The Indirect Collection Dilemma: How to Fulfil Consent Requirement?

The Digital The Digital Personal Data Protection Act, 2023 (**DPDP Act**) and the Digital Personal Data Protection Rules, 2025 (**DPDP Rules**) establish India's framework for protecting digital personal data. The framework is anchored in consent-based processing and only allows processing of personal data without consent under limited exceptions in the form of 'legitimate uses' or certain other exemptions.

The DPDP Act and the DPDP Rules will be fully in force from May 2027. This means that data fiduciaries will be required to obtain consent from data principals by providing a notice which informs them of their personal data being sought and the purposes for its processing, among other things. The DPDP Act requires consent to be obtained prior to processing digital personal data. Since 'collection' of digital personal data also amounts to 'processing' of such data, a notice seeking consent essentially will have to be provided either at the time of or prior to the collection of personal data.

Often times, however, the digital world involves several transactions where an individual is required to provide personal data of some other data principal who is not available at the point of collection of data to provide consent or is not a party to the transaction in question (**Third-Party Data Principal**). For instance, a customer may provide a friend's personal data to an e-commerce platform for a gift delivery. In such transactions, it may be impractical or difficult for the transacting customer to obtain the friend's consent (the Third-Party Data Principal) because the personal data is being provided by the transacting customer who otherwise has no legal authority under the DPDP Act to provide consent on behalf of the friend or the Third-Party Data Principal.

This primer examines how consent-based processing can raise practical business challenges in certain scenarios where a data fiduciary is processing personal data of a Third-Party Data Principal who has not been approached by the data fiduciary for purposes of taking consent. These issues potentially have a direct bearing on businesses as well as consumer experiences.

REAL-WORLD EXAMPLES OF INDIRECT DATA PROCESSING

Some of the common scenarios where a data fiduciary may face practical difficulty in obtaining consent directly from the Third-Party Data Principal could be as follows:

- **E-commerce and gifting**: A customer purchases a gift from an e-commerce platform for a friend. To complete the transaction and facilitate shipment, the customer provides the recipient's name, delivery address, contact number, and email address on the e-commerce platform. In this scenario, the recipient is a Third-Party Data Principal and her personal data is being processed by the e-commerce platform without her knowledge and without seeking her prior consent.

- **Cab hailing services**: A person books a cab for her parent by providing her name, contact details, and trip requirements. In this case, the parent is a Third-Party Data Principal, and her personal data is being processed without her prior consent.
- **"Refer-a-friend" marketing programs**: A consumer-facing internet platform or consumer app offers promotional coupons if a user provides a friend's email address to invite them to the platform, or where a bank offers promotional offers if an existing consumer provides the personal information of a friend for a referral. In this scenario, the friend is a Third-Party Data Principal, and her personal data is being processed by the platform without her prior consent.
- **Emergency contacts**: An employee onboarding a company portal, or a gym member signing up for a membership submits the name, relationship, and contact details of an emergency contract. In this case, the personal data of the emergency contact (who is a Third-Party Data Principal) is being processed by the employer and the gymnasium, respectively without prior consent.

THE CONCERNS AROUND COLLECTING PERSONAL DATA FROM A THIRD PARTY

As stated above, under the framework of the DPDP Act, digital personal data can only be processed by a data fiduciary without prior consent if it falls under certain legitimate uses or under certain exemptions.

Legitimate uses. Such legitimate uses involve processing of personal data for: (i) a specific purpose where personal data has been voluntarily provided, (ii) state functions (services/ benefits), (iii) state sovereignty & security, (iv) compliance with legal disclosure norms, (v) compliance with judgment/ order, (vi) medical emergency, (vii) public health crisis, (viii) disaster management/ public order, or (ix) employment purposes.

Exemptions. Further, the exemptions where the obligation of obtaining consent does not apply include:

- ***Enforcement of a legal right*.** Where processing is necessary for enforcing any legal right or claim.
- ***Processing by judicial bodies.*** Processing of personal data by a judicial body.
- ***Prevention of crime.*** Processing personal data in interest of prevention, detection, investigation or prosecution of a crime or contravention of any law.
- ***Certain mergers and acquisitions.*** Processing of personal data for mergers and acquisitions approved by a court or competent authority.
- ***Financial defaults.*** Processing of personal data for ascertaining financial information of a person who has defaulted in payment due on account of a loan.
- ***Processing by State.*** Processing of personal data by the state's instrumentalities for certain purposes.
- ***Research.*** Processing of personal data necessary for research, archiving or statistical purposes.

These legitimate uses and exemptions are unlikely to be applicable in the scenarios discussed above. Consequently, obtaining valid consent remains the sole basis for processing the personal data of a Third-Party Data Principal. In this context, it is critical to remember that the DPDP Act does not expressly recognize third-party consent authorization, except for in specific cases involving children or persons with disabilities (via parents or lawful guardians). Hence, the person providing the personal data of a Third-Party Data Principal has no legal basis /authorization under the DPDP Act to consent on behalf of a Third-Party Data Principal.

In this context, a post-facto effort to reach out to the Third-Party Data Principal *after* acquiring their details to seek consent *will not work*, as the collection of personal data and subsequent outreach constitutes unauthorized processing. Consent has to be obtained by the data fiduciary 'prior' to collection of the personal data of the Third-Party Data Principal.

POSITION IN OTHER JURISDICTIONS

European Union (EU): In the EU, the General Data Protection Regulation (**GDPR**) allows businesses to process personal data without obtaining consent if such processing is necessary for a legitimate interest, and where such processing does

not violate individual's fundamental privacy rights.[1] In essence, legitimate interest is a legal basis that allows a controller or third party (in EU) to process personal data without consent, provided the interest pursued is lawful, precisely articulated, real, necessary, and not overridden by the fundamental rights and expectations of the data subject. For example, an IT company may log the IP addresses of visitors accessing its website for a legitimate interest of detecting and preventing cyberattacks or unauthorized access, ensuring the security of its systems. In the EU, it appears that legitimate interest is relied upon by businesses as the appropriate ground to process third party personal data without obtaining consent subject to certain conditions.[2] Such a ground for processing personal data, however, is absent under the DPDP Act.

Singapore: The Personal Data Protection Act, 2012 (**PDPA**) also has a legitimate interest ground, similar to GDPR where personal data can be processed for a legitimate interest given that such an interest outweighs any adverse effect on the concerned individual. This legitimate interest generally refers to any interests of the business itself or of any third party. For example, a food business collecting necessary personal information of individuals entering its premises for security purposes.[3]

Australia: In Australia, the Privacy Act 1988 (**APA**), allows businesses to indirectly collect personal data of an individual without obtaining prior consent where it is "unreasonable or impracticable" to obtain data directly.[4] For example, in a medical emergency where a person is unconscious his personal data may be collected indirectly from family for his treatment as it would be impracticable to collect such data directly. Such a provision is also absent under the DPDP Act.

Compared to the legal positions that appear to exist in other jurisdictions, the DPDP Act does not contain a similar provision that could provide a reliable and predictable legal basis for processing personal data of the Third-Party Data Principals without seeking prior consent in scenarios like the ones discussed in this note.

WAY FORWARD

The DPDP Act in its current form does not provide a clear answer to these practical challenges.

While clarity on several issues (including this one) is awaited, it becomes necessary for businesses to assess these important issues and analyze how these could impact their business and operational models. Different businesses operate differently and have different requirements to process third-party data. Hence, businesses should first internally assess whether they collect third-party personal data, and if yes, then whether such collection can be proceeded by obtaining consent. If not, then a detailed assessment of the legal and financial exposure arising from such operations must be undertaken to mitigate such risks.

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*

Aayushi Sharma, Principal Associate – Email – *aayushisharma@elp-in.com*

Akash Gulati, Associate – Email – *akashgulati@elp-in.com*

1 Article 6(1)(f), GDPR.

2 *Does the GDPR really say that? Festive Edition*. Data Protection Commission Ireland. Available at: https://www.dataprotection.ie/en/dpc-guidance/blogs/does-gdpr-say-that-festive-edition [Accessed 9 Aug. 2026]; *Freddie's Flowers Privacy policy*. Available at: https://www.freddiesflowers.com/privacy-policy [Accessed 9 Aug. 2026]; *Cinema City Privacy policy*. Available at: https://www.cinemacity.cz/static/en/cz/privacy-policy-cz [Accessed 9 Aug. 2026].

3 Item 1, Part 3, First Schedule, PDPA.

4 Clause 3.6(b), Schedule 1, APA.