Data Privacy Day 2024 – Deloitte-DSCI Joint Roundtable
Event Summary
January 2024
Privacy Leadership Meet - CXO’s guide to operationalising DPDPA

As part of Data Privacy Day engagements, Deloitte India and the Data Security Council of India invited CXOs and senior leaders from IT organisations, healthcare, financial firms, and other user companies to discuss the operationalisation of the DPDPA Act. The agenda for the day included engaging tabletop exercises, a fireside chat, and insightful presentations.

The state of current affairs - compliance and responses to DPDPA

The response to the DPDPA has been multifaceted, reflecting the complexities and implications of this significant legislation and it reflects a proactive and concerted effort by organisations to navigate the challenges and opportunities presented by this legislation, while upholding the principles of data protection and privacy. The rules would make the act complete and describe in detail the nuances of implementation. It is also anticipated that the Data Protection Board will be established by the end of this year. While it may not possess authoritative powers, it will serve as a vital grievance redressal mechanism. Despite not holding formal authority, the presence of the Data Protection Board will undoubtedly influence compliance efforts, complementing its significance within the regulatory landscape.

This year marks a significant focus on implementing privacy measures within organisations. We will see efforts on the part of the organisation to establish robust privacy structures and delineate privacy roles, and measures, especially concerning products and services that interact directly with consumers to collect information and deliver services.

While defining the privacy agenda amidst emerging technologies, it’s crucial to consider various factors beyond mere digitisation. It is important to navigate the complex intersection of technology, geopolitics, and privacy concerns to ensure a proactive approach to privacy and security in this era of rapid technological advancement.

Another key consideration is the increasing aggregation and utilisation of data. Understanding privacy implications at an aggregate level is paramount, necessitating collaboration and input from multiple organisations to inform public policy and shape privacy perspectives. Initiatives like Digilocker highlight the importance of examining privacy at an aggregate level within the government ecosystem.

As we celebrate Privacy Day, it is important to foster innovation in data privacy through startups and engineering initiatives, leveraging cryptographic solutions, and exploring privacy-focused use cases across various industries, including hardware, space startups, drones, and MSMEs.

Emphasis is placed on adhering to principles and conceptual frameworks rather than prescribing specific solutions, particularly with regards to privacy management. Looking ahead, the focus shifts towards the implementation of privacy measures across various sectors, acknowledging the diverse environments and products in play. Additionally, emerging technologies, geopolitical considerations, and the aggregation of data present new challenges and opportunities, necessitating a holistic approach to privacy management.
DPDPA implementation – learnings from GDPR on what works and what doesn’t.

Is the absence of notified rules for the DPDPA indicative of a pause in progress, or should organisations proceed regardless? How does this compare to the situation in 2016 when the GDPR was in place, but enforcement was pending?

Reflecting on 2016, when the GDPR (General Data Protection Regulation) was established but enforcement was pending, organisations were still expected to prioritise compliance with the regulation. Despite the delay in enforcement, businesses were strongly encouraged to proactively work towards meeting the GDPR’s requirements. It was understood that non-compliance could lead to penalties once enforcement commenced.

It is advisable for organisations to take a proactive approach, and not wait for the rules to be enforced. Organisations need to learn and unlearn various aspects to keep up with the evolving understanding of the law, with the belief that the law itself won’t change drastically. Challenges persist in areas like third-party and vendor management, ongoing training, and budget constraints, with an emphasis on the importance of a well-trained workforce. Despite challenges and changes, there’s a belief that the law will remain constant, and the industry needs to be a part of the momentum.

How can organisations effectively initiate their journey towards privacy compliance and robust data protection measures?

To effectively initiate their journey towards privacy compliance, organisations should begin to understand their data architecture, storage practices and map the whole process and flow of data, also the cross-border transfers of data. Following this understanding, organisations should proceed by forming dedicated teams and undertaking essential actions, such as managing vendors, conducting training and awareness initiatives, and establishing a robust data governance framework. These steps are fundamental in ensuring comprehensive and systematic management of privacy compliance efforts.

Should privacy implementation be undertaken by one department, or do you think various functions have roles to play within the organisation?

During the implementation of GDPR, the process was not solely undertaken by a single team. Rather, it involved a collaborative effort encompassing the intersection of multiple teams and various departments, each playing a significant role. It is important that each function plays an active role in understanding the privacy requirements, making their function compliant, with policies, frameworks, and implementation charter managed centrally. By involving the business, organisations can tap into diverse perspectives, get hold of personal data processed across various business functions, enhance communication and coordination, and ensure comprehensive coverage of privacy-related activities.

What strategies can organisations employ to effectively persuade management to allocate budgetary resources for the privacy programme?

Organisations can employ several strategies to effectively persuade management to allocate budgetary resources for the privacy programme. Organisations need to emphasise the importance of complying with existing and upcoming privacy regulations. The relevant stakeholders need to be informed about the evolving regulatory framework and its impact on the business landscape. As regulations change, so does the nature of the operations. However, as time passes and legislation becomes more established, leadership focus on compliance tends to diminish, leading to delays in necessary actions.
It’s crucial to recognise that the right time to initiate the process is now. By proactively addressing compliance requirements and adapting to changes in the regulatory environment, we can mitigate risks and seize opportunities effectively, and present a thorough assessment of the risks associated with inadequate privacy measures, including data breaches, lawsuits, and loss of customer trust. We can also use data and case studies to demonstrate the potential costs of these risks to the organisation.

Presentation on the industry response to DPDPA

To delve into the practical implications of the DPDPA, a presentation on the industry response to DPDPA was made by DSCI based on the industry responses gathered through reading sessions across DSCI forums and with the membership base of DSCI. The session dealt with five key thematic areas, including organisational roles, notice and consent management, incident management and reporting, rights of data principals and enforcement. The following key pointers were presented:

01. There’s ambiguity in classifying entities as fiduciaries or processors, particularly while considering technological advancements, and necessitating clarity on accountability.

02. Managing notice and consent involves complexities in mode, language, and applicability, particularly for data processors lacking direct interaction with data principals, leading to questions on consent thresholds and the role of processors.

03. Incident management requires a nuanced understanding of breaches beyond typical security incidents, with accountability and a risk-based reporting approach being crucial.

04. Data principal rights, such as nomination and verification, is not defined comprehensively within the current framework, urging us to reflect on the validity and extent of such nominations.

05. Enforcement concerns revolve around the proactive engagement of regulatory bodies, industry involvement, and navigating complexities in penalties and dispute resolutions.
Addressing challenges across the workstreams of DPDPA implementation

As a follow-up to the presentation, a table-top exercise was conducted focusing on five distinct problem statements. Participants were tasked with presenting their insights and proposing solutions within these thematic areas. The exercise aimed to explore the complexities of implementing the DPDPA in real-world scenarios and foster discussions around effective strategies for compliance. The following were the areas which were discussed:

(i) **Data inventory**
Keeping track of all data collected, processed, and stored by the organisation is a significant challenge. With data spread across various systems, departments, and third-party vendors, maintaining an accurate and up-to-date data inventory becomes complex.
Implementing automated tools and systems to discover, classify, and inventory data assets can streamline the process. Regular audits and data mapping exercises are also essential to ensure completeness and accuracy.

(ii) **Data principal’s rights**
Managing data principal requests, such as access, rectification, or deletion, poses challenges due to the volume of requests, varying legal requirements, and tight timelines for response.
Establishing a clear process for handling data principal requests is crucial. This includes creating standardised request forms, implementing secure channels for communication, and training staff on proper procedures. Utilising technology solutions for request management and tracking can also improve efficiency.

(iii) **Personal data breaches**
Data breaches present a significant risk to privacy programmes, potentially leading to reputational damage, regulatory fines, and legal liabilities. Detecting, responding to, and mitigating the impact of data breaches in a timely manner is challenging.
Developing and regularly testing an incident response plan is essential. This includes establishing clear roles and responsibilities, conducting incident response drills, and collaborating with legal, IT, and communication teams, to ensure a coordinated response. Implementing robust security measures, such as encryption and access controls, can also help prevent and mitigate breaches.
Governance, audits, and accountability

Ensuring accountability for privacy within the organisation, especially in decentralised environments, can be challenging. Without clear ownership and accountability mechanisms, it’s difficult to enforce privacy policies and procedures effectively.

Experts discussed the need for a top-down rigour, and the establishment of an executive level steering committee with representation from different business functions, chaired by a CISO, CIO, or a DPO, with the responsibility to create a governance framework and roll out the privacy implementation charter. Having a privacy governance framework with clearly defined roles, responsibilities, and reporting structures is essential. This includes establishing the privacy function, conducting regular privacy training, implementing mechanisms for monitoring, and enforcing compliance, and implementing periodic privacy audits.

Grounds for processing personal data

Managing notice and consent mechanisms effectively, especially in the context of evolving regulatory requirements and user expectations, poses challenges. Ensuring that notices are clear, concise, and easily accessible, and obtaining valid consent from users can be complex.

Implementing user-friendly notice and consent mechanisms that are transparent and easily understandable is crucial. This may involve providing granular consent options, offering privacy preference management tools, and regularly reviewing and updating privacy notices to reflect changes in data processing activities and regulatory requirements. Additionally, ensuring that consent records are accurately maintained and documented is essential for demonstrating compliance.