

No. R-17/19/2024-PRPP(RU-2)
National Human Rights Commission

Minutes of the meeting of the

Open House Discussion on ‘Ensuring Privacy and Human Rights in the Digital Era: A Focus on Corporate Digital Responsibility’

1. An Open House Discussion on **‘Ensuring Privacy and Human Rights in the Digital Era: A Focus on Corporate Digital Responsibility’** was held on 18th February 2025 at Manav Adhikar Bhawan, New Delhi. The discussion was chaired by the Hon’ble Chairperson, NHRC, Shri Justice V. Ramasubramanian in the presence of Hon’ble Member, Shri Justice (Dr.) Bidyut Ranjan Sarangi, Secretary General, Shri Bharat Lal, Registrar (Law) Shri Joginder Singh, Director Lt. Col. Virender Singh and other senior officers of the Commission, and focused on the three agenda items that include, Establishing Robust Regulatory Frameworks and Compliance Mechanisms; Building a Culture of Data Privacy and Identifying Threats and Best Practices. Additionally, the Draft Digital Personal Data Protection Rules, 2025 (*hereinafter referred as Rules*) were deliberated upon. The agenda note was circulated in advance.



2. The Session commenced with a welcome address by Lt. Col. Virender Singh, Director, NHRC, to Hon’ble Chairperson and members of the Commission and other participants, including representatives from government bodies, private enterprises, associations, civil society organizations, and subject-matter experts. A list of participants is annexed.

3. In his keynote address, **Shri Bharat Lal, Secretary General, NHRC**, underscored NHRC’s commitment to addressing the challenges of digitization. He highlighted that while India contributes 20% to global data production; it holds only 3% of global data centre capacity. Acknowledging the government efforts by enacting Digital Personal Data Protection (DPDP) Act 2023 and



& Draft DPDP Rules, 2025, he also emphasized the private sector’s critical role in safeguarding privacy through self-discipline and proactive measures. He also introduced Corporate Digital Responsibility (CDR), as an emerging yet under-explored concept which was the theme of the discussion along with the agenda items.



4. **Hon’ble Chairperson, NHRC, Shri Justice V. Ramasubramanian**, commenced his inaugural speech by presenting a satirical video illustrating modern privacy concerns. Reflecting on the evolving nature of privacy, he cited the CEO of Sun Microsystems, who in 2000 declared that “privacy is dead”, and an award-winning investigative journalist, who described privacy as being on “life support”. Drawing from

his judicial experience, he shared a case of privacy infringement due to technological advancements, reinforcing the need for “digital hygiene”—a responsibility that begins at the individual level. In conclusion, he expressed gratitude to all participants from diverse sectors for contributing to this timely and critical discussion.

5. **Shri Shailendra Trivedi**, provided an analysis of the evolving nature of human rights, emphasizing the shift from the protection of individuals against state actions to the necessity of safeguarding individuals from private entities that amass vast amounts of personal data. He highlighted that Google processes over 100,000 searches per second, granting it an unparalleled ability to analyse user behaviour, which poses significant risks to privacy and human rights. He underscored the challenges posed by digital anonymity, which has facilitated the spread of misinformation and disinformation with far-reaching consequences. Additionally, he raised concerns about the increasingly prevalent practice of mobile phone confiscation in India by investigating agencies posing risks of privacy infringement, noting that such measures are not as common in other jurisdictions.



6. Addressing the issue of data localization, **Shri Trivedi** commended the RBI’s efforts in ensuring data localization within the financial sector. However, he pointed out that investigating agencies frequently encounter challenges in obtaining information from private entities in other sector, which often cite offshore data storage as a constraint. He also highlighted emerging concerns within the

banking sector, particularly regarding the ease with which authorities can now freeze bank accounts—a process that previously required a judicial order, but is now often carried out prior to legal authorization, with de-freezing necessitating court intervention.

7. Shri Trivedi emphasized that while there have been several instances where banks utilized customer data for internal marketing purposes, there has been no instance of such data being sold to third parties. He reiterated the banking sector's strong commitment to data privacy and expressed confidence that the implementation of the DPDP Act would effectively address prevailing concerns related to data protection and personal information governance.

8. **Shri Deepak Goel**, highlighted the Ministry's proactive approach in shaping the DPDP Rules, with five consultations completed and more planned as it remains open to public feedback. Emphasizing India's rapid digital growth, he noted that the country ranks third globally in terms of digital landscape and underscored that data itself is now a critical infrastructure driving future services.



9. Linking the DPDP Act, 2023 to the Supreme Court's recognition of privacy as a fundamental right, he outlined its goal of maintaining a balance between enhancing public convenience and ease of doing business. He stressed that greater data processing fuels innovation, comparing data to gold—"the more it's processed, the more valuable it becomes."

10. Addressing data control concerns, he stated that the DPDP Act empowers individuals by mandating that all entities, including the government, act as "data fiduciaries" which shall hold data as trustee. Key provisions include the right to access, correct, erase, and withdraw consent for data processing. A unique Indian innovation, the "right to nominate", allows individuals to designate digital heirs, recognizing the growing presence of deceased individuals' data online. He reaffirmed that data processing must remain purpose-driven, with clear user notifications for any new use. He further assures that the DPDP Act aligns with sectoral laws, ensuring regulatory harmony, and enforces compliance through penalties of up to ₹250 crore.



11. **Shri Sanjoy Bhattacharjee** stressed the growing importance of data governance in a digital world, citing International Development Corporation data on exponential global data growth which stands at 180 zettabytes as estimated today from 2 zettabytes in 2010. He emphasized data's role in AI training, customer

segmentation, predictive analytics, and socio-economic analysis, while cautioning against risks associated with data control. He outlined six key pillars of CDR:

- i.) Digital Privacy – Ensuring responsible data collection, storage, and processing.
- ii.) Digital Wellbeing – Enhancing accessibility through user-friendly interfaces like voice navigation and screen readers.
- iii.) AI & Algorithm Fairness – Promoting transparency, preventing bias, and informing users about data usage.
- iv.) Cybersecurity – Implementing robust controls to protect against fraud and unauthorized access.
- v.) User Autonomy & Consent – Enabling users to manage data sharing and withdraw consent at any time.
- vi.) Transparency & Accountability – Establishing clear, accessible policies and effortless consent withdrawal

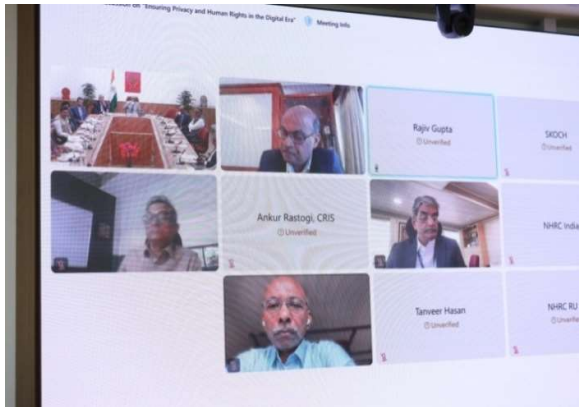
12. For CDR implementation, he proposed four strategies:

- i.) User-Centric Privacy Solutions – Embedding consent management in all processes.
- ii.) Privacy by Design – Integrating privacy measures from development to deployment.
- iii.) Stakeholder Engagement & Training – Raising awareness across organizational levels.
- iv.) Data Governance & Security – Enforcing strict policies, encryption, and access controls.

13. **Shri Rajeev Kumar Gupta** acknowledged the transformative power of digital technologies while emphasizing the ethical challenges in data privacy, regulatory compliance, and cyber security. He noted that IRDAI and RBI guidelines must evolve with technological advancements and that the DPDP Act, 2023, presents both opportunities and challenges. He stressed the importance of privacy-by-design in fintech, urging companies to integrate compliance into business processes rather than treating it as an afterthought. He underscored data as the new digital currency, advocating user education, security-by-design, and ethical AI to prevent biases. Addressing cybersecurity threats and financial fraud, he called for biometric authentication as an additional layer and emphasized joint efforts among government, IT companies, and global stakeholders to enhance data protection. While discussing the DPDP Rules, 2025, he made the following suggestions:

- i.) Clearly outlining the penal provision in the Rules to enhance accountability and deter potential violations.
- ii.) Call for balancing the provision for data localization introduced through the Rules aiming to protect national security with operation feasibility of global companies, possibly through bilateral arrangements or adequacy decisions to facilitate international data flows while safeguarding personal data.
- iii.) Providing clear guidelines on acceptable verification methods in case of children from parents to assist data fiduciaries in compliance.
- iv.) Providing detailed guidelines for the Data Protection Board regarding its composition, functions, and decision-making processes.

- v.) Aligning domestic laws with GDPR and other frameworks to facilitate cross-border collaborations.
- vi.) Continuously consulting with industry, academia, and civil society to refine the implementation framework.



14. Shri Ajay Gupta contributed additional insights with a focus on the financial services sector, where the collection, storage, and processing of personal data are deeply embedded within operational processes. He highlighted the critical role of trust in this sector, stating that financial institutions act as custodians of public money and personal financial data. To uphold customer confidence,

transparency, and reliability in service delivery are imperative. He emphasized the importance of balancing business opportunities with robust privacy protection measures. He provided an overview of key initiatives undertaken by banks to enhance data privacy, including the formation of a dedicated data privacy team, the implementation of a breach reporting mechanism, and the introduction of a structured Data Protection Impact Assessment (DPIA) to assess potential risks. He also mentioned the establishment of comprehensive personal data protection standards and protocols to ensure that customer data is handled securely and responsibly. Additionally, he introduced an e-learning module developed to educate employees on privacy and data protection, reinforcing the importance of continuous learning and vigilance in handling personal data. He concluded by reaffirming that data privacy is a shared responsibility and that businesses must treat personal information with ongoing diligence and adherence to best practices.



15. Shri Sameer Bajaj representing MakeMyTrip, introduced the company as an Indian startup founded in 2000, predating widespread mobile internet access. He highlighted its NASDAQ (National Association of Securities Dealers Automated Quotations) listing in 2010, when Indian stock exchanges were not equipped for internet-based Initial Public Offerings (IPOs), underscoring its evolution into a globally competitive corporation driven by technology and consumer

trust, with over 70% of users relying on the platform.

16. He shared that eight months ago, MakeMyTrip expanded its global accessibility while ensuring compliance with General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and other international privacy regulations. He emphasized that data

security remains a priority, noting that the company has stored Indian user data within India even before the DPDP Act came and has implemented data anonymization, encryption, and strict access controls. He highlighted MakeMyTrip's early adoption of account deletion features and its dedicated privacy email (privacy@go-mmt.com), offering Indian users the same privacy rights as GDPR-compliant entities.

17. Mr. Bajaj reiterated MakeMyTrip's commitment to global security standards such as Payment Card Industry Data Security Standard (PCI DSS), System and Organization Controls 2 (SOC 2), and ISO/IEC 27001 (International Organization for Standardization/International Electrotechnical Commission 27001), ensuring the secure handling of payment and sensitive data. He reaffirmed the company's dedication to user privacy and its willingness to collaborate on strengthening data protection frameworks.



18. **Dr. Muktesh Chander** highlighted the inevitable privacy compromises individuals may face when using digital services. He emphasized that free platforms like Google and WhatsApp operate at the cost of user data, leaving consumers with no real choice to opt out without sharing personal information. He questioned the monopolistic nature of such companies, emphasizing how personal data is routinely collected, sold, and misused. Sharing a personal experience of credit card fraud, he stressed the need for data traceability to hold violators accountable. Citing his work with the Telecom Regulatory Authority of India (TRAI), he criticized the ineffectiveness of the Do Not Disturb (DND) service, stating that telecom companies continue to violate regulations unchecked. He identified mobile SIM cards and bank accounts as key enablers of cybercrime, calling for stricter controls to prevent their misuse. He also advocated for the "right to be forgotten", sharing his own struggle to erase outdated online data. He emphasized the need for automatic data purging policies, similar to those under the General Data Protection Regulation (GDPR) and criticized Indian companies for indefinitely retaining user data beyond its intended purpose.

19. He pointed out the lack of cookie consent practices on Indian websites, despite their adoption in Europe. While optimistic about the Digital Personal Data Protection (DPDP) Act, he stressed the importance of clear, simplified legal documentation for users, rather than lengthy, complex terms and conditions. Discussing international credit card transactions, he criticized the absence of two-factor authentication, making consumers vulnerable to fraud. In conclusion, he called for stronger deterrents against data privacy violations, advocating for collaborative efforts between industry leaders, regulators, and human rights advocates to ensure individuals retain control over their personal information without compromising fundamental rights.



20. Shri Ashish Aggarwal highlighted that the DPDP Act, 2023 presents a valuable opportunity for progress in data protection. He noted that the Act, being heavily consent-based, is a positive step from a human rights perspective. However, he emphasized that effective implementation would require scalability, proper resource allocation, and the strategic use of technology. Acknowledging that the process would be a multi-year journey necessitating long-term investment, he pointed out several limitations

within the Act. These include concerns over parents consenting for children up to the age of 18, as digital literacy remains low among them; the need to ensure that consent requirements for persons with disabilities (PWDs) do not lead to exclusion; and an over-reliance on consent without a clear opt-out mechanism. Additionally, he observed that publicly disclosed data falls outside the scope of the Act, and a one-size-fits-all approach to breach reporting might lead to fatigue. He stressed the importance of adequate budget allocation, awareness campaigns, capacity building, and the NHRC, India, actively contributing to these efforts.

21. Shri Tanveer Hasan, focusing on values and principles, highlighted the need to assess data protection through the lenses of cost, price, and value. Cost refers to operational aspects, price pertains to regulatory compliance, and value is what entities like NHRC must consider. He refuted the notion that privacy hinders innovation, citing research showing that privacy-by-design fosters net positive growth for businesses. He emphasized that outreach and up skilling must be central to data privacy initiatives, particularly to bridge the digital literacy gap among older populations. He pointed out the need to cater to multilingual consumers and ensure inclusivity in digital platforms. Additionally, he stressed the importance of clearly defining jurisdictional responsibilities between the Data Protection Board and NHRC, India, to avoid regulatory overlaps and ensure a more structured implementation of data protection frameworks.

22. Shri Sameer Kochhar emphasized the need for India to develop country-specific indices to assess the status of data protection. He pointed out that corporate digital responsibility,



human rights, and privacy, while interconnected, are distinct domains with specific challenges. He raised concerns about the DPDP Act's potential impact on employment, particularly in the self-employed, MSME, and small business sectors, as compliance burdens could disproportionately affect them compared to large corporations. He further

mentioned that laws should be formulated in accordance with the domestic perspectives rather than being imitations of the western world. Additionally, he noted that human rights in business and corporate digital responsibility must consider psychological factors such as fair work allocation, mental well-being, and digital well-being, which are currently overlooked in the law. He advocated for industry-specific parameters for data protection in India, stating that a standardized framework may not be as effective across different sectors. He strongly advocated for extending the deadlines of the consultation process of Rules, as in his opinion, intense research would be required to understand the implications of its implementations.

23. Shri Neeraj Sachadeva highlighted challenges in aligning the Aadhaar Act with the DPDP Act. While the DPDP Act claims to supplement existing laws, it also overrides them in conflicts, creating ambiguity. The Aadhaar Act restricts data disclosure, whereas the DPDP Act is more flexible. He raised concerns over data breach notifications, noting the absence of a standardized template, which could lead to inconsistencies. Excessive notifications might also desensitize data principals.

24. He raised concerns about unlimited access and correction requests under the DPDP Act, which could strain resources. Citing Aadhaar's frequent date-of-birth corrections, he warned of operational challenges without restrictions. On data erasure, he noted that Aadhaar retains data for life, and deleting biometric records could compromise security and enable duplicate registrations. Data breach reporting requirements also pose challenges—immediate notification to data principals lacks a defined timeframe, while detailed reporting to the Data Protection Board is required within 72 hours, which may be difficult for large-scale breaches. He also discussed the research exemption and liability for data breaches. He also questioned the accountability for breaches under the research exemption, particularly who bears responsibility in case of a breach at a research institution. Clarity is needed on breach verification and enforcement by the Data Protection Board. These grey areas in DPDP Act implementation require further regulatory guidance.



25. In conclusion, **Hon'ble Member, NHRC, Dr. Justice Bidyut Ranjan Sarangi**, shared an incident of a woman who lacked banking knowledge owing to digital illiteracy, depended on others for transactions and risked losing her hard-earned money. He emphasized the need to simplify digital processes to ensure safe usage for those without digital literacy. Highlighting the importance of inclusivity, he posed a crucial question—how we can shape our system to benefit 1.4 billion people, including individuals at the grassroots level, who do not possess digital literacy.

26. Justice Shri V. Ramasubramanian observed that in today's world, everyone, regardless of literacy, is part of a constantly connected digital space. While entry into this space cannot

be restricted, he stressed the need for legal safeguards to protect individuals. He outlined NHRC's objective to engage stakeholders in developing a balanced regulatory framework and emphasized that the Commission will track the progress and impact of legislation and its implementation.

27. The meeting concluded with a formal vote of thanks by Lt. Col. Virender Singh, Director, NHRC, India.

List of participants

NHRC Officials

1. Shri Justice V Ramasubramanian, Hon'ble Chairperson
2. Shri Justice (Dr.) Bidyut Ranjan Sarangi, Hon'ble Member
3. Shri Bharat Lal, Secretary General
4. Shri Joginder Singh, Registrar (Law)
5. Lt Col Virender Singh, Director
6. Shri Sanjay Kumar, Deputy Secretary
7. Dr. Kanaklata Yadav, Consultant (Research)
8. Ms. Lakshmi Kumari, Junior Research Consultant
9. Ms. Madhura Naniwadekar, Junior Research Consultant
10. Shri Raghwendra Singh, Junior Research Consultant
11. Ms. Swarna Singh, Junior Research Consultant
12. Ms. Arpita Sinha, Junior Research Consultant

Participants

1. Technology, Reserve Bank of India
2. Shri Deepak Goel, Group Coordinator (Cyber Law), Ministry of Electronics & Information Technology
3. Shri Ankur Rastogi, Principal Project Engineering, EGSTM, Centre For Railway Information Systems (CRIS)
4. Shri Neeraj Sachadeva, Director (Legal), UIDAI
5. Shri Ankur Jain, Senior Information System, UIDAI
6. Dr. Muktesh Chander, NHRC Special Monitor, Cybercrime and Artificial Intelligence
7. Shri Sanjoy Bhattacharjee, Chief Data Officer, HDFC Bank
8. Shri Ajay Gupta, Executive Director, ICICI Bank
9. Shri Soumendra Mattagajasingh, Group Chief Human Resources Officer, ICICI Bank
10. Shri Rajiv Kumar Gupta, President, PB Fintech, Policy Bazaar
11. Shri Sameer Bajaj, Head of Communication & Corporate Affairs, MakeMyTrip
12. Shri Ashish Aggarwal, Vice President and Head of Policy, NASSCOM
13. Shri Tanveer Hasan A K, Executive Director, Centre for Internet & Society (CIS) in India
14. Shri Sameer Kochhar, President SKOCH Development Foundation
15. Shri Ananth Krishnan, Rtd. Chief Technical Officer, TCS
16. Ms. Ashika.V, Cellular Operators Association of India (COAI)