INDUSLAW
THOUGHT LEADERSHIP ... APPLIED

TDW (THE DATA WRAP)

Authors: Namita Viswanath | Naqeeb Ahmed | Ruhi Kanakia | Srika Agarwal | Akshita Singh | Himangini Mishra

OCTOBER 2023

INTRODUCTION

Data is the oil that fuels the digital economy. It is the raw material that powers everything - from online shopping to social media, to artificial intelligence. Just as oil was essential to the industrial revolution, data is essential to the digital revolution. Like oil, it is crucial to regulate data to avoid its misuse, protect privacy, and ensure that its vast potential benefits are harnessed responsibly and ethically.

India has experienced significant developments in the data protection space over the past few months. The Digital Personal Data Protection Bill, 2023, the fifth iteration of India's standalone data protection law, was successfully introduced, passed by both houses of parliament, and received presidential assent in August 2023. As a result, India now has a well-established, dedicated and comprehensive data law, known as the Digital Personal Data Protection Act, 2023 ("**DPDP Act**"). The DPDP Act is not yet in effect, but once effective, is set to reshape the data protection landscape in India.

SO, WHAT TRANSFORMATIVE CHANGES DOES THE DPDP ACT BRING TO THE TABLE?

The DPDP Act is a landmark piece of legislation that will regulate the processing of digital personal data in India. The DPDP Act is designed to protect the right to privacy of individuals as recognised by the Supreme Court of India, and to give them more control over their personal data. Here are some of the salient features of the DPDP Act:

Consent and notice. Any processing of personal data will be subject to consent. The consent needs to be freely given (through a clear affirmative action), specific, informed, unconditional, and should unambiguously indicate the data principal's affirmation to the processing of his/her personal data for the specified purpose. Implied consent would not work anymore where processing of digital personal data is involved. Additionally, at the time of seeking consent, the data fiduciary is required to provide to the data principal, a privacy notice in clear and plain language.

The requirement to provide a privacy notice has retrospective application i.e., data fiduciaries will be required to issue such notices to all such data principals whose personal data they are currently processing. Lastly, the data fiduciary is required to ensure that the data principal has the option of withdrawing his/her consent with ease (comparable to the ease with which consent was given).

Data retention. The data fiduciaries must cease to retain personal data (a) upon withdrawal of consent; or (b) as soon as the specified purpose (for which the personal data was collected) is no longer being served, unless an applicable law requires a longer data retention period.

Personal data breach. Data fiduciaries are required to implement reasonable security safeguards to prevent personal data breaches. In case of a data breach, the data fiduciary is required to notify the same to the Data Protection Board ("**Board**"), as well as to the concerned data principals.

Significant data fiduciaries. The Central Government can notify any data fiduciary or class of data fiduciaries as significant data fiduciaries, based on the volume and sensitivity of personal data processed, risk of harm, security of the state, etc. The DPDP Act imposes certain additional obligations on such significant data fiduciaries viz., the need to (i) appoint a data protection officer based in India; (ii) appoint an independent data auditor to evaluate compliance with the DPDP Act; and (iii) undertake periodic data protection impact assessment and compliance audits.

Rights & duties of a data principal. The DPDP Act provides certain rights to data principals such as right to erasure, right to correction, right to grievance redressal, right to nomination, and the right to withdraw consent for processing of personal data, among others. Additionally, the DPDP Act also lists down certain obligations for the data principal including, inter alia, the duty to not impersonate another person, register false or frivolous grievances or complaints, or supress any material information while providing his/her personal data.

Legitimate uses. The DPDP Act stipulates certain 'legitimate uses' for which a data fiduciary can process personal data of data principals without obtaining their explicit consent.

Consent manager. The DPDP Act also introduces the concept of 'consent managers' viz., a person registered with the Board, who acts as a single point of contact to enable a data principal to give, manage, review, and withdraw his/her consent through an accessible, transparent and interoperable platform.

Exemptions. The DPDP Act empowers the Central Government to exempt certain data fiduciaries or classes of data fiduciaries at its discretion, including startups and any 'instrumentality of the state' from certain provisions.

Penalty for violation of the DPDP Act. Penalties of up to INR 250 crore (~USD 30 million) may be imposed for non-compliance with provisions of the DPDP Act. However, no criminal liability has been envisaged under the Act.

Processing of children's data. The DPDP Act requires data fiduciaries to obtain verifiable consent of the parent or legal guardian of a child before processing the personal data of children. Further, a data fiduciary also has to ensure that such processing does not have a detrimental effect on the well-being of a child or that they do not undertake tracking, behavioral monitoring, or targeted advertising directed at children.

In essence, by giving individuals more control over their personal data and preventing its misuse, the DPDP Act creates a more transparent and accountable framework for the processing of personal data. While the date of enforcement of the provisions of the DPDP Act is yet to be notified by the Central Government, it is expected to undergo a phase-wise implementation.

Have questions about the DPDP Act? We have compiled a detailed FAQ document to answer the most commonly asked questions. The same is available here.

Need more information on the DPDP Act? Please see our detailed note on the same here.

BREACH NOTIFICATION REQUIREMENT IN INDIA

In our increasingly interconnected digital world, the protection of personal data has become a paramount concern for individuals and organizations alike. As the custodians of vast volumes of sensitive information, businesses and institutions are under constant threat from data breaches. The fallout from such incidents can be substantial, leading to not only financial losses but also reputational damage and potential legal consequences. In response to these growing concerns, data breach notification laws have emerged as a critical regulatory tool. These laws require organizations to promptly inform affected individuals and relevant authorities when a breach of personal data occurs.

In India, the central laws as well as laws framed by sectoral regulators, prescribe the modus operandi for responding to data breaches. Given the multiplicity of regulations, companies that are directly or indirectly regulated by sectoral regulators, may not always be aware of the mechanism to be followed. With this segment of The Data Wrap, we have specifically carved out the general reporting obligations and the sectoral obligations applicable to entities in the financial space and strive to provide you with a ready reckoner of how to respond to data breaches as an entity regulated by financial sector regulators.

General Reporting Obligations

In India, the general data breach reporting obligations, irrespective of the sector in which an entity operates, is prescribed under the DPDP Act and Information Technology Act, 2000 ("**IT Act"**).

DPDP Act

The DPDP Act stipulates the measures that are to be taken on the occurrence of a personal data breach.[1] Under the DPDP Act, on the occurrence of a personal data breach, the data fiduciary is required to notify the Board as well as the data principal about such breach. The form, time period, and manner in which such notification is to be provided, has been left to the rule-making powers of the Central Government, and there will be more clarity on this once 'rules' under the DPDP Act are prescribed. Separately, the DPDP Act also sets out the adjudicatory powers of the Board in terms of the Board initiating an inquiry into a personal data breach and imposing a penalty in relation to the same.

IT Act

The Indian Computer Emergency Response Team ("**CERT-In**") constituted under the IT Act, is the nodal agency for resolving cyber incidents in India. As per the CERT-In Rules and the 'Directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet' ("**CERT-In Directions**"), all service providers, intermediaries, data centres, body corporates and government organisations are required to mandatorily report cyber incidents[2] to the CERT-In within 6 (six) hours of either noticing such incidents or such incidents being brought to such entities' attention. Along with reporting of the incident, entities are also required to provide the CERT-In with logs of all their ICT systems, which is to be maintained by them in a secure manner, within India, for a rolling period of 180 (one hundred and eighty) days.[3] Non-compliance with the reporting obligations under the CERT-In may attract imprisonment for up to 1 (one) year or a penalty of up to INR 1 lakh (~USD 1250).[4]

Sectoral Reporting Requirements

Reserve Bank of India ("RBI")

The RBI, by way of several circulars, imposes breach notification obligations on entities it regulates such as commercial banks, co-operative banks, payment system operators, non-banking finance companies ("**NBFCs**") etc. Banks are required to report security incidents within 2 (two) to 6 (six) hours to the RBI, and NBFCs are required to report such incidents within 24 (twenty-four) hours to the RBI.

1. Section 2(u) of the DPDP Act defined personal data breach to mean *'any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data'.*
2. Annexure I of the CERT-In Directions set out a list of cyber incidents which to mandatorily be reported to the CERT-In, and includes data breach and data leaks.
3. Direction (iv) of CERT-In Directions.
4. Section 70B(7) of the IT Act.

Separately, the RBI has also prescribed, by way of several circulars, breach notification requirements in relation to outsourcing of financial services by RBI-regulated entities. Such various circulars, *inter alia*, require (a) banks to notify RBI immediately on the occurrence of any breach of security and leakage of confidential customer related information;[5] (b) co-operative banks to notify RBI/ National Bank for Agriculture and Rural Development ("**NABARD**") immediately on the occurrence of any breach of security and leakage of confidential customer related information;[6] (c) payment system operators to notify RBI on the occurrence of any breach of security and leakage of confidential customer related information;[7] and (d) NBFCs to notify RBI on the occurrence of any breach of security and leakage of confidential customer related information.[8]

Securities Exchange Board of India ("SEBI")

SEBI had issued an advisory in relation to cyber-security best practices for all SEBI-regulated entities. The said advisory reiterates the need to comply with the advisories issued by the CERT-In, which would include the CERT-In Directions, and mandates SEBI regulated entities to implement advisories issued by the CERT-In in a prompt manner, and in letter and spirit.[9] This implies that SEBI regulated entities are also bound by the requirement of reporting cyber incidents to the CERT-In within 6 (six) hours. Additionally, SEBI also imposes obligation on certain regulated entities to report occurrences of cyber incidents to SEBI. Stock brokers have an additional obligation to report occurrences of cyber incidents to stock exchanges and depositories. Further, if the system of a SEBI regulated entity has been identified as a "protected system" by the National Critical Information Infrastructure Protection Centre ("**NCIIPC**"), then they are also required to report the cyber-attacks, cyber threats, cyber incidents and breaches to the NCIIPC as well.

Insurance Regulatory Authority of India ("IRDAI")

The IRDAI, on April 24, 2023, issued the IRDAI Information and Cyber Security Guidelines ("**CS Guidelines**"), which sets out in a comprehensive manner the cyber security measures and standards IRDAI regulated entities are required to adhere to. Such regulated entities include insurers including foreign re-insurance branches and insurance intermediaries regulated by the IRDAI.[10] These regulated entities are required to report cyber incidents to CERT-In within 6 (six) hours of noticing or being brought to notice about such incidents, along with a copy of the same to the IRDAI.[11]

To sum up, in the table below, we provide a concise overview of the legal requirements and process for data breach notifications.

5. Clause 5.6.5 of the Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks dated November 3, 2006.
6. Clause 5.6.5 of the Guidelines for Managing Risk in Outsourcing of Financial Services by Co-operative Banks dated June 28, 2021.
7. Clause 8.1 (e) of the Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators dated August 03, 2021.
8. Clause 5.6.5 of the Directions on Managing Risks and Code of Conduct in Outsourcing of Financial Services by NBFCs dated November 9, 2017.
9. Para 10 of Annexure A to Advisory for SEBI Regulated Entities (REs) regarding Cybersecurity best practices dated February 22, 2023.
10. Para 1.4 of the CS Guidelines.
11. Para 3.5 of Policy Number 2.5 of the CS Guidelines.

SL No.	Type of incident	Reporting Entity	Entity / person to which incident is to be reported to	Reporting Timeline and Form
Reporting Obligation under DPDP Act				
1.	Breach of personal data	All data fiduciaries.	Board and the affected data principals.	To be prescribed in rules.
Reporting Obligations under the IT Act				
2.	Cyber incidents which include data breaches and data leaks	All service providers, intermediaries, data centres, body corporates and government organisations.	CERT-In	Within 6 (six) hours of either noticing such incidents or such incidents being brought to such entities' attention.
Reporting Obligations under RBI laws				
3.	Cyber incident	Scheduled Commercial Banks (excluding Regional Rural Banks); Local Area Banks; Small Finance Banks; Payments Banks; Primary (Urban) Co-operative Banks; NBFCs (Upper Layer and Middle Layer); Credit Information Companies; and All India Financial Institutions (EXIM Bank, National Bank for Agriculture and Rural Development, National Bank for Financing Infrastructure and Development, National Housing Bank and Small Industries Development Bank of India).	RBI	Within 6 (six) hours of detection of cyber incident by the service provider of the reporting entity.
4.	Any breach of security and leakage of confidential customer related information	Banks	RBI	Immediately.
		Co-operative banks	RBI and NABARD	
		Payment System Operators	RBI	
		NBFCs	RBI	
5.	Security incidents, which include data breach, data destruction, theft, loss, destruction or corruption of sensitive customer or business information	Banks	RBI	Within 2 (two) to 6 (six) hours in the template prescribed by the RBI.
		NBFCs	RBI	Within 24 (twenty-four) hours in the template prescribed by the RBI.

SL No.	Type of incident	Reporting Entity	Entity / person to which incident is to be reported to	Reporting Timeline and Form
Reporting Obligations under SEBI laws				
6.	Cyber-attacks, cyber threats, cyber incidents and breaches	Stock brokers/depositories participants	Stock exchanges / depositories, SEBI, and CERT-In, and National Critical Information Infrastructure Protection Centre ("NPIIC if entity has been recognised as "protected system" by NPIIC".	Within 6 (six) hours of noticing/detecting such incidents or being brought to notice about such incidents, in the incident reporting form prescribed by SEBI.
		KYC Registration Authorities	SEBI, CERT-In and NPIIC if entity has been recognised as "protected system" by NPIIC.	
		Qualified Registrars to an Issue and Share Transfer Agents		
		Mutual Funds/AMCs		
		Portfolio Managers		
Reporting Obligations under IRDAI laws				
7.	Cyber incidents	Insurers including foreign re-insurance Branches and insurance intermediaries such as insurance brokers, re-insurance brokers, insurance consultants, corporate agents, surveyors and loss assessors regulated by the IRDAI.	CERT-In with a copy to IRDAI	Within 6 (six) hours of either noticing such incidents or such incidents being brought to such entities' attention, and to be reported to Cert-In and IRDAI.

THE DATA RETENTION CONUNDRUM: WHEN TO AND WHEN NOT TO RETAIN?

Data retention refers to storing of data for a specified period of time typically for business purposes or for compliance with applicable laws. Deciding on the data retention period is a complex issue. On the one hand, retaining data can help organizations make better business decisions, comply with legal and regulatory requirements, and protect themselves from liability. On the other hand, retaining data could also increase the risk of data breaches and can also lead to privacy concerns.

Data retention laws are not new to India. What is new and noteworthy are the fines under the DPDP Act for failure to comply with the data retention requirements specified therein. As per the DPDP Act, a data fiduciary must cease to retain personal data (a) upon withdrawal of consent by a data principal; or (b) as soon as it is reasonable to assume that the specified purpose (for which the personal data was collected) is no longer being served, unless an applicable law requires a longer data retention period.

Are there laws that prescribe data retention requirements in India? Yes, in fact there are multiple laws that impose data retention requirements on certain data sets processed by persons in India. We have captured some of the key data retention requirements in the below table:

SL No.	Statue	Data Sets	Data Retention Period
1.	The Income Tax Act, 1961	Domestic transactions or international transactions exceeding the aggregate value of INR 1 Crore (~USD 120k) – includes details such as description of the ownership structure, description of business, details of assets employed, etc.	8 years from the end of the current financial year.
		Books of accounts and documents relevant for calculation of total income.	6 years from the end of the current financial year.
2.	The Companies Act, 2013	Records relating to (a) sums of money received and expended; (b) sales and purchases of goods and services; (c) assets and liabilities, etc.	8 years from the end of the current financial year.
		Company charter documents, shareholder minutes documents, board of director minutes documents and statutory registers.	Lifetime of the company.
3.	The Minimum Wages Act, 1948	Name of the employee, wage paid, number of working hours and place of work.	3 years from the date of last entry in records.
4.	The Payment of Wages Act, 1936	Personal details of an employee including wages paid and description of work.	3 years from the date of last entry in records.

SL No.	Statue	Data Sets	Data Retention Period
5.	The Prevention of Money-Laundering Act, 2002	Details of transactions, including that of attempted transactions.	5 years from the date of transaction.
		Documents for identification of clients and beneficial owners, business correspondence with clients and account files relating to clients.	5 years from the conclusion of business relationship or closing of a client account.
6.	The Employees' State Insurance Act, 1948	Name of an employee, wages paid, insurance number, period of service, details of the accident occurred during the employment, etc.	5 years from the date of last entry in records.

What are the required actions?

Persons collecting data including those data sets captured above will need to revisit their data retention protocols and process and align them with the applicable data retention laws. Further, they may also be required to establish robust systems to ensure adherence to the specified data retention periods and the appropriate disposal of data sets once these retention periods have concluded.

JUDICIAL UPDATES

Judicial precedents play a pivotal role in shaping the ever-evolving landscape of laws. In this section, we delve into recent judicial precedents that have left an imprint on data privacy. These cases provide valuable insights into the evolving legal interpretations and challenges surrounding data protection, setting important benchmarks for individuals, organizations, and policymakers alike.

Kerala HC on Google's use of AI tools to remove identifiers from online judgements.

While hearing a review petition filed by Google LLC ("**Google**") against a December 2022 judgement, the Kerala High Court ("**Kerala HC**") refused to expunge remarks from this earlier judgement pronounced in the case of *Vysakh K.G. v. Union of India & Anr* ("**Impugned Judgement**").[12] Through the Impugned Judgement, the Kerala HC had observed that Google had the responsibility to take down judgements and other information that disclosed personal details of parties. It had also suggested that Google should use artificial intelligence ("**AI**") tools to identify and remove private information from judgements and court documents.[13]

Several cases regarding the deletion of personal information from court judgements published by the platform 'Indian Kanoon' and indexed by Google, were placed before the Kerala HC in December 2022. The Kerala HC upheld the right to privacy, observing that judgements arising out of matrimonial and family disputes are purely private disputes, and the publication of judgements online and allowing them to be viewed in the digital space is violative of the litigant's right to privacy. Additionally, it observed that search engines, like Google, must erase or redact personal data contained in the judgements from the digital domain, and retaining judgements in the digital domain forever is violative of the litigants' fundamental right to be forgotten.[14]

The Kerala HC clarified that Google could not claim to be a "mere intermediary" only with reference to *"the claim based on fundamental rights and not with reference to any normal activities of Google referable to Information Technology Act and the relevant Rules".*[15]

Rajasthan HC quashes three interception orders for phone tapping of a private individual.

In a suit filed seeking the quashing of 3 interception orders ("**Interception Orders**") passed by the Government of Rajasthan, the Rajasthan High Court ("**Rajasthan HC**") held that the orders suffered from manifest arbitrariness and violated the fundamental rights of citizens.

On October 28, 2020, the Secretary (Home), Government of Rajasthan passed an order under Section 5 of the Indian Telegraph Act, 1885 ("**Telegraph Act**") and Section 69 of the IT Act, to intercept the mobile number of an accused suspected of using the mobile number for illegal activities relating to the incitement of the commission of an offence affecting public safety. Subsequently, 2 separate orders dated March 17, 2021 were passed to intercept the 2 mobile numbers of the petitioner, Mr. Shashikant Joshi, citing the same reasons. Following the interception of the mobile numbers, a first information report came to be registered under relevant provisions of the Prevention of Corruption Act, 1988. Thereafter, the petitioner challenged the Interception Orders on the ground that his right to privacy was infringed by the authorities through their action of tapping his mobile number.

The Rajasthan HC observed that executive instructions cannot supersede statutory rules. As such, the Interception Orders were not sustainable since they were authorized by an incompetent authority. The court relied on judgements such as *PUCL v. Union of India*[16] and *K.S. Puttaswamy v. Union of India*[17] to opine that since the reasons for interception were not recorded as required by Section 5(2) of the Telegraph Act, the Interception Orders suffered from manifest arbitrariness, thus violating the petitioner's right to privacy.

Delhi HC refuses to grant injunction to late actor's father against the further telecast of the film Nyay: The Justice

In a petition filed by the late actor Sushant Singh Rajput's father against the makers of the film "Nyay: The Justice" ("**Film**"), the Delhi HC refused to injunct the further telecast of the Film, which was released on the OTT platform 'Lapalap' in June 2021.[18]

---

12. Vysakh K.G. v. Union of India, 2022 SCC Online Ker 7337.
13. Google Inc. v. Union of India, Review Petition No. 107 of 2023.
14. Google Inc. is a client of IndusLaw and the information herein is based on statements in the media and not our professional knowledge of the relevant update.
15. https://hckinfo.kerala.gov.in/digicourt/Casedetailssearch/fileviewcitation?token=MjEyNDAwMDAxMjAyMDIzXzEucGRm&lookups=b3JkZXJzLzIwM-jM=&citationno=MjAyMzpLRVI6MjEzNzI=
16. People's Union for Civil Liberties vs. Union of India & Ors., AIR 1997 SC 568.
17. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
18. Krishna Kishore Singh v. Sarla A Saraogi & Ors., Civil Suit (Commercial) No. 187/2021.

Dismissing the petition, the Delhi HC observed and held that (a) assuming that the Film infracts the publicity rights of Sushant Singh Rajput or defames him, the infracted right is personal to the late actor and cannot be said to have been inherited by his father. The rights ventilated in the plaint i.e., the right to privacy, the right to publicity and the personality rights which vested in the late actor, are not heritable.; (b) the Film, being based on information in the public domain, which, at the time of its original dissemination, was never challenged or questioned, cannot be sought to be injuncted at this distance of time. Injuncting the further dissemination of the Film would, therefore, infract the defendants' rights under Article 19(1)(a) of the Constitution of India.

The Delhi HC issued notice to the respondents to file their response and the appeal has been listed to be heard next on November 16, 2023.

Kerala HC directs Thodupuzha Police to remove online images of woman facing humiliation and cyber-attacks

In a suit filed by a certified ayurvedic therapist to remove her images and personal details from social media platforms, the Kerala HC observed that privacy is a core element of human dignity and ordered the Director General of Police to take certain measures to enforce the same.

The matter was partly heard on September 26, 2023, and was later listed for hearing on October 6, 2023. No information regarding the proceedings held on October 6, 2023 or the subsequent date of hearing is currently publicly available on the Kerala HC's official website.

That's it, folks. Hope you enjoyed the wrap!

INDUSLAW
THOUGHT LEADERSHIP ... APPLIED

www.induslaw.com

OUR OFFICES

BENGALURU
101, 1st Floor, "Embassy Classic"# 11
Vittal Mallya Road
Bengaluru 560 001
T: +91 80 4072 6600
F: +91 80 4072 6666
E: bangalore@induslaw.com

HYDERABAD
204, Ashoka Capitol, Road No. 2
Banjarahills
Hyderabad 500 034
T: +91 40 4026 4624
F: +91 40 4004 0979
E: hyderabad@induslaw.com

CHENNAI
#11, Venkatraman Street, T Nagar,
Chennai - 600017 India
T: +91 44 4354 6600
F: +91 44 4354 6600
E: chennai@induslaw.com

DELHI & NCR
2nd Floor, Block D
The MIRA, Mathura Road, Ishwar Nagar
New Delhi 110 065
T: +91 11 4782 1000
F: +91 11 4782 1097
E: delhi@induslaw.com

9th Floor, Block-B
DLF Cyber Park
Udyog Vihar Phase - 3
Sector - 20
Gurugram 122 008
T: +91 12 4673 1000
E: gurugram@induslaw.com

MUMBAI
1502B, 15th Floor
Tower – 1C, One Indiabulls Centre
Senapati Bapat Marg, Lower Parel
Mumbai – 400013
T: +91 22 4920 7200
F: +91 22 4920 7299
E: mumbai@induslaw.com

#81-83, 8th Floor
A Wing, Mittal Court
Jamnalal Bajaj Marg
Nariman Point
Mumbai – 400021
T: +91 22 4007 4400
E: mumbai@induslaw.com