Regulatory Hotline

February 02, 2024

PRIVACY AND DATA PROTECTION IN INDIA: 2024 WATCHLIST AND 2023 WRAP

INDIA'S HISTORIC DATA LAW

2023 was a milestone year for data protection and privacy in India with the enactment of the much-anticipated personal data protection legislation- the *Digital Personal Data Protection Act, 2023* ("**DPDPA**"). The DPDPA has been in the making since 2017 and after several stakeholder consultations and revisions, the DPDPA was enacted by the Indian Government in August 2023. While the implementation and enforcement of the DPDPA has been passed over to 2024, stakeholders are gearing up for this new law.

In line with the long-standing dual privacy regulation approach, sectoral regulators have also taken the front foot by further developing the existing sector-specific data protection obligations. In the past year, regulators such as the Insurance Regulatory and Development Authority ("**IRDAI**"), Securities and Exchange Board of India ("**SEBI**") and the Reserve Bank of India ("**RBI**") have issued guidelines to their respective sectors which *inter alia* also requires regulated entities in the respective industries to undertake higher security measures for storage of data, privacy and confidentiality. This time around, the regulators have focused on the key impact areas including cybersecurity and data storage on cloud services. These developments reflect the general interest of the Government in equipping itself for sectoral data privacy issues.

The Courts have been instrumental in protecting the right to privacy as well as adjudicating on various matters pertaining to the guardrails for exercising this right. However, broadly, in numerous instances, the Supreme Court and High Courts have emphasized on the need for the Government to implement the standalone data privacy law (i.e. the DPDPA). With the passage of the DPDPA in August 2023, we expect 2024 to see a surge in privacy litigation therefore, requiring the Courts to adjudicate on statutory rights in addition to the Constitutional right to privacy.

The key developments and milestones in data privacy regulations for 2023 are discussed below.

NEW DATA LAW: DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The DPDPA[1] has been published in the official gazette on August 11, 2023, however, its provisions are yet to be notified to come into force.[2] The DPDPA in its current form provides a principal-based framework for data protection compliances

The DPDPA is applicable to (a) processing of digital personal data in India and (b) processing of personal data outside India (irrespective of the location of the entity processing) in connection with offering goods or services to data principals located within the territory of India. Digital personal data is (i) personal data[3] in digital format and (ii) personal data which is collected in a physical format and subsequently digitized.

The DPDPA prescribes compliances for data fiduciaries[4] (akin to data controllers). In brief, the DPDPA lays down requirements with respect to consent and notice, security of personal data, transfers and disclosures of personal data, cross-border transfer restrictions, data breach notification requirements and data principal rights and grievance redressal mechanism. The Data Protection Board of India is the designated regulator under the DPDPA. In the event of non-compliance with the DPDPA, penalties in the range of INR 500 million (approx. USD 5.9 million) to INR 2.5 billion (approx. USD 30 million) may be triggered.

The Central Government will subsequently issue rules which will elaborate on the implementation aspects of the DPDPA. The rules will provide further clarity on notice requirements; functions of the consent manager; procedure for data breach notifications; parental consent for children's data[5]; grievance; exemptions for processing of personal data; redressal procedures etc.

Reportedly the Rules may be issued for public consultation very soon , however the implementation of the DPDPA itself may likely be in June, 2024 or later.[6]

Our hotline accessible **here**[7] discusses the provisions and implications of the DPDPA in detail.

HIGHER PENALTIES UNDER CURRENT DATA LAW

Till such time the DPDPA is notified to come into force- the current data privacy framework under the *Information Technology Act, 2000* ("**IT Act**") and the *Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011* ("**Data Protection Rules**")continue to be applicable.

In 2023, by way of the Jan Vishwas (Amendment of Provisions) Act, 2023, the penalty provisions under the IT Act have been amended to introduce higher penalties. Accordingly, for contravention of any rules (including the Data Protection Rules and The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013), regulations, directions or orders made under the IT Act, a penalty of INR 100,000 (approx. USD 1200) and liability

Research Papers

Littler International Guide (India) 2024
November 08, 2024

Unmasking Deepfakes
October 25, 2024

Are we ready for Designer Babies
October 24, 2024

Research Articles

The Bitcoin Effect
November 14, 2024

Acquirers Beware: Indian Merger Control Regime Revamped!
September 15, 2024

Navigating the Boom: Rise of M&A in Healthcare
August 23, 2024

Audio

Digital Lending - Part 1 - What's New with NBFC P2Ps
November 19, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part I
August 26, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part II
August 26, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

"Investment return is not enough" Nishith Desai with Nikunj Dalmia (ET Now) at FII8 event in Riyadh
October 31, 2024

Analysing SEBI's Consultation Paper on Simplification of registration for FPIs
September 26, 2024

for compensation (payable to the person affected by such contravention) of INR 100,000 – 1,000,000 (approx. USD 1200-12,000) may be triggered. Additionally, if a service provider, intermediary, data centre, body corporate or any person fails to cooperate with any request for information or directions issued by the CERT-In, a penalty for imprisonment for a term which may extend to one year or a fine which may extend to INR 1,00,00,000 (approx. USD 120,300) may be triggered.

RBI Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, 2023

The RBI has issued the *Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices, 2023*[8] ("**RBI IT Direction**"), which will be effective from April 1, 2024. The RBI IT Direction replaces several guidelines and directions previously issued by the RBI for information security and system management.[9]

The RBI IT Direction applies to the following RBI regulated entities- Scheduled Commercial Banks (excluding Regional Rural Banks); Small Finance Banks; Payments Banks; Non-Banking Financial Companies; Credit Information Companies; and All India Financial Institutions (EXIM Bank, NABARD, NaBFID, NHB and SIDBI). The RBI IT Direction does not apply to Local Area Banks and NBFC-Core Investment Companies.

Among other compliances, the RBI IT Direction requires the above-mentioned RBI regulated entities to institute an information technology (IT) Governance Framework that takes into account information security organizational structure, risk management, IT auditing, and business continuity/ disaster recovery management. Specifically, the regulated entities should adopt a cyber incident[10] response mechanism and also report the incidents to the RBI and the Indian Computer Emergency Response Team ("**CERT-In**") - the designated regulator under the general cyber security framework in India.[11]

Further, in contracting with vendors who are non-RBI regulated entities, the RBI regulated entity is required to put in place adequate controls in line with applicable legal, regulatory requirements and standards for protection of customer data.

RBI Master Direction on Outsourcing of Information Technology Services

The RBI has issued the *Master Direction on Outsourcing of Information Technology Services by Regulated Entities, 2023* (as described below) on 10 April 2023[12] ("**RBI Outsourcing Direction**"). The RBI Outsourcing Direction came into effect on October 1, 2023. Previously, the RBI had published draft directions for public consultation on June 23, 2022, pursuant to which the final RBI Outsourcing Directions have been finalized.

The RBI Outsourcing Direction applies to the following RBI regulated entities- Scheduled Commercial Banks (excluding Regional Rural Banks); Local Area Banks; Small Finance Banks; Payments Banks; Primary (Urban) Co-operative Banks; Non-Banking Financial Companies; Credit Information Companies; and All India Financial Institutions (EXIM Bank, NABARD, NaBFID, NHB and SIDBI). Specifically, the RBI Outsourcing Direction is triggered when the aforementioned RBI regulated entities outsource material IT functions.[13]

The RBI Outsourcing Direction lays down the obligations and compliances which RBI regulated entities are required to contractually pass to its vendors and service providers who are non-RBI regulated entities. *Inter alia,* these include compliance with applicable privacy laws to protect customer data; confidentiality and privacy of data; notification of data breaches to the RBI regulated entity; enabling data portability on termination of services; audits.

Importantly, in terms of breach reporting, RBI IT Direction lays down that the regulated entities should ensure that their service providers notify them of cyber incidents without undue delay, in order to ensure that the regulated entity is able to report the cyber incident within 6 hours of detection to the RBI. This requirement appears to be in line with timelines for cyber security incident reporting to the CERT-In under the general cyber security framework (which applies to all entities including RBI regulated entities).

SEBI Framework for Adoption of Cloud Services by SEBI Regulated Entities, 2023

The SEBI has issued the *Framework for Adoption of Cloud Services by SEBI Regulated Entities, 2023*[14] ("**SEBI Cloud Framework**") in March 2023. A period of one year (i.e. until March 6, 2024) has been provided for implementation. The SEBI Cloud Framework applies to SEBI registered entities- Stock exchanges; clearing corporations; depositories; stock brokers through exchanges; depository participants through depositories; asset management companies; mutual funds, trustee companies; boards of trustees of mutual funds; Association of Mutual Funds in India (AMFI); qualified registrars to an issue; share transfer agents and KYC registration agencies.

Among other compliances, the SEBI Cloud Framework requires the above-mentioned SEBI regulated entities which are availing cloud services through a public cloud, community cloud and hybrid cloud to ensure that data/information (all data related to financial services provided by the SEBI regulated entity) including logs (data center, disaster recovery) are stored and processed within the legal boundary of India. The SEBI Cloud Framework does not expressly restrict access to data stored in India to be given to persons outside India. The SEBI Cloud Framework specifies that the requirement to store the data in India is to ensure SEBI's right to access regulated entities' data and SEBI's rights of search and seizure are not affected by the adoption of cloud services. Therefore, this appears to be the rationale behind the data localization requirement.

Additionally, SEBI regulated entities are required to ensure that their cloud service providers are meeting the minimum security requirements and adopt a security management policy in line with the SEBI Cloud Framework.

IRDAI Guidelines on Information and Cyber Security for Insurers, 2023

The IRDAI has issued the *Guidelines on Information and Cyber Security for Insurers, 2023* ("**IRDAI CS Guidelines**") in April 2023. The IRDAI CS Guidelines apply to all insurers including FRBs, Insurance Intermediaries covering Brokers, Corporate Agents, Web Aggregators, TPAs, IMFs, Insurance Repositories, ISNP, Corporate Surveyors, MISPs, CSCs and Insurance Information Bureau of India (IIB). The IRDAI CS Guidelines replaces several guidelines and directions previously issued by the IRDAI for security of data and systems in the insurance sector.[15]

Among other compliances, the IRDAI CS Guidelines require the above-mentioned stakeholders in the insurance sector to adopt a Board-approved cyber security policy and conduct independent assurance audit annually. Further, all information security incidents[16] are required to be reported to the relevant stakeholders parties including the IRDAI, CERT-In (within 6 hours of detection), law enforcement and customers. Specifically, as per the audit checklist in the IRDAI CS Guidelines, the

Scope of judicial interference and inquiry in an application for appointment of arbitrator under the (Indian) Arbitration and Conciliation Act, 1996
September 22, 2024

regulated entities are required to confirm whether ICT infrastructure, Critical and Business data stored in India, therefore, implying that the IRDAI requires such data to be localized.

Supreme Court: Consenting to Privacy Policy Should Not Be Pre-Condition to Usage Of Platform

In the matter pertaining to the privacy policy of WhatsApp,[17] the Constitution Bench of the Supreme Court of India has directed the platform to widely publicize (by way of publication of full-page advertisements on two occasions in five national newspapers) its stand that its users in India do not have to accept its 2021 privacy policy in order to use the mobile application. The directions have been issued in light of the ongoing issue pertaining to the platform's privacy policy since 2016 . The privacy policy enabled the platform to access and use personal information of users, giving the Indian users without an option to opt-out. Controversially, the privacy policy enabled the widespread sharing of user data with group entities. In 2016, WhatsApp revised its privacy policy for Indian users which was disputed on grounds that it violated Article 21 of the Indian Constitution (i.e. right to privacy derived from the fundamental right to life). In view of the Supreme Court Directions, users who did not consent to the 2021 privacy policy were enabled to continue to use the platform without accepting the 2021 policy. Users who had previously consented to the 2021 privacy policy were not provided an opt-out option. (*Further readings: In our 2021 data wrap[18] we have discussed the anti-trust judgement on WhatApp's Privacy Policy*).

The final judgement on this matter has been deferred in light of the anticipated changes in the personal data regime in India. It is anticipated that the final verdict on this privacy policy dispute will be passed in 2024 in light of the DPDPA being notified.

ROAD AHEAD

2023 is a landmark with the introduction of the DPDPA, the first significant step in privacy laws in India after the *Puttaswamy v. Union of India* judgement. In view of the fact that most of the legal and regulatory development is recent, the Government, industry and stakeholders are in the continuous process of understanding the new developments and capacity building. Importantly, Courts in India have been emphasizing the Indian Government to accelerate the enactment of the new data law.[19] Significant litigations on the WhatsApp Privacy Policy and Government surveillance[20] are yet to be concluded and it would be interesting to see how the enactment of the new law will impact the Courts' verdicts.

In terms of the road ahead for privacy in India, as industry regulators play a more proactive role and with the implementation of the DPDPA around the corner, 2024 will be a historical year. The rules under the DPDPA will also be a gamechanger in terms of shaping the future of the personal data protection laws and striking a balance between business interests and individual's privacy. With both the industry and regulators navigating the challenges of the new regime, we foresee increased collaboration and Government's proactiveness in keeping up with new-age technological developments and data implications. 2024 may also be the year where we see increased regulatory focus on previously unchartered areas such as privacy in artificial intelligence based applications; children's data privacy; consumer privacy rights etc.

– Varsha Rajesh, Purushotham Kittane and Huzefa Tavawalla

You can direct your queries or comments to the authors.

---

[1]Once the provisions of the DPDPA are notified to come into force, it will effectively replace the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

[2]Currently, the Government has not officially indicated the timeline for enforcement of the DPDPA. Basis publicly available information, we understand that the DPDPA may be notified in the first quarter of 2024. However, do note that the Government may adopt different dates for the notification of different provisions and compliances may be triggered accordingly.

[3]As per DPDPA 'personal data' means " *any data about an individual who is identifiable by orin relation to such data."*

[4]As per DPDPA, 'data fiduciary' means "*any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data*."

[5]For reference see: https://indianexpress.com/article/india/aadhaar-based-consent-for-children-to-go-online-9071238/ (last accessed on January 29, 2024).

[6]See: https://www.cnbctv18.com/technology/data-protection-framework-postponed-dpdp-notifcation-after-lok-sabha-elections-18823331.htm (last accessed on January 29, 2024).

[7]See: https://www.nishithdesai.com/SectionCategory/33/Technology-Law-Analysis/12/60/TechnologyLawAnalysis/10703/1.html (last accessed on January 29, 2024).

[8]See: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/107MDITGOVERNANCE330357200100%4C67AC25B84292D85567.PDF (last accessed on January 29, 2024).

[9]Specifically, the RBI IT Direction replaces Risks and Control in Computer and Telecommunication Systems, 1998; Information System Audit - A Review of Policies and Practices; 2004; Operational Risk Management - Business Continuity Planning, 2005; Business Continuity / Disaster Recovery Planning, 2006; RBI Direction on Phishing Attacks, 2006; Business Continuity Plan (BCP), Disaster Recovery (DR) drill and Vulnerability Assessment-Penetration Testing (VAPT), 2010; Business Continuity Plan (BCP) and Disaster Recovery (DR); Vulnerability Assessment Penetration Testing(VAPT), 2012; Sharing of Information Technology Resources by Banks – Guidelines, 2013; Business Continuity Planning (BCP), Vulnerability Assessment and Penetration Tests (VAPT) and Information Security, 2013; Security Incident Tracking Platform – Reporting, 2014; Risk Governance Framework-Role of Chief Information Security Officer (CISO), 2017; Master Direction - Information Technology Framework for the NBFC Sector, 2017.

[10]As per the RBI IT Direction 'cyber incident' is "*a cyber event that adversely affects the cyber security of an information asset whether resulting frommalicious activity or not*."

[11]Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 and directions issued thereunder.

[12]See: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/102MDITSERVICES56B33FD530B1433187D75CB7C06C8F70.PDF (last accessed on January 29, 2024).

[13]IT services which if disrupted or compromised shall have the potential to significantly impact the RE's business operations; or b) may have material impact on the RE's customers in the event of any unauthorised access, loss or theft of customer information.

[14]See: https://www.sebi.gov.in/legal/circulars/mar-2023/framework-for-adoption-of-cloud-services-by-sebi-regulated-entities-res-_68740.html (last accessed on January 29, 2024).

[15]Specifically, the IRDAI CS Guidelines have replaced the guidelines previously issued in 2017, 2020 and 2022.

[16]As per the IRDAI CS Guidelines 'Security/Operational incident' is "an adverse event where: the IT resource is attacked or threatened with an attack; accessed/monitored/modified without authorisation; and used in a manner inconsistent with the established organization's/regulatory policy resulting in a real or Page 90 of 175 possible loss of confidentiality, integrity or availability of the IT resource or information. Examples of Security incidents are: internal or external attempts (either failed or successful) to gain unauthorised access to the IT system or its data; DLP violations; Attempts (either failed or successful) to gain access to blocked sites as per proxy rules; denial of service (DoS) or unauthorised disruption to IT system and infrastructure; actual or suspected loss of proprietary, confidential or entrusted information of the organization; changes to system hardware, firmware or software characteristics without the department head knowledge, instruction or consent; malicious code (virus, Trojan horse) attacks; social engineering (tricking someone to disclose confidential/proprietary information like passwords that could compromise system security); signature update failure; and hoaxes (deliberate trickery intended to gain an advantage e.g. false virus warnings may lead some user to ignore all virus warning messages, leaving them vulnerable to a genuine, destructive virus). Examples of Operational incidents are: firewall hardware failure; anti-virus appliance hardware failure; and IDS hardware failure.

[17]*Karmanya Singh Sareen v. Union of India*, SLP(C) 804 of 2017, Order dated February 1, 2023

[18]See: https://www.nishithdesai.com/NewsDetails/5105 (last accessed on January 29, 2024).

[19]See: *Karmanya Singh Sareen v. Union of India*, SLP(C) 804 of 2017.

[20]*Apar Gupta v CPIO, MHA & Ors* is a 2022 PIL filed in the Delhi High Court challenging the interception and monitoring activities carried out by the Indian Government under the Information Technology Act, 2000 and Telegraph Act, 1885.