WHITEPAPER

tsaaro

DRAFT DIGITAL PERSONAL DATA PROTECTION BILL 2022:

Provisions, Controls & Tools

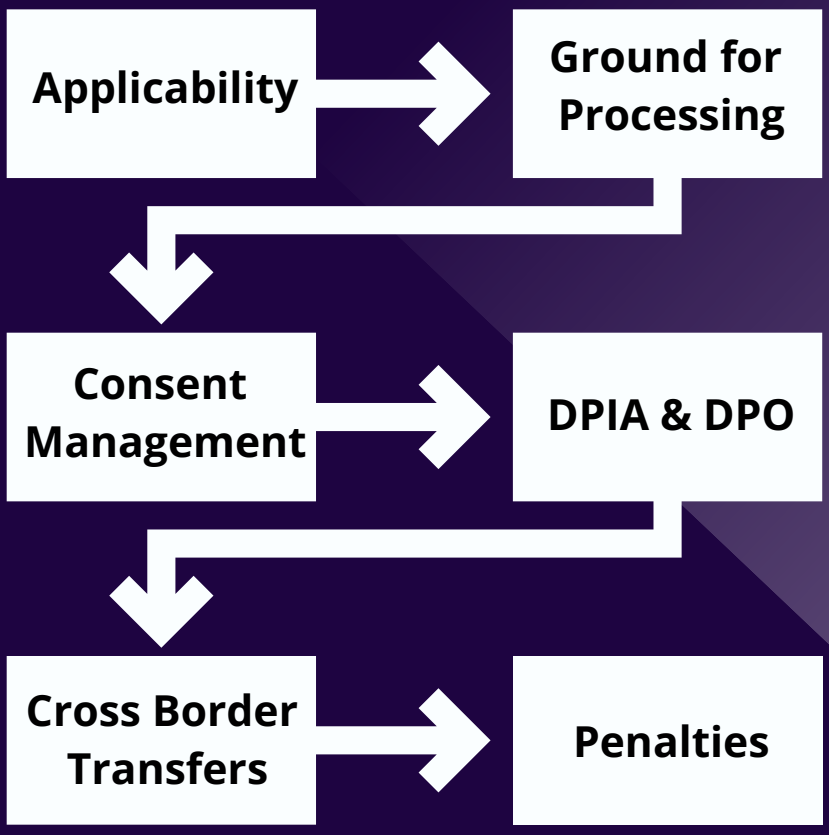


Table of Contents

A. Introduction

B. Executive Summary

C. Restriction on Disclosure

D. Provisions Analyzed

D1. Applicability

D2. Grounds of Processing

D3. Consent

D4. Deemed Consent

D5. Data Controllers & Data Processors

D6. Significant Data Fiduciary

D7. Children's Personal Data

D8. Rights of Data Principals

D9. Cross Border Transfer of Personal Data

D10. Data Protection Board

E. Conclusion

A. Introduction

This paper is an in-depth analysis of the newly introduced Draft Digital Personal Data Protection Bill 2022. The Draft 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 Draft 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 Draft 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 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 4:
The Bill only applies to processing of **"digital" personal data** i.e., the data is collected online, or collected offline but digitized within the Indian territory. The provisions can also apply to processing outside India in cases where profiling or offering of goods & services happens in India.

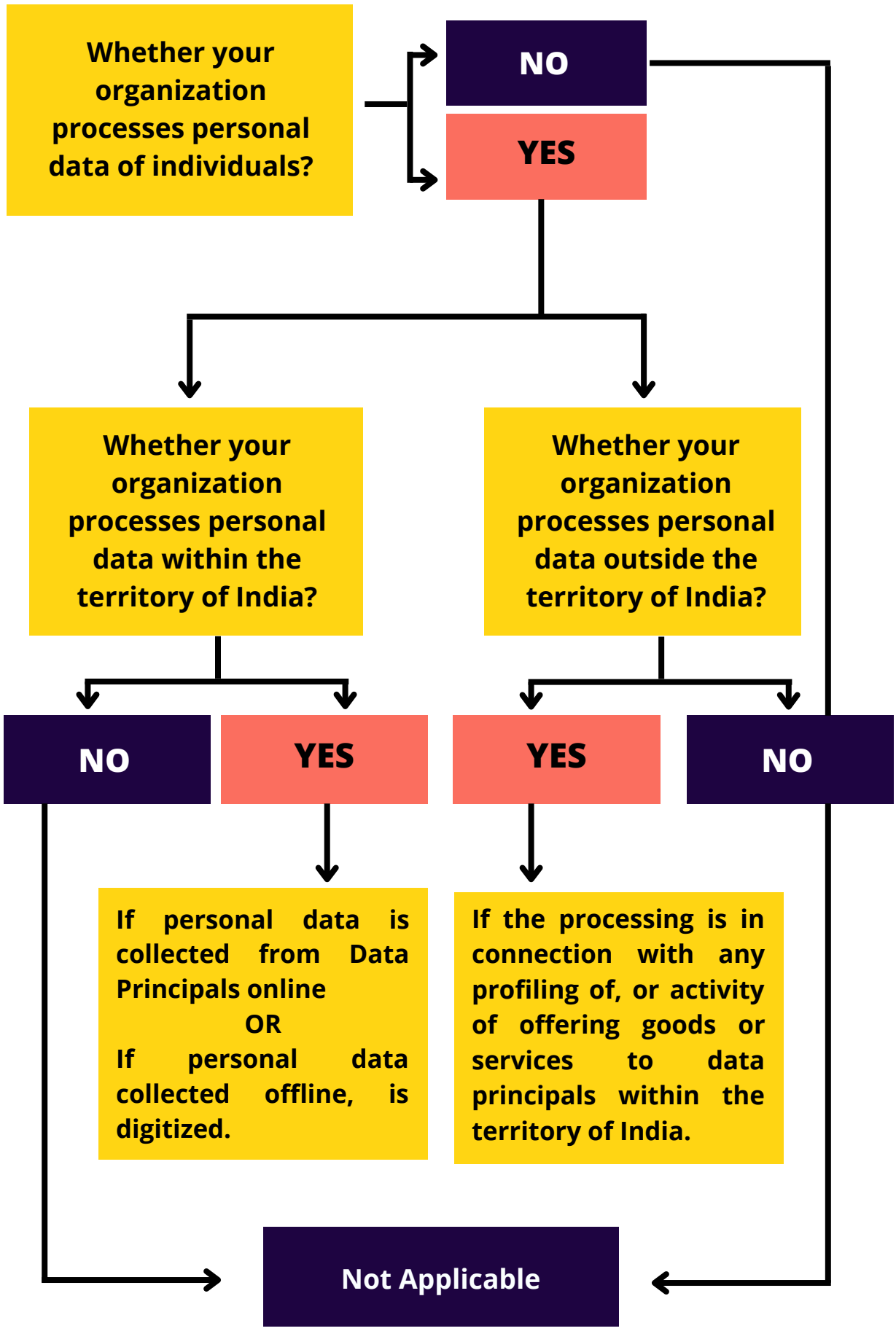
This provision bars processing on offline personal data, processing for domestic use, non-automated processing and when personal data about a person has been in existence for at least 100 years. Although the internet and the digitalization of data present many advantages, they also present many obstacles. The Bill applies to digital personal data in recognition of this and to keep the spotlight on the increasing digital nature of interactions.

Comparison to its Previous Iterations
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 Draft 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, in accordance to Section 4 ?
3. Is there any process set in place to digitize data collected offline?
4. Are automated means used to undertake the processing?

Applicability Matrix



D2. Grounds for Processing Digital Personal Data

Section 5:
Processing shall be considered to be **legitimate** if it aligns with the provisions of this Act, or where the Data Principal has given or is deemed to have given her **consent**. Lawful purpose has been defined as any purpose that is **not prohibited by law**.

FINANCIAL PENALTY: Upto 50 crores

Comparison to Other Laws
European Union: GDPR lays down grounds of processing under Article 6. These are: legitimate interest, consent, vital interest, contractual necessity, public interest & 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?

D3. Consent

Section 7:

The 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's **Notice-related requirements** 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. For a person to have any real control over their personal data, consent shouldn't be irrevocable and permanent. As a result, the Bill stipulates that the Data Principal may withdraw consent.

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 going to be a hallmark of the bill and that's why **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. Deemed Consent

Section 8:
The Data Principal is deemed to have given consent to the processing of her personal data if such processing is necessary in cases when data when provided **Voluntarily,** or any function is performed by state under any law or for compliance of **judicial orders, medical emergency, outbreak of diseases, ensuring safety during disasters, purposes related to employment**, in furtherance of **public interest** and in **fair and reasonable cases**.

FINANCIAL PENALTY:	Upto 50 crores

Compliance Road-Map
Just like the provision for consent, deemed consent can also be managed via **policies and procedures in place along with tools and solutions**. In order to understand deemed consent, organizations can look into the following:

1. Does the organization determine the purpose and means of processing personal data?
2. Are there safeguards in place to ensure the accuracy and completion of personal data?
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?
5. Is there a procedure established for sending notifications to the board and impacted data subjects in case of a data breach incident?

D5. Data Controllers

Section 9:

Data Controllers have been termed as **Data Fiduciary** under the Bill. There are obligations laid down on such data fiduciaries like the data processed shall be accurate, **technical and organizational safeguards** are implemented to protect the data and reasonable security safeguards (also applies to Data Processors) are to be put in place to avoid any data breaches.

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. Does the organization **determine the purpose and means** of processing personal data?
2. Are there **safeguards** in place to ensure the accuracy and completion of personal data?
3. Are there **technical and organizational measures [TOM]** established to ensure adherence to the provisions of the bill?
4. Are there reasonable measures in place to secure personal data from breach incidents?

D6. Significant Data Fiduciary

Section 11:
A specific category called **Significant Data Fiduciary** has been mentioned in the 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 250 crores

Penalties
In event of a **data breach** that goes **unnotified**, data fiduciaries and data processors can be charged a financial penalty of up to 200 crores. Failure on the part of **Data Processor** or **Data Fiduciary** to take reasonable security safeguards to prevent data breaches can result into penalty of up to 250 crores. In event of non compliance with additional obligations of the Significant Data Fiduciary, it can result into a penalty up to 150 crores.

Compliance Road-Map
The Indian Bill mandates DPIAs for the Significant Data Fiduciaries and appointment of a DPO. But for a **well-rounded compliance framework** to shield the organizations, more steps need to be taken like **training and awareness programs** for the employees, **consent management,** documentation of **data subject request** forms and processes, **Data Inventory**, **DPIA, Periodic Audits** etc.
Significant Data Fiduciaries can also **leverage tools and solutions that aid with the automation** of these exercises.

D7. Protection of Personal Data of Children

Section 10

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. They are prohibited from undertaking processing of personal data of children that is **likely to cause harm** to the children; tracking or behavioral monitoring of children or targeted advertising directed at children. These obligations do not extend to processing of sensitive personal data of children and are subject to exemptions which may be prescribed.

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, an authorized parental consent is required.

Compliance Road-Map

It is recommended that the organizations must incorporate appropriate measures to ensure that the verifiable consent of the lawful guardians is recorded prior to the processing of personal data of children.

D8. Rights of Data Principals

1.

Right to 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 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 grievance with the data fiduciary. In case the data principal is not satisfied with the response to the grievance registered, or does not receive any response within seven days, a complaint could be filed before the Data Protection Board of India.

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 Draft Bill.

D8. Rights of Data Principals

Comparison to Other Laws

The rights identified under GDPR, Data Protection Bill, 2021 & the Draft Bill, 2022, have been enumerated hereunder.

Sl. No.	Data Subject Rights under European Union GDPR	Data Principal Rights under Data Protection Bill, 2021	Data Principal Rights under DPDPB, 2022
1	Right of access by the data subject	Right to confirmation & access	Right to information about personal data
2	Right to rectification	NA	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	NA	Right of grievance redressal
7	NA	NA	Right to nominate

Compliance Road-Map

It is recommended for organizations to **inform** the **data principals** of the **rights** vested with them under the Draft Bill, through the **privacy policy.** The **implementation** of appropriate **data subject requests tool** is considered best practice.

D9. Transfer of Personal Data

Section 17

The proposed Bill states that the Central Government would **conduct an assessment of factors** deemed necessary to it, and **notify countries** beyond the territory of India, to which data fiduciaries would transfer the personal information. The factors are yet to be ascertained.

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

The organizations that transfer personal data beyond the territory of India must ensure that a **Transfer Impact Assessments** is conducted to assess and analyze whether the third-parties / vendors have appropriate measures incorporated to protect the personal data. The best practice is to ensure that the organizations have **Data Processing Agreements** in place, in case of any such transfer of personal data beyond India.

D10. Data Protection Board

Section 19

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 Data Protection Board

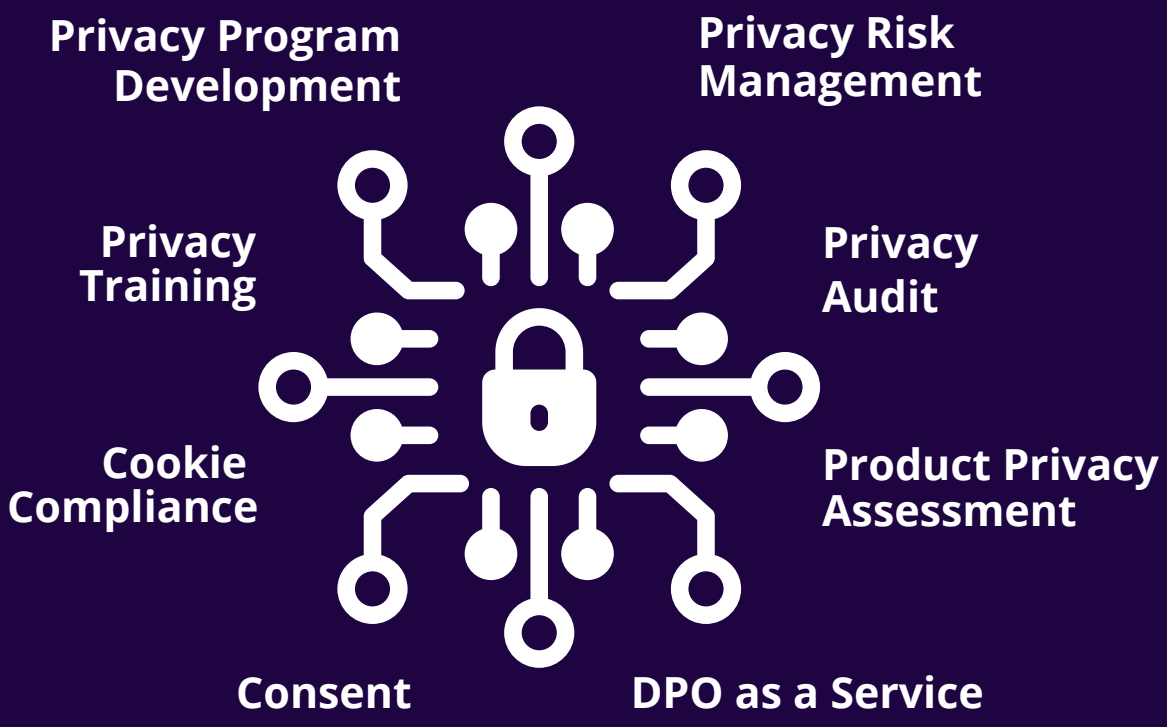
- Determination of non-compliance with the provisions under the Draft Bill;
- Performing functions as assigned by the Central Government of India;
- Direct data fiduciaries to adopt pertinent & immediate measures to remedy any personal data breach or mitigate the harm caused to data principals;
- Pronouncing decisions against the complaints filed & impose the suitable penalties for any non-compliance that is identified.

E. Conclusion

The Draft Digital Personal Data Protection Bill 2022 is a lean and simple piece of law that focuses on "digitized" personal data. Additionally, MeitY has invited comments till 17 December, 2022.

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

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
Data Protection Consultant, Tsaaro

Poojan Bulani
Data Protection Consultant, Tsaaro

CONTACT US

Tsaaro Bangalore Office
Manyata Embassy Business Park,
Ground Floor, E1 Block,
Beech Building, Outer RingRoad,
Bangalore- 560045
India
P: +91-0522–3581

Tsaaro Gurugram Office
Level 1, Building 10A,
Cyber Hub, DLF Cyber City,
Gurugram, Haryana 122002
India
+91522–3581306

Tsaaro Amsterdam Office
Regus Schiphol Rijk
Beech Avenue 54-62,
Het Poortgebouw,
Amsterdam, 1119 PW,
Netherlands
P: +31-686053719

Email us
info@tsaaro.com