‘Voluntarily’ provided personal data: How far can you go?

A. INTRODUCTION

The Digital Personal Data Protection Act, 2023 (**DPDP Act**) together with the Digital Data Protection Rules, 2025 (**DPDP Rules**) notified in November 2025, establishes India’s framework for the protection of digital personal data[1]. As readers would recall, the DPDP framework will be rolled out in phases, with its substantive provisions coming into effect fully by May 2027.

Under the DPDP framework, a data fiduciary can process personal data for lawful purposes either: (i) with the consent of the data principal; or (ii) for certain ‘legitimate uses’.[2] One such legitimate use[3] is where a data principal ‘*voluntarily*’ provides her personal data for a specified purpose and has not indicated that she does not consent to the use of her personal data. Notably, the General Data Protection Regulation **(GDPR)** does not recognize a comparable ground for processing based on voluntary provision of personal data by a data subject for a specified purpose.

In this primer, we examine the scope of voluntary provision of personal data as a ground for processing, its practical implications for businesses, and the potential steps that data fiduciaries may consider to ensure proper use of this processing ground.

B. VOLUNTARY PROVISION OF PERSONAL DATA

- ***What might constitute a “voluntary” provision of personal data?*:** Under Section 7(a) of the DPDP Act, a data fiduciary may process personal data without issuing a notice and seeking consent in terms of Section 6, where a data principal has voluntarily provided it for a specific purpose without indicating any objection to its use. However, what is meant by “*voluntary provision*” of personal data has not been defined under the DPDP Act. Rather, the concept of “*voluntary provision*” of personal data has been explained through two illustrations: (i) provision of personal data by a customer to a pharmacy to receive an electronic receipt of payment, after making a purchase (**First Illustration**); and (ii) an individual electronically messaging a real estate broker and sharing personal data in order to be informed about rental accommodation options (**Second Illustration**).

  These illustrations highlight a common theme, *i.e.*, individuals ‘*actively*’ and ‘*voluntarily*’ share their personal data with a clear expectation of its use for a specific purpose. That said, in a vast majority of real-world scenarios, data principals do initiate the sharing of personal data to access a product or service. If read broadly, this could allow data

[1] For this primer, in the context of the DPDP Act, “personal data” refers to “digital personal data”.
[2] Section 4, DPDP Act.
[3] Section 7(a), DPDP Act.

fiduciaries to routinely rely on "voluntary provision" as a legitimate use, effectively bypassing the DPDP Act's notice-and-consent architecture.

Such an interpretation could be problematic. If this ground is extended to cover all instances where users, for example, input personal data while signing up for an e-commerce platform, or accessing a service, the notice-and-consent framework risks becoming largely redundant. One could possibly argue that in many digital contexts, the user is not "volunteering" data in any meaningful sense but is responding to a pre-designed interface where disclosure is a condition for entry into the service ecosystem.

A cautious and facts-specific reading is therefore warranted: Section 7(a) of the DPDP Act should apply only where the data principal clearly and affirmatively initiates the disclosure for a specific, reasonably expected purpose, and not where the data fiduciary relies on mandatory sign-up fields or bundled onboarding flows to bypass its primary obligations of transparency and consent. This is especially important because the illustrations themselves tie processing to the specific purpose for which the data was shared, not to a general waiver of notice and consent across the broader relationship.

- ***Processing for specified purpose:*** A data fiduciary's use of voluntarily provided personal data can very easily 'overstep' the boundaries of this 'legitimate use'. For instance, in the First Illustration, the pharmacy's processing of the customer's personal data (such as her e-mail, phone number) to send marketing related texts or e-mail messages or in the Second Illustration, the real estate broker sharing the individual's contact details with any other person who then processes this personal data for other purposes such as marketing or targeted advertising.

  These illustrative instances above highlight how a data fiduciary's use of voluntarily provided personal data can go beyond the contours of this 'legitimate use' and step into the realm of data processing which can only be undertaken on the basis of consent which will trigger the obligation on the data fiduciary to issue a notice and obtain consent for processing.

C. CONSIDERATIONS FOR BUSINESSES

To determine the availability of this 'legitimate use' basis for processing, data fiduciaries must consider certain practical guidelines, some of which are indicated below:

- ***Identify if the personal data was shared truly 'voluntarily'.*** Treat "voluntary provision" as a narrow exception. If personal data is collected as a pre-condition to access a product or service, businesses should default to notice and consent, unless the disclosure is clearly and independently initiated by the user for a specific purpose.
- ***Processing limited to the 'specific purpose'.*** Businesses must not process personal data other than the purpose for which the data principal has voluntarily shared her personal data.
- ***Minimize data collection.*** The point of interaction (such as online forms, etc.) must ideally contain only such data fields as are strictly necessary for the specified purpose. For instance, a shade-match tool on an e-commerce platform must not contain fields for unrelated data such as contact details.
- ***Classification in internal records.*** Internal records should ideally map and categorize personal data that would be collected for 'legitimate use' (such as use of voluntarily provided data) and processing of personal data that would require consent.
- ***Limit internal access.*** Appropriate process and technical controls (such as role-based access, prompts, approval checks, etc.) may also be implemented to limit use of voluntarily provided data sets and avoid their use beyond specified purposes. For instance, a clinic can implement an internal system to separate appointments related data from marketing related data.
- ***Training for relevant teams.*** Customer-facing and other similar support teams must be trained to clearly distinguish 'kosher' use of voluntarily provided personal data from consent-based processing and to prevent any internal leakage or overuse of such data sets.

D. CONCLUSON

As India's data protection regime moves towards full operationalization, businesses preparing for compliance under the DPDP framework must approach reliance on non-consent-based grounds of processing such as use of voluntarily provided data, with caution. While the law permits such use of voluntarily provided personal data, nuanced questions such as what would truly qualify as 'voluntarily' provided as opposed to 'solicited' data remain open and will define a clearer line between non-consent (legitimate use) and consent-based processing. Until clearer regulatory guidance emerges, a conservative approach is advisable and where there is ambiguity, businesses must lean towards obtaining prior consent for processing personal data.

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*

Parthsarathi Jha, Partner – Email - *parthjha@elp-in.com*

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