

Digital Personal Data Protection Act, 2023: How does it increase trust in UPI and what gaps remain?

by Rohit Elias

In 2016, the National Payments Corporation of India (NPCI) launched the Unified Payment Interface (UPI) that revolutionized payments in India. UPI permits seamless money transfers between individuals without having to rely on typing in the correct bank account details. Perhaps more importantly, it easily allows individuals to pay for products and services provided by small merchants such as street vendors in a cost-effective manner. Small merchants do not have to worry about the initial set-up fees of point-of-sale systems or transaction costs associated with debit or credit cards as a result of UPI. It can also easily be integrated into a multitude of various applications and currently PhonePe and Google Pay remain the two most popular third-party app providers of UPI. Individuals use these providers on a daily basis to make transactions that reveal significant information about themselves and until recently there were few requirements on companies to be transparent about how they use such data.

While UPI transformed the banking and financial realm, the Digital Personal Data Protection (DPDP) Act of 2023 (and the subsequent 2025 DPDP rules) is considered an important development within the privacy law landscape in India. The DPDP Act establishes several rights that safeguard personal information and places a significant burden on private companies to take reasonable steps to prevent data breaches. With this legislation, third-party app providers are generally required to explain how the data collected is going to be used and obtain explicit consent before using an individual's data.

Prior to the DPDP Act, third-party app providers could potentially use data gathered from UPI transactions to profile and influence consumer behavior. Since individuals use UPI extensively, third-party app providers can indirectly access demographic information such as an individual's religion. For example, individuals who frequently donate to Hindu religious organizations could reasonably be classified as Hindu by third-party app providers. Companies can potentially utilize this information to create targeted advertisements. With PhonePe and Google Pay already enjoying a duopoly in the third-party app provider market, access to such information may allow them to hold on to their market positions by using such data to further ad revenue generation. While Indian authorities have already tried to curtail the market share of PhonePe to 30% of the total third-party app provider market, the DPDP's regulations would likely help in creating a fairer market environment and make way for more competition in the market.

Nevertheless, there are several shortcomings with the DPDP legislation. Perhaps most crucially, it does not create various categories of data based on its sensitivity. The legislation deviates from international equivalents such as the European Union's General Data Protection Regulation (GDPR) on privacy law and does not establish separate categories for 'personal', 'sensitive' and 'non-personal' data. Doing so is crucial because a data leak that

exposes some PhonePe users' email addresses is not as concerning as a breach exposing banking credentials. While the latter situation may benefit from individual notices being sent to the concerned customers, doing the same in the former situation may be unnecessary. Having a common approach for all breaches may be resource-intensive for companies and it may discourage companies from paying special attention to highly sensitive data such as passwords, phone numbers and banking information. Failure to categorize data in such a manner results in a 'one size fits all' approach to data management.

In the unfortunate case where a data breach or misuse occurs, the redressal system may not provide sufficient recourse. The DPDP Act of 2023 establishes guidelines to set up the Data Protection Board of India (DPBI). However, critics like Aman Sonkar state that the DPBI lacks an independent process to appoint DPBI members and a dedicated budget, which could result in interference from large private sector companies and government bodies. Considering that UPI providers such as PhonePe and Google Pay have a significant presence in the market, the lack of safeguards against undue external influences on the DPBI is concerning and may undermine the benefits of the DPDP in the context of UPI systems. Additionally, individuals who live in rural areas and have disputes with UPI providers on matters such as the inability to withdraw consent on data sharing or who feel that their data is being misused have significant barriers to legal recourse as the DPBI may be located far away from their residence. Legislative changes such as requiring an independent budget for the board, mandating fixed-term appointments for board members which cannot easily be terminated and setting up regional offices could help strengthen the DPDP and indirectly enhance trust in UPI.

India's UPI system has made strides within the financial world and similar systems are being set up in other countries such as the United Arab Emirates and Singapore. The DPDP Act of 2023 has taken significant steps towards data privacy and governance so that the Indian public can maintain trust in digital systems such as UPI. However, the weaknesses in the legislation need to be addressed to mitigate doubts regarding how secure data is in the hands of third-party app providers.

Bibliography

- Badgi, Kuhu, and Alek Kuzmenchuk. "Ten Years of UPI: Implications of India's Digital Public Infrastructure for Data Protection." *Centre for Strategic and International Studies*, May 1, 2026. <https://www.csis.org/blogs/strategic-technologies-blog/ten-years-upi-implications-indias-digital-public-infrastructure>.
- Malik, Payal, and Harishankar Jagadeesh. "Time for India to Blaze the Trail Further on UPI: Build Guardrails for Data Privacy." *The Indian Express*, February 7, 2025. Accessed August 3, 2026. <https://indianexpress.com/article/opinion/columns/time-for-india-to-blaze-the-trail-further-on-upi-build-guardrails-for-data-privacy-9821824/>.
- States that the Indian Government caps total market share of a third party app provider to 30%
- Naithani, Paarth. "Analysis of India's Digital Personal Data Protection Act, 2023." *International Journal of Law and Management* 67, no. 5 (July 11, 2024): 543–53. <https://doi.org/10.1108/ijlma-05-2024-0174>.
- Nath, Sonia, and Rumi Dhar. "Sonia Nath and Rumi Dhar. An Analysis of the Digital Personal Data Protection Act 2023." *Christ University Law Journal* 15, no. 1 (July 13, 2026): 93–120. <https://doi.org/10.12728/culj.28.5>.
- Sarkar, Kingsuk, and Manash Jyoti Rabha. "The Success of Unified Payments Interface (UPI) System in India's Fintech Ecosystem—What's Unique?" In *Business and Management in Asia: Finance and Investments in the Digital Age.*, 105–20, 2025. https://doi.org/10.1007/978-981-96-3452-1_7.
- Sonkar, Aman. "The Digital Personal Data Protection Act, 2023: Analysing Its Implications, Challenges, and Future Prospects." *International Cybersecurity Law Review* 6, no. 4 (November 7, 2025): 547–69. <https://doi.org/10.1365/s43439-025-00164-2>.
- The Digital Personal Data Protection Act, 2023*. No. 22 of 2023. India

