaishnavi Sharma serves as a Research Associate at The Dialogue, specialising in privacy and data governance research. She earned her undergraduate degree from Maharashtra National Law University, Mumbai, with a strong focus on constitutional law. Her primary areas of interest encompass fundamental rights, including freedom of speech and expression, assembly, and privacy, both in offline and online contexts.

Copyeditor

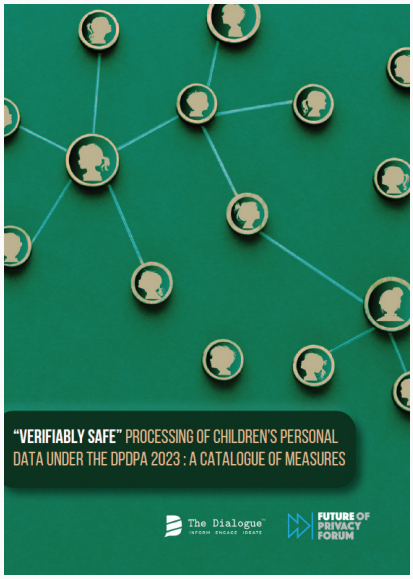
Akriti Jayant, Head of Communications, The Dialogue™

Designer

Shivam Kulshrestha, Senior Communications Associate (Graphic Design), The Dialogue™

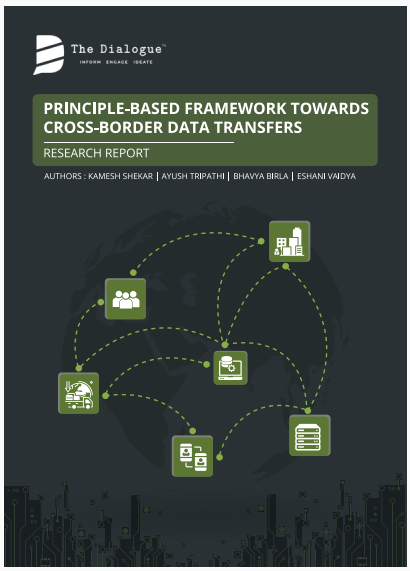
MORE FROM OUR RESEARCH

Analysis: Comparative Analysis of India's Digital Personal Data Protection Bill, 2022 and 2023

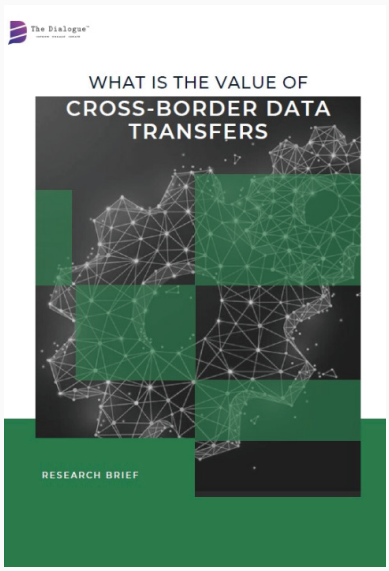


Policy Brief: "Verifiably Safe" Processing of Children's Personal Data under the DPDPA 2023 : A Catalogue of Measures

Research Paper: Privacy Technologies in India – Strategies to Enhance the Ecosystem



Research Paper: Principle-based Framework Towards Cross-Border Data Transfers



Research Brief: What is the Value of Cross-border Data Transfers

Research Paper: The Institutionalisation of India's Data Protection Authority

thedialogue.co

@_DialogueIndia

@thedialogue_official

@the-dialogue-india

@TheDialogueIndia