Power of the Central Government to call for information under the DPDP Act

The Digital Personal Data Protection Act, 2023 (**DPDP Act**), along with the Digital Personal Data Protection Rules, 2025 (**DPDP Rules**) forms India's comprehensive data protection framework. The substantive provisions of the DPDP Act and the DPDP Rules (together, **DPDP Framework**) are set to come into effect by May 2027.

Under the DPDP Framework, the Central Government is empowered to call for information from either the Data Protection Board of India (**DPBI**), an intermediary, or a data fiduciary for the purposes of the DPDP Act. [1] In this primer, we examine the scope of this power, the purposes for which information may be sought, and what it means for businesses.

Power to call for information. Section 36 of the DPDP Act provides that the Central Government may require **DPBI**, an **intermediary**, [2] or a **data fiduciary** to **furnish such information** as it may call for the **purposes of the DPDP Act**. The provision is broad in its scope as casts obligations not only a data fiduciary but also on an intermediary. Under the Information Technology Act, 2000 (**IT Act**), an intermediary generally refers to a person who, on behalf of another person, receives, stores, transmits or provides services with respect to electronic records. For example, telecom service providers, search engines, etc. Therefore, intermediaries, that are primarily governed by the IT Act, may also be required to maintain and share such information that the Central Government calls for under the DPDP Act.

Information that may be sought. The term 'information' as defined under the IT Act includes data, message, text, images, sound, voice, codes, computer programmes, software, and data bases or micro film or computer generated micro fiche.[3] Given the breadth of this definition, the information that may be sought under Section 36 of the DPDP Act may not necessarily be limited to personal data. Depending on the purpose for which the call for information is made, it may potentially extend to compliance records, governance documents, internal policies, technical information, reports, datasets, or other records maintained by the intermediary or data fiduciary.

Purposes for seeking information. While Section 36 of the DPDP Act confers the power to call for information, Rule 23 read with the Seventh Schedule of the DPDP Rules prescribes the purposes for which such information may be sought and identifies the officers authorized to exercise this power on behalf of the Central Government. The prescribed purposes are as follows:

[1] Section 36, DPDP Act.
[2] Section 2(1)(w), IT Act.
[3] Section 2(v), IT Act.

To use the personal data of a data principal in the interest of sovereignty, integrity, or security of India by the State or any of its instrumentalities.

The person authorised to call for such information would be an officer of the State or any of its instrumentalities as notified by the Central Government under Section 17(2)(a) of the DPDP Act.

To use the personal data of a data principal to either perform any function or disclose any information for fulfilling any obligation under the prevailing laws by the State or any of its instrumentalities.

A call for information under this purpose will be issued by a person authorised under the applicable law.

To assess whether a data fiduciary, or a class of data fiduciaries, should be notified as a Significant Data Fiduciary.

The person authorised to call for such information would be an officer of the Central Government in the Ministry of Electronics and Information Technology (**MeitY**), as designated by the Secretary of the MeitY.

Obligation to maintain confidentiality over disclosure. Where the Central Government considers that the disclosure of the fact that information has been furnished to it may prejudice the sovereignty, integrity, or security of India, it may direct the data fiduciary or intermediary not to disclose the same to the concerned data principal.[4] Such disclosure may be made only with the prior written permission of the authorized person.

The purposes stated above appear to be broadly worded and in absence of effective checks would give sweeping powers to the Central Government to seek information from data fiduciaries and others. In particular, the power to call for information *'in interest of sovereignty, integrity and security of India'* provide considerable latitude to the Central Government to justify access to information. The manner in which such power will be ultimately exercised by the Central Government is yet to be observed. When such call for information takes place after the implementation of the DPDP Act, it will shed light on the manner in which the Central Government is exercising these powers.

Even though the Central Government has wide powers under Section 36 of the DPDP Act to call for information for the outlined purposes, information request by the Central Government should ideally be tested against principles laid down in the *Puttaswamy* judgment which recognized the right to privacy as a constitutional right and directed the State to develop an appropriate framework to provide for the same.[5] The Supreme Court in *Puttaswamy* held that the right to privacy of an individual can only be impugned upon, if it meets the following criteria:

- **Legality**: The call for information must be based on legitimate grounds, as provided by law.
- **Necessity**: The call for information is necessary to achieve a legitimate aim.
- **Proportionality**: The call for information is proportionate and ensures there is a rational nexus between the objects and the means adopted to achieve them.

WHAT DOES IT MEAN FOR BUSINESSES?

Businesses carrying out the functions of a data fiduciary under the DPDP Act or an intermediary under the IT Act can receive such call for information under Section 36 of the DPDP Act, once the DPDP Act and the DPDP Rules are fully in

[4] Rule 23(2), DPDP Rules.
[5] *Justice KS Puttaswamy (retd.) & Anr. v. Union of India*, 2017 SCC OnLine SC 996.

force *i.e.,* on May 13, 2027. As discussed above, the scope of information sought can be broad and go beyond personal data.

While the practical implications of such powers are yet to be seen, businesses must be aware of the possibility of such requests and be prepared to suitably deal with them. Anyone receiving such requests should be careful in responding to them and bear in mind some of the following considerations:

- Careful assessment of the request must be carried out prior to complying with it to ensure that the information requested is received from the authorized sources only and the nature and scope of the information requested is within the ambit of the law.
- Careful examination of possible implications under any existing legal or contractual obligations in relation to the information that the Central Government has sought for.
- Organizations should establish internal protocols for handling governmental information requests. Such protocols should identify responsible personnel, and ensure appropriate involvement of legal, privacy, compliance, and information security teams before any information is furnished.
- Since the Central Government may direct an intermediary or data fiduciary not to disclose the furnishing of information to the concerned data principal, businesses should ensure that their internal response procedures adequately account for such directions and the restrictions accompanying them.
- Suitable legal advice should be taken prior to responding to the information requests.
- The request should be complied with after careful scrutiny to minimize potential exposure, and proper documentation should be maintained in relation to such compliance for evidentiary and audit purposes.

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*

Bhaavi Agrawal, Senior Associate – Email – *bhaaviagrawal@elp-in.com*