PSA
LEGAL COUNSELLORS

Digital Personal Data Protection Act, 2023 & Draft Rules, 2025

Insights For Businesses

©PSA 2025. All Rights Reserved | www.psalegal.com

Contents

©PSA 2025. All Rights Reserved

Acronyms

CERT-In: Indian Computer Emergency Response Team
CG: Central Government
CM: Consent Manager
DC: Data Controller
DF: Data Fiduciary
DP: Data Principal
DPA: Data Processing Agreement
DPBI: Data Protection Board of India
DPDPA: Digital Personal Data Protection Act, 2023
DPIA: Data Protection Impact Assessment
DPO: Data Protection Officer
DPR: Data Processor
DPDP Rules or rules: Draft Digital Personal Data Protection Rules, 2025
DS: Data Subject (An identifiable natural person under GDPR)
GDPR: General Data Protection Regulation
IT Act: Information Technology Act, 2000
MeitY: Ministry of Electronics and Information Technology
PD: Personal Data
PETs: Privacy Enhancement Tools
SDF: Significant Data Fiduciary
SDPI Rules: Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011

Note 1: Indian Rupees have been converted to USD applying a rate of INR 85 to 1 USD and rounded off

©PSA 2025. All Rights Reserved

Notice to Data Principal

Section 5 requires DF to give notice to the DPs before processing any data.

Now, rule 3 clarifies this notice must be standalone, clear, in plain language, and shall include an itemized description of PD, the specified purpose, and goods/services or uses to be enabled.

It shall also include the manner to withdraw consent (*with the same ease as giving consent*), DS rights and the manner of making a complaint to DPBI.

The option to withdraw consent, arguably, should be as granular as the consent itself.

Consent Manager

Section 6(7) provides for a CM. Under rule 4, the CM should:

- be an Indian company
- have a minimum net worth of INR 2 million or about USD 235,000
- act in a fiduciary capacity towards the DP
- not sub-contract or assign its obligations
- avoid any conflict of interest with the DF

More details in the First Schedule.

Processing under Certain Circumstances

State or its instrumentalities, while processing PD under section 7(b) or 17(2)(b) must comply with the Second Schedule.

This includes ensuring lawful processing, data minimization, purpose limitation, and reasonable security measures.

Thus, the State has put a fairly strict onus on itself when acting as a DF.

©PSA 2025. All Rights Reserved

Data Breach Notification

Section 8(6) requires DFs to inform each affected DP and DPBI about PD breaches.

Rule 7 clarifies that data breaches must be reported "without delay" to (a) each affected DP with a description of the breach, relevant consequences, mitigation steps, safety measures, and (b) DPBI with details of the breach and its likely impact. Further, within 72 hours, an updated report is to be provided to DPBI with details of the breach, mitigation steps, details of the responsible individual, remedial measures and a report of notifications to DPs. This shall apply to all breaches, regardless of harm.

Possibly, this requirement will overwhelm DPs and overburden DFs and DPBI. DFs must, therefore, enhance their data security teams. We expect to see a significant increase in SecOps hirings and a rise in data breach/cybersecurity insurance offerings.

Reasonable Security Safeguards

Section 8(5) requires DFs to take reasonable security safeguards to prevent PD breaches.

While no specific security safeguards have been prescribed, rule 6 sets certain minimum standards to be followed, such as securing PD through encryption/masking/use of virtual tokens, implementing appropriate access controls, maintaining logs to detect unauthorised access, data backups, etc. This could pose a burden on smaller DFs. That being said, all these security safeguards can be implemented in the manner the DF deems appropriate.

Additionally, DFs must retain data breach logs for one year or as specifically prescribed under any other law.

Contact Details for Inquiries

Section 6(3) requires DFs to provide the business contact details of a DPO (where applicable), or of any other person authorized to respond to a DP's inquiries.

Rule 9 clarifies that this contact information must be displayed on the DF's website/app and should be included in all communications with the DP. It is unclear whether such an authorised person, who is not a DPO, will have any liability exposure.

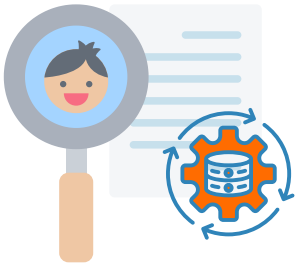
©PSA 2025. All Rights Reserved

Data Retention & Data Deletion

DFs are required to delete PD when they can reasonably assume that the data is no longer serving its purpose (section 8(7)) and when a DP withdraws its consent (section 12(3)).

The only exception to these requirements is when the data must be retained under any law. Rule 8 provides for deletion and retention of PD for only three kinds of DFs, namely (a) e-commerce entities with 20 million or more registered users in India; (b) social media intermediaries with 20 million or more registered users in India; and (c) online gaming intermediaries with 5 million or more registered users in India. Such entities may retain PD for up to 3 years from the last interaction or the rules' commencement. These DFs must inform the DPs 48 hours prior to deleting their PD. No timeline has been mentioned for any other type of DFs. Arguably, such other DFs can make their own policies on retention and deletion of PD.

Processing of Child's Personal Data



Under section 9(1), before processing the data of a child or person under guardianship, the DF must obtain verifiable consent from the parent or guardian. Rule 10 requires the DF to confirm the "parent" is an identifiable adult. It is unclear how DFs are supposed to address instances where a child falsely claims to be an adult. Rule 10 also refers to virtual tokens mapped to the DP's ID and age. If adopted, India could be one of the first countries to deploy such a sophisticated age-gating technique.

Under rule 11, certain entities like healthcare providers, educational institutions, childcare providers, etc. are exempt from complying with section 9(1) and 9(3) (prohibiting tracking, behavioral monitoring or targeted advertising to children). While section 9(1) exemption appears reasonable, section 9(3) exemption may unfairly allow these entities to target advertisements to children.

Fourth Schedule also exempts DFs from compliance with section 9 (1) and (3), where the purpose of processing includes legal duties, benefits of the child, etc. However, these expressions are vague, and it is unclear how they will be interpreted.

©PSA 2025. All Rights Reserved

Additional Obligation of SDF

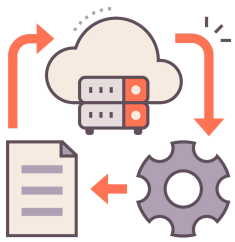
Section 10(2) empowers the state to notify any DF as a SDF. The rules do not prescribe any criteria for determining who qualifies as a SDF. Section 35, read with rule 22(1), further allows CG to procure data from any DF to ascertain if it should be classified as significant or not.

Under rule 12, SDFs must conduct DPIA and audit annually and report its observations to DPBI. The SDFD must also ensure that any "algorithmic software" used for processing PD does not pose any risk to the DP's rights. It is unclear how this due diligence must be conducted. CG may also require SDFs to process certain PD (including traffic data relating to its flow) in India. This appears to be an indirect way to enforce data localization and could significantly increase the cost of compliance if a specific data set is prohibited from cross-border transfer.

Rights of Data Principal

Chapter III (sections 11 to 15) provides DP rights such as access to information, correction and erasure of personal information, withdrawal of consent, and nomination. Rule 13 further requires DFs and CMs to publish on their website/apps the method for DPs to access these rights. Moving forward, we expect DFs to deploy software solutions to facilitate these rights.

Processing PD Outside India



Section 16 empowers CG to restrict PD transfers to other countries. Rule 14 requires DFs processing data in connection with activities targeting DPs in India to comply with any CG directive with respect to making PD available to any foreign country or any foreign entity. This could create compliance hurdles for DFs processing data outside India, as they may be required to comply with foreign laws as well.

Data Protection Board of India

Section 18 provides for setting up a DPBI. The rules expand on this and provide details regarding member appointments, terms of service, and other procedures. Rule 19 specifies DPBI will function as a digital office, using techno-legal measures to conduct proceedings without requiring physical attendance. Fourth and Fifth Schedule of the rules cover the terms and conditions of service of DPBI and its employees.

©PSA 2025. All Rights Reserved

Concept 1: Consent & Notice Requirements under DPDPA & Draft Rules

1. What does the law say?

DPDPA provides two legal grounds for processing of PD: (a) consent, and (b) certain legitimate uses (section 4 (1)). Where consent is the basis for processing PD, it must be: (a) free, (b) specific, (c) informed, (d) unconditional, and (e) unambiguous, with a clear affirmative action indicating that DP agrees to processing of their PD for the specified purpose, and is limited to the PD necessary for fulfilling that purpose (section 6 (1)).

Request for consent

Every request for consent must be presented in clear and plain language (English or other Eighth Schedule languages) and must include details of DPO (where applicable) or any other person designated to address communications from DPs. Request for consent must be accompanied/preceded by a standalone "notice".

2. What should a notice to DP include?

Notice to DP should be in clear and plain language (*English or any other Eighth Schedule language*), including details necessary to enable DP to give informed consent, including at minimum

- itemised description of PD to be obtained
- purpose for which the PD is to be processed, along with itemised description of goods/services
- communication link to access the website/app of the data fiduciary, along with any other means through which the data principal may:
  - withdraw her consent
  - exercise her rights (*including right to grievance redressal*)
  - make a complaint with DPBI

(section 5(1) & (3) r/w Draft Rules 3)

Consent for legacy data

Where DP has provided consent prior to commencement of DPDPA, DFs must, as soon as reasonably practicable, issue a notice containing the above-stated details (section 5(2)(a)). Consequently, we suggest DFs should identify all legacy PD collected prior to the commencement of DPDPA and map it to the purpose of its collection. After issuing the required notice, DFs may continue processing unless consent is withdrawn by DP (section 5(2)(b)).

©PSA 2025. All Rights Reserved

3. Key questions

(a) Can consent be withdrawn?

Where DP has provided consent for processing of PD, she may withdraw her consent at any time. The process for withdrawal should be as easy as the process of providing consent (section 6(4)). Such withdrawal of consent shall not affect the lawfulness of its prior processing (section 6(5)).

(b) What should DFs do after withdrawal of consent?

After a DP has withdrawn her consent to the processing of PD, DF should

- Within a reasonable time, cease/ensure its DPRs cease processing of PD, unless processing is required or authorised under DPDPA, Draft Rules, or any other applicable law (section 6(6))
- Erase the PD of P, unless its retention is necessary for compliance with applicable law (section 8(7)(a))

(c) Who are CMs?

A DP may give, manage, review, or withdraw their consent through a "CM". Such a appointed CM must be registered with DPBI and remain accountable to DPs (sections 6(7) to 6(9)).

Way Forward

DPDPA imposes penalties of up to INR 500 million or about USD 6 million for failing to obtain valid consent. To ensure compliance, companies must update their consent mechanisms and privacy notices in line with the listed requirements. Further, data discovery must be conducted for all legacy PD and must be mapped with the purpose of collection.

Additionally, looking forward, we see CMs playing a key role in DPDPA ecosystem. Therefore, DFs must carry out their due diligence to ensure that the CMs engaged by them are capable of effectively (and technically) managing consent on behalf of DPs.

©PSA 2025. All Rights Reserved

Concept 2: Consent Managers

1. Who is a CM?

Under section 2(g) of DPDPA, CM is "a person registered with DPBI, who acts as a single point of contact to enable a DP to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform".

*DPs may give, manage, review, or withdraw their consent through a CM. In other words, **it is not mandatory** for DFs to appoint CMs. (section 6(7)). Such a CM shall remain accountable to DPs and act on their behalf (section 6(8)). Further, CM shall provide grievance redressal to DP (where applicable) for any act or omission related to their obligations concerning PD or DP's rights under the DPDPA (section 13(1)).*

2. Who can apply to be a CM?

Section 6(9), read with rule 4 of DPDP Rules, provides that any Indian company may make an application for the position of CM to the DPBI, subject to the conditions that such a company:

- possesses the technical, operational, and financial capacity to fulfill their obligations
- has a net worth of at least INR 20 million
- ensures their financial condition and management are sound
- ensures their business volume, capital structure, and earnings prospects are adequate
- ensures their operations prioritize DP's interests
- ensures their charter documents include provisions relating to avoiding "conflict of interest"
- ensures their directors, key managerial personnel, and senior management have a reputation for fairness and integrity
- certifies their (a) interoperable platform aligns with data protection standards and (b) complies with technical & organizational measures

Breach in registration conditions

Where the CM breaches any condition of registration, DPB may impose a penalty of up to INR 500 million or about USD 6 million. (section 27(1)(d)).

©PSA 2025. All Rights Reserved

3. What are the obligations of CM?

Under rule 4, CM shall:

- enable a DP using their platform to give consent either directly to a DF onboarded on the platform or through another DF onboarded, who maintains such PD of the DP with their consent
- ensure the contents of PD are not readable while sharing
- maintain records of (a) consent given, denied, or withdrawn by DP; (b) notices; (c) data shared
- avoid conflicts of interest with DF, including DF's promoters, and key managerial personnel
- have measures to prevent "conflicts of interest" of their directors, key managerial personnel, or senior management with DF
- not sub-contract or assign obligations under DPDPA and act in a fiduciary capacity to the DP
- maintain a website/app as the primary means for DP to access the services
- transfer control of the company (by sale or merger) only with prior approval of the DPBI
- set up an audit and reporting mechanism covering safeguards, continued registration and DPDPA adherence
- publish details relating to promoters, directors, key managerial personnel, senior management, and shareholders with 2% shareholding on the website/app

Breach in obligations	*On a DP's complaint about a CM's obligation breach, DPBI may inquire and impose a penalty of up to INR 500 million or about USD 6 million. (section 27(1)(c)).*

©PSA 2025. All Rights Reserved

4. Concerns

Business activities: It is unclear if CMs can operate beyond offering consent management services. It is important they can undertake other business activities as well, otherwise, they will rely solely on DFs for income and this could make scaling challenging.

Processing of PD: CMs may process and store transactional data, including PD. It is unclear if this could make them DFs themselves.

Cancellation/suspension: Rule 4(5) of DPDP Rules provide that DPBI may suspend or cancel a CM's registration. This could suddenly disrupt the business with DFs.

Conflict of interest: Rule 4 read with clause 9 of Part B of the First Schedule provides CMs must avoid "conflict of interest" with the DFs. However, it does not clarify if it should be limited to DFs onboarded onto the platform.

Interoperable platform standards: Unlike RBI's account aggregator framework, for which specific guidelines on interoperability standards have been prescribed, no such standards have been prescribed for CMs. We believe some form of technical standards will be released in due course.

Way Forward

We foresee CMs playing a crucial role in the DPDP ecosystem. For this, it is essential that CMs do not solely depend on DFs for their business and operate in a clean environment where all transparency and interoperability standards are well defined.

©PSA 2025. All Rights Reserved

What if these GDPR cases on "Consent" happened in India?

What is consent as per GDPR?

Article 4(11) defines "Consent" as any freely given, specific, informed and unambiguous indication of DS's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of their PD.

Article 6(1)(a) r/w article 7(1) recognizes consent as a legal basis for processing PD, placing the burden on DCs to prove that consent was lawfully obtained. Further, article 7(3) grants DS the right to withdraw consent at any time.

Key Judgments

1. France

- **Background:** CRITEO, a French company specializing in targeted web advertising tracked its users' browsing behaviour through cookies to display personalized ads. On November 8, 2018, an association named "Privacy International" filed a complaint with French data protection authority, i.e., Commission Nationale de l'informatique et des Libertés (CNIL), alleging PD was not lawfully processed. A second complaint was submitted on December 4, 2018, by an association called "None of Your Business," asserting that users were not allowed to withdraw their consent/object to data processing.

- **Findings:** CNIL concluded that CRITEO failed to obtain valid user consent for processing under articles 6(1)(a) and 7(1) of GDPR. Further, consent withdrawal mechanism as required under article 7(3) was not effective. Consequently, CNIL on June 15, 2023, imposed a fine of EUR 40 million or about USD 45 million on CRITEO.

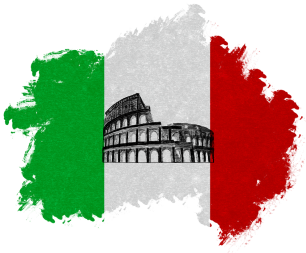
What will happen in India?

- **Relevant DPDPA Provision:** Section 4(1) r/w section 6(1) provides that processing of PD may be done based on consent that is free, informed, specific, unconditional and unambiguous. Section 6(4) further stipulates that where consent is the basis of processing, the DP may withdraw their consent at any time with the same ease as providing it. Additionally, section 8(7) requires data to be deleted upon withdrawal of consent unless retention is legally required.

- **Penalty:** Failure to obtain adequate consent/not providing withdrawal option/failure to delete PD may lead to a penalty of INR 500 million or about USD 6 million for each violation and collectively INR 1.5 billion or about USD 18 million.

©PSA 2025. All Rights Reserved

2. Italy



- **Background:** Multiple users filed complaints against Wind Tre SpA, a telecommunications provider offering mobile, fixed-line, broadband, and IT services, alleging they were sending promotional communications via phone calls, SMS, e-mails, faxes, etc., without obtaining explicit user consent. It was alleged these communications were provided even after withdrawal of consent /objection to the same. Additionally, Wind Tre operated two applications, namely, MyWind and My3 mobile. These applications required consenting to marketing, profiling, third-party communication, etc., upon each login and did not allow consent withdrawal for the next 24 hours.

- **Findings:** The Italian data protection authority, i.e., Garante per la protezione dei dati personali (**Garante**) concluded promotional communications were sent without valid user consent. Moreover, the MyWind and My3 apps hindered user rights by not allowing users to withdraw consent for 24 hours. These actions were deemed non-compliant with articles 6(1)(a), 7(3) and 21 (right to object). As a result, on July 9, 2020, a penalty of EUR 17 million or about USD 19 million was imposed.

What will happen in India?

- **Relevant DPDPA Provision:** Under section 6(1), provided consent must be limited to the purpose of data processing. Further, section 6(4) r/w section 8(7)(a) allows DP to withdraw their consent at any time, and requires DF to erase the PD, upon consent withdrawal, unless retention is legally required.

- **Penalty:** Failure to obtain explicit consent/failure to provide consent withdrawal options/non-erasure of PD may each attract a penalty of up to INR 500 million or about USD 6 million. Combined, these violations could lead to a penalty up to INR 1.5 billion or about USD 18 million.

3. Spain

Background: CaixaBank S.A., a financial institution, was accused of sharing a DS's data, including ID number, date of birth, income, salary, employment, etc., with a credit scoring company for profiling purposes even after their banking relationship terminated in 2014.

©PSA 2025. All Rights Reserved

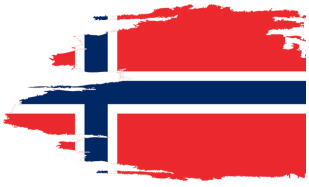
- **Findings:** The Spanish data protection authority, i.e., Agencia Española de Protección de Datos (AEPD) concluded that CaixaBank failed to obtain valid consent. The obtained consent was neither informed nor specific, as users could not give granular approval for each processing purpose. CaixaBank's privacy policy also lacked clarity on the specific data being used, the extent of profiling and the potential for receiving third-party marketing or pre-approved credit offers. Furthermore, the data was shared with the profiling entities without a valid contract. This was held in violation of articles 4(11), 6(1)(a), 7(1), and 28(3) (Processor contract), and a fine of EUR 3 million or about USD 3 million was imposed on October 10, 2021.

What will happen in India?

- **Relevant DPDPA Provision:** Under section 6(1), consent must be free, informed, specific, unconditional and unambiguous. Section 8(2) mandates where a DF engages a DPR to process data on its behalf, it must be under a valid contract. Additionally, section 8(7) requires that once the specified purpose is fulfilled, the DF must erase data and ensure its processors do the same, unless retention is required by law.

- **Penalty:** Failure to obtain valid consent/engaging a processor without a proper contract/failing to erase PD could attract a penalty of up to INR 500 million or about USD 6 million for each violation. The total penalty may extend to INR 1.5 billion or about USD 18 million.

4. Norway



Background: Grindr LLC, a US company, operated a GPS-based social networking app. On January 14, 2020, the Norwegian data protection authority, i.e., Datatilsynet, received 3 complaints from the Norwegian Consumer Council (NCC) alleging that Grindr unlawfully shared data with its advertising partners. Further, Grindr's consent mechanism required users to accept the privacy policy by clicking "Proceed," followed by "I accept the Privacy Policy." If users selected "Cancel," then access to the app was denied.

- **Findings:** Following the investigation, it was confirmed that Grindr shared PD, such as identity details, address, device information, age, gender, etc., with its advertising partners. Additionally, Grindr's consent mechanism relied on bundled consent for all processing activities, without allowing users to accept or decline specific purposes. This violated articles 4(11), 6(1)(a) and article 7(1). Datatilsynet also concluded that Grinder made withdrawal of consent difficult, requiring users to either change device-level settings or subscribe to a paid version of the app, violating article 7(3). As a result, on December 13, 2021, a total fine of EUR 6.5 million or about USD 7 million was imposed.

©PSA 2025. All Rights Reserved

What will happen in India?

- **Relevant DPDPA Provision:** Section 6(1) provides consent must be specific and unconditional. Further, section 6(4) stipulates where consent is the basis for processing, DP may withdraw consent at any time with the same ease as providing it.

- **Penalty:** Failure to obtain adequate consent/not providing a withdrawal option may lead to a penalty of INR 500 million or about USD 6 million for each violation and INR 1 billion or about USD 12 million collectively.

5. Poland

Background: ClickQuickNow, a Polish company operating in data processing, hosting, and related services, was alleged to be creating obstacles for DPs to withdraw consent or request erasure of data.

- **Findings:** Upon investigation of the complaints, Polish data protection authority, i.e., Urząd Ochrony Danych Osobowych (UODO), concluded that ClickQuickNow failed to implement adequate technical and organizational measures to allow individuals to easily withdraw consent (article 7(3)) and exercise their right to erasure (article 17). As a result of these violations, on February 10, 2021, a fine of EUR 47,000 or about USD 53,000 was imposed.

What will happen in India?

- **Relevant DPDPA Provision:** Section 6(4) provides where consent given by DP is the basis of processing, it may be withdrawn with the same ease as providing it. Further, section 8(4) requires DFs to implement appropriate technical and organizational measures to ensure effective observance of the provisions of DPDPA. Additionally, section 8(7) states that a DPO should erase PD upon DPs withdrawing their consent or upon fulfilment of purpose, unless retention is required as per law.

- **Penalty:** Failure to provide appropriate withdrawal mechanism/not implementing appropriate technical and organisational measures/non-erasure of data can lead to a penalty of INR 500 million or about USD 6 million for each violation and collectively, a total penalty of up to INR 1.5 billion or about USD 18 million.

©PSA 2025. All Rights Reserved

6. Luxembourg

Background: A collective complaint was filed with Luxembourg's data protection authority i.e. Commission Nationale pour la Protection des Données (CNPD) by French NGO "La Quadrature du Net" on behalf of 10,000 individuals in 2021, alleging that Amazon Europe Core S.A.R.L's targeted advertising practices were not based on valid, freely obtained consent.

- **Findings:** Although the full reasoning remains confidential due to professional secrecy obligations, CNPD concluded that Amazon Europe Core S.A.R.L's targeted advertising breached GDPR consent requirements under articles 6(1)(a) and 7(1) As a result, on March 18, 2025 a fine of EUR 746 million or about USD 845 million was imposed. Further, Amazon filed an appeal against the judgment, but the same was dismissed by the Administrative Court of Luxembourg.

What will happen in India?

- **Relevant DPDPA Provision:** As stated, section 6(1) requires processing to be based on consent that is free, informed, specific, unconditional, and unambiguous. DP may withdraw the provided consent as per section 6(4).

- **Penalty:** Failure to obtain adequate consent/not providing an appropriate withdrawal mechanism, can lead to a penalty of INR 500 million or about USD 6 million for each violation, and a total penalty of INR 1 billion or about USD 12 million.

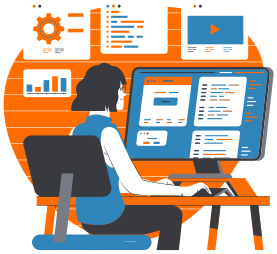
©PSA 2025. All Rights Reserved

Concept 3: Significant Data Fiduciary

1. Who is an SDF?

Under the DPDPA, a SDF is a sub-category of DFs.

Section 2(z) of the DPDPA defines SDF as “any DF or class of DFs as may be notified by the CG under section 10."



2. How is an SDF determined?

As per section 10(1) of the DPDPA, a DF or class of DFs may be notified as an SDF, based on the following factors:

- volume and sensitivity of PD processed
- risk to DP rights
- potential impact on India’s sovereignty and integrity
- risk to electoral democracy, State security, and public order

3. What are the compliance requirements of SDFs?

- **Appointing a DPO:** SDFs must designate an India-based DPO to represent them. Such a DPO should be accountable to the Board of Directors and serve as a grievance redressal point of contact under DPDPA. (section 10(2)(a))
- **Appointing an independent data auditor:** Such auditor must be engaged to conduct data audits and evaluate SDF's compliance with the DPDPA. (section 10(2)(b))
- **Conducting DPIA and periodic audits:** SDFs must conduct annual DPIA and audits to ensure compliance with the DPDPA and DPDP Rules. A summary of significant observations must also be submitted to DPBI. (section 10(2)(c)(i) & (ii) and rule 12(1) & (2))
- **Algorithmic software:** SDF must exercise “due diligence” to ensure “algorithmic software” deployed by them does not pose risks to DPs’ rights. (rule 12(3))
- **Data transfer restrictions:** SDF must ensure that PD, as specified by the CG on the basis of recommendations of a committee and “the traffic data pertaining to its flow” is not transferred outside India. (rule 12(4))

©PSA 2025. All Rights Reserved

4. What if SDFs fail to comply?

Under section 33(1) read with the Schedule to DPDPA, if the DPBI concludes, after an inquiry, that SDFs have failed to observe their obligations under section 10(2), it may impose a penalty up to INR 1.5 billion or about USD 18 million.

5. Issues

- **Lack of defined thresholds:** The notification of a DF as SDF depends on factors like "volume and sensitivity of PD processed," but no clear thresholds have been defined. Additionally, rule 22(1) allows CG to procure information from DF to determine if they should be notified as SDF. This means any DF or class of DF could be notified as SDF at any time.
- **Indirect form of data localization:** Rule 12(4) requires SDFs to take measures to keep certain PD (as specified by a committee formed by the CG) and traffic data related to its flow within India. This could create operational and technical challenges for SDFs. Further, it is not clear why this restriction on localization is applied only to SDFs and not DFs. Going forward, it is likely if any DF processes data which the CG requires to be localized pursuant to rule 12(4), such DF may be notified as SDF.
- **Due diligence for algorithmic software:** DPDP Rules require SDFs to conduct due diligence for any "algorithmic software" deployed by them. However, given that nearly all software today deploys some form of algorithm, this could create operational inefficiencies and impact deployment timelines. Further, they may have to maintain an audit trail to demonstrate compliance.
- **Cost of compliance:** If mid/small DFs are notified as SDFs, their cost of compliance will significantly go up. While large corporations may manage these expenses, smaller DFs may face significant financial strain in meeting the regulatory obligations.
- **DPIA and audits:** Requiring SDFs to conduct a DPIA annually, even without them deploying any new software or making changes to processing activities, may be unnecessary and burdensome. Ideally, DPIAs should be conducted when there is a change in how data is processed.

Way Forward

Given no substantial penalties for non-compliance, DFs processing a high volume of/sensitive PD should proactively conduct gap assessments to ensure compliance with regulatory requirements, especially since CG has the power to notify them as SDF.

©PSA 2025. All Rights Reserved

Concept 4: Navigating the Fiduciary-Processor Relationship

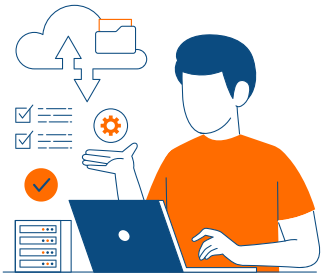
1. What is processing?

Processing is a wholly or partly automated operation or set of operations performed on digital PD. It includes "operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction" (section 2(x)).

Who is a DF & a DPR?

DF is "any person who alone or in conjunction with other persons determines the purpose and means of processing of PD" (section 2(i)). Further, a DPR means "any person who processes PD on behalf of a DF" (Section 2(k)). Data processors are to be engaged only under valid contracts (Section 8(2)).

2. What are the obligations of a DF?



- Comply with DPDPA and Draft Rules (section 8(1))
- Engage a DPR (if required) to process PD on its behalf under a valid contract (section 8(2))
- Ensure completeness, accuracy, and consistency of PD used for making decisions/when disclosed to another data fiduciary (section 8(3))
- Implement appropriate technical and organisational measures (section 8(4))
- Protect PD in its or DPR's possession by taking reasonable security safeguards such as encryption, masking, etc. (section 8(5) r/w rule 6(1)(a))
- Give DPBI and affected DPs information of a PD breach (section 8(6))
- Unless required by law, erase or cause its processors to erase personal data, upon withdrawal of consent or fulfilment of specified purpose (section 8(7))
- Publish contact information of DPO or authorised personnel on its website or app (section 8(9) r/w rule 9)
- Establish an effective grievance redressal mechanism for DPs (section 8(10))

Presumption regarding DFs

DFs are solely liable for any breach or non-compliance under DPDPA. This appears to have been done on the premise, that DFs will be in a position to negotiate their agreements with DPRs. This may not always be the case, as some processors (like cloud service providers) are onboarded by creating an account without any contract negotiation.

©PSA 2025. All Rights Reserved

3. What questions should DF ask DPR?

- Do you process PD for any secondary purpose?
- How will you cease processing if directed? What measures are in place to ensure this?
- How do you comply with data retention and deletion requirements?
- Do you engage sub-processors? If yes, are they engaged with prior approval and under contracts with similar obligations?
- Do you have a documented Information Security Policy? How is it implemented across teams?
- Do you transfer data outside India?
- How do you ensure that only authorized personnel access PD? Do you use unique user accounts, multiple-factor authentication, etc.?
- Do you encrypt PD during storage and transit? If yes, do you use any industry-standard protocols (e.g., HTTPS/TLS RFC 2818/8446)?
- Have you implemented security standards such as SOC 2, NIST, or ISO 27001?
- Do you have a documented incident response policy outlining actions to be taken in case of a PD breach? Do you have any insurance coverage for the same?
- Do you conduct any security awareness training for your employees, consultants, or partners on topics such as data handling or incident management?
- Do you use any third-party tools that allow more effective audit diligence mechanism?

What should a DF do?

Given that a DF is solely liable under DPDPA, it is important that its legal, infosec and IT teams work together while formalising their engagement with a DPR. Additionally, a DF should establish an internal risk metrics outlining the minimum standards (e.g., data security practices, compliance history, financial stability, breach response capabilities etc.) which a DPR should meet.

4. What are some essential clauses of a DPA?

- **Scope of processing:** Defines categories of PD being processed, purpose of processing, processing activities undertaken, and duration of processing.
- **Purpose limitation:** PD shall not be processed for any secondary purposes, unless otherwise agreed.
- **Obligations of DP:** States obligations of DPR, including processing PD in compliance with data protection laws.
- **Support:** Requires DPR to provide all necessary resources, including but not limited to logs and other documents, in a timely and effective manner as and when required. Further, they must cooperate with DF in fulfilling its legal obligations.

©PSA 2025. All Rights Reserved

- **Data retention and deletion:** Requires DPR to delete PD upon fulfilment of specified purpose or as and when instructed by the DF, unless retention is required by law.
- **Data security:** DPR should implement appropriate technical and organizational measures and undertake reasonable security safeguards in protection of PD.
- **Data updation:** DPR to update, correct, or complete PD as and when communicated by DF.
- **Data breach:** All PD breach on the end of DPR to be promptly reported to DF. Further, DPR must provide assistance in case of breach.
- **Audit rights:** DF will have audit rights to ensure DPR's compliance.
- **Confidentiality:** All obtained PD to be treated as confidential and to be disclosed only on a need-to-know basis.
- **Indemnity:** DPR must indemnify DF against any loss/damage arising from (a) breach of its obligations, (b) failure to implement reasonable security safeguards, (c) PD breaches caused by its acts or omissions, (d) its failure to comply with data retention or deletion requirements.
- **Use of sub-processors:** Restricts engagement of sub-processors without prior written approval of DF. Sub-processors to be engaged only under valid contracts with similar obligations.
- **Cross-border data transfer:** Cross-border transfers to be done with prior written consent of DF and in compliance with data protection laws.

Assessment of DPRs

DPDPA imposes penalties on DF ranging from INR 500 million or about USD 6 million to INR 2.5 billion or about USD 29 million. These could be imposed even if the breach is by DPR. Therefore, it is critical a DF should evaluate the effectiveness of the "indemnity clause" in its DPA as well as conduct a high-level diligence and meet the senior leadership teams of the processor.

Way Forward

DFs should review existing contracts with DPRs to identify potential risks, even if such contracts cannot be negotiated. If DF has no ability to negotiate its contract with DPR, it should evaluate whether the DPs should be communicated of the uneven bargaining power. Subject to how the DPBI may enforce the DPDPA, such disclosure to DP may serve as a mitigating factor for levying a penalty on DF.

©PSA 2025. All Rights Reserved

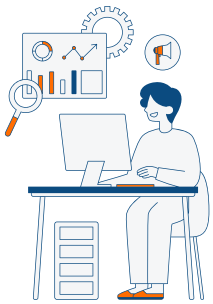
Concept 5: Age Gating

1. What does the law say?

Under section 9 of DPDPA, read with rule 10 of DPDP Rules, verifiable consent is required for processing the PD of (i) a child (<18 years of age) and (ii) a person with disability (PWD) having a lawful guardian.

Why?

The DPDPA recognizes the need to safeguard children's data and ensure accountability. The provisions also attempt to capitalise on prospective virtual token systems andd identification tools already in place to streamline the verification process.



2. What must DFs do?

DFs must adopt technical and organisational measures to obtain verifiable consent of a parent/guardian before processing any child or PWD data. Consent must comply with the general consent provisions under section 6 and it has two additional aspects:

Identity of Parents	Proof of Guardianship
Ensuring the identity and age (>18 years) of the parent/guardian. This can be done by verifying • age and identity details already available, or • voluntarily provided government-issued identity or virtual token (like DigiLocker)	For PWD, DFs must verify the guardian is appointed by court, designated authority, or local level committee Arguably, DFs are not required to verify if the "parent" giving consent is the actual parent of the child

Is Consent Necessary?

Yes, a child's PD cannot be processed without obtaining consent in the manner mentioned above, unless exempted.

©PSA 2025. All Rights Reserved

3. Exemptions

Certain entities are exempt under Part A & B of Schedule IV of the DPDP Rules from obtaining consent for certain data. Exemptions also apply to restrictions against tracking and behavioural monitoring of children.

Part A: Health & Education

Healthcare, mental health establishments & allied health establishments are allowed to process data to the extent necessary for protecting health of a child.

Creche, childcare, and educational institutions are allowed to process tracking and behavioural monitoring data to the extent necessary for safety of a child.

Part B: Law & Order

Processing necessary for providing any legal benefit (subsidy, service, etc) and for discharging any legal duty is exempt.

Processing for creating a user account, ensuring harmful information is not accessible to the child, and for confirming that the DP is not a child are also exempt.

Penalty *While there is no specific penalty, section 33(1) read with Schedule I of the DPDPA provides a penalty of up to INR 2 billion for failure to meet obligations under the Act or allied Rules.*

4. Concerns

Blank Spots

- No clarity on what a DF should do if a child falsely claims to be an adult
- No mode to verify if the person giving consent on behalf of a child is the parent
- No procedural clarity if the child or PWD is without a parent or legal guardian

Issues

- Exemptions for healthcare and education are broad and vaguely worded
- Healthcare is arguably exempt from restrictions on targeting advertisements to children

Way Forward *Given the strict penalties and clear restrictions, DFs should employ strict measures to ensure no child or PWD data is processed without parental consent.*

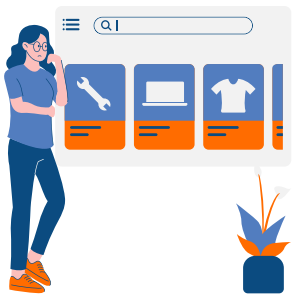
©PSA 2025. All Rights Reserved

Concept 6: Data Retention

1. What does the law say?

Section 8(7) of DPDPA states that "A DF shall, unless retention is necessary for compliance with any law for the time being in force (a) erase PD, upon the DP withdrawing her consent or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier; and (b) cause its DPR to erase any PD that was made available by the DF for processing to such DPR."

Any failure to meet these requirements can lead to a penalty up to INR 500 million or about USD 6 million.



Fulfilment of Specified Purpose

Rule 8 of DPDP Rules provides 3 types of DFs namely, (a) e-commerce entities with at least 20 million registered users in India, (b) social media intermediaries with at least 20 million registered users in India and (c) online gaming intermediaries with at least 5 million users in India, must erase PD of DPs within 3 years from when DPs last approached them for the fulfilment of specified purpose/exercised their rights or from commencement of the rules, whichever is earlier. Further, DFs must provide 48 hours' prior notice to the DPs before deleting their PD.

2. When can data be retained as per applicable laws?

Section 38(1) provides the provisions are in addition to, and not in derogation of, any other law. Read together with section 8(7), this implies that DFs may retain PD where such retention is required to comply with any other laws or sector-specific regulations. However, the specific retention requirements may vary across sectors, depending on the nature of the data collected.

Requirements under Financial Laws

Act/Regulation/ Rule	Section/ Rule/Para	Retention Period	Data to be retained	Application
Income Tax Act, 1961 r/w Income Tax Rules, 1962	Rule 6(F)	6 years	Accounts	Every assessee

©PSA 2025. All Rights Reserved

Act/Regulation/ Rule	Section/ Rule/Para	Retention Period	Data to be retained	Applicability
Idem	Rule 10(D)	8 years	Book of accounts	Person executed a transaction, international or domestic
Central Goods and Services Act, 2017	Section 35	6 years	Records	Any person filing tax returns
Companies Act, 2013	Section 128	8 years	Accounts	Company
Prevention of Money Laundering Act, 2002	Section 12	5 years	Record of transactions and other documents	Reporting entity
Master Circular on memorandum of instructions governing money changing activities, 2014	Para 4.13(i)	5 years	Record of transactions	Authorized persons
Banking Regulation Act, 1949 r/w Banking Companies (Period of Preservation of Records) Rules, 1985	Rule 2	5 years	Accounts and other documents like cheque book registers, delivery order registers, etc	Banking Companies
Idem	Rule 3	8 years	Accounts and other documents such as all personal ledgers, overdue loan register, etc	*Idem*

©PSA 2025. All Rights Reserved

Act/Regulation/ Rule	Section/ Rule/Para	Retention Period	Data to be retained	Applicability
Securities and Exchange Board of India Act, 2002 r/w Securities Contracts (Regulation) Rules, 1957	Rule 15(1)	5 years	Transaction records	Regulated entities of SEBI
Master Circular For Mutual Funds	Para 8.5.10	8 years	Records of mutual funds	Member of recognized stock exchange
Master Circular on KYC Guidelines, Anti Money Laundering Standards of PMLA, 2002, Obligations of NBFCs	Para 4	At least 10 years	Necessary records of transactions and other documents	Non-banking financial company
Master Circular on KYC Guidelines, Anti Money Laundering Standards of PMLA, 2002, Obligations of Banks	Para 2.24 (c)	At least 5 years	*Idem*	Banks
International Financial Services Centres Authority (Payment Services) Regulations, 2024	Regulation 24(4)	10 years	Log of transactions	Payment of service provider operating in IFSC
Insurance Act, 1938 r/w IRDAI (Minimum Information Required For Investigation And Inspection) Regulations, 2020	Section 14(1)(a) & (b) r/w Regulation 24	10 years	Documents of policy records and claims	Insurer
Foreign Exchange Management Act, 1999 r/w Master Circular on Miscellaneous Remittances from India, 2015	Para 2.5	1 year	Documents relating to sale of foreign exchange	Authorized persons

©PSA 2025. All Rights Reserved

Requirements under Technology Laws

Act/Regulation/ Rule	Section/ Rule/Para	Retention Period	Data to be retained	Applicability
IT Act, 2000 r/w Information Technology (Intermediary Guidelines and Digital Media Ethics) Rules, 2021	Rule 3(1)(g) and (h)	180 days	Information regarding user registration and information which is removed or disabled	Intermediary
Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 r/w Aadhar Authentication Regulation, 2016	Rules 26 and 27	6 months and archived for 5 years	Authentication records	Unique Identification Authority of India
Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 r/w Aadhaar Authentication and Offline Verifications Regulation, 2021	Rule 18(1) to (3) and 20 (1) to (3)	2 years and archived for 5 years	Logs of authentication transactions	Requesting entities and authentication service agencies
Telecommunications Act, 2023 r/w Department of Telecommunication circular dated October 21, 2021 (Amendment of Unified License Agreement)	Para 1	2 years	Commercial records, call details, exchange detail record, IP details record	Unified licensee
CERT-In Directions, 2022	Para (iv)	180 days	Logs of information communication technology systems	Service providers, intermediaries, data centers, and a body corporate

©PSA 2025. All Rights Reserved

Act/Regulation/ Rule	Section/ Rule/Para	Retention Period	Data to be retained	Applicability
Idem	Para (vi)	5 years	KYC information and records of financial transactions	Virtual asset service providers, virtual asset exchange providers, and custodian wallet providers

Requirements under Health Laws

Act/Regulation/ Rule	Section/ Rule/Para	Retention Period	Data to be retained	Applicability
Medical Council of India Act, 1956 r/w Code of Medical Ethics Regulations, 2002	Regulation 1.3.1	3 years	Medical records of indoor patients	Every physician
Electronic Health Record Standards, 2016	Para Electronic Medical Records Preservation, Pg 22	Lifetime of Patient	Electronic medical records	Medical doctor or healthcare institution
Clinical Establishments (Registration and Regulation) Act, 2010, r/w Clinical Establishment (CG) Rules, 2012	Rule 9(iv)	Varies from state to state	Electronic medical/health records	Every clinical establishment

©PSA 2025. All Rights Reserved

PSA LEGAL COUNSELLORS

Requirements under Other Laws

Act/Regulation/ Rule	Section/ Rule/Para	Retention Period	Data to be retained	Applicability
Public Records Act, 1993 r/w Record Retention Schedule, 2012	Physical Records Category C, Pg vii	3,5,10 years depending upon category	Public records	Government bodies and public authorities
Right to Information Act, 2005	Section 8(3)	20 years	Public records as held by the department	*Idem*
Retention Schedule for records relating to substantive functions of the Ministry of Civil Aviation	Para (xvi) and (xvii)	3,5,10, 25 years depending upon category	Public records	The various departments of the Ministry of Civil Aviation
Minimum Wages Act, 1948 r/w Minimum Wages Central Rules, 1950	Rule 26A	3 years	Employee details and others	Every employer
Payment of Wages Act, 1936	Section 13A	3 years	Wage records	Every employer

Way Forward

With the current structure of the DPDP Rules, it appears DFs, other than those covered under rule 8, may determine their data retention period. This should give sufficient flexibility to DFs provided the retention period determined by them is not excessive or unreasonable. We recommend DFs formulate a data retention policy where they can retain data for at least a period of 3 years to comply with the general requirement under the Limitation Act, 1963. Of course, this has to be subject to any other sectoral laws as well.

Lastly, the data retention obligations should also be passed on to DPRs through a DPA executed with DFs.

©PSA 2025. All Rights Reserved

Under Chapter 3 of GDPR, DCs are obligated to uphold DS rights, ensuring all required communications and actions are fulfilled without undue delay, within 1 month of receipt of request (extendable up to 3 months). Further, where a request cannot be fulfilled, DS must be informed of reasons within 1 month.

All communications must be provided in a concise, transparent, intelligible, and easily accessible format, using clear and plain language. All requests are to be fulfilled free of costs, unless the requests are repetitive, in which case a reasonable fee may be charged/request may be refused.

DPDPA, r/w DPDP Rules requires DFs to provide certain rights to DPs. Example, right to access, grievance redressal, etc. Further, the means to make a request or grievance redressal timeline should be listed on the website or app of DFs/CMs (rule 13). No right to charge any fee has been given to the DFs.

Consent & Withdrawal

GDPR

Where PD is collected directly from DS, DCs should provide its identity and its/DPO's contact details, purpose of collection, legal basis, legitimate interests, data recipients, cross-border transfers, retention period, DS rights (withdrawal, erasure, lodge complaint etc.) consequences of not providing data, and information relating to automated decision-making. For indirect collection, DCs shall also provide source and categories of PD collected (articles 13 & 14).

Further, DS may withdraw their consent at any time (article 7(3)).

DPDPA

A request for consent to DPs must be accompanied by a notice outlining the PD to be collected, the intended purpose, manner in which DP can withdraw consent/access grievance redressal, and the process for making a complaint to DPBI (section 5).

Further, the DP may withdraw its consent at any time (section 6(4)).

©PSA 2025. All Rights Reserved

Comparison

Under the GDPR, the information required to be provided at the time of data collection is detailed and extensive. In contrast, the DPDPA mandates only limited disclosures in its consent notice. If a GDPR compliant company processes PD on the basis of consent, it would also end up complying with the consent requirements under DPDPA. Of course, this is with a caveat that GDPR allows processing of PD on other grounds as well.

Access Information

GDPR

DS can ask the DC to confirm if its PD is being processed and if yes, then it can ask the purpose of collection, categories of PD collected, details of recipients (including cross-border), retention period, details about other rights, collection source (if not collected from DS), and existence of any automated decision-making (article 15).

DPDPA

DPs may, subject to certain restrictions, access a summary of their PD processed, processing activities undertaken, identities of DFs and DPRs with whom data has been shared, etc (section 11).

Comparison

Right to access is far more detailed in GDPR. A data fiduciary that complies with GDPR is highly likely to have complied with data principal rights under DPDPA.

Correction & Erasure

GDPR

DS may request rectification or completion of inaccurate/incomplete PD and erasure where purpose is fulfilled, processing is unlawful,

DPDPA

DPs may request correction, completion, or updation of inaccurate or incomplete PD. Further, they may also request

©PSA 2025. All Rights Reserved

unlawful, no legal or legitimate grounds exist, erasure is required by law, or PD was collected for society services. However, DCs may retain PD if required for the exercise of their right of freedom of expression, legal obligations, public interest in public health, legal claims, or archiving purposes in public interest, scientific or historical research/statistical purposes (articles 16 & 17).

erasure of PD. DF may, however, continue to process PD to fulfill specified purpose/ or compliance with law (section 12).

Comparison

Right to erasure under GDPR is narrower, as it lists grounds on which erasure requests can be made. It also outlines exceptions where erasure can be refused, such as for freedom of expression, legal obligations, or public interest. In contrast, DPDPA allows DPs to make erasure requests for any reason, with continued processing only for the fulfillment of purpose or compliance with law. DFs compliant with GDPR will have to relook at this right to comply with DPDPA.

Grievance Redressal

GDPR

The DS may complain to a supervisory authority in the Member State of their residence, workplace, or where the alleged infringement occurred. DSs may also pursue other administrative or judicial remedies (article 77).

DPDPA

DPs have to first approach the DF or CM (if applicable) regarding any grievance they may have. This remedy must be exhausted before approaching the DPBI (section 13).

Comparison

GDPR does not explicitly require DCs to provide a grievance redressal mechanism. Instead, the DS can file a complaint directly with a supervisory authority in case of disputes. In contrast, DPDPA mandates DFs to redress concerns before DP can approach the DPBI. DFs compliant with GDR have to ensure that they have the means and bandwidth to address the grievances raised by DPs.

©PSA 2025. All Rights Reserved

PSA LEGAL COUNSELLORS

Other Rights

GDPR

- **Restriction of Processing:** DS can request restriction of processing if (a) PD is inaccurate, (b) PD is unlawfully processed, (c) PD is no longer needed to be processed by the DC but DS requires the DC to process it for establishment, exercise or defense of legal claims, or (d) it has exercised its right to object (article 18).
- **Notification Obligation:** DC must inform all data recipients of all rectification, erasure, or processing restriction requests by the DS (article 19).
- **Right to Data Portability:** DS can request DCs to share their PD in a structured, machine-readable format. DS can then transfer this data to any other DC provided the original processing was based on consent or contract and carried out using automated means (article 20).
- **Right to Object:** DS may object to any processing, including profiling, and DC must show a legitimate ground to continue such processing (article 21(1)).
- **Automated Decision Making:** DS may not be subject to decisions made solely by automated processing, including profiling, which produces legal effects except where decisions are necessary for a contract, authorized by law, or based on explicit DS consent (article 22).

DPDPA

- **Right to Nominate:** DPs may nominate any other individual to exercise rights on their behalf, in case of their death or incapacity (section 14).

Conclusion

There is a myth that GDPR compliance is sufficient to comply with DPDPA. However, the devil is always in the details. While GDPR grants more rights to DS, there are certain conditions attached to it. For instance, the right to erasure is an untethered right, but it can only be exercised if certain conditions mentioned in article 17(1) are met. However, under DPDPA, it is an absolute right, with the only exception being that the DF is required to process PD to fulfill a specified purpose or to comply with law. Therefore, if you are GDPR compliant, you still have to take steps to ensure compliance with DPDPA. Non-compliance with rights given to DPs can attract penalties up to INR 500 million or about USD 6 million per breach.

©PSA 2025. All Rights Reserved

What are data subject rights?

Under Chapter 3 of the General Data Protection Regulation (GDPR), DCs are obligated to provide DS with certain rights, such as the right to be informed (article 13 and 14), right to access (article 15), right to rectification (article 16), right to erasure (article 17), right to restrict processing (article 18), right to object (article 21) etc., collectively called as DS rights.

What are DP rights?

DPDPA also requires DFs to provide certain rights to DPs, including right to access (section 11), right to correction and erasure (section 12), right to grievance redressal (section 13) and right to nominate (section 14), collectively know as DP rights.

Key Judgments

1. Austria - Right to Erasure

- **Background:** An entity based in Austria that organized football leagues published information on its website about players who had participated in the league matches. This information included PD such as name, photograph, nationality etc. On September 23, 2020, Mr. Roberto, a football player who had previously taken part in the matches, sent an e-mail requesting deletion of his PD from the website. However, the entity refused, citing the need to retain PD for statistical purposes. As a result, Mr. Roberto filed a complaint with Österreichische Datenschutzbehörde, i.e. the Austrian Data Protection Authority (**Austrian DPA**).

- **Findings:** Austrian DPA noted article 17(1) of the GDPR, provides DS with a right to request erasure of their PD without undue delay. The controllers are obligated to comply if any of the conditions under article 17(1)(a) to (f) are met. In the present case, Mr. Roberto had raised a request for deletion of his PD with the intention of never participating again. Therefore, pursuant to article 17(1)(a), PD was "no longer necessary in relation to the purposes for which they were collected or otherwise processed". Consequently, on **January 4, 2024**, a fine of EUR 11,000 or about USD 12,500 for non-compliance, along with EUR 1,100 or about USD 1,250 for costs, was imposed.

©PSA 2025. All Rights Reserved

What will happen in India?

- **Relevant DPDPA Provision:** Under section 12(3) of DPDPA, a DF shall, upon receiving a request for erasure, erase PD, unless retention is required for fulfilment of specified purpose or for compliance with applicable law.

- **Penalty:** Applying the facts of the above case, failure to comply with data erasure requests can lead to a penalty up to INR 500 million or about USD 6 million for each violation.

2. Spain - Right to Access

- **Background:** Michael Page International, an employment agency, based out of United Kingdom, with subsidiaries all around Europe, operated under different brands including "Michael Page". The complainant, a Dutch citizen, had created an account on the website of Michael Page and had uploaded her CV. On September 28, 2018, she sent a request to access her PD. However, the company withheld her request, asking for an ID to verify her identity. Thereby, the complainant filed a complaint before the Dutch Data Protection Authority stating that asking for an ID to fulfil data access request was excessive. Later, the case was transferred to Agencia Española de Protección de Datos i.e. the Spanish Data Protection Authority (**Spanish DPA**)

- **Findings:** Spanish DPA stipulated that the identity verification process must take place only when there is a reasonable doubt regarding the identity of the person who made the request. In the present case, the controller could not prove the existence of a reasonable doubt. Instead, identity verification was a standard procedure. Therefore, the controller was held in violation of articles 12(2) and 12(3). Consequently, via a judgement published on **February 25, 2022**, a fine of EUR 300,000 or about USD 334,000 was imposed.

What will happen in India?

- **Relevant DPDPA Provision:** Under section 11 of DPDPA, a DP may request access to their PD from DF. Upon receiving such a request, DF is required to provide a summary of the PD being processed and the processing activities undertaken. Further, subject to certain conditions, DF shall also provide (i) identities of DFs and DPRs with whom data has been shared, along with details of data shared; and (ii) any other relevant information.

- **Penalty:** Applying the facts of the above case, failure to fulfil data access requests can lead to a penalty up to INR 500 million or about USD 6 million for each violation.

©PSA 2025. All Rights Reserved

3. Czech Republic - Right to be Informed

- **Background:** The DC, a company based in Czech Republic, was alleged to have transferred PD of users of its antivirus software to its sister company. This transfer occurred without obtaining user consent. Further, the controller misinformed the users about the same, claiming that the transferred data was anonymized and used solely for statistical trend analytics. Following this, an anonymous complaint was filed with the Úřad pro ochranu osobních údajů i.e, the Czech Data Protection Authority (**Czech DPA**), along with multiple media reports.

- **Findings:** After an investigation, the Czech DPA concluded that the controller had unlawfully transferred PD of users of its antivirus software and browser extensions to its sister company, which affected around 100 million users. The data included pseudonymized browsing histories linked to unique identifiers. Further, the Czech DPA determined that even partial browsing history can constitute PD due to the risk of re-identification. Consequently, the acts of the controller was held in violation of articles 6(a) and 13 (1), and a fine of EUR 13.9 million or about approx. USD 15.8 million was imposed on **April 10, 2024**.

What will happen in India?

- **Relevant DPDPA Provision:** Section 5(1)(i) and section 5(2)(i) of DPDPA, requires DFs to provide DPs with information regarding the "PD and the purpose for which the same is processed". Further, section 6(1) requires that the obtained consent be limited to the purpose for which it was obtained.

- **Penalty:** Applying the facts of the above case, using PD beyond the specified purpose may attract a penalty of up to INR 500 million or about USD 6 million per violation.

Under GDPR, DS has a right to be informed when (i) information is collected directly from them (article 13) or (ii) information is obtained from other sources (article 14). While the DPDPA does not require a DF (say DF 2) to specially disclose if it received PD from another fiduciary (say DF 1 who had originally obtained consent to share data with fiduciary 2), we recommend it should be disclosed whenever a DP exercises her right to access.

©PSA 2025. All Rights Reserved

4. Italy - Right to Rectification and Erasure

- **Background:** DC is a medical center based in Italy. DS requested access to his COVID-19 PCR test results, however, he discovered that they had been sent to a wrong email address. Further, after finally receiving the results, he noticed that there were certain inaccuracies in the report such as date of birth and tax ID. Subsequently, he requested DC to rectify (article 16) and erase (article 17) his PD and restrict processing (article 18). However, he received no response. Thereby, he filed a complaint before the Garante per la protezione dei dati personali, i.e., the Italian Data Protection Authority (**Italian DPA**).

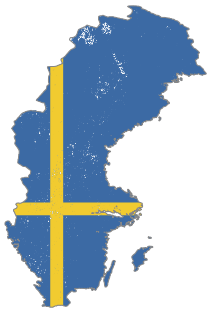
- **Findings:** Italian DPA concluded that it was the responsibility of DC to ensure that the data was accurate and where necessary, kept up to date, which it failed to fulfil. Further, the reports were sent to an unauthorized third party, which was a violation of the controller's security obligation. Additionally, the controller failed to reply to the request within one-month. Consequently, a fine of EUR 10,000 or about USD 11,500 was imposed for violation of articles 12, 15, 16, 17, and 18 on **August 31, 2023**.

What will happen in India?

- **Relevant DPDPA Provision:** Under section 12 of DPDPA, a DP has a right to request correction/completion/updation of their PD. Upon receiving such a request, DF should correct/complete/update the inaccurate/misleading/incomplete PD. Furthermore, upon receiving a request for erasure, a DF should erase PD, unless retention is required for fulfilment of specified purpose or under applicable law.

- **Penalty:** Applying the facts of the above case, failure to comply with data correction and erasure requests may lead to a penalty up to INR 500 million or about USD 6 million for each violation and a combined penalty up to INR 1 billion or about USD 12 million.

5. Sweden - Right to Access



- **Background:** Spotify AB, a digital music, podcast, and video streaming service found in 2006 and headquartered in Sweden, became the subject of an ex officio investigation by the Integritetsskyddsmyndigheten i.e. Swedish Data Protection Authority (**Swedish DPA**) in January 2019. This followed a complaint from "noyb", along with additional complaints from Netherlands and Denmark, alleging that Spotify provided incomplete and unintelligible information in response to data access requests. The investigation aimed to assess whether Spotify AB's general practices for handling access requests complied with GDPR.

©PSA 2025. All Rights Reserved

- **Findings:** The Swedish DPA concluded that while Spotify's method of providing access to PD met the general requirements of article 15, the information was not presented in a way that fulfilled the purpose of right to access. Specifically, it did not enable DS to understand how their data was being processed or assess the lawful basis. Additionally, the provided information was not concise, clear, or easily accessible, violating articles 12(1), 15(1)(a) to (d), (g) and 15(2). As a result, on **June 12, 2023,** a fine of EUR 5 million or about USD 5.7 million was imposed.

What will happen in India?

- **Relevant DPDPA Provision:** Under section 11 of DPDPA, a DP may request access to their PD from DF Upon receiving such a request, DF is required to provide a summary of the PD being processed and the processing activities undertaken. Further, subject to certain conditions, the fiduciary shall also provide (i) identities of DFs and DPRs with whom data has been shared, along with details of data shared; and (ii) any other relevant information.

- **Penalty:** Applying the facts of the above case, failure to fulfil data access requests can lead to a penalty up to INR 500 million or about USD 6 million for each violation.

©PSA 2025. All Rights Reserved

Concept 8: Data Breach

The DPDPA and DPDP Rules provide for various compliance requirements in case of PD breach.

1. What does the law say?

Under section 8(6), DFs must intimate the DPBI & each affected DP of a "PD breach."

Rule 7 further clarifies that notifications

- *Be as per "best knowledge"*
- *Be sent to user accounts OR any other mode of communication*

2. What is a PD Breach?

Under section 2(u), PD breach is any (i) unauthorized processing of PD, or (ii) accidental disclosure, acquisition, sharing, use, alteration, destruction, or loss of access to PD compromising its confidentiality, integrity, or availability.

This definition is extremely wide and will pose challenges in implementation.

3. How to notify DPs of the breach?

Under rule 7, the DF must notify each affected DP "without delay," with details including:

- description of breach (nature, extent, time, and location)
- consequences relevant to such DP
- mitigation measures undertaken
- safety measures recommended for the DP to adopt
- contact information of authorized personnel

©PSA 2025. All Rights Reserved

4. How to notify the DPBI?

Under rule 7, DFs must report the breach, including its nature, extent, time, location, and likely impact to DPBI "without delay."

DFs must also send an updated report with (a) detailed information on the breach, (b) summary of the event, circumstances, & cause, (c) risk mitigation measures taken, (d) responsible parties, (e) steps to prevent future breaches, and (f) status of notifications to affected DPs to the DPBI "within 72 hours" (or longer if permitted).

Sub-clause (f) implies that DPs must be notified within 72 hours, i.e., before providing a detailed report of the breach to the DPBI.

5. What if DFs fail to inform?

Under section 33(1) read with the Schedule of DPDPA, if a DF fails to inform affected DPs or the DPBI about a PD breach, penalties up to INR 2 billion or about USD 23 million will be imposed.

6. Concerns

- **Cost of Compliance:** Overall, compliance requirements under DPDPA and DPDP Rules are quite extensive. While larger organizations have resources for compliance, start-ups and other small companies could face financial difficulties.

- **Sectoral reporting requirements:** Depending on nature of breach, DFs may need to notify CERT-IN within 6 hours & other sectoral regulators (SEBI, IRDA, RBI, etc.) as prescribed. This will be onerous, given the different reporting standards & timelines.

- **72-hour reporting timeline:** Considering the details required to be disclosed to the DP & DPBI, complying in such a short timeframe will present substantial challenges.

©PSA 2025. All Rights Reserved

- **Inclusion of vague expressions:** Certain terms such as "accidental disclosures" are extremely vague. It is unclear if DFs will need to notify in cases like where an unauthorized employee manages to walk past the laptop of a colleague that has certain PD on display.

- **Wide Reporting Requirements:** DPDPA requires reporting of all breaches, regardless of harm to the DPs. This may overburden DFs & the DPBI. DPs may also feel overwhelmed by frequent breach notices which may, in the long run, erode their trust and discourage them from giving their consent. This could impact significant data-driven businesses.

- **Bandwidth of the DPBI:** Given the number of PD breaches reported, the DPBI might not have sufficient manpower or budget to effectively assess all reports. Consequently, higher expenses could lead to greater penalties imposed by DPBI.

Way Forward

DFs must (i) create dedicated teams to manage breach reporting requirements, (ii) invest in advanced security systems and compliance tools, (iii) adopt a proactive approach by enhancing vigilance and responsiveness to minimize impact, (iv) invest in data breach/cybersecurity insurance, (v) engage Standard Operating Procedures (SOPs) in reporting, and (vi) ensure proper coordination between IT and legal teams.

©PSA 2025. All Rights Reserved

What if these GDPR cases on "Personal Data Breach" happened in India?

What is a Personal Data Breach as per GDPR?

Article 4(12) of GDPR defines a PD breach as the "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

PD breach as per DPDPA

Section 2(u) of DPDPA defines PD breach as "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."

What should a Controller/Fiduciary do in case of a PD breach?

GDPR

Notification to DS: Pursuant to article 34 r/w article 33(3), where a PD breach is likely to result in high risk to the rights and freedoms of natural persons, the controller must notify the affected DS without undue delay, using clear and plain language, including **(a)** name and details of data protection officer or authorized contact; **(b)** likely consequences of the breach; and **(c)** mitigate measures.

Notification to Supervisory Authority (SA): Under article 33, where a PD breach is likely to pose a risk to the rights and freedoms of natural persons, the controller must notify without undue delay, and where feasible, within 72 hours of becoming aware, including **(a)** nature of the breach, along with categories and approximate number of affected data subjects and records; and **(b)** information provided to DS, as outlined above. Further, the controller must also document the breach, its impact, and the remedial measures taken, in a manner that SA can verify.

DPDPA

Notification to DP: Section 8(6) r/w rule 7(1) requires DFs to notify each affected DP, without delay with **(a)** description of breach (nature, extent, time, and location), **(b)** relevant consequences, **(c)** mitigation measures undertaken, **(d)** safety measures recommended, **(e)** contact information of authorized personnel.

Notification to DPBI: Section 8(6) r/w Rule 7(2) states DFs must provide a description of the breach and its likely impact to the DPBI, without delay. Further, an updated report must be provided within 72 hours with **(a)** updated information of the breach, **(b)** broadened facts of the event, circumstances and cause, **(c)** risk mitigation measures, **(d)** responsible parties, **(e)** remedial measures, and **(f)** status of notifications to affected DPs.

©PSA 2025. All Rights Reserved

Penalties

GDPR

For severe violations, fines up to EUR 20 million or about USD 24 million or 4% of the company's total global turnover, from the previous financial year, whichever is greater. For less severe violations, EUR 10 million or about USD 12 million or 2% of the total global turnover from the previous financial year, whichever is greater.

DPDPA

Where a DF fails to inform affected DPs or the DPBI about a PD breach, penalties up to INR 2 billion or about USD 23.5 million may be imposed. Further, DPBI may impose a penalty up to INR 2.5 billion or about USD 29 million for failure to take reasonable security safeguards to prevent a PD breach.

Key Judgments

1. Spain - Carrefour (2025)

- **Background:** Carrefour Spain, a subsidiary of the French retail giant Carrefour, reported five data breaches between January and September 2023, all stemming from unlawful access to client's accounts using Credential Stuffing (*a cyberattack where stolen username-password pairs are used in automated login attempts*). Notably, the company became aware of the first breach as early as October 2022 but failed to report it until January 2023. Furthermore, Carrefour did not inform affected customers about the first two breaches. Carrefour argued that it had reported the third breach to its customers, but even then, the communication merely stated that the password was required to be reset and explained how that could be done.

- **Findings:** The Spanish Data Protection Authority (**Spanish DPA**) launched an investigation in May 2023. While Carrefour claimed only 974 accounts were affected, the Spanish DPA found nearly 119,000 compromised accounts. It concluded that attackers may have access to the PD of customers, including their names, contact details, and addresses. It held Carrefour in violation of article 5(1)(f), article 24(1), and article 32, for failing to take proactive security measures. Notably, two-factor authentication was implemented only after the fifth breach. Additionally, the company failed to inform DS about the breach in the prescribed manner, in violation of Article 34. Further, it failed to report the actual number of affected individuals to SA in violation of article 33. Accordingly, on March 14, 2025, the penalty was imposed **(a)** EUR 2 million or about USD 2.4 million for violating article 5(1)(f); **(b)** EUR 1 million or about USD 1.2 million for violating article 32; and EUR 200,000 or about USD 240,000 for violating article 34. Additionally, the company was asked to report the breach to the DS.

©PSA 2025. All Rights Reserved

What will happen in India?

- **Analysis & Penalty:** In this case, unauthorized third parties accessed customer accounts. Under DPDPA, such unauthorized use constitutes a PD breach under section 2(u). Accordingly, the company would be in violation of section 8(5) as it failed to take reasonable security safeguards for the protection of PD, attracting a penalty of up to INR INR 2.5 billion or about USD 29 million per violation. Additionally, since the company failed to notify DPs of the breach, it would be held in violation of section 8(6). For this, a further fine of up to INR 2 billion or about USD 23.5 per violation could be imposed.

Key Takeaway *Implement and maintain strong, proactive data security controls (e.g. multi-factor authentication, timely intrusion detection, thorough breach response) and meet all DPDPA reporting obligations, including promptly notifying both, the DPBI and affected individuals when a breach occurs.*

2. Ireland - Meta (2024)

- **Background:** In July 2018, Meta Platforms Ireland Limited (**MPIL**), introduced a video upload feature on Facebook. Following this, the Facebook's 'View As' function allowed users to preview their profile as it would appear to another user. When used together with Facebook's video uploader, the system generated a "user token" that enabled third parties to access the full profile of that user. Due to this approximately, around 29 million Facebook accounts were affected globally, including 3 million in the EU/EEA. The breach was shortly remedied after discovery by MPIL and its US parent.

- **Findings:** The Irish Data Protection Commission (**Irish DPC**) launched two inquiries and found MPIL liable for allowing unauthorized access to the PD of millions of users, including names, emails, phone numbers, dates of birth, gender, children's data, etc. Thus, on December 17, 2024, fines were imposed **(a)** EUR 8 million or about USD 9.5 million for breach of article 33(3) (Incomplete breach notification); **(b)** EUR 3 million or about USD 3.6 million for breach of article 33(5) (Inadequate breach documentation); **(c)** EUR 130 million or about USD 154 million for violation of article 25(1) (Failure to implement data protection by design); **(d)** EUR 110 million or about USD 130 million for violating article 25(2) (Failure to ensure data minimization by default). Cumulatively, EUR 251 million or about USD 295 million.

©PSA 2025. All Rights Reserved

What will happen in India?

- **Analysis & Penalty:** If this case had happened in India, MPIL would be obligated to protect the PD in its possession using reasonable security safeguards. The combination of the 'View As' and video upload features had enabled unauthorized use of PD of the users by third parties. This qualifies as a PD breach under Section 2(u) of the DPDPA. Consequently, a penalty of up to INR 2.5 billion or about USD 29 million per violation may be imposed on Facebook by DPBI. Additionally, if MPIL would have failed to provide required information as per Draft Rule 7 in its breach notification to DP and DPBI, a penalty up to INR 2 billion or about USD 23.5 million per violation, could have been imposed by DPBI. Furthermore, the obligation to ensure data minimization is set out under section 6(1) of DPDPA. If Facebook failed to comply with this requirement, a penalty of up to INR 500 million or about USD 6 million may also be imposed.

Key Takeaway *Ensure that data protection is built into system design from the outset (Privacy by Design, Data Minimization), and rigorously validate features before launch to prevent misuse of access-controls or tokens that could lead to large-scale breaches.*

3. Spain - Vodafone (2024)

- **Background:** On 14 December 2022, a DS filed a complaint with the Spanish DPA against Vodafone Spain, alleging that a third party, without his consent, requested a duplicate SIM card. This was done by logging into the DS' account and requesting delivery to an address different from the billing address. In response, Vodafone Spain argued that the third party used valid access credentials obtained through social engineering and that it could not reasonably verify identities when correct login details were provided. Further, it stated that the third party had presented a fake ID to the logistics provider to complete the delivery. Notably, Vodafone Spain failed to provide evidence of any signature or recording of activation call required to use the SIM card.

- **Findings:** The Spanish DPA found that Vodafone Spain had failed to implement adequate measures to prevent impersonation. It held that, as a large-scale DC, Vodafone Spain was expected to have safeguards against such risks. Additionally, Vodafone Spain failed to demonstrate compliance with its own security policy, as it failed to produce the verification call recording or delivery signature. Accordingly, on May 5, 2024, the DPA imposed a fine of EUR 200,000 or about USD 240,000, based on Vodafone Spain's annual turnover for failure to lawfully process the PD of the DS under article 6(1) GDPR.

©PSA 2025. All Rights Reserved

What will happen in India?

- **Analysis & Penalty:** Applying the facts of the above case, a third party requested for a duplicate SIM card means that DP's credentials and password were available with a third party, which amounts to unauthorized use which falls within the definition of section 2(u). The DPBI could, accordingly, impose a fine for failure to protect PD in its possession using reasonable security safeguards imposing a fine up to INR 2.5 billion or about USD 29 million per violation. Further, the consent of DP was used for a purpose other than the specified purpose. Consequently, an additional fine of INR 500 million or about USD 6 million per violation may be imposed.

Key Takeaway

Companies often presume that privacy compliance is limited to implementation of technical and organizational measures. However, building a privacy compliant ecosystem requires more than just policies. It also demands day-to-day manual operations of the company adopt a privacy-conscious approach. Every action taken should align with privacy principles.

4. Croatia - EOS Matrix d.o.o. (2023)

- **Background:** On March 22, 2023, an anonymous petition was filed with the Croatian Supervisory Authority (**Croatian SA**) alleging unauthorized processing of PD by EOS Matrix d.o.o., a debt collection agency. The complaint was accompanied by a USB stick containing PD of 181,641 individuals, including 294 children. These individuals were debtors of various credit institutions, whose debt EOS had acquired through cession contracts. The data included names, dates of birth, and personal identification numbers.

- **Findings:** Following its investigation, the Croatian SA concluded that EOS had failed to implement adequate technical measures under article 32 of the GDPR. Specifically, since the company's main database containing the PD of around 370,000 individuals, lacked the ability to detect abnormal activity such as increase in number of data retrievals, data transfers outside the system, or compromised user access etc. Further, EOS also processed PD without a valid legal basis under article 6(1) of the GDPR, including PD of individuals who were not even debtor. Moreover, the company's privacy policies from May 2018 to October 2020, falsely stated that health data was not being processed, violating the transparency obligations under articles 12(1), 13(1), and 13(2). In addition, it was discovered between May 2018 and January 2019, EOS recorded telephone conversations of 49,850 individuals without a lawful basis, resulting in a further breach of articles 6(1) and 5(2) of the GDPR. Consequently, on October 5, 2023, Croatian SA imposed a fine of EUR 5,470,000 or about USD 6,500,000 for violations of articles 5, 6, 9, 12, 13 and 32 of the GDPR.

©PSA 2025. All Rights Reserved

What will happen in India?

- **Analysis & Penalty:** Under Indian law, companies are mandated to implement a set of reasonable security safeguards. Since, EOS failed to adopt such measures it would be held in violation of section 8(5), attracting a penalty of up to INR 2.5 billion or about USD 29 million per violation. Additionally, section 4(1) permits the processing of PD only on the basis of **(a)** consent or **(b)** legitimate use. As EOS lacked any valid legal ground for processing PD, it would be liable for an additional fine of up to INR 500 million or about USD 6 million per violation. Further, the DPDPA imposes additional obligations on companies when processing data of children. Any failure to do so attracts additional penalty of INR 2 billion or about USD 23.5 million per violation.

Key Takeaway

Ensure that only data processed with a lawful basis is collected and securely retained, especially when it includes sensitive health information, and enforce robust technical and organizational measures (TOMs) to detect anomalies, prevent unauthorized access or exfiltration, and enable full transparency toward DPs.

5. Germany - H&M (2020)

- **Background:** H&M operated a service center in Nuremberg. Since at least 2014, it maintained extensive records of the private lives of some of its employees, with notes permanently stored on a network drive. The company recorded the information through "*Welcome Back Talks*" in which the management recorded details of vacation experiences, illnesses, etc. Additionally, information was gathered through one-on-one or informal corridor conversations, where managers gathered personal details about the lives of the employees, such as their family issues, religious beliefs, etc. In some cases, the data was digitally stored and made accessible to approx. 50 managers across the company. Further, the company used the collected data for building employee profiles, which helped them in making employment decisions. In October 2019, a configuration error made these personal records accessible company-wide for several hours. Following this, an investigation was launched by the German Data Protection Authority (**German DPA**).
- **Findings:** After its investigation, the German DPA concluded that H&M's practices demonstrated a serious disregard for protecting employee's confidential data. As a result, on October 2, 2020, a fine of EUR 35.3 million or about USD 42 million was imposed.

©PSA 2025. All Rights Reserved

What will happen in India?

- **Analysis & Penalty:** Applying the facts of the present case, "employment" is a legitimate ground of processing PD under section 7(i) of DPDPA. In H&M's case, however, the kind of data collected was highly extensive and could not be said to fall within the scope of PD collected for the "*purpose of employment*". Further, no employee's consent was obtained.

  Thus, H&M had no lawful basis for collecting and storing the PD. Furthermore, as per section 2(u), any "*unauthorized processing*" of PD, constitutes as a PD breach. Additionally, the PD collected was made accessible to up to 50 managers and later company wide, which compromised the "*confidentiality*" of PD. Consequently, a penalty of up to INR 2.5 billion or about USD 29 million per violation may have been imposed by DPBI, for failure to implement reasonable security safeguards.

Key Takeaway

Companies must reassess the type of PD they collect and store. Data should only be collected if there is a "clear and necessary purpose". Map each data to its "purpose" and if the "purpose" is vague - don't collect.

©PSA 2025. All Rights Reserved

Concept 9: Cyber Insurance

Cyber insurance is an essential tool for managing and mitigating digital risks. It provides financial protection against losses arising from cyberattacks, including legal expenses, regulatory penalties, or data recovery costs. This coverage is critical when customer or employee data is compromised due to hacking, data theft, or accidental exposure.

What kind of losses are covered?

- **First-party losses:** Direct financial losses like costs on data recovery, business interruptions, incident responses, and mitigation efforts.
- **Third-party losses:** Claims from customers/clients /vendors involving legal defense costs, regulatory penalties, and settlements.

Case Study: Marks & Spencer Cyber Incident

Background: In April 2025, UK retail giant Marks & Spencer (M&S) suffered a cyber incident that resulted in the loss of customer data and caused operational disruptions. The breach led to a temporary suspension of M&S's online clothing business and caused a GBP 750 million drop in its market value.

Findings revealed that the incident was caused by human error rather than a technical failure, highlighting that even the most advanced cybersecurity systems cannot eliminate risk entirely.

M&S has estimated a total loss of about GBP 300 million, with disruptions expected to continue through July 2025.

Cyber Insurance Policy: M&S's cyber insurance policy is expected to cover losses up to GBP 100 million and the remaining GBP 200 million will have to be absorbed by the company itself.

How can a cyber insurance policy help?

As illustrated by the M&S case, a cyber insurance policy can help companies recover from a financial loss following a cyber incident. Beyond financial coverage, a well-structured policy can provide access to breach response teams, lawyers, public relations support, etc. These resources are vital for swift recovery and minimizing long-term damage.

©PSA 2025. All Rights Reserved

Assessing your Cyber Insurance Needs

- Understanding coverage limits, deductibles + exclusions
- Balance policy costs with potential incident impacts
- Match coverage to liability exposure
- Conduct data mapping to identify personal data and processing activities
- Evaluate security practices to understand gaps and vulnerabilities
- Study industry trends to identify common threats and assess exposure to similar risks
- Estimate the potential financial impact in case of a cyber incident (including fines under DPDPA & GDPR)

Key actions

- Data mapping
- Evaluate security practices
- Study industry trends

Why is this essential?

Organizations should assess their risk profile by carefully evaluating deductibles, coverage limits, and the types of incidents covered. It's important to weigh the likelihood and potential cost of cyber events against the policy premiums to ensure that the insurance policy provides meaningful value without becoming a financial burden.

Steps to determine the right cyber insurance policy

Form an internal committee: Establish a cross-functional internal committee comprising key stakeholders such as the CEO, CFO, CISO, and relevant department heads to asses the organization's cyber risk exposure, business priorities, and risk appetite.

Engage experts: Where required, businesses may engage a third-party insurance broker/cybersecurity advisor to support the evaluation process and identify suitable insurance carriers to get favorable deals on premiums.

Key points to keep in mind before engaging a cyber insurance provider

Verify key inclusions (i) Coverage for DPDPA/GDPR related risks; (ii) Access to breach response supplies; (iii) Pre-breach risk assessments + post-incident support

©PSA 2025. All Rights Reserved

Key questions

- Does the policy offer full limits for all coverage areas? Confirm whether the policy provides dedicated limits or shared/aggregate limits across various coverage elements?
- Is there coverage for reputational harm following a cyber incident?
- Waiting period for business interruption coverage? To what extent does the policy respond to business interruption losses? Does it cover loss of revenue, extra operating expenses, and costs of system restoration?
- What aspects are covered under cyber insurance? Does the policy address first-party losses (*like cyber extortion and business interruption*), third-party liabilities (*privacy violations and data breaches*)?
- Is there a provision for annual premium adjustment? Does the policy allow for recalibration based on risk profile changes or claim history?
- What are the limits of insurance for each type of coverage?
- Does the policy cover losses arising from rogue employees or internal threats?
- Does the policy include data re-creation, not just restoration?
- Is the cost of notifications covered under the event management section?
- Is social engineering fraud covered?
- What are the exclusions under the policy?

Some key clauses of a cyber insurance policy include

Technology/professional errors and omissions: Covers legal damages and claims arising from mistakes or failures in technology or professional services.

Privacy regulatory claims: Covers fines, penalties, and legal expenses due to regulatory actions stemming from privacy law violations.

Security breach response: Covers costs for crisis management, forensic investigations, legal costs, breach notification, and public relations following a breach.

©PSA 2025. All Rights Reserved

Multimedia liability: Provides coverage for claims related to online content that may result in defamation, copyright violations, trademark infringement, or reputational harm.

Cyber extortion: Reimburses ransom payments and related costs resulting from cyber-extortion or ransomware threats.

PCI DSS assessment: Pays for penalties or assessments levied by payment card networks after a data breach involving cardholder data.

Loss of funds or property: Reimburses for direct financial loss to the company or its clients caused by cyber-enabled theft.

Legal expenses (*post-incident*): Covers legal consultation, defense, and actions taken to address cyber incidents or clear wrongful charges.

Data restoration and malware decontamination: Covers costs to restore compromised data and clean devices affected by malware or cyberattacks.

Network security liability: Pays for third-party damages resulting from a cyber incident originating from your systems/devices.

Third-party breach: Reimburses legal expenses for claims filed by you against a third party that caused a breach of your data.

Business interruption and digital asset restoration: Covers income loss and costs to restore digital assets due to security breaches or system disruptions.

Filing a Cyber Insurance Claim

Subject to the terms of the policy, the claim settlement process may be as follows

Reporting and filing: The cyber incident must be reported to the appropriate regulatory authority within the prescribed timeline (*For instance, CERT-In requires reporting within 6 hours of the incident*). Additionally, a complaint must be filed at the nearest police station and/or the local cyber cell.

Notifying the insurance provider: The insurance provider must be notified of the incident (*typically within 1–2 days*).

Submitting a written claim: The claim form must be submitted (*typically within 30 to 90 days*) along with the required supporting documents, including, a copy of FIR, any invoices related to expenses, screenshots of findings, proof of loss incurred, copies of any legal notices or court summons, etc.

©PSA 2025. All Rights Reserved

Verifying the claim: Once the claim and documents have been submitted, the insurance company may appoint an investigator or forensic expert to verify the claim.

Claim settlement: After verification of the claim, the compensation is transferred to the beneficiary's account, usually within 5 to 7 days from the date of the expert's final report.

Way Forward

Cyber insurance is a vital safety net, but it is not a substitute for robust security practices or legal compliance. Organizations must (i) train their employees, as often the weakest link is human error, (ii) fulfil all obligations under applicable privacy laws, as non-compliance would always result in rejection of claims, (iii) invest in cybersecurity infrastructure, (iv) get their cyber insurance policies reviewed by experts.

©PSA 2025. All Rights Reserved

The Team

Dhruv Suri
Partner
d.suri@psalegal.com

Rishi Sehgal
Senior Associate
r.sehgal@psalegal.com

Aastha Mathur
Senior Associate
a.mathur@psalegal.com

Pragya Kriti
Associate
p.kriti@psalegal.com

Saniya Gandotra
Associate
s.gandotra@psalegal.com

©PSA 2025. All Rights Reserved

Scan for Website: www.psalegal.com

14 A & B, Hansalaya
15, Barakhamba Road
New Delhi 110 001
contact@psalegal.com