INDUSLAW®
THOUGHT LEADERSHIP ... APPLIED

FAQs ON THE DIGITAL PERSONAL DATA PROTECTION BILL, 2023

Authors: Namita Viswanath | Shreya Suri | Naqeeb Ahmed | Ananya Dash | Nikhil Vijayanambi | Ruhi Kanakia

The Lok Sabha passed the 'Digital Personal Data Protection Bill, 2023' ("**DPDPB**") on August 07, 2023, thereby introducing the first comprehensive personal data protection regime in India, after several years of legislative efforts and an inclusive consultation process. It prescribes various obligations on 'data fiduciaries' and 'significant data fiduciaries' while processing the personal data of 'data principals'. Considering the landmark nature of the DPDPB and the fact that a data protection framework for India has been in the pipeline for several years now, as well as the increasing need of an Indian data protection framework that meets global adequacy standards, it appears that this relatively business-friendly version of the DPDPB might be enacted soon, almost in its current form.

The DPDPB, in many ways, will require organisations to take a re-look into their existing information technology policies and processes, to ensure compliance with this new law. In order to help you and your organisation understand the intricacies of the DPDPB and the obligations that you may have to undertake once the same is enacted, we have prepared this document answering pertinent questions on the compliance with the DPDPB, which could come up frequently. We have prepared a note capturing the key provisions of the DPDPB, along with a detailed analysis of the same, which can be accessed here.

ON APPLICABILITY

When do the provisions of the DPDPB come into force?

As on this date, the provisions of the DPDPB are not in force. They will come into force on a date notified in the official gazette by the Central Government. The Central Government may also opt to notify different provisions to take effect on different dates, in a phase-wise manner.

Would my organisation be considered as a 'data fiduciary' or a 'data processor'?

If your organisation collects personal data of data principals for a specified purpose and determines the manner in which such personal data should be processed digitally, your organisation would be a 'data fiduciary' and would have to comply with the obligations on data fiduciaries set out under the DPDPB *(more particularly described in FAQ No. 2(ii))*.

If your organisation only processes personal data on behalf of another organisation, your organisation would be considered as a 'data processor'. In this case, the organisation on whose behalf you are processing such personal data, would be the data fiduciary.

In what scenarios would my entity be treated as a significant data fiduciary?

There are no prescribed criteria stipulated under the DPDPB to be construed as a 'significant data fiduciary'. The Central Government may, at its discretion, notify any data fiduciary or a class of data fiduciaries as a 'significant data fiduciary' after an assessment of some relevant factors, such as:

- The volume and sensitivity of personal data processed by the data fiduciaries;
- The risk to the rights of data principals;
- The potential impact on the sovereignty and integrity of India;
- The risk to electoral democracy;
- The security of the state; and
- Public order.

Therefore, your organisation will only be considered a 'significant data fiduciary' if it falls within the specified class of data fiduciaries, and fulfils the prescribed criteria, as may be notified by the Central Government in the future.

Who is considered as a 'data principal' for the purposes of data processing?

A data principal is the individual to whom the personal data relates. However, when the personal data is in relation to a child, the data principals would include the parents or lawful guardians of such child; and when the personal data is in relation to a person with disability, the data principal would include her lawful guardians acting on her behalf.

Note that 'processing' has been defined under the DPDPB as a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

What type of data does the DPDPB apply to?

The DPDPB is applicable to the processing of personal data in following scenarios:

- Processing of personal data collected in digital form (i.e., digital personal data); and
- Processing of personal data collected in non-digital form and digitised subsequently.

However, the provisions of the DPDPB will not apply if:

- You are an individual processing personal data for any personal or domestic use; or
- You are processing personal data that has been made publicly available by the data principal or any other person who is under an obligation under Indian laws to make such personal data publicly available.

Are there different categories of personal data?

Unlike the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**SPDI Rules**"), which categorises personal data into 'personal information' and 'sensitive personal data or information', the DPDPB does not classify personal data sets into different categories. It treats all digitised personal data uniformly.

Will the compliances under the Information Technology Act, 2000 remain applicable to my organisation post the implementation of the DPDPB?

Yes, the compliances under the Information Technology Act, 2000 ("**IT Act**") will continue to apply post the enactment of the DPDPB. However, Section 43A of the IT Act *(compensation for failure to protect sensitive personal data)* and the rules framed thereunder (i.e., the SPDI Rules) – which is largely the current data protection framework in India, is proposed to be repealed by the DPDPB (upon enactment and notification of the relevant section). That said, other provisions of the IT Act will continue to remain applicable. However, in case of any inconsistencies between the provisions of the IT Act and DPDPB, it is proposed that the provisions of DPDPB would prevail.

ON GENERAL OBLIGATIONS ON DATA FIDUCIARIES

I am operating an offshore online platform and I offer my services to data principals in India – do the provisions of the DPDPB apply to me?

The provisions of the DPDPB primarily apply to the processing of personal data within the territory of India.

For processing of personal data by organisations outside India, the DPDPB only applies to a limited extent, i.e., when an organisation outside India processes the personal data of the data principals located in India, in order to offer any goods or services to them.

This means, if you are operating an offshore online platform offering your goods and / or services to the users in India and process the personal data of such users in order to offer such goods and / or services to them, you would be considered as a data fiduciary under the DPDPB and would have to comply with the obligations set out therein.

As a data fiduciary, what are the obligations I have under the DPDPB?

Your obligations as a data fiduciary under the DPDPB will, inter alia, include:

a. **General obligations:**
   - Ensuring that you are only collecting personal data of data principals for a lawful purpose;
   - Ensuring that personal data processed by you is complete, accurate and consistent;
   - Implementing an appropriate technical and organizational measures to ensure effective observance of the provisions of the DPDPB;
   - Implementing reasonable security safeguards to prevent personal data breach and protect the personal data in its possession;
   - Transferring personal data for processing to any country outside India, as permissible under DPDPB, only in accordance with the terms and conditions prescribed by the Central Government.

b. **Obligation to provide notice:** If you want to request the consent of a data principal to process her personal data, you must provide a notice to the data principal, in clear and plain language, along with a request for consent. The data principal must be given the option to access the contents of the notice in English or any of the 22 (twenty-two) languages specified in the Constitution of India. If a data principal has given her consent before the commencement of the DPDPB, then you must provide such data principal with such notice, in the same manner as mentioned above as soon as it is reasonably practicable.

   The notice must contain:

   - A description of the personal data sought to be collected from the data principal and the purpose for its processing;
   - the manner in which the data principal may exercise her right to withdraw consent and to grievance redressal; and
   - the manner in which the data principal may make a complaint to the Data Protection Board ("**Board**").

c. **Obligation in relation to requesting consent:** You can only process the personal data of a data principal - (i) for which the data principal has provided her consent *(except in cases of legitimate uses, more particularly described*

in FAQ No.4(iii)); and (ii) which is required for the specific purpose for which consent has been sought, and nothing further. Every request for consent should be provided in the following manner:

- It must be presented in clear and plain language; and
- It must contain the contact details of the person authorised by you to respond to any communication from the data principal.

You must also ensure that you allow the data principal to withdraw her consent at any time, as easily as she has been allowed to provide her consent.

d. **Obligation to correct and erase personal data:** If a data principal requests you to correct, complete or update her personal data for which she has previously given consent to process, you must correct, complete, or update the same in accordance with such data principal's instructions.

Additionally, you must ensure that you erase the personal data of the data principal, and that your data processor also erases any personal data of the data principal, on the occurrence of either of the following:

- The data principal requests you to erase her personal data;
- The data principal withdraws her consent;
- It has become reasonable to assume that the purpose for which the personal data was collected is no longer being served by retaining the personal data; or
- Retention of the personal data is no longer necessary for compliance with any law.

d. **Obligations while processing personal data of children:** While processing the personal data of a child, you must:

- Obtain the verifiable consent of the parents or lawful guardians before processing her personal data in a manner as may be prescribed by the Central Government;
- Ensure that you do not process any personal data of a child in a manner which may be detrimental to the well-being of the child;
- Ensure that you do not monitor the behaviour of any child or target advertising directed at children.

However, the obligation (i) of obtaining verifiable consent; and (ii) to not undertake the behaviour monitoring of children or target advertisements directed at children, can be done away with for specific data fiduciaries or for certain purposes, as may be prescribed by the Central Government. Additionally, the Central Government can exempt certain data fiduciaries from complying with this obligation by reducing the age limit for seeking verifiable parental consent, subject to a determination by the Central Government that the processing is being carried out in a verifiably safe manner.

e. **Obligations while processing personal data of persons with disabilities:** While processing personal data of a person with disability, you must obtain the verifiable consent of the lawful guardians, before processing the personal data of such person with disability, in a manner as may be prescribed by the Central Government.

f. **Grievance Redressal:** You are required to establish an effective mechanism to redress the grievances of data principals.

g. **Obligation to provide information:** If the data principal requests you for access to the following types of data, you must provide access to the same:

- A summary of the personal data of the data principal which is being processed by you and the processing activities undertaken by you with respect to such personal data;

- The identities of any other data fiduciaries and data processors with whom the personal data has been shared;
- The description of the personal data shared with such other data fiduciaries or data processors; and
- Any other information as may be prescribed by the Central Government.

However, the obligation to provide the identities of the data fiduciaries as well as the type of personal data shared with them will not apply if the personal data has been shared pursuant to a request made in writing by such other data fiduciary in order to prevent, detect, or investigate offences or cyber incidents, or for the prosecution or punishment of offences.

Are there differing obligations for me as a data fiduciary, as compared to a significant data fiduciary?

Unlike the SPDI Rules which prescribe uniform requirements for all types of data fiduciaries, the DPDPB imposes additional obligations on data fiduciaries notified as significant data fiduciaries. In addition to the obligations of a data fiduciary as captured in FAQ No. 2(ii), a significant data fiduciary has the following obligations:

a. **Undertaking additional measures:** The significant data fiduciary must undertake a periodic data protection impact assessment, a periodic audit, and any other measure as may be prescribed by the Central Government.

b. **Appointing a data protection officer:** The significant data fiduciary must appoint a 'data protection officer' ("**DPO**") to serve as the point of contact for the grievance redressal mechanism of the significant data fiduciary. The DPO must be based in India and be responsible to the board of directors or a similar governing body of the significant data fiduciary. The significant data fiduciary must provide the business contact details of such DPO, along with every request for consent made to the data principal.

c. **Appointing an auditor:** The significant data fiduciary must appoint an independent data auditor to evaluate the compliance of the significant data fiduciary with provisions of the DPDPB.

What is a data protection impact assessment? Does my organisation need to undertake a data protection impact assessment?

A data protection impact assessment requirement is applicable to significant data fiduciaries. It involves an assessment of the - (i) description of the manner in which the personal data is processed; (ii) the purpose of processing personal data; (iii) the harm in relation to the processing of personal data and the measures for managing the risk of such harm; and (iv) such other matters with respect to processing of personal data, as may be prescribed by the Central Government.

Your organisation will be required to undertake a data protection impact assessment, only if your organisation is classified as a significant data fiduciary.

What is a data protection impact assessment? Does my organisation need to undertake a data protection impact assessment?

A data protection impact assessment requirement is applicable to significant data fiduciaries. It involves an assessment of the - (i) description of the manner in which the personal data is processed; (ii) the purpose of processing personal data; (iii) the harm in relation to the processing of personal data and the measures for managing the risk of such

harm; and (iv) such other matters with respect to processing of personal data, as may be prescribed by the Central Government.

Your organisation will be required to undertake a data protection impact assessment, only if your organisation is classified as a significant data fiduciary.

My organization is compliant with all personal data related obligations currently in force under the SPDI Rules. Once the DPDPB is enacted, what are the additional obligations that my organisation needs to comply with?

If your organisation is currently compliant with all personal data related obligations currently in force, you will still need to take relevant steps to comply with the DPDPB once it is enacted. The following are some of the additional obligations that your organisation will need to comply with:

- **Obtaining consent from individuals before collecting or processing personal data.** The DPDPB requires your organisation to obtain consent in the prescribed manner (more particularly described in FAQ No. 4(iv)) from individuals before collecting or processing the personal data of the data principals. This consent must be free, specific, informed, unconditional and unambiguous.
- **Implementing appropriate security measures to protect personal data.** The DPDPB requires organisations to implement appropriate security measures to protect all types of personal data from a personal data breach, as opposed to implementing such measures only for sensitive personal data, which is the current requirement under the SPDI Rules.
- **Allowing access to data principal's personal data.** The DPDPB gives the data principal the right to access to her personal data that is held by a data fiduciary. The data principal also has the right to request an organisation to correct, complete, update or erase her personal data. Hence, your organisation will need to enable these rights.
- **Reporting data breaches to the Board.** The DPDPB requires organisations to report data breaches to the Board as well as to the affected data principals.

In addition to these obligations, the DPDPB introduces a number of other provisions your organisation will need to be aware of. You will accordingly need to reassess your organisation's data processing policies and practices, including appropriate user experience and interfaces, to ensure that the same are aligned with the DPDPB and the rules to be issued thereunder. Please refer to our comprehensive note on the DPDPB (available here) for more details.

ON OBLIGATIONS IN RELATION TO PROCESSING PERSONAL DATA OF A CHILD

Who is a 'child' for the purposes of data processing?

A child for the purpose of data processing means an individual who has not completed eighteen years of age.

Can my organisation process children's personal data? If yes, what are the dos and don'ts applicable to me?

Yes, your organisation can process children's personal data, subject to the following conditions:

- You obtain verifiable consent of the parents or lawful guardians of the child, before processing her personal data;
- You ensure that you do not process any personal data of a child in a manner which may be detrimental to the well-being of the child; and
- You ensure that you do not monitor the behaviour of any child or target advertisements directed at children.

ON CONSENT AND LEGITIMATE USE

What can I consider to be valid 'consent' of a data principal while processing her personal data? Would notice or a click wrap mechanism be regarded as a valid consent?

For consent to be considered valid under the DPDPB, it must be free, specific, informed, unconditional and unambiguous. The data principal must provide a clear affirmative action signifying agreement to the processing of her personal data for the specified purpose and limited to such personal data as is necessary for the specified purpose. A click wrap mechanism i.e., a click to accept can be considered a valid form of consent if it meets the above criteria.

What are the consequences of a data principal withdrawing her consent?

If a data principal withdraws her consent to the processing of personal data, your organisation must, within a reasonable time, cease, and ensure that any other entity processing her personal data on behalf of your organisation, ceases processing of the personal data of such data principal. If a data principal withdraws her consent to process her personal data for a particular purpose, your organisation or any other entity processing her personal data on behalf of your organisation, must stop processing her personal data for that purpose. However, if your organisation has already processed the personal data for that purpose before the withdrawal of consent, the processing that was done before the withdrawal of consent will still be considered lawful.

What are the legitimate uses, where my organisation does not require to obtain consent of the data principals?

In the context of DPDPB, your organisation may process the personal data of a data principal for any of the following legitimate uses without obtaining the specific consent of the data principal:

In relation to private organizations:

- For specified purposes where a data principal has voluntarily provided her personal data to you and has not indicated that she does not consent to the use of her personal data;
- For purposes of employment or for safeguarding an employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a data principal who is an employee;
- For fulfilling an existing legal obligation to disclose any information to the state or any of its instrumentalities. This is, however, subject to the processing being in accordance with the information disclosure requirements under any law in force;
- For responding to a medical emergency involving a threat to the life or immediate threat to the health;
- For taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health;
- For taking measures to ensure safety of, or provide assistance or services to, any individual during any disaster, or any breakdown of public order.

Additional grounds in relation to the state or instrumentalities of the state:

- To provide any subsidies, benefits, services, certificates, licences or permits to a data principal if:
  a. The data principal has previously consented to the processing of her personal data by the state or any of its instrumentalities for the subsidies, benefits, services, certificates, licences or permits; or
  b. Such personal data is available in digital form in, or in non-digital form and digitised subsequently from any database, register, book or other document which is maintained by the state or any of its instrumentalities and is notified by the Central Government.

However, this exemption is subject to the processing of personal data being in accordance with the policies issued by the Central Government, or under any law for governance of personal data.

Do I need to provide a notice to my data principal every time I seek her consent? What is the form and manner of provision of notice?

Yes, every time your organisation seeks the consent of a data principal, you must provide a notice to the data principal in clear and plain language, containing a description of the personal data sought to be collected and the purpose of processing such personal data. This must be provided either preceding or at the time of making a request for consent.

The notice must be provided in writing or by electronic means, or in any other manner as may be prescribed by the Central Government and must be easily accessible to the data principal. It is important to note that if the data principal has given her consent to process her personal data for a specific purpose before the commencement of the DPDPB, your organisation must provide a notice to the data principal as soon as possible, (a) describing the personal data and the purpose of its processing; (b) the manner in which she may exercise her rights to withdraw consent and to grievance redressal; and (c) the manner in which she may make a complaint to the Board. You may continue to process the personal data, unless the data principal withdraws her consent.

Who is a consent manager? What role do they play in the collection and processing of personal data?

A consent manager is a person or an entity that acts on behalf of the data principal. The consent manager enables a data principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform. A consent manager has to be registered with the Board, and must adhere to the technical, operational, financial, and other conditions as may be prescribed by the Central Government.

Can I collect personal data available in public domain and process the same without the consent / notice to the data principals?

The DPDPB does not apply to personal data made publicly available by the data principals voluntarily or made available by any other person who is under an obligation under the Indian laws to make such personal data publicly available. As a result, no consent/notice obligations will be triggered when it comes to processing such type of publicly available personal data.

ON THE RIGHTS OF DATA PRINCIPALS

Does a data principal have a right to access, update or request erasure of her data? What is my organisation's obligation with respect to above?

Yes, every data principal will have a right to access, correct, complete, update or request the erasure of the personal data you have processed. Your organisation must ensure that data principals are allowed to access, correct, complete, update and request the erasure of her personal data. When requested, your organisation must accordingly correct the inaccurate or misleading personal data, complete the incomplete personal data, or update the personal data. Upon receipt of a request to erase the personal data, you must erase such personal data unless retention of the same is necessary for a specified purpose or for compliance with any law.

If a data principal has already signified her consent to allow my organisation to share her personal data with another organisation, does my organisation have to specify the details of all other organisations with whom the personal data will be / has been shared?

There is no obligation on you to upfront disclose the details of recipients of personal data (i.e., organisations to whom you are sharing the personal data) with the data principals. However, under the DPDPB, the data principal has a right to request for the identities of such recipients, in which case, you will be bound to provide such details to the data principal.

Can a data principal nominate someone on her behalf to exercise her rights?

Yes, a data principal does have the right to nominate someone on her behalf for the purpose exercising her rights, in case of her death or incapacity. The nominee will act on behalf of the data principal in the event of her death or if the data principal is unable to exercise her right due to unsoundness of mind or infirmity of body.

If a data principal has a grievance regarding our data processing processes, does she first approach my organisation or the Board?

The data principal must first file a grievance with your organisation before she can approach the Board.

What are my organisation's obligations with respect to providing a grievance redressal mechanism for my users?

Your organisation must enable all data principals to contact and file the grievances they may have with regard to acts or omissions by your organisation, or to exercise her rights under the provisions of the DPDPB. Your organisation may designate a grievance officer to ensure compliance with this requirement.

ON PROCESSING OF PERSONAL DATA OUTSIDE INDIA

Is there a concept of data processors and data controllers (similar to the General Data Protection Regulation ("GDPR")) under the DPDPB?

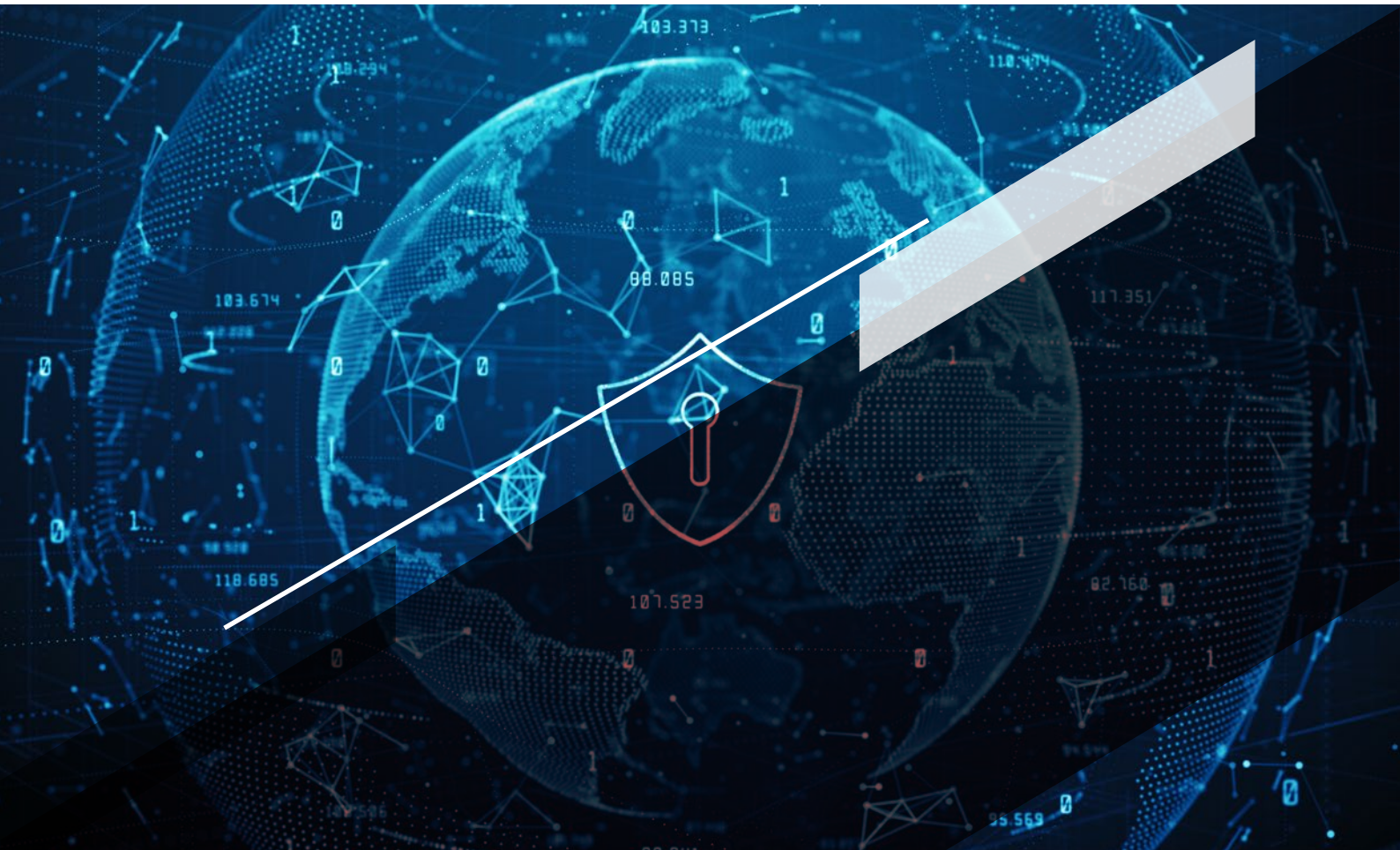
The DPDPB also recognises the concept of data controllers and data processors under the GDPR, as data fiduciaries and data processors, respectively.

Can my organisation transfer personal data outside of India?

Yes, subject to certain conditions. The DPDPB allows the Central Government to restrict the transfer of personal data outside India to certain countries which it may notify in due course. However, this will not interfere with the applicability of any law in India which prescribes a higher degree of protection or restriction on a data fiduciary while transferring personal data outside India.

Are there any restrictions with regard to retaining personal data only inside India?

No, the DPDPB does not require personal data to be retained only in India. However, depending on the nature of the business undertaken by your organisation, restrictions or conditions may be placed by sectoral laws and regulations, which may be applicable to your organisation.



ON EXEMPTIONS UNDER THE DPDPB

My organisation is an MSME, will my organisation have to comply with all the obligations under the DPDPB?

All obligations imposed on data fiduciaries will apply to your organisation, even if you are an MSME.

My organisation is a startup, will my organisation have to comply with all the obligations under the DPDPB?

All obligations imposed on data fiduciaries will apply to your organisation, even if you are a startup. However, the Central Government has the power to notify certain categories of startups, depending on the volume and nature of personal data processed, to whom certain provisions of the DPDPB will not apply.

Note that 'startup' is defined under DPDPB to mean a private limited company or a partnership firm or a limited liability partnership incorporated in India, which is eligible to be and is recognised as such in accordance with the criteria and process notified by the department to which matters relating to startups are allocated in the Central Government.

My organisation is an IT/ITeS entity and processes data of foreign residents. Do I have to comply with the DPDPB in respect of personal data of such foreign residents?

The DPDPB is applicable to all data fiduciaries that process personal data within the territory of India, and only in some instances, to data fiduciaries that process personal information outside India *(more particularly described in FAQ No. 2(i))*. However, processing of personal data by a person within India, of data principals not within the territory of India in furtherance of a contract with such person outside India, has been exempted from complying with Chapter II *(Obligations of Data Fiduciary)* and Chapter III *(Rights And Duties of Data Principal)* of the DPDPB, with the exception of implementing reasonable security safeguards to protect the personal data in their possession.

ON THE DATA PROTECTION BOARD

In case of a personal data breach, what should my organisation do?

In the event of a personal data breach, your organisation must notify the Board and each of the affected data principals of the breach, and the nature of the leaked personal data. The Central Government will issue directions in the form and manner in which to notify the Board and affected data principals of a personal data breach.

What are the penalties that can be imposed under the DPDPB?

The penalties that may be imposed varies depending on the nature of the non-compliance and the same are as follows:

Sl. No	Breach of provisions of the DPDPB	Penalty
1	Breach in observing the obligation of a data fiduciary to take reasonable security safeguards to prevent personal data breach	Up to INR 250,00,00,000 (Indian Rupees Two Hundred and Fifty Crores)
2	Breach in observing the obligation to give the Board or affected data principal notice of a personal data breach	Up to INR 200,00,00,000 (Indian Rupees Two Hundred Crores)
3	Breach in observance of additional obligations in relation to children	Up to INR 200,00,00,000 (Indian Rupees Two Hundred Crores)
4	Breach in observance of additional obligations of 'significant data fiduciary'	Up to INR 150,00,00,000 (Indian Rupees One Hundred and Fifty Crores)
5	Breach in observance of the data principals' duties	Up to INR 10,000 (Indian Rupees Ten Thousand)
6	Breach of any terms of the voluntary undertaking made by a person and accepted by the Board	Up to the extent applicable for the breach in respect of which the proceedings were initiated under the DPDPB.
7	Breach of any other provision of DPDPB or the rules made thereunder.	Up to INR 50,00,00,000 (Indian Rupees Fifty Crores)

What actions can the Board take if there is an inquiry into my organisation?

Apart from imposing penalties, the Board is empowered to direct the implementation of any remedial or mitigation measures to control a personal data breach. The Board is also empowered to refer your organisation and the affected data principals to a mediation process. Further, the Board may accept an undertaking from your organisation to take or refrain from taking certain actions in exchange for not continuing proceedings before the Board.

Rather than approaching the Board, can I approach the court for damages against my organisation handling my personal data?

No, civil courts do not have the jurisdiction to hear matters that fall within the purview of the Board. However, you may appeal the order of the Board by approaching the Telecom Disputes Settlement and Appellate Tribunal within 60 (sixty) days of issuance of an order by the Board.

What rights do the data principals have against my organisation in the event of a data breach?

In the event of a personal data breach, the data principal shall be required to exhaust the opportunity of redressing her grievance and subsequently may intimate the Board of the breach, leading to an inquiry into your organisation.

ON GOVERNMENT ACCESS

Do the obligations of data fiduciaries under the DPDPB also apply to the government and its agencies?

Yes. However, the instrumentalities of the state can be exempted from the provisions of the DPDPB if it is in relation to processing of personal data in the interests of sovereignty and integrity of India, security of the state, friendly relations with foreign states, maintenance of public order or preventing incitement to any cognizable offence relating to any of these. Additionally, the obligation to erase the personal data of data principals does not apply to the personal data processed by the state or the instrumentalities of a state.

Does the Central Government have access to the personal data collected by my organisation, and can my organisation refuse to disclose said personal data?

The Central Government has the power to ask the Board or any data fiduciary (including your organisation as a data fiduciary) to provide them with such information as it may call for, and in such an instance, your organisation will have to comply with such a request.

NEXT STEPS

What should I do next while I wait for DPDPB to come into effect?

It is recommended that you establish an internal team dedicated to data protection, responsible for formulating suitable protocols and strategies aligned with the DPDPB. This encompasses the establishment of reporting standards, the management and response to cybersecurity incidents, and the timely handling of data principals' requests. Adaptations to your company's information technology infrastructure and operational procedures, such as consent collection and processing parameters, are essential to ensure robust data security measures. Appropriate changes to any user experience and interface of your digital platforms may also be necessary.

Concerning existing personal data in your possession / control, it is advisable to identify inactive data principals and follow data retention policies to delete such records. Active data principals will need to provide consent for the utilization of the personal data – a privacy notice in line with the requirements of the DPDPB will need to be provided to them and you can continue processing the personal data of such data principals has withdrawn her consent. Further, it is also pertinent that you revisit your data processing framework to evaluate the nature of data sets collected, means and type of processing, the manner of its collection, the scope of the current consent forms, the data storage and retention protocols, data transfer mechanism etc., and ensure to set a process to align the same with the requirements under the DPDPB. Additionally, you may also have to relook at your data processing, data sharing and other data related contracts with third parties (including data process) in the context of DPDPB. Given the substantial repercussions of non-compliance, including significant fines and operational disruptions, it is crucial to prioritize and dedicate substantial efforts to ensure ongoing data compliance.

For any further queries on the DPDPB, please reach out to us at data.queries@induslaw.com

INDUSLAW
THOUGHT LEADERSHIP ... APPLIED

www.induslaw.com

OUR OFFICES

BENGALURU
101, 1st Floor, "Embassy Classic"# 11
Vittal Mallya Road
Bengaluru 560 001
T: +91 80 4072 6600
F: +91 80 4072 6666
E: bangalore@induslaw.com

HYDERABAD
204, Ashoka Capitol, Road No. 2
Banjarahills
Hyderabad 500 034
T: +91 40 4026 4624
F: +91 40 4004 0979
E: hyderabad@induslaw.com

CHENNAI
#11, Venkatraman Street, T Nagar,
Chennai - 600017 India
T: +91 44 4354 6600
F: +91 44 4354 6600
E: chennai@induslaw.com

DELHI & NCR
2nd Floor, Block D
The MIRA, Mathura Road, Ishwar Nagar
New Delhi 110 065
T: +91 11 4782 1000
F: +91 11 4782 1097
E: delhi@induslaw.com

9th Floor, Block-B
DLF Cyber Park
Udyog Vihar Phase - 3
Sector - 20
Gurugram 122 008
T: +91 12 4673 1000
E: gurugram@induslaw.com

MUMBAI
1502B, 15th Floor
Tower – 1C, One Indiabulls Centre
Senapati Bapat Marg, Lower Parel
Mumbai – 400013
T: +91 22 4920 7200
F: +91 22 4920 7299
E: mumbai@induslaw.com

#81-83, 8th Floor
A Wing, Mittal Court
Jamnalal Bajaj Marg
Nariman Point
Mumbai – 400021
T: +91 22 4007 4400
E: mumbai@induslaw.com