



Decoding the Digital Personal Data Protection Act 2023 for **BUSINESSES**

The DPDP Act 2023 is comprehensive, and aims at striking a balance between the rights of individuals and the data processing requirements of business



Key Takeaways for Businesses From Digital Personal Data Protection Act 2023

1. TO WHOM DOES IT APPLY?
2. PRIVACY ASPECTS TO FOLLOW FOR BEING COMPLIANT AND EASE OF DOING BUSINESS
3. THE ACT ENSURES EASY COMPLIANCE
4. WATCH OUT FOR THE PENALTIES IN CASE OF NON-COMPLIANCE
5. PRIVACY ENABLEMENT – A BOON FOR BUSINESS GROWTH



SECTION 1

TO WHOM DOES IT APPLY?



The DPDP Act 2023 applies to the processing of digital personal data, whether it's gathered in a digitized format or initially collected in a non-digital form and then transformed into digital data.



Foreign entities which process personal data to offer goods and services to Data Principals within the territory of India.



Does not apply to the processing of personal data by an individual for personal or domestic purposes, nor does it apply to the processing of publicly available personal data.



The State and its instrumentalities are exempted when processing of personal data is for specified purposes. The Central Government can also notify certain classes of Data Fiduciaries as being exempt from some key obligations under the Act. This includes exemptions that may be notified in favour of startups.



SECTION 2

PRIVACY ASPECTS TO FOLLOW FOR BEING COMPLIANT AND EASE OF DOING BUSINESS



Businesses can process data only for lawful purposes based on consent and for certain other legitimate uses in accordance with requirements laid under the Act or any other applicable rules or regulations enacted under it.



To obtain informed consent, it is required to furnish a notice in clear and plain language (English and the Scheduled languages) containing a description of personal data and its intended use.



Businesses are expected to put the necessary organizational and technical safeguards to ensure compliance with the Act, and take reasonable security safeguards to prevent any breach of personal data.





Publish business contact information of a Data Protection Officer (DPO) or of any other person who is responsible for responding to individuals' inquiries about the processing of their personal data.



Businesses may engage, appoint, use, or involve a data processor to process personal data on its behalf only under a valid contract.



Obtain verified parental consent while processing children's data and to not undertake any processing which could have a detrimental impact on the well-being of a child.



A notified Significant Data Fiduciary (SDF) is required to appoint a Data Protection Officer (DPO) and an independent data auditor to assess SDFs compliance with the Act.



The Act allows the transfer of data to other jurisdictions unless otherwise notified by the Central Government. A negative list approach is followed for cross-border data transfers.



SECTION 3

THE ACT PROVIDES MULTIPLE CHANNELS FOR COMPLIANCE

- ✓ To ensure the enforcement and compliance of this Act, a Data Protection Board is established.
- ✓ Availability of alternate dispute resolution mechanisms to settle disputes.
- ✓ To encourage businesses to act proactively in ensuring legally compliant data processing.



SECTION 4

WATCH OUT FOR THE PENALTIES IN CASE OF NON-COMPLIANCE

Significant non-compliance attracts financial penalties as mentioned in the schedule based on assessment of certain factors.

! Failure to implement security safeguards for preventing data breach – **Up to Rs. 250 crore**

! Failure to notify the Board and affected principals of data breach – **Up to Rs. 200 crore**

! Non-compliance with obligations regarding children's data – **Up to Rs. 200 crore**

! Breach of additional obligations by Significant Data Fiduciary – **Up to Rs. 150 crore**

! Any other non-compliance –
Penalty– **Up to Rs. 50 crore**



SECTION 5

PRIVACY ENABLEMENT – A BOON FOR BUSINESS GROWTH



- ✓ Privacy protection builds digital trust and promotes efficiency.
- ✓ Encourages privacy technology innovation.
- ✓ Privacy-compliant data processing enables data-driven decision making and creates value for an organization.
- ✓ Transparency and accountability standards provide a competitive edge.
- ✓ Privacy protection reduces business risks and simplifies compliance.
- ✓ Enhances credibility and creates consumer trust in services.