MRSI
SHAPING TOMORROW, TODAY

KHAITAN & CO ADVOCATES SINCE 1911

Practical Guide to the Digital Personal Data Protection Act and Rules for the Indian Market Research and Insights Industry

Foreword

Dr. Sandeep Arora
DPDP Champion, MRSI
Committee Former President, MRSI

Nitin Kamat
Chairperson, DPDP
President, MRSI

The enactment of the **Digital Personal Data Protection Act 2023 and Rules 2025** mark an important milestone in India's evolving digital and business landscape. Data is now central to decision-making, innovation, and growth. As a result, the way personal data is collected, processed, protected, and governed has become a matter of both legal responsibility and institutional trust. For the consumer insights and market research industry in India, this is a significant development.

Our industry holds a unique place in the economy. It helps organizations understand people better through their needs, beliefs, behaviours, motivations, opinions, and preferences. In doing so, it contributes to better decisions, products, services, communication, and policy thinking. In India, the consumer insights and market research sector has grown into an industry of meaningful scale. It is currently estimated at approximately USD 3.5 billion (Year 2025) with an aggressive growth rate. It spans primary research, data collection, analytics on existing datasets, specialist insights services, and export-oriented firms supporting international clients and global mandates.

At the heart of this industry lies one foundational principle: **Trust**

For decades, the market research profession has recognized that its credibility depends on the responsible treatment of data, the dignity of respondents, and the integrity of research processes. This is why our industry has long been guided not only by commercial discipline, but also by strong traditions of professional self-regulation, reflected most recently in the **ICC/ESOMAR International Code of Ethics 2025,** which all MRSI members are committed to abiding by.

In that sense, the principles underlying the DPDP Act and Rules do not arrive in unfamiliar territory for our profession. While the Act introduces statutory obligations and sharper expectations around governance, accountability, and documentation, the industry is not starting from scratch. Even with certain waivers available to the research fraternity, alignment with its requirements should be viewed not as an undue burden, but as a natural progression that formalizes and strengthens values the profession has long embraced.

At the same time, this transition deserves due seriousness. The Act and Rules call for greater clarity of roles. It requires stronger internal processes, more explicit safeguards, and a more disciplined approach to data governance across the value chain. These considerations apply not only to research agencies, but also to clients (research users), panel partners, fieldwork specialists, analytics firms, technology providers, processors, and others involved in the creation and delivery of insight. They are relevant for domestic work. They are equally relevant for cross-border engagements involving Indian entities or Indian respondents.

It is in this context that this document assumes real value.

This guidance, prepared jointly with the leading full-service law firm Khaitan & Co, is intended as a practical guide for the consumer insights and market research fraternity in India and overseas. It explains the DPDP Act and Rules in the context of how our industry actually works, and helps turn broad principles into practical action. The inclusion of a simple checklist to assess whether a project is DPDP-aligned makes the document especially useful. At a time when regulation is evolving, the real challenge is often not intent, but clarity. This document aims to bring that clarity, improve readiness, and support a more consistent approach across both buyers and sellers of research.

As an industry, we should approach this moment not only with seriousness, but also with confidence. Compliance and competitiveness are not opposing forces. Industries that inspire trust are often the ones that sustain relevance and growth over time. For market research, this is especially true.

We are grateful to all those who have contributed to this effort. Our sincere appreciation extends to the two MRSI Data Protection committees that were formed at two significant stages of DPDP, first being the formulation of the DPDP Act and the current committee taking the initiative forward. A big thank you to the committee members, past and present: Abhinav Goel, Chandan Mukherji, Jyoti Malladi, Manoj Dawane, Prasun Basu, Ritesh Srivastava, Siddharth Banerjee, Sidharth Chaturvedi and Subhransu Rout for their time and effort.

We wish to express our heartfelt thanks to the Khaitan & Co. team, namely Supratim Chakraborty, Sumantra Bose and Siddharth Sonkar, for their invaluable guidance throughout, who brought this document to the level of optimal perfection for the benefit of our industry at large.

We would like to express our gratitude to the MRSI Managing Committee of 2022-24 and 2024-27, for their continuous support. We would like to thank the MRSI members for assisting us with their inputs at different stages of the DPDP Act and Rules formalised by the Government. It enabled MRSI to approach the Law makers to look at the Research and Insights Industry with a different lens, as a consequence of which we were successful on getting an exemption in the DPDP Act.

Last but not the least, we commend the efforts of the MRSI Secretariat team led by Mitali Chowhan and Nidhi Hosangady and supported by Deepa Ahuja who worked tirelessly in coordination with our partner, Khaitan and Co. and all the stakeholders for seamless execution.

We hope this document will be read and used in that spirit. It is both a guide for the present and an investment in the future credibility of our profession. We are confident that it will serve as a valuable resource for agencies, users of research, compliance teams, and industry leaders as they align with the new law while continuing to uphold the highest standards of responsible and trusted practice.

Table of content

A. Introduction

This guidance document is prepared by the Market Research Society of India (**"MRSI"**) to support its members in carrying out market, opinion and social research in adherence with India's Digital Personal Data Protection Act 2023 (**"DPDPA"**) and its accompanying Digital Personal Data Protection Rules 2025 (**"Rules"**).

This document endeavours to establish India-specific guidance on safeguards and measures for compliance that should be implemented while processing personal data in the course of carrying out market research in furtherance of availing an exemption under the DPDPA and the Rules. Over and above this guidance, researchers should additionally remain updated on any changes to applicable law and regulation and/or guidance available from time to time towards ensuring continued compliance.

B. Definitions

For the purposes of this guidance:

(i) **"Child"** means an individual below the age of eighteen years.

(ii) **"Data principal"** means the individual to whom personal data relates.

(iii) **"Data fiduciary"** means the entity which determines the purpose and means of processing personal data either alone or jointly with others.

(iv) **"Personal data"** includes any information about an individual who is identifiable by or in relation to such data.

(v) **"Anonymisation"** refers to the irreversible process of removing or altering identifiers such that it becomes impossible to identify an individual, either directly or indirectly.

(vi) **"Pseudonymisation"** refers to the processing of personal data in a manner that replaces identifiable information with artificial identifiers (such as codes or tokens), such that the data cannot be attributed to a specific individual without the use of additional information. As re-identification remains possible, pseudonymised data continues to be treated as personal data under the DPDPA.

C. Criteria to Avail the Research Exemption

The research exemption under the DPDPA does not provide a blanket exemption from all obligations under this legislation. Instead, it relaxes certain requirements, such as relying on a lawful basis of processing (e.g., such as consent), where personal data is processed strictly for research purposes and subject to prescribed conditions. Organizations are therefore expected to carefully assess whether their processing activities would fall within the scope of this exemption as envisaged.

The exemption will not apply in circumstances where personal data is used to make decisions about, or take actions affecting, specific individuals. By way of illustration, the following activities would fall outside the purview of the research exemption:

(i) Using research responses to make decisions or take action in relation to a specific individual;

(ii) Linking survey responses to identifiable customer profiles;

(iii) Converting research respondents into marketing or sales leads; and

(iv) Using research data to directly target, profile, or influence specific individuals for commercial purposes.

Even where the exemption is applicable, it can only be availed if the standards specified under the Rules are implemented. Further, the availability of the exemption is subject to important limitations. The processing of personal data must be genuinely undertaken for research purposes and not instead be used as a mechanism to circumvent the requirements under the DPDPA. Specifically, personal data collected in the course of carrying out research should not subsequently be used for the purposes of targeted advertising, marketing outreach, customer acquisition activities or other unrelated commercial purposes.

In practice, this means that research organisations must ensure that the objective of the project is clearly defined as research, that the personal data collected is strictly necessary for that objective, and that appropriate technical and organisational safeguards are implemented throughout the lifecycle of the research project. Where these conditions are not satisfied, the processing may fall outside the scope of the exemption and the full obligations of the DPDPA may apply.

D. Core Principles to Abide by While Processing Personal Data in Research

When relying on the research exemption, MRSI members should ensure that the processing of personal data adheres to the key standards set out in the DPDPA. These standards require that processing is carried out in a lawful and responsible manner and that reasonable security safeguards are implemented to prevent personal data breach.

Specifically, research organisations must ensure that personal data is only processed for clearly defined purposes, that the data collected is restricted to the extent necessary for those purposes, and that reasonable efforts are made to ensure the accuracy, completeness and consistency of the personal data being used. Personal data should only be retained for as long as necessary to achieve the research objective or to comply with applicable legal obligations.

Where personal data is collected through offline modes (such as paper surveys, field interactions, or in-person interviews) and subsequently digitised, such data will fall within the scope of the DPDPA.

E. Purpose Limitation

Members must clearly define the purpose for which the research is being carried out before collecting any personal data. The objective of the research should be clearly documented internally and should explain why the collection of personal data is necessary for the research exercise. This documentation should form part of the organisation's internal governance processes and may be relied upon to demonstrate that the processing falls within the scope of the research exemption.

Audio and video recordings collected in the course of qualitative research constitute personal data under the DPDPA and must be processed in accordance with its requirements, subject to the applicability of the research exemption.

Organisations should ensure that such recordings are collected strictly for defined research purposes and that access is restricted to authorised personnel on a role-based basis. Given that such recordings may be shared across multiple stakeholders (such as internal teams, clients, and external vendors), appropriate contractual, technical, and organisational safeguards must be implemented to prevent unauthorised access, misuse, or disclosure.

Retention of audio and video recordings should be limited to what is necessary for the purpose of research, including any validation, audit, or quality control requirements. Where feasible, organisations should consider adopting anonymisation techniques.

F. Data Minimisation

Research organisations should ensure that the design of surveys, interviews, panels, and other research instruments only collect information to the extent required to fulfil the objective of the research. In practice, this means avoiding the collection of disproportionate or unrelated personal information. For example, research questionnaires may appropriately seek information relating to geographic location, age range, product usage habits or purchasing behaviour where these variables are in fact necessary for the research in question. However, collecting sensitive information such as government identification numbers, financial account information or other intrusive categories of personal data should generally be avoided unless such information is strictly necessary for the research that is being carried out.

While carrying out panel-based research (such as online panels, media viewership panels, digital tracking, and behavioural research panels), organisations must treat such engagements as a continuing relationship with participants, as opposed to one-off data collection exercises. Accordingly, as a best practice, organisations should adopt a granular and transparent approach to participant onboarding and engagement. This may, for instance, encompass obtaining explicit consent to participate in the panel (with mechanisms such as double opt-in, where feasible), providing clear information regarding the nature and frequency of participation, and the types of data that may be collected, including any passive or behavioural tracking. Organisations should also implement privacy-by-design measures, such as maintaining a separation between panel identity databases and research response datasets and implementing appropriate mechanisms for exercise of rights as a data principal, where applicable.

G. Anonymisation and Pseudonymisation

Research organisations should adopt measures to ensure that personal data is appropriately anonymised or pseudonymized, wherever technically feasible. Anonymisation should, in general, be the preferred approach, particularly at the stage of data analysis and reporting. Where anonymisation is not immediately possible, pseudonymisation techniques may be used to segregate identifying information from research datasets. Where automated tools or artificial intelligence systems are utilised to analyse and glean insights from research data, organisations should ensure that such systems operate on anonymised or pseudonymised datasets wherever

feasible and that appropriate safeguards are implemented to prevent unintended re-identification.

H. Accuracy and Data Quality

Reasonable efforts should be put to ensure the completeness, accuracy and consistency of personal data that is processed. Research organisations should therefore implement appropriate quality assurance measures during data collection and processing. These measures may include validation checks within survey instruments, monitoring fieldwork quality, implementing procedures for correcting obvious errors in datasets, and removing duplicate or clearly inaccurate records. While research data is often based on self-reported responses, organisations should nonetheless implement reasonable processes to ensure that the datasets used for analysis are reliable and internally consistent. Maintaining high standards of data quality also bolsters the credibility and integrity of research outputs.

I. Consent Where Necessary

Where the exemption for research may not be available (for instance, where the intended use of the personal data is wider than the initially envisaged research), the DPDPA expects data fiduciaries to be able to demonstrate that free, specific, informed, unconditional and unambiguous consent was procured from data principals, where consent is the lawful basis of processing. Such consent is expected to be obtained through an affirmative act of the individual. The law does not prescribe a specific format for obtaining consent. Therefore, organisations may take the liberty of adopting from a wide range of acceptable mechanisms, including written consent forms, digital click-through acceptance, or audio/video recordings, as long as such mechanisms create a reliable and demonstrable record of the individual's informed and affirmative agreement.

Insofar as maintaining logs of such consent to demonstrate compliance is concerned, while the DPDPA does not prescribe a maximum retention period for such records and organisations should retain such records for as long as necessary to demonstrate compliance, taking into account the lifecycle of the personal data, the nature of the research activity, and any applicable audit, regulatory, or dispute resolution requirements.

J. Retention and Storage of Personal Data

Personal data collected for the purposes of research must only be retained for as long as necessary to achieve the research purpose, unless required to be retained for a longer period in furtherance of any obligation under applicable laws. Research

organisations should as a result put in place internal data retention policies that articulate the duration for which personal data may be retained.

Once the objective of research is fulfilled, personal data should ordinarily be deleted, anonymised, or otherwise securely disposed of unless there exists a legitimate purpose for continued retention. Organisations should periodically review how long research datasets are being stored to ensure that personal data is not retained beyond the necessary period of retention.

K. Security Safeguards

Technical safeguards may include measures such as encryption, obfuscation, masking, or the use of virtual tokens mapped to personal data, in addition to using secure cloud or server environments, network security protections, and appropriate access control mechanisms to restrict access to authorised personnel. Organisations should also implement mechanisms which provide visibility into the accessing of personal data, including the use of logs, monitoring and periodic review mechanisms to enable the detection of any unauthorised access to personal data, as well as facilitating any investigation and remediation.

Where research organisations engage third-party vendors, survey platforms, fieldwork agencies or other service providers that process personal data on their behalf, appropriate contractual provisions should be implemented to ensure that such entities (in their capacity as data processors) are *inter alia* required to adopt appropriate technical and organizational safeguards to protect personal data. Additionally, organisations should implement appropriate internal governance measures, including commitments of confidentiality from employees and contractors, staff training, incident response procedures, and oversight mechanisms to ensure the effective observance of security practices.

Organisations engaging third-party vendors or processors to facilitate research activities should also internalise robust governance and oversight mechanisms to ensure compliance with applicable data protection obligations. At a minimum, organisations must consider ensuring the following:

(i) Data processing agreements are executed with all relevant vendors, incorporating explicit obligations on the vendor to implement *appropriate technical and organizational measures* and *reasonable security safeguards* to prevent a personal data breach in accordance with applicable law.

(ii) Vendors are subject to strict confidentiality obligations, including restrictions on access to personal data only on a need-to-know basis.

(iii) Vendors are required to implement appropriate technical and organisational security measures, including:

(a) safeguarding personal data through technical measures such as encryption, masking, obfuscation, or tokenisation;

(b) access controls to ensure that only authorized personnel have access to personal data;

(c) logging, monitoring, and reviewing mechanisms to enable detection and investigation of unauthorised access to personal data;

(d) measures to ensure the availability and resilience of processing systems, encompassing data backups and recovery mechanisms in case of a personal data breach, cyber security incident or system failure; and

(e) retain logs and relevant data for a minimum period of one year, or such longer duration as may be required under applicable law, and to enable detection, investigation, and remediation of security incidents.

L. Transparency and Respondent Intimation

As a best practice, where personal data is collected *directly* from participants in a research, members conducting the research should, to the extent practically feasible, provide an intimation to the data principal regarding the details and the nature of processing. This intimation should explain the purpose of the research, identify the research organisation responsible for the processing, and provide information about how the respondent may contact the organisation with questions regarding the processing of their personal data.

M. Data of Children and Persons with Disabilities

The DPDPA also imposes specific restrictions in relation to the processing of children's personal data. This includes prohibitions against behavioural monitoring and tracking of children's personal data online, as well as requirements relating to obtaining verifiable parental consent. It also provides for safeguards in relation to the processing of personal data of persons with disabilities where consent is required to be provided by a lawful guardian appointed in accordance with Indian guardianship laws. While these provisions may not be specifically applicable where personal data is processed purely for research purposes, research organisations

irrespectively exercise heightened caution while conducting research that includes personal data of children (persons under the age of eighteen) or persons with disabilities.

As a recommended practice, research organisations should consider implementing safeguards that reflect the underlying intent of the law. This may include avoiding behavioural monitoring or tracking of children in research environments and ensuring that research participation involving children is conducted with the knowledge and consent of a parent or lawful guardian wherever feasible and designing research methodologies and instruments in a manner which prioritises mitigation of risks to vulnerable participants.

Considering the sensitivity of such data, research organisations should also ensure that data collected from children or persons with disabilities is handled with an enhanced level of confidentiality and that reporting and publication of research findings does not enable identification of individual participants.

Where personal data of children is processed for purposes beyond the scope of the research exemption, the data fiduciary is required to obtain verifiable consent from a parent or lawful guardian. In this regard, the data fiduciary is required to verify that the individual providing consent is an adult but is not required to independently establish the parent-child relationship. This verification may be undertaken using reliable identity and age-related information already available with the organisation, or through details voluntarily provided by the individual, including via tokens issued by authorised entities. However, in case of persons with disabilities, verifiable consent requires confirming whether the person claiming to be a guardian has been appointed by a court of law, or by a designated authority or by a local level committee, under the law applicable to guardianship.

N. Legal Consequences of Non-Compliance

Members should be aware that failure to comply with the obligations under the DPDPA may result in regulatory action by the Data Protection Board of India (**"Board"**) (the enforcement authority envisaged under the DPDPA). Where, following an inquiry, the Board determines that a breach of the DPDPA or the Rules is significant, it may impose monetary penalties, considering factors such as the nature and gravity of the breach, the type of personal data affected, whether the breach is repetitive, whether the entity derived any gain or avoided any loss as a result of the breach, the effectiveness of mitigation measures taken, and whether the penalty is proportionate and necessary to ensure compliance. Certain contraventions may attract substantial monetary penalties. For instance, failure to implement reasonable security safeguards to prevent personal data breaches may attract penalties of up to INR 250 crore (USD 30 million approx.) for each instance of non-compliance. Members should therefore ensure that the safeguards described in this guidance are implemented in practice and supported by appropriate internal

governance,security measures, and oversight mechanisms.

O. Cross-border data transfers

Considering the global nature of the research and insights industry, organisations may in the course of carrying out research functions transfer personal data outside India. Such transfers must comply with any restrictions or conditions that may be prescribed by the Government of India in relation to transfers to specific jurisdictions under the DPDPA.

As a best practice, organisations should at the minimum ensure that appropriate contractual safeguards are implemented while transferring personal data to overseas recipients, to ensure that the recipient maintains the same or better level of protection as required under the DPDPA, its underlying rules and notifications.

Key Points Checklist to Avail the Research Exemption

Where personal data is intended to be collected and processed for research purposes, organisations must consider examining the following aspects prior to relying on the research exemption contained under the DPDPA read with the Rules:

Serial No.	Action Item	Confirmation status
1.	The purpose of the research is clearly defined and properly documented, and the processing qualifies as a genuine research activity under the DPDPA read with the standards prescribed under its underlying rules.	
2.	Personal data is used strictly for research purposes and not to in furtherance of making decisions about, or targeting, profiling, or otherwise affecting identifiable individuals.	
3.	Research participants are provided with a transparent notice regarding the research and the processing of their personal data, and consent is collected and documented as a matter of best practice.	
4.	Personal data collected is limited to what is necessary for the purpose of research, and any sharing with internal teams, vendors, or freelancers is restricted on a need-to-know basis.	
5.	Personal data collected for research is not repurposed for ancillary purposes such as marketing, customer acquisition, profiling, or other unrelated commercial objectives.	
6.	Personal data is retained only for as long as necessary for the purpose of research (including quality control or audit requirements), or longer where required by applicable law, and is thereafter deleted or anonymised.	
7.	Reasonable security safeguards are implemented, including appropriate technical and organisational measures such as access controls, encryption or masking, logging and monitoring, and data backup mechanisms.	
8.	Vendors and processors are engaged under appropriate contracts requiring them to act only on documented instructions, implement reasonable security safeguards, and support breach response to enable the organisation's compliance with applicable laws.	
9.	Appropriate internal governance measures, including documentation, training, and oversight mechanisms, are in place to demonstrate compliance with the DPDPA.	