

# Yes Means Yes: Managing Consent Under India's New Data Protection Law

## Background

Unlike the General Data Protection Regulation (“**GDPR**”) of the European Union which allows non-consensual data processing under various circumstances, India's recently published Digital Personal Data Protection Act, 2023 (the “**DPDP Act**”) relies heavily on consent as a ground for processing personal data.

Thus, other than a few ‘legitimate uses’ (such as when an individual voluntarily provides their personal information for a specified purpose or if processing is necessary for employment-related purposes), consent is the only legal basis for processing personal data under the DPDP Act.

Since the legal framework under the DPDP Act ultimately aims to *protect* personal data for the benefit of specifically identifiable individuals related to such data (“**data principals**”), it imposes corresponding obligations on, and limits, the processing of such data by “**data fiduciaries**”, *i.e.*, those entities which determine the purpose and means of data processing, including in conjunction with other entities.

Accordingly, the DPDP Act seeks to set up an enforceable system that involves:

- securing explicit permission from each data principal before collecting and/or processing their personal information;
- giving data principals the right to specify a limited purpose with respect to which they approve the use of their data;
- providing data principals with an option to withdraw their permission later, unless the purpose specified is rendered moot and/or no longer applies *before* such consent can be withdrawn; and
- requiring personal data to *not* be retained once the purpose of processing has been accomplished.

While data fiduciaries need to start thinking about such new obligations, they also need to look out for specific government-made rules which, when prescribed, are likely to instrumentalize various provisions of the DPDP Act, including with respect to the methods and means for providing notices and seeking consent. Given the quantum of financial penalties involved, non-compliance and/or breaching obligations under the DPDP Act may prove costly for most entities.

For a general overview of notice and consent requirements, see our previous note [here](#).

## Notice and Consent Requirements

Once the DPDP Act is in force, notices need to be sent within a reasonable time to every individual whose personal data an organization already has or processes, even if their consent had been obtained in the past. Accordingly, establishing an efficient notice-and-consent mechanism, as well as implementing appropriate technical and organizational measures to facilitate compliance, remain key requirements. Nevertheless, a data fiduciary may continue to process its legacy personal data until and unless the individual concerned withdraws their consent.

For now, entities could invest in appropriate technological expertise and/or technical assistance, such that each of their personal or mixed datasets can be ingested into a consolidated platform, including outsourced ones. This process can be secured through customized configurations and access controls – including through commercial arrangements with third parties via appropriate agreements. Thus, short- or long-term contracts can be negotiated with the owners of such platforms – often large technology companies, startups or information technology (“IT”) infrastructure or IT-enabled service providers. The aim should be to check for notice and consent status with respect to each data principal, including in the future as well as on a continuous basis.

### Language capabilities

Each such statutory notice needs to contain certain mandatory information in a templated form (e.g., about consent withdrawal and grievance redressal rights, as well as providing a description of how a complaint can be made to the Data Protection Board of India (the “DPBI”). The manner and ways in which such notices can or ought to be sent to data principals will be specified through government-made rules. Importantly, these notices are required to be made available in over twenty languages if specific individuals so require. Accordingly, developing language capabilities could be a priority area of focus for now, including on account of the fact that providing multiple linguistic options during notice and requests for consent is likely to remain a recurrent obligation (for data fiduciaries).

## Consent Management

Pursuant to an organization’s data mapping exercise (please refer to our note in this regard, available [here](#)), each individual whose personal data is being/has been processed by an organization needs to be specifically identified from internal databases. The internal data map should yield valuable information about those processing activities of the organization that are (and will continue to be) based on a data principal’s explicit consent (as opposed to being covered under ‘legitimate use’).

Further, like with notices, every request for consent is required to be presented to individuals in clear and plain language, giving them the option to access such request in English or any language specified in the Eighth Schedule to the Indian Constitution. It should further provide the contact details of a pre-authorized person who will remain responsible in respect of responding to communications from data principals if and when they choose to exercise their rights under the DPDP Act.

Accordingly, data fiduciaries could start planning for an eventual rollout of a consent request process (where each request needs to be accompanied or preceded by the statutory notice). Subsequently, individuals need to be contacted for the purpose of giving such notice. This process can be automated.

However, in case of proprietary processes or systems that store unstructured data, certain manual interventions and discovery modes may also be necessary.

The contacting of individuals could take the form of batch emails – which, in turn, may produce an auditable log – including that of individuals who wish to withdraw their consent. Upon withdrawal, absent any legal requirement/authorization in this regard, data processing with respect to such individuals needs to stop within a reasonable period. Importantly, the DPDP Act requires the consent withdrawal process to be made as easy as it was to provide consent in the first place. Thus, if consent could be provided with a single click, such consent should be similarly retractable (e.g., involving a link to unsubscribe).

Entities need to keep such prescriptions in mind while structuring their consent mechanisms. Further, entities need to ensure that when consent is withdrawn, all other entities processing the corresponding data – including contracted data processors – also stop processing it, failing which the primary entity may be held liable for a breach. The cessation of processing must be followed up with data erasure. Further, data principals may ask for their personal data to be corrected, completed, updated or erased, even when they had previously consented to the processing of such data. Accordingly, data fiduciaries may need to track and synchronize the status of consents across platforms and systems.

In addition, when an organization's data processing relies on consent, if a question arises in this regard during a proceeding, such organization will be required to prove that a notice was indeed given, and consent was indeed provided. Accordingly, data fiduciaries should plan to retain consent logs for the purpose of demonstrating compliance, if required.

## Consent managers

Individuals will be permitted to give, manage, review or withdraw consent through a “**consent manager**”. Under the DPDP Act, a consent manager will be an entity registered with the DPBI to act as a single point of contact for the purpose of providing various consent options to data principals through a transparent, accessible and interoperable platform.

The consent manager is required to (i) be accountable to the data principal, and (ii) act on the latter's behalf, in a manner and subject to such obligations as may be prescribed. The manner of accountability and registration (including accompanying conditions), as well as the obligations of such consent managers may be specified through rules. However, it appears that data fiduciaries themselves are not required to appoint, or enter into arrangements with, consent managers.

## Consent management platforms

Nevertheless, it may be possible (and/or necessary) for data fiduciaries to use a separate and standalone consent management platform (“**CMP**”) – as opposed to the interoperable platforms provided by registered consent managers to (and for the benefit of) data principals. Such CMPs could be used by data fiduciaries as a tool to collect, track, manage and synchronize individual consents at their end. This way, CMPs can automate the consent process, obtain permission for using cookies to track data, and allow users to update their cookie preferences. Importantly, if a cookie is able to identify a particular user, it may be subject to the DPDP Act's requirements – similar to rules made in this regard under the GDPR and the California Consumer Privacy Act (“**CCPA**”), respectively.

If an organization uses third-party apps (e.g., social media), scripts can be blocked until the user consents to the use of cookies. This may prevent third parties from unintentionally making a website non-compliant with the DPDP Act. In this regard, too, CMPs may be able to track and record individual users. Thus, CMPs can alert entities about issues that could put them at risk in terms of violating obligations under the DPDP Act. In addition, CMPs can display cookie banners that request consents for data collection and provide information to users about what data is being collected, how it will be used and who it will be shared with – as required under the DPDP Act.

Consent managers will remain accountable to individual consent-givers (*i.e.*, data principals) – including through technical, operational, financial and other eligibility conditions, pursuant to which their registration and consequential duties will oblige them to provide grievance redressal options and make them liable to complaints, including before the DPBI. On the other hand, it may be possible for data fiduciaries to choose a CMP from among multiple options based on their own requirements. Eventually, the goal for a data fiduciary is to have a central repository of compliant consent responses for use across internal departments and subsequent processing. Conversely, protocols can be set on such CMPs to automatically purge non-responders or consent-withdrawers from the organizational database.

Absent further clarification through rules, it is unclear whether such CMPs will be permitted (or mandated) to be linked to a consent manager's interoperable platform, including for the purpose of real-time consent coordination.

## Standard of consent

Like the GDPR – and unlike the CCPA – the requirements of a valid consent under the DPDP Act is high (it needs to be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and is required to signify an agreement to the processing of personal data for the specified purpose, and must remain limited to such personal data as is necessary for that purpose).

Accordingly, it is likely that an 'opt-in' consent (where users need to take an affirmative action to confirm their approval) will be required in India – rather than an 'opt-out' consent (where companies inform users about the collection/use of data and allow such users to opt-out if they so wish). Thus, options like unchecking a pre-filled/pre-checked box, or filling out a form to withdraw consent, is likely to not be permitted under the DPDP Act. While requiring users to manually consent to some or all of a company's policies on data collection/use gives individual consumers greater control over their personal information, it raises the responsibility for companies to obtain explicit permission before processing, rather than having a system where users consent by default.

Further, certain 'right to access' provisions under the DPDP Act – similar to the GDPR and the CCPA – enable individuals users to submit a request to data fiduciaries for the purpose of finding out *what* an organization knows about them and *how* it uses such information. Specifically, these rights under the DPDP Act allow data principals to obtain:

1. a summary of their data, as well as the processing activities undertaken with respect to such data;
2. the identities of all other entities with which such data has been shared, along with a description of that shared data; and
3. any other information related to personal data and its processing, as may be prescribed.

Accordingly, organizations will need to respond to such requests within a reasonable time. This task can create a significant compliance burden, especially if such requests are not stored properly (e.g., in a consolidated dashboard). In that regard, companies may need to automate their workflows to manage such requirements.

Lastly, since an organization's data landscape is likely to keep changing over time, data mapping tools – whether in-house or third-party run/owned – may need to scan for data stores on a regular basis.

## Children's Data

When personal data relates to an individual who is below the age of 18 (a “**child**,” as defined in the DPDP Act), the corresponding data principal will include the parents or lawful guardian of such child. Similarly, in the case of a person with disability, a data principal will include the lawful guardian acting on the former's behalf. Certain special obligations apply for the processing of such data, such as the need to obtain verifiable parental/guardian consent. This, too, may pose various logistical issues for data fiduciaries, other than the fact that the cut-off age under the DPDP Act for the purpose of defining a child is significantly higher than the global threshold – as discussed in our note [here](#) and [here](#). However, separate platforms – such as e-lockers and e-document wallets – may be used for the purpose of obtaining such consents, as well as for the purpose of age verification.

## Other Considerations

The DPDP Act expressly excludes publicly available information from the scope of data protection. However, unlike the GDPR's Article 14, it does not impose an obligation to inform corresponding individuals about the use of such data. Accordingly, publicly available information may be freely used by businesses – including through their artificial intelligence (“**AI**”) and machine learning (“**ML**”) platforms – for the purpose of training, analytics, evaluation, targeted advertising and profiling. However, for an overview of regulatory challenges and other considerations with respect to the use of AI in the Indian context, see our [note](#) here.

## Foreign Companies

Foreign companies should note that the DPDP Act's extraterritorial application is limited to such processing activities that are connected with the offering of goods and services to people in India. However, the DPDP Act's extraterritorial application will not extend to the ‘profiling’ of individuals in India. Thus, any form of processing with respect to the personal data of individuals in India that analyzes or predicts aspects concerning their behavior, attributes or interests may be conducted without providing notice or obtaining consent – as long as such processing happens outside Indian territory and does not offer goods and services to people in India.

Outsourced data processing which involves the personal information of individuals who are not in India will also be allowed to be conducted (in India) without notice or consent obligations – as long as a contract exists between entities in and outside the country, respectively, as discussed [here](#).

## Conclusion

The role of the consent manager has been expanded upon in the DPDP Act relative to past versions of the law. Thus, data principals may use an interoperable platform, as provided by such consent manager, to administer and/or revise the status of their consent. Accordingly, a consent management process, as may be established by data fiduciaries at their end, ultimately needs to have arrangements or interface with consent managers (who will remain accountable to data principals). Such coordination may be required to ensure that unregistered CMPs used by data fiduciaries are linked with, and/or have access to, the interoperable platforms managed by registered consent managers. It may even be possible to merge the two.

Subject to the government-made rules in this regard, the outsourced consent management business may witness a significant surge, including among software providers, start-ups and large technology companies.

Lastly, the DPDP Act may impose significant compliance burdens, especially for client-facing companies and business-to-consumer (“**B2C**”) entities. Such entities, in particular, may require internal sensitization, including across marketing and sales departments, about notice and consent management. Further, organizations may need to conduct privacy training and awareness programs for employees and contractors who handle personal information and monitor consent. A chief information security officer (“**CISO**”) could ensure compliance with standard operating procedures containing easy-to-understand consent tracking protocols. Such procedures should stem from, and complement, an internal policy related to data protection. This policy could also include fundamental organizational principles with respect to (i) notice and consent management, (ii) data retention and erasure, (ii) confidentiality, and (iii) data integrity.

---

*This insight has been authored by **Deborshi Barat** (Counsel); he can be reached at [d Barat@snrlaw.in](mailto:d Barat@snrlaw.in) for any questions. This insight is intended only as a general discussion of issues and is not intended for any solicitation of work. It should not be regarded as legal advice and no legal or business decision should be based on its content.*

© 2023 S&R Associates

**S&R**  
**ASSOCIATES**  
ADVOCATES



### NEW DELHI

64 Okhla Industrial Estate  
Phase III  
New Delhi 110 020  
Tel: +91 11 4069 8000

### MUMBAI

One World Center, 1403 Tower 2 B  
841 Senapati Bapat Marg, Lower Parel  
Mumbai 400 013  
Tel: +91 22 4302 8000