



DIGITAL PERSONAL DATA PROTECTION BILL 2023:

Provisions, Controls & Tools

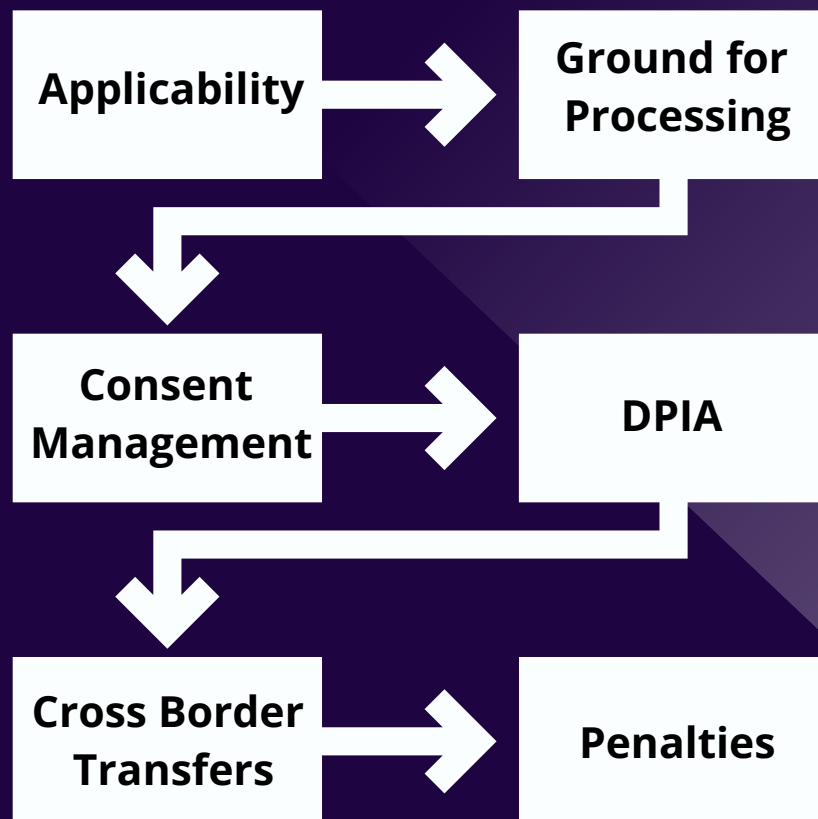


Table of Contents

A. Introduction

B. Executive Summary

C. Restriction on Disclosure

D. Provisions Analyzed

D1. Applicability

D2. Grounds of Processing

D3. Consent

D4. Data Controllers & Data Processors

D5. Significant Data Fiduciary

D6. Children's Personal Data

D7. Rights of Data Principals

D8. Cross Border Transfer of Personal Data

D9. Data Protection Board

E. Conclusion

A. Introduction

This paper is an in-depth analysis of the newly introduced Digital Personal Data Protection Bill 2023, which has been passed in the Lok Sabha. The Bill is a simple and lean piece of law representing India's position on data protection principles vis-à-vis the roles and responsibilities of individuals & businesses. It highlights the key provisions of the Bill that the organizations will have to look into before they embark on their privacy compliance journey.

B. Executive Summary

Ten key provision sets have been identified and explained clearly without diluting their legal consequences. The report provides for a comparison with Bill's global contemporaries. Further, the paper also provides a compliance roadmap in order to fulfill the mandate of the provisions that have also been laid down.

The paper is a point-in-time review and the observations and recommendations are made based on the framework of the 2023 Bill.

C. Disclaimer

The information presented in this document is provided as-is and shall not be construed as legal advice. The assessment is a "point in time" analysis dependent on the 2023 Bill. Due to any changes made to the Bill, the findings at a later stage may not be the same as those reflected in this report. This is not a legal advice & should only be used for reference purposes.

D. PROVISIONS ANALYZED

D1. Applicability

Section 3:

The 2023 Bill applies to processing of **“digital” personal data** i.e., the data is collected online, or collected offline but digitized subsequently within the Indian territory. The 2023 Bill also applies to processing of personal data outside India in cases, where there is an offering of goods and services to Data Principals within the territory of India.

This provision exempts processing of personal data when:

- an individual for personal or domestic purposes,
- personal data that has been made public by a data principal or under a legal obligation, or
- personal data that is necessary for research, archiving, or statistical purposes and data is not used for data principal-specific decisions and the processing complies with government-prescribed standards.

Comparison to its Previous Iterations

The Draft Bill of 2022 had previously proposed the applicability of the Bill to processing of digital personal data as well as where profiling and offering of goods and services were targeted at India.

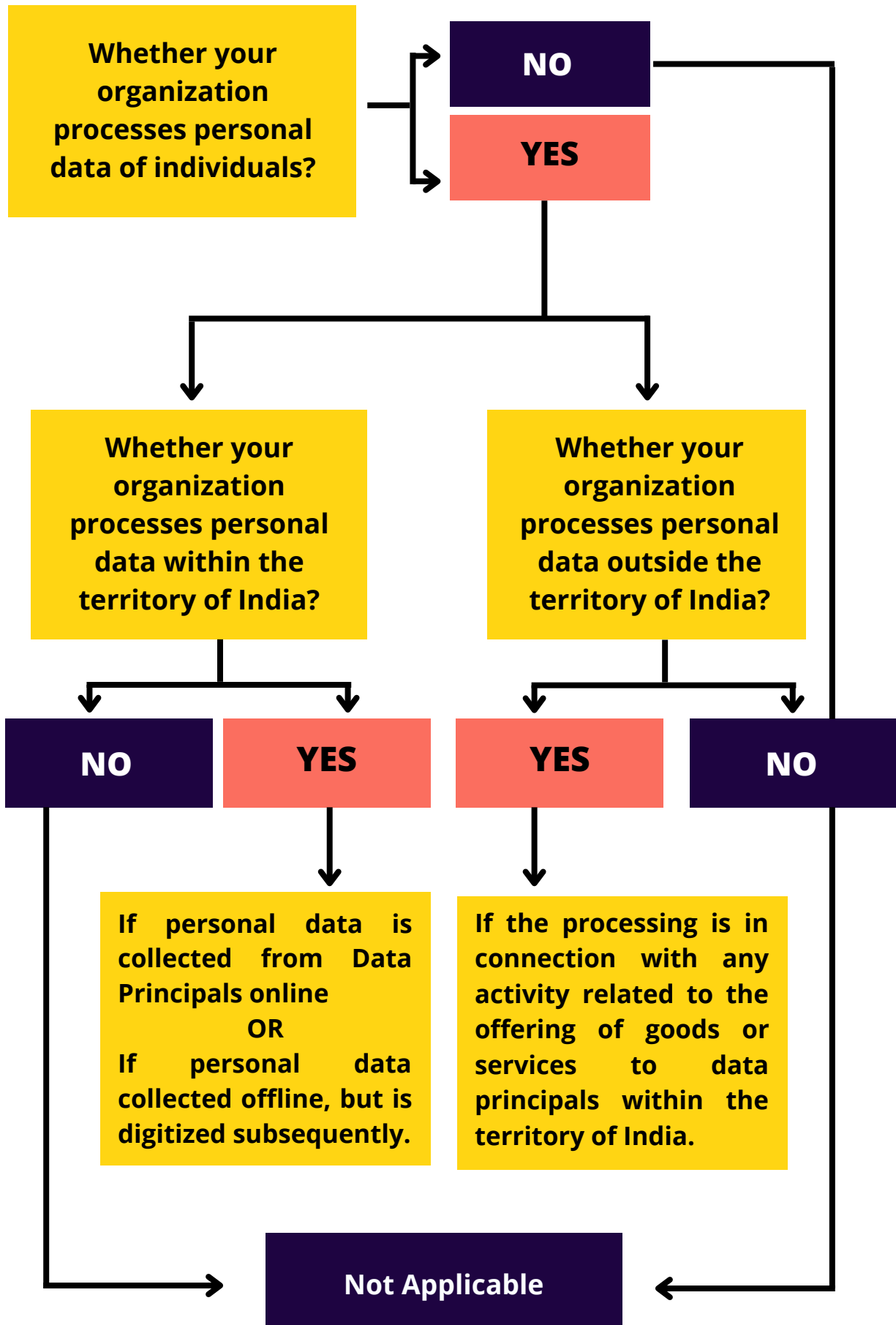
The Joint Parliamentary Committee had previously proposed a change in applicability of the data protection legislation to personal & non-personal data, under the Data Protection Bill, 2021. But this Bill only extends the applicability to personal data in a digitized format.

Compliance Road-Map

Before organizations begin their **compliance journey** and strategize their **policies and procedures**, they must strictly look into the applicability of the Bill on their format of processing. Questions to consider can be:

1. What are the sources of data collection?
2. Is processing done within the Indian territory or outside but the goods/services are targeted at the Indian population?
3. Is there any process set in place to digitize data collected offline?

Applicability Matrix



D2. Grounds for Processing Digital Personal Data

Section 4:

Processing shall be considered to be **legitimate** if it aligns with the provisions of the 2023 Bill, or where the Data Principal has given her **consent**, and is for a lawful purpose. Lawful purpose has been defined as any purpose that is **not prohibited by law**.

FINANCIAL PENALTY:  Upto 50 crores

Comparison to Other Laws

The Draft Bill of 2022 provided processing of digital personal data for lawful purposes including when in circumstances when deemed consent is provided by an individual.

European Union: GDPR lays down grounds for processing under Article 6. These are: legitimate interest, consent, vital interest, contractual necessity, public interest and legal obligation

Compliance Road-Map

Lawful basis or legal grounds for processing digital personal data acts as a shield for organizations against regulatory and financial penalties. Additionally, choosing a legitimate purpose for processing aids the business to limit its processing within the contours of the law and attracts consumer trust and builds goodwill.

In order to assess the legal ground to rely on, organizations should keep in mind the following:


1. Is the purpose of processing legitimate or is the purpose in violation of any law in force?
2. Whether the grounds for processing personal data is proportional to the rights vested with the data principals?

D3. Consent

Section 6:

The 2023 Bill emphasizes on a person's **right to know** what personal information a Data Fiduciary is collecting and the reason behind such collection. The Bill provides that valid consent needs to be **specific, informed, unconditional and unambiguous** and involves a **clear affirmative action** which should **signify agreement to the processing** of the individual's **personal data** for the specified purpose.

The **Notice-related requirements** under the 2023 Bill focus on three things: it has to be written in **clear words**, it has to be in **simple language** and be available in the **languages listed on the Eighth Schedule of the Constitution of India**. Consent should not be irrevocable and permanent, and the Data Principal may withdraw consent at any time. The Bill stipulates that consent of data principles should be managed by a Consent Manager.

FINANCIAL PENALTY:  Upto 50 crores

Comparison to Other Laws

GDPR, under Article 7, discusses consent and its essentials. Consent has to be freely given, unambiguous, in clear and plain language. There must also be an option to withdraw consent.

Compliance Road-Map

Consent management is a hallmark of the bill and therefore **solutions and tools** can help **automate consent management**. In order to assess the legal ground to rely on, organizations should keep in mind the following:

1. When should Data Principals be **notified** of processing their personal data?
2. Whether the notice contains the required information in **clear and plain language**?
3. Is the notice **itemized**?
4. Is there a process for the **withdrawal of consent** being provided?

D4. Data Fiduciaries

Section 8:

Data Controllers have been termed as **Data Fiduciary** under the 2023 Bill. There are obligations laid down on such data fiduciaries for **processing of personal data accurately and in line with legitimate uses** (Section 7), **deletion and retention** of personal data, **breach notification**, **grievance management**, **processor management** and implementation of **technical and organizational safeguards** to efficiently protect personal data.

FINANCIAL PENALTY:  Upto 250 crores

Comparison to Other Laws

Under the GDPR, data controllers are the organizations with a horizon of responsibilities and obligations. Data controllers are the organizations that define the purpose and means of data processing, just like under the Indian Bill.

Compliance Road-Map

For a well-rounded compliance framework, Data Fiduciaries have to identify the privacy risks in the organization and accordingly undertake **Data Inventories**, Data Protection Impact Assessments (**DPIA**), and draft appropriate **Data Processing Agreements with Processors**.

- 1.Has the organization **defined appropriate time-periods** for data retention and deletion?
- 2.Are there **efficient mechanisms** in place to ensure grievances and personal data breach management?
- 3.Are there **technical and organizational measures** established to ensure adherence to the provisions of the bill?
- 4.Are there reasonable measures in place to secure personal data from breach incidents?

D5. Significant Data Fiduciary

Section 10:

A specific category called **Significant Data Fiduciary** has been mentioned in the 2023 Bill. This category has additional obligations like appointment of a Data Protection Officer (**DPO**) and an Independent Auditor, implementation of Data Protection Impact Assessments (**DPIA**). Such class of data fiduciaries shall be notified by the government on the basis of a list of criteria given in the Bill.

FINANCIAL PENALTY:  Upto 150 crores

This provision has been maintained from the previous Draft Bill of 2022.

Compliance Road-Map

For a well-rounded compliance framework to shield the organizations, certain steps will be required to be taken appointment of relevant persons, conducting training and awareness programs for the employees, consent management, documentation of data subject request forms and processes, Data Inventory, DPIA, Periodic Audits etc.

- 1.Does your organization have **well-trained professionals** to undertake the role of a **Data Protection Officer and Data Auditor**?
- 2.Has your organization **documented procedures and processes** to conduct **data audits and periodic assessments** of business functions?
- 3.Does your organization have **systematic processes** in place for **consent and privacy rights management**?
- 4.Does your organization have **privacy-sensitive employees** and conduct **effective trainings and up-skilling exercises**?

D6. Protection of Personal Data of Children

Section 9

The data fiduciaries are entrusted with the obligation to obtain verifiable **consent from the lawful guardians** prior to the processing of personal data of children or a person with a disability. They are prohibited from undertaking the processing of personal data of children that is **likely to cause harm** to the children; tracking or behavioural monitoring of children or targeted advertising directed at children.

FINANCIAL PENALTY:  Upto 200 crores

Comparison to Other Laws

European Union: GDPR defines a child to be any individual below the age of 16 years. Prior to the processing of the personal data of children, authorized parental consent is required.

California: CPRA provides for explicit consent from children between the age of 13 - 16, and from parents/ lawful guardians for children below the age of 13. The protection of children's data is also aligned with Children's Online Privacy Protection Act (COPPA) which stipulates verifiable parental consent.

Compliance Road-Map

It is recommended that the organizations ensure compliance with the provisions laid down in the 2023 Bill in the following manner:

1. Does the organization process personal data belonging to children?
2. Has the organization **incorporated** appropriate **measures to ensure that the verifiable consent of the lawful guardians is recorded prior to the processing** of personal data of children?

D7. Rights of Data Principals

1.

Right to Access Information about Personal Data

The data principal is vested with the right to obtain - a confirmation from the data fiduciaries if their personal data is being processed; a summary of their personal data being processed & the processing activities; identities of all the data fiduciaries with whom their personal data was shared by identifying the categories of personal data so shared; and, any other information which may be prescribed.

2.

Right to Correction & Erasure of Personal Data

The data principal would have the right to correction, completion, updating and erasure of their personal data. The data fiduciary is obligated to correct the data principal's inaccurate or misleading personal data; to complete their incomplete personal data; to update their personal data; to erase their personal data that is no longer necessary for the purpose for which it was processed unless retention is mandated for a legal purpose.

3.

Right of Grievance Redressal

The data principal is vested with the right to a 'readily available' means of registering a grievance with the data fiduciary or consent manager. The data fiduciary shall be required to respond to such grievances within the period as may be prescribed by the Central Government by way of rules or notification.

4.

Right to Nominate

The data principal has the right to nominate any other individual, who in the event of death / incapacity (unsoundness of mind) of the data principal, could exercise the rights guaranteed under the Bill.

D7. Rights of Data Principals

Comparison to Other Laws

The rights identified under GDPR, the Draft Bill, 2022, & the 2023 Bill have been enumerated hereunder.

Sl. No.	Data Subject Rights under European Union GDPR	Data Principal Rights under DPDPB 2022	Data Principal Rights under DPDPB, 2023
1	Right of access by the data subject	Right to confirmation & access	Right to access information about personal data
2	Right to rectification	Right to correction & erasure	Right to correction & erasure of personal data
3	Right to erasure ('to be forgotten')	Right to correction & erasure; Right to be forgotten	Right to correction & erasure of personal data
4	Right to restriction of processing	NA	NA
5	Right to data portability	Right to data portability	NA
6	Right to object	Right of grievance redressal	Right of grievance redressal
7	NA	NA	Right to nominate

Compliance Road-Map

It is recommended for organizations to ensure compliance with the legal grounds in the following manner:

1. Has the Organization **informed** the **data principals** of the **rights** vested with them under the Draft Bill, through the **privacy policy**?
2. Has the Organization **implemented** the appropriate **data subject requests tool**?

D8. Transfer of Personal Data

Section 16

The Bill stipulates a general rule against transfer of personal data to any country outside the territory of India as notified by the Central Government and such transfers are subject to satisfaction of at least one of the conditions prescribed under Section 17 of the Bill.

FINANCIAL PENALTY:



Upto 50 crores

Comparison to Other Laws

European Union: GDPR lays down certain safeguards to protect the personal data that is being transferred to third countries / international organizations, which are primarily inclusive of - Binding Corporate Rules, Standard Contractual Clauses and Adequacy Decisions.

Compliance Road-Map

It is recommended to the Organizations comply with the provisions and legal grounds laid down in the 2023 Bill in the following manner:

1. Has the organization that transfers personal data beyond the territory of India ensured that a **Transfer Impact Assessment** is conducted to assess and analyze whether the third parties/vendors have appropriate measures incorporated to protect the personal data?
2. Has the Organization implemented measures to ensure that the **Data Processing Agreements** are in place, in case of any such transfer of personal data beyond India?

D9. Data Protection Board

Chapter V (Section 18-26) and Chapter VI (Section 27 and 28)

The Bill proposes the establishment of the Data Protection Board of India, which would perform the functions as notified by the Central Government of India. The Board has been identified as an **independent body**, functioning as a **digital office** by adopting the **techno-legal measures** as may be prescribed.

Comparison to Other Laws

European Union: GDPR mandates every Member State to establish an independent supervisory authority in order to monitor the application of the regulatory requirements, to protect the rights & freedoms of the data subjects whose personal data is processed and, to facilitate the free flow of the personal data within the Union.

Functions of the Data Protection Board

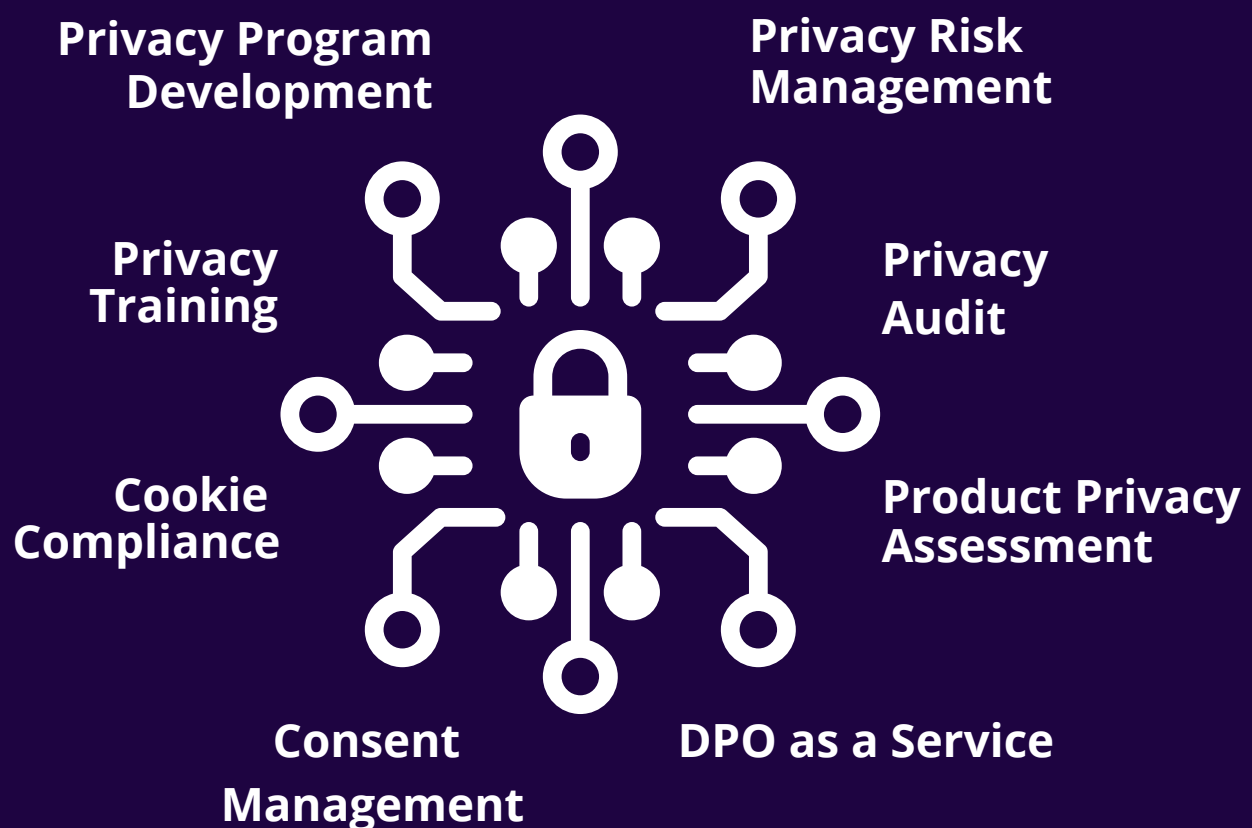
- Investigation and inquiry into personal data breaches, as well as imposing urgent remedial and mitigating measures for breach containment.
- Take cognizance of violations of the Bill on the receipt of a complaint filed by a data principal against a data fiduciary and/or consent manager, and to impose penalties.
- Take cognizance and initiate inquiries on the violations by an intermediary, as per references made by the Central Government.
- Take appropriate action against any consent manager on being intimated of any breach of registration condition, and impose penalties.
- Impose penalties against the appropriate party as per Schedule of the Bill.

E. Conclusion

The Digital Personal Data Protection Bill 2023 is a lean and simple piece of law that focuses on "digitized" personal data.

This analysis reports serves as a compliance guide for the organizations that want to develop a roadmap in anticipation of the Indian Act on Data Protection.

Tsaaro can help you on this journey of compliance with our holistic data protection services.



Think Privacy, Think Tsaaro

About Tsaaro

At Tsaaro, we empower businesses to manage their compliance with data privacy and cybersecurity regulations. Our Mission is to assist businesses in achieving this because we are fervently committed to safeguarding the individuals who are the sources of the data. We have been at the forefront of ensuring that companies instill the best data protection and cybersecurity safeguards at their organisation and helped them save up to \$100,000 which they would have paid in fine to Regulatory Authorities. Our strength lies in assessing security and privacy risks, monitoring threats, and safeguarding applications against compliance issues.

100+

Total Projects Completed

60+

Clients across 7 Geographies

22+

Regulations/Standards Covered

150+

Privacy & Security Experts



Vodafone

EXL

EXL



Vistara
Vistara Airlines



TITAN
Titan



Flipkart



DarwinBox

Our Services





WHY TSAARO?

Tsaaro provides Privacy & Cybersecurity services to help organizations meet regulatory requirements while maintaining a robust security infrastructure.

Our industry-standard privacy services include DPO-as-a-service, DPIA, Privacy Program Development, Privacy Risk Management, Cookie Compliance Program, Consent Management, to name a few, delivered by our expert privacy professionals recognized by IAPP.

Akarsh Singh (CEO & Founder, Tsaaro)

Akarsh is a CIPP/E, CIPM, CIPT, Fellow in Information Privacy by IAPP, and an IAPP Advisory Board Member. His expertise lies in Data Privacy and Information Security Compliance.

Krithi Shetty

Senior Data Protection Consultant, Tsaaro

Shilpa Margaret Kurian

Data Protection Consultant, Tsaaro

CONTACT US

Tsaaro Bangalore Office

Manyata Embassy Business Park,
Ground Floor, E1 Block,
Beech Building, Outer Ring Road,
Bangalore- 560045
India
P: +91 77609-23421

Tsaaro Gurugram Office

Level 1, Building 10A,
Cyber Hub, DLF Cyber City,
Gurugram, Haryana 122002
India
+91 77609-23421

Tsaaro Amsterdam Office

Regus Schiphol Rijk
Beech Avenue 54-62,
Het Poortgebouw,
Amsterdam, 1119 PW,
Netherlands
P: +31- 639875167

Email us
info@tsaaro.com