Your contract is not a consent form: DPDP Act and the deliberate rejection of contractual necessity

At the heart of the much-discussed Digital Personal Data Protection Act, 2023 (**DPDP Act**) lies consent, which serves as the primary legal basis for the processing of digital personal data and shapes its implications for businesses. Under the DPDP Act, digital personal data can be processed **only** with the consent of the data principal *or* for certain specified "legitimate uses"[1] provided for in the statute which operates as a statutory exception to the consent requirement.

Against this backdrop, one of the DPDP Act's differing features is the exclusion of "contractual necessity" as an independent "legitimate use" for processing personal data without the requirement of obtaining a consent. Unlike many global data protection regimes,[2] which allow processing without consent where it is necessary to perform a contract, the DPDP Act does not confer contractual relationships with the cloak of a "legitimate use" to justify processing of digital personal data. This divergence from international practice has far-reaching implications for several businesses operating in India, requiring them to rethink how contracts are drafted, how data flows are structured, and how compliance is operationalized in practice.

INDIA'S DEPARTURE UNDER THE DPDP ACT

"Contractual necessity" is the legal basis in many data protection regimes that allows personal data to be processed when it is objectively necessary to perform a contract with the individual who is a party to that contract.

The DPDP Act's provisions on legitimate uses are context-specific, primarily addressing public interest, legal obligations, or employment-related scenarios, and do not provide scope to rely on contractual necessity as a legitimate use. Routine commercial contracts in India cannot therefore claim such a carve-out, unlike in some other jurisdictions where contractual performance may be recognized as a basis for data processing. Section 7 of the DPDP Act reflects a deliberate policy choice, *i.e.,* private contracts should not determine the boundaries of lawful data processing. The legislature appears to have assumed that most modern contracts are standard-form, non-negotiable, and ill-suited to act as proxies for meaningful consent.

WHAT DOES THIS MEAN FOR BUSINESSES PROCESSING DATA IN INDIA?

- ***Commercial necessity does not imply legal authority***. Data processing that is operationally necessary to deliver a service under a contractual agreement, does not constitute a lawful basis for processing personal data under the DPDP Act.

---

1 Section 7, DPDP Act prescribes certain legitimate uses where a data fiduciary need not obtain consent before processing of digital personal data.

2 EU's GDPR (Article 6(1)(b)); South Africa's Protection of Personal Information Act (Section 11(1)(b)); Philippine's Data Privacy Act of 2012 (Section 12(b)) etc.

FOR EXAMPLE:

A hospital cannot rely solely on its patient admission form to process patient health records for research, marketing, or analytics purposes. To process such information for these secondary purposes, the hospital would require explicit valid consent from the patients.

- ***Legitimate use is not a backdoor for processing***. The legitimate use ground as laid out in the DPDP Act cannot be interpreted to cover contractual performance as a ground to process digital personal data of the individual who is a party to a contract. Such processing will not only be invalid but may raise serious consequences for violation.

FOR EXAMPLE:

An asset management company cannot rely on "legitimate use" to process investor data for cross-selling unrelated financial products merely because the investor has signed an investment management agreement and agreed to avail of services under the agreement.

- ***Contracts cannot replace consent***. Contracts will continue to govern legal and commercial rights and obligations, but they will not provide the legal basis to processing of digital personal data under the DPDP Act.

FOR EXAMPLE:

A consumer facing internet platform (say for example Instagram) may need explicit consent for personalized recommendations, or targeted advertising, even if such features are central to its business model. Mere agreement to avail of the service offered by the social media platform and opening of an account by an individual will not be sufficient for processing of data for purposes of sending targeted marketing messages to the account holders.

WHAT ARE THE NEXT STEPS FOR BUSINESSES IN INDIA?

It is abundantly clear that consent has become the primary legal basis for processing data under the DPDP Act, and businesses must remain cognizant that the "legitimate use" exception is limited in its scope and application. Here are some next steps that data fiduciaries can consider during the run up to the DPDP Act fully becoming operational by May 13, 2027.

- ***Re-map data flows that were historically contract driven***. Data fiduciaries must identify processing that previously depended or relied upon contractual necessity and determine whether it fits within a narrow "legitimate use" or whether such processing will require fresh, explicit consent. If it does in fact require fresh consent, businesses must:
  - ***Embed consent in design***. Make consent granular, purpose-specific, and easily revocable.

- ***Compliance beyond GDPR for India***. Organizations that consider themselves "GDPR-compliant" will need to reassess reliance on contractual necessity when operating in India and align their practices with the requirements under the DPDP Act while continuing to meet any compliances under the laws of other jurisdictions. Simply put, compliance playbooks built around EU or other jurisdictions' lawful bases cannot be the basis for processing of digital personal data for their India based operations.

- ***Plan for enforcement***. Regulatory scrutiny is likely to focus on substance over form. Over-reliance on broad consent language, implied consent, or creative interpretations of "legitimate use" may be viewed as evasive. Data fiduciaries should assume that consent design, withdrawal functionality, and actual data practices will be tested and not merely the language contained in contracts or privacy notices.

The DPDP Act places India at the stricter end of the global data protection spectrum. By excluding contractual necessity, it reinforces that commercial relationships do not determine the legality of processing personal data.

For businesses, it is critical to undertake a timely assessment of their existing policies and practices regarding data processing. This would allow them to identify areas that may present possible regulatory exposure and enable them to design, test and adopt required measures to address the gaps. Accordingly, consent-first systems and a clear data privacy governance structure are now non-negotiable. Businesses that embrace these principles will not only reduce their legal risks but also earn user trust in India's increasingly consent-driven digital ecosystem.

We hope you have found this information useful. For any queries/clarifications please write to us at insights@elp-in.com or write to our authors:

Ravisekhar Nair, Partner – Email -*ravisekharnair@elp-in.com*

Abhay Joshi, Partner – Email - *AbhayJoshi@elp-in.com*

Ketki Agrawal, Principal Associate- Email – *ketkiagrawal@elp-in.com*