

A close-up photograph of a person's hands. One hand holds a white pen, and the other rests on a tablet. The tablet is open, showing some text on its screen. The background is a dark, textured surface.

20 FEB 2024

RESEARCH REPORT

Digital Personal Data Protection Act 2023 - Study

PRESENTED BY:
DPDP Consultants

TABLE OF CONTENTS

Introduction	03
I. Methodology	05
II. Key findings	06
1. Awareness	06
2. Concerns and Expectations	09
3. Solutions and Steps to be DPDPA Compliant	10
III. Conclusion	14

INTRODUCTION

In the last ten years, India has surprised the world by proliferating in various aspects; the most significant one has been digitalisation, and the acceptance of digital transformation has been rapid in India; adaptation has been seamless considering the 140-crore population. India is now a digitally powered economy.

With innovation and technology invariably comes significant responsibilities. For a country like India, arguably the most challenging responsibility is ensuring data privacy and security of the digital data of each individual.

At the onset, what looked like the tip of the iceberg is now clearly visible and is more prominent than expected, in the light of which the discretionary need for personal data protection has metamorphosed into a fundamental right, materializing eventually as a constitutionally protected data protection law (the DPDP Act of 2023). Did we run too fast and too far, or was it the need of the hour? Only time will tell.

The good news is that there are no oppositions, no more debates, no more "ifs" and "buts", and most importantly, no more delays. It is out and here to stay. The Digital Personal Data Protection Act 2023 begins a long journey.

Today, while India contends with the world's top economies, it has also commendably joined the race for privacy protection laws with the likes of GDPR - Europe, the Data Protection Act 2018 - United Kingdom, and the California Consumer Privacy Act - United States. This is just the first milestone achieved.

Through a comprehensive study involving a sample size of 500 interviews, this report focuses on awareness of the Digital Personal Data Protection Act 2023, its implementation and the possible consequences of non-compliance.

Furthermore, it touches upon the need and urgency to implement data protection tools and support necessary to cater to the vast and multifaceted Indian economy.

While India is known for its ability to adapt to new laws and occasional abrupt statutory announcements quickly, it will be interesting to see how the country faces the challenges of enforcing DPDP compliance in the coming years.

JOURNEY SO FAR

**Privacy Declared as a
Constitutionally Protected
Right**

2017

This emerged from the assurance of life and personal liberty outlined to Article 21 of the constitution

**Personal Data Protection Bill
(PDPB) is Introduced**

2019

The bill is passed to the Joint Parliamentary Committee (JPC) for examination

**The Bill is Tabled for the 2021
Parliament Winter Session**

2021

JPC takes time to analyse the draft due to the harsh criticism from several fronts

**PDPB is Withdrawn & a new
bill DPDP is Introduced**

2022

In Aug, 2022, PDPB 2019 was withdrawn, and a new version - Digital Personal Data Protection Bill was presented for public consultation in Nov. 2022

**DPDP Bill is Passed Receives
Presidential Assent**

2023

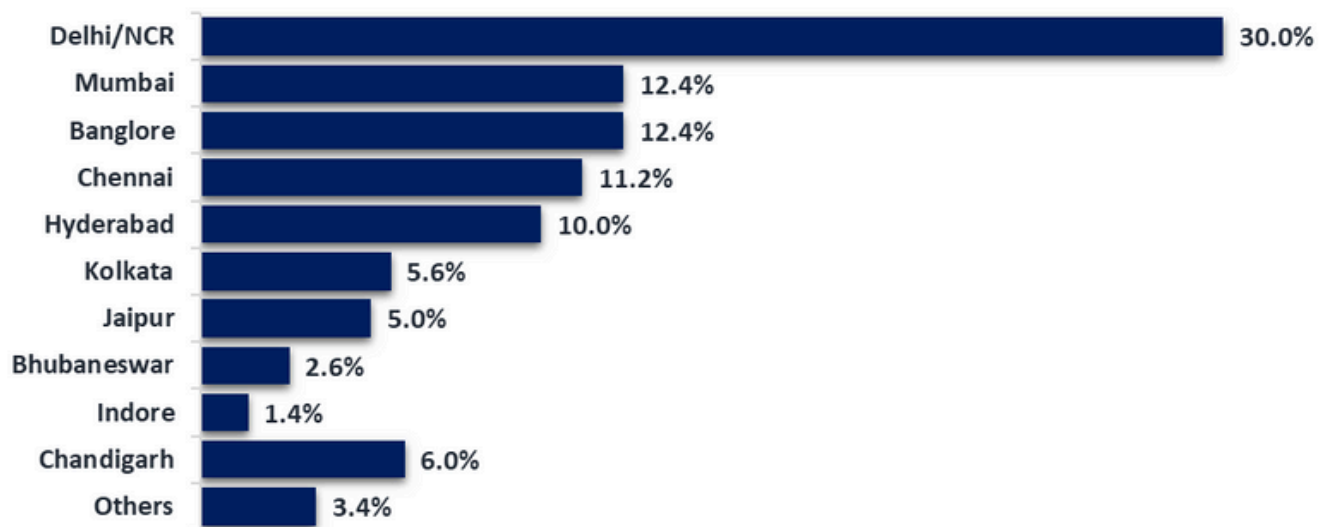
On August 11, 2023, India finally celebrates the enactment of a comprehensive Data Privacy Law.

METHODOLOGY

Sample :

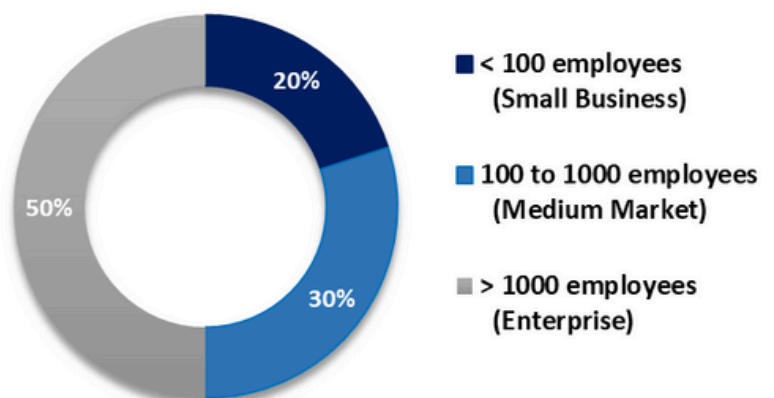
We collaborated with a premier primary research firm, Mindforce Research to survey a diverse sample of 500 participants across India, including **67%** from metropolises such as Delhi, Mumbai, Bangalore, Chennai and Kolkata, along with **33%** of tier-2 cities like Bhubaneswar, Chandigarh and Indore.

CITY WISE DISTRIBUTION



With an employee size ranging from 50 to 1000+, the participants were picked from various organisational functions, including Finance/Accounting, Human Resources, Legal/ Compliance, IT/Security, Marketing/Advertising, Sales, and Operations. The focus industries cover Automotive, Financial Services, Healthcare, Manufacturing, NGO, Real Estate, Retail, Travel and Tourism, and Technology, encompassing C-level executives, Vice Presidents, Directors, Managers, and Outside Consultants.

ORGANIZATION SIZE

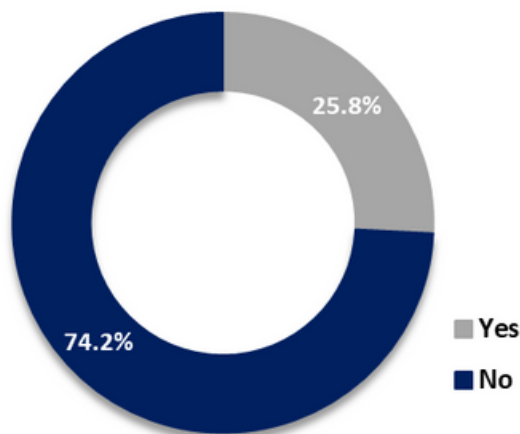


Data Collection: The study used quantitative and qualitative phone surveys and interviews to gather information from participants over a period of two months.

KEY FINDINGS

1 Awareness :

It is encouraging to see that within a span of just five months, **74.2%** of participants, from small businesses to large enterprises, mentioned that they had heard about the Digital Personal Data Protection Act 2023 through sources such as colleagues, friends and thanks to "Digital India", even from the latest available articles and blogs on the internet.



ORGANIZATIONAL AWARENESS OF DPDP ACT 2023

- Interestingly, around **32%** of medium-sized business respondents were unaware of the DPDP Act 2023.
- **40%** of managers to director level personnel have no hint that such a law has been passed

A concerning and unexpected observation was made — **33%** of respondents had no clue of the potential violations of the DPDP Act, which can lead to fines of up to **INR 250 Crore**. A general notion is that companies would contact lawyers and legal firms to seek implementation and support in compliance matters. Law firms will only be able to support the specifics of the law, but implementation is not something that law firms can take on. Looking at the breaches and penalties, this law seems less lenient if one relies only on research reports and half-baked online information.

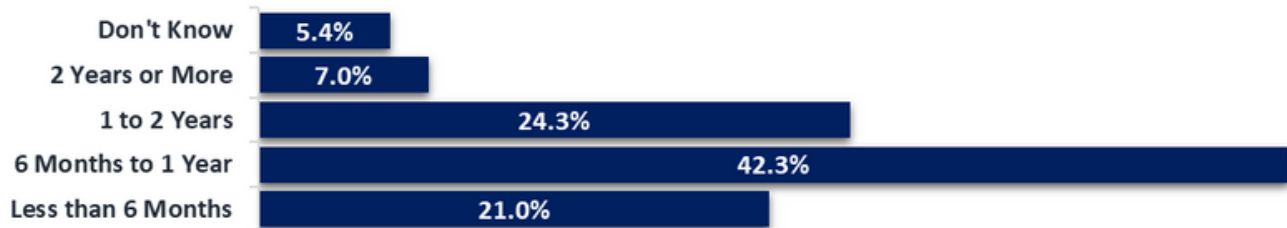
We have seen the classic example of GST. Initially, with GST, various businesses failed to map their accounting software and IT systems, which were concerned with the new tax provisions, to create invoices for GST and various required abstract reports. Moreover, their staff did not possess the necessary skills and knowledge, as training materials were not readily available. Many businesses relied on the available knowledge on the internet for implementation through self-learning and avoided expert advice and consultation. Unfortunately for many, it turned out to be a penny-wise, pound-foolish move. Some faced penalties under the following heads:

Incorrect Returns: Submitting incorrect or inaccurate information in GST returns such as understating tax liability, providing false information, and not rectifying errors promptly.

Non-Compliance: Failure to comply with GST regulations, such as not registering for GST when required, not maintaining proper records, and not issuing correct tax invoices.

ANTICIPATED ENFORCEMENT AND IMPLEMENTATION TIMELINE

IN YOUR OPINION, BY WHEN DO YOU EXPECT THIS LAW TO BE ENFORCED?

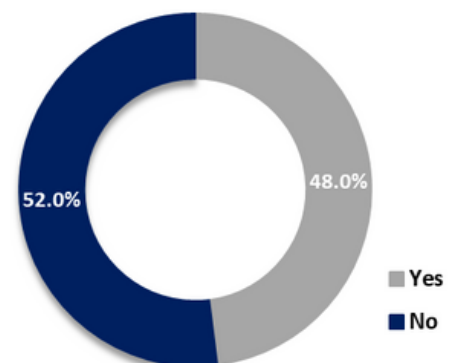


- While these figures are in place, **50%** of the respondents are confused about when to implement compliance measures.
- Another **30%** are still waiting for some rules to be implemented and made more transparent, while others would follow the flock to tackle this issue as and when it happens.
- Overall, about **74%** of participants feel the law will be enforced anytime between 6 months to 2 years.

RESPONDENTS WHO KNEW ABOUT DPDP COMPLIANCE

- **48%** of respondents understand which companies must comply with the DPDP Act 2023.
- It is not surprising to see that **67% of IT professionals** knew about and stumbled upon the subject mostly while researching and updating themselves with data security.
- This contrasts with only **53.3% of compliance professionals** who might be involved with routine aspects of the companies' legalities.

RESPONDENTS WHO KNEW ABOUT DPDP COMPLIANCE



STRATEGIES AND AUTOMATION TRENDS IN PERSONAL DATA PROTECTION

Primarily, all companies, in some way or another, handle or process people's personal data such as name, E-mail, phone number, Aadhar, PAN, Biometrics, and even financial information like bank account details and credit card numbers.

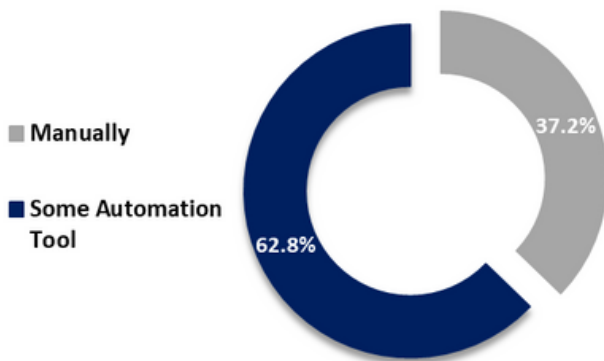
Section 6 of the Digital Personal Data Protection Act 2023 seeks consent from all individuals whose data is stored and/or processed into a company's ecosystem, when asked how companies plan to be compliant.

- **50%** of companies are looking at automation tools to manage consent from all individuals whose data is stored and/or processed into their ecosystem.
- However, only **40%** of the retail and tourism industry participants showed interest in using automation/tools, which essentially use much more personal data for multiple purposes ranging from transaction details to updating customers on the latest offers, deals and launches.
- Around **80%** of IT/Technology companies are open to automation/tools to manage the consent of individuals/customers.

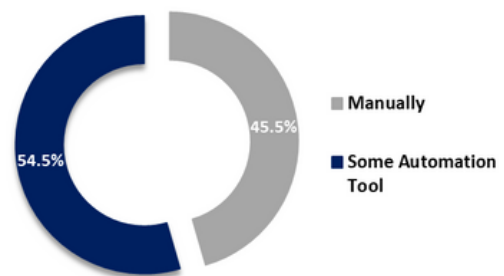
DATA RETENTION AND AUTOMATION AWARENESS IN TRAVEL & TOURISM

The Digital Personal Data Protection Act 2023 is extremely clear about data retention. An organisation cannot collect/store/share any personal data they do not require. **67%** of travel and tourism professionals feel they can manually archive organisational data, and about **55%** of outside consultants who participated suggest they archive data manually for their clients

PLAN TO ARCHIVE ORGANIZATIONAL DATA



OUTSIDE CONSULTANT



- While companies feel the need and urgency of using consent management tools, merely **7%** know about automation/tools, even though these are primarily tech-driven organisations.

MASSIVE KNOWLEDGE GAP IN CRITICAL DATA PRIVACY COMPLIANCE REQUIREMENTS (DPIAS AND DATA PRIVACY FRAMEWORK)

Furthermore, companies are still unaware of terms such as Data Protection Impact Assessment (DPIA). 73% of participants have not heard or are unaware of the Data Protection Impact Assessment. Of the 27% who are aware of such a term, 42% do not have a predefined format in place, while only 3.6% are aware of tools available in the market that help with the automation of DPIA.

Similarly, 53% of directors and high-level contributors in organisations are not well informed when asked if they knew that the Data Protection Board would decide which companies will be categorized as 'Significant Data Fiduciaries' based on the processing of PI. In addition, 38% of companies have no predefined data privacy framework at all. Some have just heard of the term data security framework because they do not have access to any training program that can fulfil the obligations of different sections of the Digital Personal Data Protection Act 2023, as expressed by 68% of the participants.

In a detailed discussion/interview with one of the CTOs of a 1000+ employee tech-driven global organisation, the conversation led to an inquiry about readiness for existing data privacy frameworks with the following response:

"AS FAR AS THE CUSTOMER DATA IS CONCERNED, WE ARE USING ISO 27000 COMPLIANCE FOR DATA FRAMEWORKS. HOWEVER, WE DO NOT HAVE A THIRD-PARTY DEVICE INSTALLED INSIDE OUR PREMISES, AND WE HAVE TAKEN PRELIMINARY MEASURES FOR A LONG TIME FOR ALL GEOGRAPHIES WE ARE DEALING WITH BUT NOT FOR THE INDIA DATABASE."

They mentioned that they are knowledge-wise ready but have no specific tools deployed as yet

2 Concerns and Expectations :

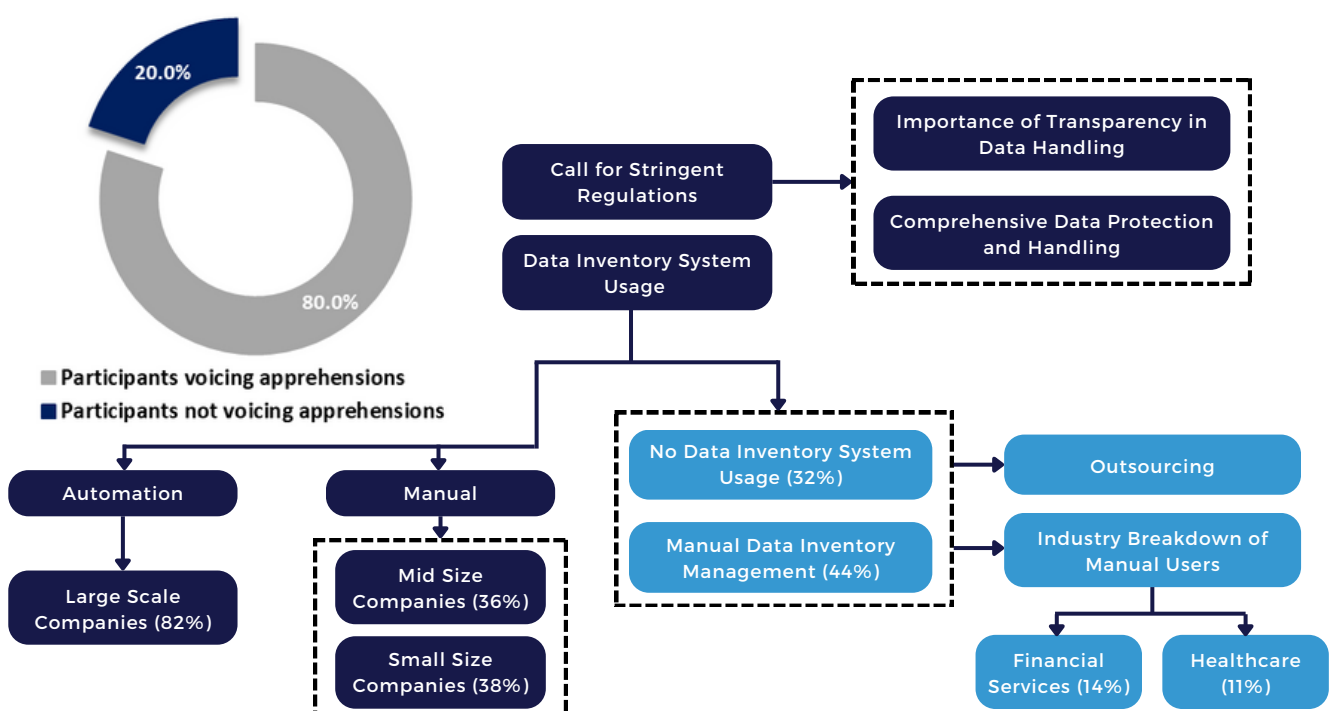
The DPDP Act 2023 has left many corporates feeling uncertain and in need of clarity on numerous related subjects and aspects. More than 80% of participants voiced apprehensions regarding the potential misuse of personal data by corporations and government entities. They called for stringent regulations to protect their data privacy and stressed the importance of transparency in data handling procedures. The prevailing sentiment is that we must ensure that personal information is comprehensively protected and responsibly handled within the digital space.

However, participants mentioned that the timing related to law enforcement and its impact on businesses are causing significant concern to most companies. More so now, as lots of news about big names coming under the scanner for KYC (Know your customer) are getting reported lately in the media. It is essential to address these concerns and ensure that the DPDP Act 2023 provides all stakeholders with the necessary protection and guidance.

32% of participants mentioned that they currently don't use data inventory systems for data-sharing within the organisation or outsourced to a third party for processing, and **44%** use manual data inventory managing methods.

A deeper investigation revealed that out of the ones using Manual Data Inventory, **14%** are from financial services, while **11%** are from the healthcare industry – and while this is just a sample size, we can well estimate what the population size would look like based on the existing trends.

82% of large-scale participating companies and **67%** of C-Level executives participants mentioned that if many requests come from individuals who need timely resolutions and can remind the management about unresolved queries, they are looking at automation tools to manage such queries/requests. Still, on the other hand, **36%** of small businesses and **38%** of mid-size companies think that they can resolve a large number of requests manually coming from individuals who need timely resolutions.



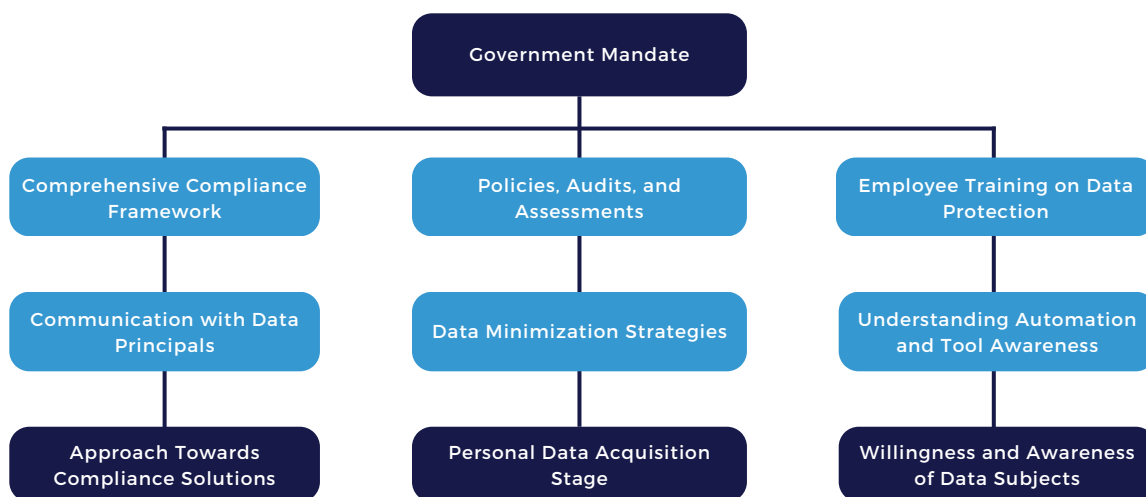
3 Solutions and Steps to be DPDPA Compliant

The DPDP Act is not merely a recommended set of practices or a certification – it is a government mandate – a law that requires 100% adherence in letter and spirit. To ensure that businesses seamlessly implement it and welcome it as a business enabler instead of seeing it as an unnecessary burden imposed upon them, there is a solid need to make a comprehensive compliance framework encompassing policies, regular audits, and assessments available.

All employees must be trained effectively in their data protection responsibilities and the importance of notices and consent as promulgated in the DPDP Act. It becomes even more important to communicate to data owners (referred to as Data Principals in the Act) as to how their personal data will be processed, stored, and utilised, incorporating data minimisation strategies to collect only the necessary information, thereby reducing risks associated with excessive data processing and storage.

A million-dollar question is, how one starts and what the correct approach is. It is not about just being compliant but to stay compliant ever after. To understand the awareness regarding automation and tools available and their importance and implementation, we asked our participants about their approach towards compliance solutions and actioning them out.

The first one that comes to mind is the personal data acquisition stage of any business, and with that comes the willingness and consent of the data subject/principal to share their data.



A) DATA PROTECTION CONSENT MANAGEMENT

There are tools designed on SAAS models that help businesses get valid consent and automate the entire process, ensuring a foolproof system for collection, management, withdrawal, and refresh requests within companies.

Additionally, as per the DPDP Act, all consents must be accompanied by a notice in all Indian languages that specify the personal data to be collected and the purpose of processing. A consent management tool allows businesses to automate this process seamlessly rather than depending on tedious traditional methods like collecting consent over emails.

Section 6 of the Digital Personal Data Protection Act 2023 discusses seeking consent from all individuals whose data is stored and/or processed into your ecosystem. When participants were asked how they would manage the consent of their customers/data principals, 51% responded that they would use E-mail or manual methods to ensure consent management. The remaining 49% are looking at automation and tools as a solution. Interestingly, 93% aren't even aware of any automation/tools that help in consent management.

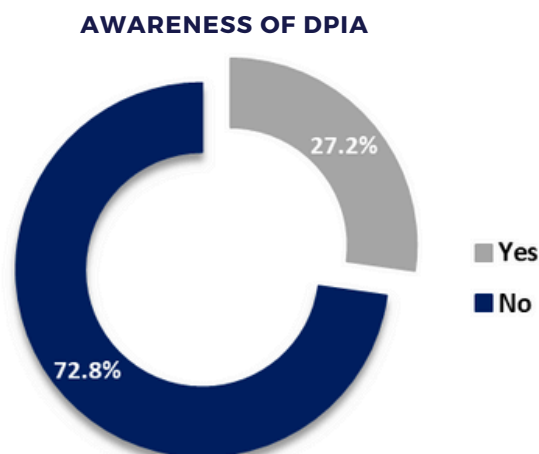
Data constantly flows in a business ecosystem from various sources – from a coffee machine vendor to your CRM and Cloud telephony provider. The importance of data consent management is even more essential today because the law states that even if any business holds data before the commencement of the DPDP Act 2023, it is required to send a notice to all data principals specifying the nature of data, the reason for processing and the rights of the data principals. Consent is not limited to when data is captured “hereafter” but is relevant for all data captured “since” and after that shared or processed. Consent management tools ensure that personal data has a systematic approach to be collected, managed, withdrawn, and refreshed, along with an automated data inventory that helps ensure the mapping of personal data to provide evidence.

B) DATA PROTECTION IMPACT ASSESSMENT (DPIA)

As the name suggests, DPIAs are a systematic approach to analyse, identify, minimise and handle risks associated with the processing of personal data. To align with the DPDP Act 2023, it is recommended that all companies proactively engage in DPIAs to maintain data protection compliance and ensure a high standard of data hygiene. This approach helps meet regulatory obligations and builds a solid foundation for safeguarding individuals' data privacy across all levels of data processing.

When the participants were asked about their awareness of DPIA (Data Protection Impact Assessment), only 27% were found to be acquainted with the term. After further assessment, the lot who knew about DPIA (Data Protection Impact Assessment) were asked if they had a predefined format for DPIA (Data Protection Impact Assessment). 58% said they have some kind of format available already.

While a handy format can be suitable for SMEs, Significant Data Fiduciaries (SDFs) and other prominent organisations would require a more vigorous and scalable approach to manage the massive data handling and collection.



DPIA automated tools allow DPOs to conduct DPIAs through a user-friendly platform, tracking risks identified during the assessment and ensuring that all concerned persons know the developments and the mitigation of these identified risks. DPIA tools will make the process more seamless and manageable than a traditional format without automation.

DPIA automated tool helps in pre-built templates and workflows that guide organisations through the impact assessment process, making it more efficient and standardised. It ensures identifying and evaluating the potential data privacy risks associated with specific data processing activities. It further assists in tracking and managing compliance with various data protection regulations, facilitating the generation of reports that can be shared with regulatory authorities to demonstrate compliance.

C) DATA PROTECTION AWARENESS PROGRAM (DPAP)

Businesses are ensuring that they stay updated on new developments and progress of the DPDP Act 2023. However, only a handful, and in some cases only a small number of employees, are updated with the implementation, measures and potential penalties imposed on breach of the Act.

For companies to be 100% compliant with the law, the entire company, including different functions and employees, need to be trained for it. This part, unfortunately, is often overlooked, but needless to say, is a non-negotiable part of data privacy compliance moving forward.

By doing so, the employees can process data responsibly, know their obligations, and respond swiftly in case of possible breaches or infringements.

In this research, we found that 68% of participants mentioned having no access to any training program that can fulfil the obligations of different sections of the Digital Personal Data Protection Act 2023.

While 59% of all participants know that potential violations of the Act can lead to fines of up to INR 250 Crore, surprisingly, 33% of legal and compliance function participants were unaware of such penalties.

Without proper training, it's impossible to comply with the DPDP Act. A Data Protection Awareness Program should be the norm for all organisations, whether small, medium or large.

A well-informed staff is equipped to handle the implementation of compliance in every stage, function, and process of the organisation, which reduces the risk of breaches leading to penalties of up to INR 250 crore. Demonstrating a 360-degree approach to data protection fosters the trust of the customers and other stakeholders. It is essential to know that data privacy is not solely the responsibility of the compliance and IT departments but is a shared responsibility across all functions. Completing a data privacy awareness program increases each employee's accountability regarding the proper handling and protection of information, thereby reducing the probability of data breaches. In this era where data is termed the new "oil", a complete compliance to DPDP Act 2023 provides a competitive advantage as customers and business partners tend to attach more value to organizations that prioritise data privacy and security.

D) DATA PRINCIPAL GRIEVANCE REDRESSAL (DPGR)

According to Chapter 3 Section 12 of the Digital Personal Data Protection Bill, a Data Principal has the right to inquire, correct, complete, update or request removal of his/her personal data from the company records. These requests made by the Data Principals need to be addressed within a reasonable time. Further, an individual shall have a right to have readily available means of grievance redressal if companies fail in their performance of obligations with respect to the processing of their personal data.

The Data Principal Grievance Redressal tool allows data principals to raise such queries through a user-friendly platform. It will enable requests to be accessed by the Data Protection Officers manually or in an automated way. The primary goal is to reduce the response time to these requests and ensure compliance while informing all the board members of any such query and management of the same.

Only 48% of participants knew that under the DPDP Act 2023, businesses must share a timely legal response to any questions from individuals who reach out concerning how their personal information is stored/processed. This also raises the question of how soon and how much volume can be managed to respond to such queries, more so when such data is shared with third parties and other internal departments.

The Data Principal Grievance Redressal tool enables businesses to identify patterns or recurring issues in data processing, leading to internal improvements in processes, policies, and overall data handling practices. A well-designed grievance redressal system can positively impact an organisation's reputation, showcasing a customer-centric approach and willingness to address customer concerns. It enhances transparency in data processing practices and builds trust among customers or data principals by providing a clear and accessible channel for addressing concerns related to their personal information.

CONCLUSION

Barely six months have passed since the DPDP Act 2023 received the President's assent and became a law in force. After the Digital Personal Data Protection Act enactment, it would be interesting to see how rapidly the awareness spreads and how soon Indian companies will become data privacy compliant.

There are still areas in the law that need more clarity, but while all that unfolds, one needs to learn from the past that awareness and expert handholding are the keys to compliance with law and legislation.

In India, organisations have a considerably large population to cater to. Automation tools can be a boon and arguably the only way to overcome such challenges. There is, however, a sigh of relief to see that experts from India who are well-versed in various data privacy laws across the globe are now ready to take on the challenge of helping Indian companies learn and get compliant with the DPDP Act.

This move ensures that we need not reinvent the wheel or face failure from implementors as when we look at other geographies and their data privacy laws – especially GDPR –everything is tried and tested.

It is truly encouraging to see the acceptance of businesses that are moving towards automation and tools to ensure the readiness to invest. 60% of participants mentioned that they are ready to invest Rs.25,000 - Rs.1,50,000 quarterly, half-yearly or in an annual subscription.

This stance proves that businesses are not hesitant to switch their traditional methods to ensure compliance, not only to avoid hefty penalties that go up to INR 250 crores, but also not to get distracted from their core business operation managing complexities and obligation of law and ensure that they have the trust and comfort of their customer, which eventually works as a business enabler.

While companies look at the Implementation of the DPDP Act from a mandatory compliance standpoint, the trends from other parts of the world like Europe and the UK prove that their businesses are perceived more seriously and respected and have a preferred choice to do business with.

We also see quick and evident trends where, on Feb 28th 2024, RBI asked banks to comply with the **DPDP Act provision under the updated regulatory sandbox.**

Organisations with the onset of data laws echo: **"If we work with a non-compliant vendor, it will make our company non-compliant."** It is clear that only a compliant company may expect to work with another compliant company. Since the data protection responsibilities rest entirely on the data fiduciary and not on data processors (the data fiduciary will bear the penalty), the question is, should companies then find data processors who can share the penalty fine or should they ensure that their processors are compliant with DPDP Act 2023?

It has been observed in Europe and the UK that companies who are data privacy compliant are the preferred choice of the clients as it gives them a sense of security of their data along with the assurance that they would handle every aspect responsibly and will be conscious of executing everything within a legal framework.

PRIME MINISTER NARENDRA MODI STATED IN HIS FINAL ADDRESS TO THE 17TH LOK SABHA ON FEB 10TH 2024, THUS:

“UNTIL YESTERDAY, WHAT HAD NO VALUE HAS NOW BECOME INVALUABLE, LIKE DATA. THE ENTIRE WORLD IS DISCUSSING THE CAPABILITY OF DATA.”

HE CONTINUED:

“THE ACT ALSO HAS GUIDELINES FOR HOW THE DATA SHOULD BE USED. INDIA IS ALSO POISED TO FULLY USE DATA’S CAPABILITY – WHICH PEOPLE CALL ‘GOLD MINE’ AND ‘NEW OIL’ – WHILE KEEPING PROTECTION IN MIND,”.

FURTHER, HE CONCLUDED BY SAYING:

“INDIA IS SPECIAL IN THIS FIELD BECAUSE IT IS FULL OF DIVERSITY. THE KIND OF INFORMATION THAT WE HAVE AND THE DATA THAT IS GENERATED ABOUT US IF SOMEONE WERE TO LOOK AT ONLY DATA OF OUR RAILWAY PASSENGERS, IT BECOMES A SUBJECT OF RESEARCH FOR THE WORLD. WE HAVE RECOGNISED ITS POWER AND THUS COME OUT WITH THIS ACT.”

CONTACT US



0120-6930999, 1800-5711333



info@dpdpconsultants.com



www.gdprconsultants.in,
www.dpdpconsultants.com



4th floor, GM IT Park, Plot no 32-33, Sector
142, Noida, Uttar Pradesh 201305