CII-TATA COMMUNICATIONS CENTRE FOR DIGITAL TRANSFORMATION

Confederation of Indian Industry

protiviti®
Global Business Consulting

NAVIGATING DATA PRIVACY IN DIGITAL INDIA

Digital Personal Data Protection Act, 2023: Industry Impact and Roadmap to Compliance

Table of Contents

Introduction

Government of India has a vision of digital India and is heading towards the goal of "Internet for all". Internet subscriber base in India has grown exponentially since 2014 when there were 250 million subscribers and now crossed over 850 million[1]. The rapid adoption of digital technology in India has led to a dynamic evolution of the data privacy landscape. This evolution is being driven by factors such as the increasing use of cloud computing, mobile devices, and greater penetration of digital technologies. The Government of India has also initiated the Digital India as a flagship program with a vision to transform India into a digitally empowered society and knowledge economy.

> *Digital India is not just a name, it is a big vision for the development of the country. The goal of this vision is to carry that technology to the common people, which works for the people and works by connecting with the people.*[2]
>
> *- Shri Narendra Modi, Honorable Prime Minister of India*

The widespread adoption of digital technology has resulted in data privacy emerging as a critical concern globally. India is no exception, as the increased use of digital technology and the consequent rise in the quantity of personal data being generated has heightened concerns about data privacy in the country.

India is identified amongest the largest populations of internet users in the world, and as a result, personal data is being generated at an unprecedented rate. As the volume of personal data increases, so does the threat of data breaches and cyber-attacks. In recent years, India has witnessed several high-profile data breaches, which exposed the personal information of millions Indian citizens. This escalation was particularly pronounced during the Covid-19 situation, as remote work and the rapid adoption of digital platforms became the norm. India witnessed an alarming number of cybersecurity-related incidents, with 1.4 million incidents reported in 2021 and 0.21 million incidents in January and February 2022 alone as per Cert-In reports. Notably, big data breaches occurred within prominent companies across sectors. In addition, there has been a growing concern about the use of personal data by companies for targeted advertising and other purposes using various online platforms. The rise of social media and messaging apps has made it easier for fake news, identity theft and misinformation to spread, highlighting the need for stricter regulation of online content. These breaches resulted in severe consequences for individuals, including financial losses, reputational damage, and even physical harm.

To address the growing need for data protection, the Indian Government has taken several steps to regulate the collection, storage, and use of personal data and still endeavors to strengthen it.

The Indian government has recognized the importance of data privacy and has taken steps to protect personal data. Protecting personal data is not only a legal requirement, but also an ethical responsibility for individuals, organizations, and the government. The Digital Personal Data Protection Act, 2023 shall help to ensure that the use of personal data is ethical, responsible and the individuals have control over their personal data.

Source:

[1] *https://trai.gov.in/sites/default/files/PR_No.08of2023.pdf*

[2] *https://www.narendramodi.in/text-of-prime-minister-narendra-modi-s-address-at-the-india-mobile-congress-launch-of-5g-services-in-india-564831*

Evolution of Legal and Regulatory Framework for Data Privacy in India

Overview of the Current Legal and Regulatory Framework

India's legal and regulatory framework on data privacy has been evolving consistently and moving in the right direction. The timeline of key aspect is as follows:

2000

Data protection / privacy laws in India are mainly governed by the Information Technology Act of 2000 and its associated rules and regulations

2008

Amendments were made to the Act to include provisions for data protection and privacy, including penalties for unauthorized access to personal data.

2016

Aadhaar Act 2016 provisioned protection of privacy by providing a legal framework for the collection, storage, and use of Aadhaar-related information.

2017

The Supreme Court of India declared the right to privacy as a fundamental right under the Indian Constitution. This decision paved the way for the development of a comprehensive data privacy framework in India.

2018

A committee was established by the government of India to develop a data protection law, which was headed by Justice B.N. Srikrishna. In July of that year, the committee submitted its report that proposed the implementation of a thorough data protection law that would oversee the acquisition, retention, and utilization of personal data in India.

2019

The Personal Data Protection (PDP) Bill was introduced in the Indian Parliament. The bill is based on the recommendations of the Srikrishna committee and aims to provide a comprehensive framework for data protection in India.

2021

The Medical Termination Of Pregnancy (Amendment) Act, 2021 restricts registered medical practitioners from disclosing the identity and personal information of a woman who has undergone an abortion. According to the rules, this information can only be shared with individuals authorized by law to receive such information.

2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were introduced by the GOI to regulate digital content and social media platforms addressing concerns related to fake news, misinformation, illegal content, and user privacy.

2022

In September 2022, the RBI issued Digital Lending Guidelines that imposes strict data privacy standards by mandating consent to process personal data and restricting the free flow of information between borrowers and lenders.

2022

The government withdrew the PDP Bill in August 2022, citing the extensive changes made to the 2019 bill by the Joint Parliamentary Committee (JPC) and prepared a new draft bill, namely, the Digital Personal Data Protection Act, 2022.

2023

The Digital Personal Data Protection Act was passed by the Lok Sabha and Rajya Sabha. Subsequently, on 11th August 2023, the President's assent was received on the Digital Personal Data Protection Act, 2023.

Further India has also signed various international agreements and treaties that have implications for data privacy, including the General Data Protection Regulation (GDPR) of the European Union, the Convention on Cybercrime of the Council of Europe, and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

India has a legal and regulatory framework for data privacy that is rapidly evolving. The Digital Personal Data Protection Act, 2023 is expected to significantly enhance data privacy protection in India. The framework aims to strike a balance between protecting personal data, promoting innovation and growth in the digital economy.

Key Takeaways from the Digital Personal Data Protection Act, 2023

With multiple revisions of the bill the Indian Government has made significant efforts to create a legislation that effectively safeguards the privacy of its vast user base of over 850 million internet subscribers. The Personal Data Protection Bill underwent thorough examination by experts nationwide and concerns were raised by organizations due to provisions such as data localization. Following the scrutiny and review of multiple amendments by the Joint Parliamentary Committee, the bill was withdrawn in August 2022, with the assurance of a new bill that aligns with India's comprehensive legal framework.

The Ministry of Electronics and Information Technology (MEITY) had introduced a fresh bill, outlining the rights and responsibilities of the "Digital Nagrik" (digital citizen) as well as data fiduciary and emphasizing the lawful utilization of collected data. Taking inspiration from successful models in Singapore, Australia, and the European Union, the bill is built on the principles of lawfulness, data minimization, purpose limitation, accuracy, storage limitation and accountability. This also enables individuals to exercise their rights while ensuring a balance between privacy and business needs. President's assent was received on the Digital Personal Data Protection Act, 2023.

It is notable that the language of the document has been crafted to empower women, using "Her" and "She" to represent all individuals, regardless of their gender. This unprecedented linguistic choice in India's legislative history marks a significant stride towards inclusivity.

Key Highlights of the Digital Personal Data Protection Act, 2023 are as below:

Data Principal and Data Fiduciary

- The 'Data Principal' is the individual to whom the personal data relates to. For children (under 18 years), their parents or lawful guardians are recognized as their Data Principals. In case of persons with disability, their lawful guardian is recognized as their Data Principal.
- The Data Fiduciary is the entity (such as an individual, company, or state) that defines purpose and means of processing data.

Applicability and Scope

- The scope pertains to personal data within the territory of India acquired through online channels or personal data initially obtained offline and subsequently digitized. Accordingly, the following are exempt from the purview of this legislation – all offline personal data, anything not digitized, data processed for personal or domestic purpose, data shared publicly by Data Principal (to whom the data is related to) or legally obligated disclosure of personal data based on current Indian laws.
- The scope shall also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any profiling of, or activity of offering goods or services to Data Principals within the territory of India.

Applicability to Data

- The act does not distinguish between personal and sensitive personal data. It adopts a comprehensive approach to protect all personal data uniformly, requiring consent for data collection.

Lawful Basis of Processing, Consent and Legitimate uses

- Data Fiduciaries are required to provide a detailed notice to the Data Principal, clearly stating the itemized list of personal data they intend to collect and the purpose for its processing. Access to this information shall be provided in English or any language specified in the eighth schedule of the Constitution of India.
- Further, the contact details of the data protection officer/ authorized person shall also be provided to the data principal for responding to any communication for exercising the rights.
- The Data Principal shall have the right to give, manage, review or withdraw consent to the Data Fiduciary. This shall be done through a 'Consent Manager' (i.e. a single point of contact to enable these actions through an accessible, transparent and interoperable platform).
- Legitimate use includes processing of personal data for a purpose where data principal has voluntarily provided the data (and not indicated denial of consent). Further, this includes data that is processed to fulfill state duties, uphold the sovereignty, integrity and security of the nation, to administer benefits, disclosures for fulfilling legal obligations, assistance in a health emergency, disaster/ public order situations or safeguarding the employer from loss of liability.

Data Protection Board

- The Central Government is also tasked to establish Data Protection Board of India as an independent body which will oversee the compliance of the law, when passed. The board shall have the power to penalize the Data Fiduciaries as well as Data Principals in case of non-compliances.
- Further, for providing more power to the individuals, modes such as alternate dispute resolutions and appeal against the board to high court has been identified.

Registration

- The consent manager needs to register with the Data Protection Board.

Cross Border Data Transfer

- The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to a country or territory outside India.

Appointment of a Data Protection Officer and Data Auditor

- The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of relevant factors, including the volume/ sensitivity of personal data processed, harm to the Data Principal, potential impact on the sovereignty and integrity of India, risk to electoral democracy, security of the State, public order and such other factors as it may consider necessary.
- Significant Data Fiduciaries shall be obligated to appoint a Data Protection Officer based in India who shall be responsible to the board of directors or significant governing body.
- Significant data fiduciaries are required to appoint an independent data auditor who shall evaluate the compliance with the provisions of the act periodically. Further, periodic Data Privacy Impact Assessment (DPIA) shall be performed.

Rights of the Data Principal

- A Data Principal shall have the right to grievance, right to access, right to correction & erasure of the personal data for which consent was previously given.
- Data Principals have the right to appoint another individual who will exercise their rights under the Act in case of the Principal's death or incapacity.

Breach Notification

- The Act mandates that, following a data breach, the Data Fiduciary must alert the Data Protection Board and each impacted Data Principal.
- This positive step ensures that Data Principals, whose personal data has been compromised, are informed about any data breaches, no matter the level of risk involved.

Penalties

- Non-compliance by Data Fiduciary : Penalty of upto INR 250 Crores on breach in observing the obligations of the act related to aspects such as :
  - Reasonable security safeguards
  - Providing a notice to the Data protection board / Data principal in case of a breach
  - Obligations related to children
  - Additional obligations of significant Data fiduciaries
  - Any other provisions of the Act
- Non-compliance by Data Principal : Upto INR 10,000.

Timeline for Compliance

- While the Act doesn't outline a specific implementation schedule, it does require organizations to take a more proactive stance in adhering to the Act's provisions.

The Act aims to establish a harmonious balance between the right to privacy and the needs of national security. It includes provisions that allow for exemptions in cases where the processing of personal data is necessary to protect national security interests. This approach ensures the protection of privacy rights while also addressing the legitimate concerns of national security and leveraging data for beneficial purposes, with due consideration to individual privacy.

Overall the Digital Personal Data Protection Act, 2023 is in the right direction and should pave the road towards better protection of data and strengthen the data protection system of India overall robust and mature in the long run.

Key Privacy Considerations across Industries

While privacy regulations have broad requirements applicable across industries, it is important to focus on industry-specific data privacy considerations in line with both global and local requirements.

The following representative list highlights such considerations categorized by industry sectors.

Banking, Financial Services and Insurance (BFSI) & Fintech

This sector is among the most regulated and already has requirements provided by regulators such as Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), Insurance Regulatory and Development Authority of India (IRDAI) and Unique Identification Authority of India (UIDAI) covering aspects of cyber security with some elements of privacy. For larger organizations spread across multiple geographies, there is a need for complying with global privacy regulations such as General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and others as applicable. This industry has played a significant role in driving the widespread adoption of digital technologies, analytics, and governance practices.

- **Customer Personal Data Protection:** Enhanced measures for organizations to collect, store, and process customer data.
- **Customer Communication and Marketing with Consent Management:** Emphasis should be on obtaining informed consent from individuals for the collection, use, and disclosure of their personal data.
- **Strengthened Data Privacy Practices:** Data privacy requirements shall drive this sector to further invest in robust privacy measures. This includes encryption, identity management, secure data storage and regular security audits to safeguard customer data from unauthorized access and breaches.
- **Data Handling Practices:** Data privacy requirements influence how organizations collect, store, process, and share customer data. Institutions must obtain consent, provide clear information about data usage, and enable customers to exercise their privacy rights, such as accessing or deleting their data. These practices enhance transparency and empower customers to control their personal information.
- **Data Sharing and Partnerships:** Data privacy requirements impact how banks share customer data with third parties and engage in partnerships. Institutions must ensure compliance when sharing data for analytics, risk assessment or collaboration with other financial service providers. Strict requirements regarding data anonymization and consent can affect data sharing practices.
- **Data Breach Notification and Response:** In the event of a data breach, organizations should have a mechanism to promptly notify authorities and affected individuals. Institutions must have incident response plans in place to effectively address breaches, mitigate harm, and fulfill reporting obligations.
- **Cross-border Data Transfers:** For multinational banks, data privacy requirements pose challenges when transferring customer data across borders. Adequate safeguards must be implemented to ensure compliance to the local regulation and that data transferred to countries with different privacy laws maintains an appropriate level of protection.

Healthcare and Lifesciences

This sector handles a sizable volume of personal data including health information. The healthcare sector is already subject to multiple global data privacy regulations, such as Health Insurance Portability and Accountability Act (HIPAA) in the United States, GDPR in the European Union and shall be subject to the Digital Personal Data Protection Act,(2023). Key aspects to be considered are as follows:

- **Patient Confidentiality and Trust:** Safeguarding patient privacy is essential for building and maintaining trust in healthcare organizations. Data privacy ensure that patients' personal and medical information is handled with utmost confidentiality and is not disclosed without their consent. This fosters a trusted relationship between healthcare providers and patients.
- **Security of Electronic Health Records (EHRs):** Data privacy requirements shall reinforce the necessity of having robust security measures for electronic health records. Healthcare organizations must implement access controls, encryption, and audit trails to protect patient personal data from unauthorized access, breaches, and cybersecurity threats. This ensures the confidentiality and integrity of patient information.
- **Research and Development (R&D):** Processes followed for research activities may need to be aligned with the privacy regulation since these frequently entail the processing of personal health data. Organizations must navigate privacy requirements while promoting research advancements and upholding data privacy and participant rights through the implementation of suitable safeguards.
- **Health Information Exchange (HIE):** Data privacy requirements impact the exchange of patient information between various healthcare entities (including cross border exchange as applicable). Organizations must establish secure mechanisms and protocols for sharing patient data while maintaining privacy and complying with the regulations. This enables seamless coordination of care, improved healthcare outcomes, and reduced duplication of tests and procedures.
- **Telemedicine and Remote Monitoring:** The emergence of telemedicine and remote monitoring technologies introduces new challenges for data privacy. Healthcare providers must ensure that patient data transmitted and stored through these platforms are adequately protected to maintain confidentiality and prevent unauthorized access.

Manufacturing

Manufacturing companies often handle valuable intellectual property, such as product designs, trade secrets, and manufacturing processes. With the data privacy requirements additional measures will be needed for protection of personal information. Key considerations are as follows:

- **Customer Data Protection:** The manufacturing sector increasingly collects and analyzes customer data for various purposes, including market research, product development, product purchase/warranty/support and personalized marketing. Data privacy requirements would need to ensure that customer data is collected and used with proper consent, securely stored, and protected from unauthorized access or disclosure.
- **Supply Chain Data Management:** Manufacturing companies collaborate with suppliers, distributors, and other partners across their supply chain (within the country and outside). Data privacy requirements necessitate the implementation of robust data management practices, including secure data sharing protocols, data protection agreements, and compliance verification for all third parties and partners
- **Internet-of-Things (IoT) and Connected Devices:** IoT and connected Devices pose unique privacy risks. The manufacturers would need to consider the privacy-by-design principles and provide the customers accurate information about the data collection, related purpose and the consent needed.

Information Technology

IT companies lead the way in supporting their clients' business transformations. Amidst the COVID outbreak, IT companies underwent their own adaptations and transformations, enabling their teams to swiftly adjust and serve clients in a contact less world. The sector has its own unique challenges and key considerations to address these are as follows :

- **Enhanced Cybersecurity Measures:** Data privacy requirements drive the adoption of robust cybersecurity measures to protect IT/ITES companies from cyber threats, including encryption, access controls, and regular security audits.
- **Business Opportunities and Market Advantage:** Adhering to data privacy requirements can provide IT/ITES companies with a competitive edge. Companies that can demonstrate compliance and effective data privacy practices may be preferred by clients and partners over competitors who do not prioritize data privacy.
- **Enhancements in Emerging Technologies:** Emerging technologies such as Artificial Intelligence, Machine Learning, Big Data Analytics, Virtual or Augmented Reality tend to collect/ process/ transmit large volumes of information for their operation. Organizations will need to keep the privacy regulations in mind while the development of these technologies is undertaken.
- **Trust and Reputation:** IT/ITES companies that prioritize data privacy can build a reputation for trustworthiness and responsible data handling. This can attract customers, partners, and investors who value data privacy and security.
- **Data Sharing and Cross-border Transfers:** Large IT/ITES companies tend to work across geographies must ensure that data is transferred securely and in compliance with applicable local/ global regulations while conducting international business or working with global clients.
- **Data Breach Response and Notification:** Data privacy requirements emphasize a timely response and notification process in the event of a data breach. IT/ITES companies must have incident response plans in place to detect, investigate, contain, and notify affected parties about data breaches.
- **Data Governance and Accountability:** Data privacy requirements emphasize the need for robust data governance practices, including data classification, access controls, data retention, and data disposal. IT/ITES companies must establish accountability mechanisms to ensure compliance with these practices.

Media and Telecommunications

The Media and Telecommunication industry encompass various sub-industries, including print, TV, telecommunication, OTT (Over-the-top), Gaming, Films, VFX (Visual Effects), Audio and Digital. Each of these sectors plays a significant role in the dynamic landscape of the industry. The impact of data privacy on the Media, and Telecommunications sector is significant. Key areas of consideration are as follows:

- **Targeted Advertising and Personalization:** Media and Telecommunications companies heavily rely on user data for targeted advertising and personalized content delivery. Data privacy requirements emphasize obtaining user consent for such practices and ensuring responsible use of user data while respecting privacy preferences.
- **Data Monetization and Partnerships:** Media and Telecommunications companies often engage in data-sharing partnerships for insights and monetization purposes. Data privacy requirements emphasize the importance of establishing robust data-sharing agreements that protect user privacy while enabling effective collaboration and data-driven initiatives.

- **Consumer Perception and Trust:** By adhering to data privacy regulations, media and telecommunications companies can build a positive reputation and gain the trust of their users. Demonstrating a commitment to protecting user privacy helps attract loyal customers who value their data privacy rights.
- **Innovation and Ethical Data Use (including that through AI/ML/Automation):** Data privacy requirements encourage ethical data use practices in the media and telecom sector. By incorporating privacy-by-design principles, companies can innovate responsibly, ensuring user privacy is respected throughout the development and deployment of new technologies and services.
- **Consent and Transparency:** Data privacy regulations emphasize obtaining user consent and providing clear information about data collection, processing, and usage practices. This empowers users to make informed choices and have control over how their data is utilized by media and telecommunications companies.
- **Privacy for Children:** Privacy regulations place particular emphasis on safeguarding the privacy of children. Media and entertainment companies that specifically target or gather personal data from children must adhere to specific obligations. These include obtaining parental/lawful guardian consent and implementing suitable privacy measures to protect the privacy of child users.

Energy and Utilities

Energy and utility organizations are currently undergoing extensive transformations across their entire value chain. Factors such as the pandemic, geopolitical instability, climate change, fluctuating oil prices, and evolving workforce dynamics, have contributed to the acceleration of these changes. This transformation has been facilitating these initiatives is the integration of digital technologies such as Cloud Computing, Analytics, Mobility Solutions, Smart Meters, Internet-of-Things (IoT), Operational Technology (OT) Convergence, Artificial Intelligence (AI), Machine Learning (ML), Augmented Reality (AR), Virtual Reality (VR), Metaverse, and more. Key privacy considerations are as follows:

- **Customer Data Privacy:** Energy & utility companies collect information such as personal details and energy consumption data on a regular basis. Organizations will need to implement robust security measures to safeguard personal information, from unauthorized access, breaches or misuse. Further, ensure a process of seeking consent prior to collection and processing of personal data.
- **Smart Grids and Data Exchange:** Smart grid technologies require information exchange between customers, utility companies and service providers for smooth functioning. Processes for consent, data minimization and security will accordingly need to be enhanced.
- **Third Party Management:** In the energy and utilities sector, it is common for companies to seek services of third-party vendors for various functions such as customer billing, data analytics, and system maintenance. Robust vendor privacy management processes should be implemented to ensure compliance with privacy regulations.
- **Reporting and Incident Response:** Energy and Utility companies tend to fall in the category of critical national infrastructure. To effectively address privacy breaches, organizations need to establish incident response plans, conduct comprehensive investigations, and implement suitable remedial measures.

Consumer Products

There is always immense competition for seeking and retaining a shoppers' attention as they demand more convenience and innovation. Major consumer product and retail brands continue to use new ways to connect to customers through technology. Key considerations related to privacy are as follows:

- **Customer Profiling, Targeted Advertising and Analytcis:** Organizations should ensure compliance to privacy needs such as consent, prior to initiating targeted advertising and customer profiling.
- **Customer Communication and Marketing:** Processes related to email marketing, telemarketing, and direct marketing activities would need to be enhanced to ensure compliance with the privacy regulations.
- **User Rights and Data Management:** Enhance the processes to ensure right to access, modify and remove the data principal's information as per need.
- **Privacy by Design in Product Development:** Privacy by design principles, such as minimizing data collection, ensuring data security, and providing user-friendly privacy/ consent options, shall be a crucial aspect of compliance.

Real Estate and Infrastructure

The sector faces a challenging situation, balancing the requirement for high-quality infrastructure within tight timelines and the necessity to comply with environmental and governance regulations. In addition to these pressures, there are rising resource and labor costs, along with other crucial factors influencing the sector's operations. Key privacy considerations are as follows:

- **Personal Data Handling:** Information related to property transactions, tenant information, and customer details will need enhanced processes for securing.
- **Customer Communication and Marketing:** Processes related to email marketing, telemarketing, and direct marketing activities would need to be enhanced to ensure compliance with the privacy regulations.
- **Rights of Tenent and Customers:** Organizations collect information related to their tenants and customers. There is a need for right to access, correct, and delete personal data held by real estate and infrastructure companies. A mechanism to manage this should be set up be real estate and infrastructure companies.

Global Capability Centers (GCC)

GCCs are the tech and shared services centres of MNCs in India, and these are growing rapidly as global companies look for talent to help them digitally transform. There are more than 1500 GCCs currently and it is estimated that these should grow to 2000+ by end of 2026 as per report by NASSCOM. Data privacy requirements have an impact on GCC operating in various industries. Some key considerations are as follows:

- **Compliance with Local Regulations:** GCC operating across various countries must adhere to local data privacy regulations as well as global ones. For example, in the European Union, they must comply with the General Data Protection Regulation (GDPR), while in India, they will need to adhere to the Digital Personal Data Protection Act, 2023. Compliance with these regulations is crucial to avoid legal consequences, reputational damage, and financial penalties.
- **Cross-border Data Transfer Compliance & International Collaboration:** GCC often handles data that flows across borders, either between the parent company and the center or among different centers globally. Data privacy requirements necessitate compliance with regulations governing cross-border data transfers. This includes implementing appropriate safeguards, obtaining necessary consents, or utilizing approved data transfer mechanisms such as standard contractual clauses. International collaboration is crucial in ensuring a consistent interpretation and application of privacy regulations, enabling GCCs to navigate privacy complexities across borders.
- **Data Security Measures:** Data privacy requirements emphasize that GCC implement robust data security measures to protect Personal data. These measures include encryption, access controls, regular security audits, and incident response plans.
- **Consent Management and Data Principal Right to Access:** GCC must establish processes to manage consent and handle data subject such as the right to access, rectify, or delete personal data. Compliance with data privacy requirements involves having mechanisms in place to address these requests effectively and within specified time frames.
- **Vendor Management:** GCC often engage third-party vendors to support their operations. Data privacy requirements extend to these vendor relationships, necessitating organizations to conduct due diligence, implement appropriate contracts, and monitor vendor compliance with data privacy obligations.
- **Data Governance and Documentation:** GCC must establish robust data governance frameworks and maintain documentation to demonstrate compliance with data privacy requirements. This includes keeping records of data processing activities, conducting privacy impact assessments, and implementing privacy by design and default principles.
- **Employee Training and Awareness:** Ensuring employees within GCC are aware of data privacy requirements, their roles in accordance with applicable local and global privacy regulations.

Data Privacy Considerations on Emerging Technologies

The impact of emerging technologies on data privacy is a complex and multifaceted issue. On one hand, new technologies offer many benefits and opportunities for individuals and organizations, such as greater efficiency, increased productivity, and improved customer experiences. However, these benefits must be balanced with the need to protect personal data information and maintain privacy rights.

Organizations using or specializing in emerging technologies such as Virtual Reality, Artificial Intelligence, Machine Learning Internet-of-Things (IoT), Robotic Process Automation (RPA), Web 3.0, and Metaverse, among others, produce and process substantial amounts of personal data.

This data can be used to gain valuable insights and informed decision-making, but it also presents significant risks if not properly secured and protected.

Additionally, emerging technologies such as facial recognition and biometric identification raise concerns about personal privacy and the potential for misuse. These technologies have the ability to track individuals' movements and activities, leading to concerns about surveillance and invasion of privacy. Overall, emerging technologies offer many benefits, however, they also present significant challenges to data privacy. It is important for individuals and organizations to stay informed about these risks and take proactive steps to protect personal data information and maintain privacy rights in the face of advancing technology. Some of these challenges include:

Rapid Pace of Technological Innovation

Emerging technologies are often developed at a rapid pace, and traditional privacy regulations may not always keep up with these advancements. This can create a gap in data privacy protection, leaving individuals vulnerable to data breaches and misuse.

Complex Data Ecosystems

Emerging technologies often involve complex data ecosystems, with data being generated, collected, and shared across multiple platforms and devices. This can make it difficult to control and secure data, leading to increased risks of data breaches and unauthorized access.

Lack of Transparency

Many emerging technologies, such as machine learning algorithms and AI systems, are highly complex and difficult to understand. This can make it challenging to ensure transparency and accountability in data processing, leading to potential privacy violations.

Cross-border Data Transfers

Emerging technologies often involve cross-border data transfers, which can create legal and regulatory challenges. Different countries may have different privacy laws and regulations, and it can be difficult to ensure compliance with all of these requirements.

Limited User Control

Some emerging technologies, such as IoT devices and smart home systems, may collect data without users' knowledge or consent. This can limit users' control over their own data and create privacy risks.

Overall, ensuring data privacy in emerging technologies is a complex and ongoing challenge. It requires a proactive approach from individuals, organizations, and policymakers to develop effective privacy policies and regulations that can keep up with the rapid pace of technological innovation and manage data breaches with an effective incident response plan.

Data Breaches and Incident Response

It is critical for organizations to manage data breaches and effectively responding to incidents is critical for Indian organizations to mitigate the risk and maintain trust with stakeholders. The following steps outline best practices for organizations to manage data breaches and respond to incidents:

- **Establish an Incident Response Plan:** Organizations should develop a comprehensive incident response plan that outlines the steps to be taken in the event of a data breach or incident. The plan should define roles and responsibilities, communication protocols, escalation procedures, and a clear chain of command. Regular testing and updating of the plan are essential to ensure its effectiveness.
- **Detect and Investigate the Incident:** Organizations should deploy robust monitoring and detection systems to identify potential data breaches or security incidents promptly. Suspicious activities, such as unauthorized access attempts or unusual data patterns, should be investigated thoroughly to determine the scope and impact of the incident.
- **Contain the Breach:** Once a data breach or incident is detected, immediate action should be taken to contain it. This may involve isolating affected systems, disconnecting compromised accounts or devices, and implementing temporary measures to prevent further unauthorized access or data loss.
- **Assess the Impact:** Organizations should conduct a thorough assessment to understand the extent of the breach and the potential impact on Data Principal and the organization itself. This assessment should involve identifying the types of data compromised, the number of affected individuals, and the potential risks associated with the breach.
- **Notify Affected Individuals and Authorities:** Indian organizations have a legal obligation to notify mandatorily report cyber incidents to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents along with the affected individuals and the relevant authorities in the event of a data breach. Further, the Digital Personal Data Protection Act, 2023 mandates that, following a data breach, the Data Fiduciary must alert the Data Protection Board and each impacted Data Principal.
- **Mitigate and Remediate:** After a data breach, organizations should take immediate action to mitigate the impact and prevent future incidents. This may involve patching vulnerabilities, strengthening security controls, enhancing employee training and awareness, and implementing additional safeguards to protect personal data.
- **Communicate Transparently:** Open and transparent communication is crucial during and after a data breach. Organizations should proactively communicate with affected individuals, stakeholders, and the public, providing timely updates, clarifying the steps taken to address the breach, and offering assistance or support as needed. Transparent communication helps maintain trust and demonstrates a commitment to data privacy.
- **Learn from the Incident:** Organizations should conduct a thorough post-incident review to identify lessons learned and areas for improvement. This review should inform updates to security & privacy policies, procedures, and technologies to prevent similar incidents in the future. Regular training and awareness programs can also help educate employees about data privacy best practices.

Way Forward

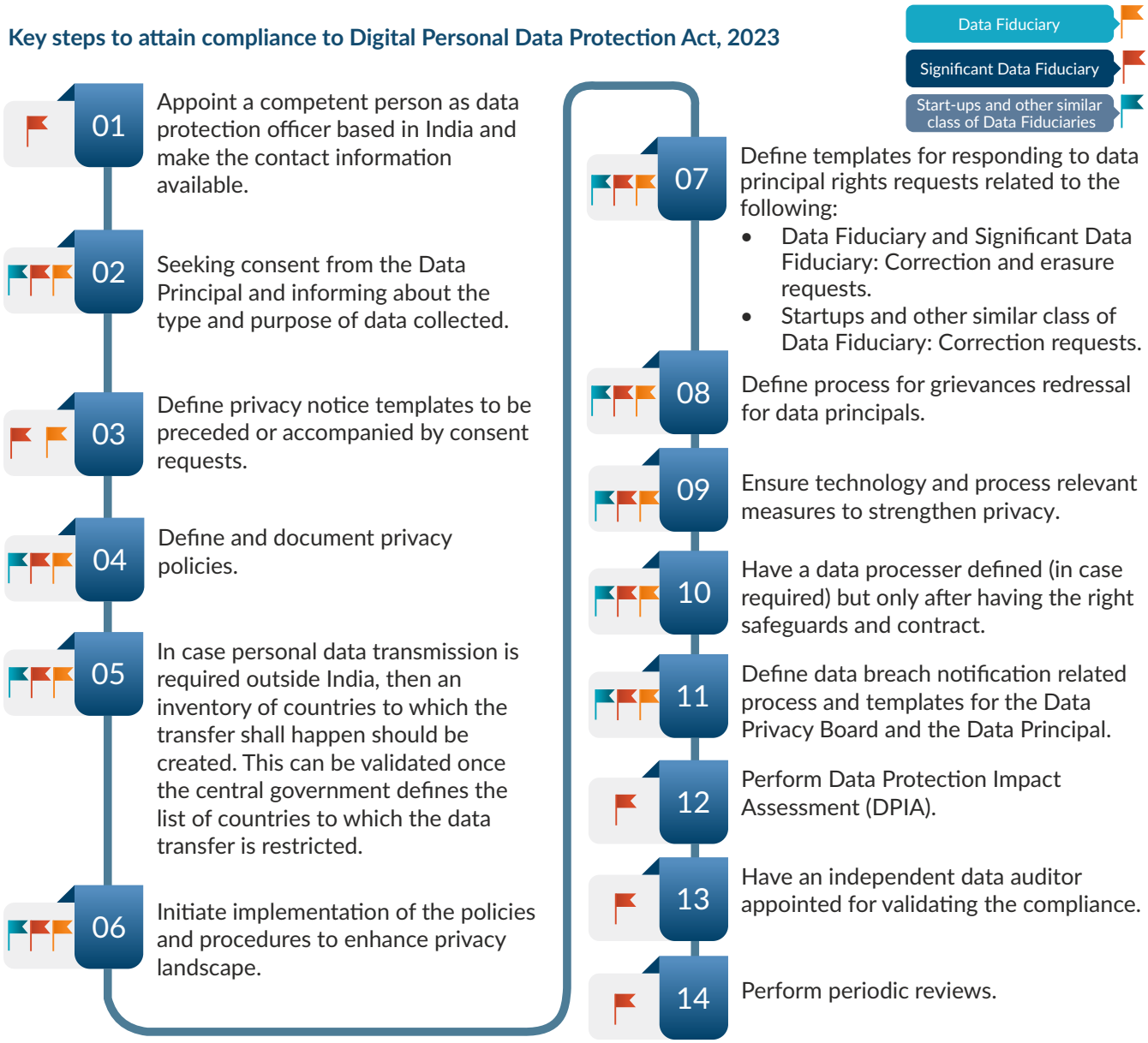
In the current digital era, data privacy has become a critical topic. It is of utmost importance to establish and enforce comprehensive data privacy processes in order to safeguard individuals' personal information and uphold their rights. The reach of privacy laws extends across diverse sectors compelling organizations to adjust their data management practices and allocate resources towards strong measures.

While protecting personal data can be challenging, but through a systematic roadmap and the right investments organizations can take steps towards managing the risks.

Building a Comprehensive Data Privacy Program: Key Steps to Embed Data Privacy and Protection

In an era marked by increasing scrutiny and regulatory expectations surrounding data privacy and protection, organizations must treat these efforts as formal compliance initiatives. By adopting a privacy lens, businesses can ensure that every aspect, from partnerships to marketing strategies, product launches, and other changes, aligns with their data privacy and protection commitments. Below is a roadmap to achieve compliance to the objectives of the Digital Personal Data Protection Act, 2023 along with additional best practices for personal data protection and mitigating the risk of a breach.

Key steps to attain compliance to Digital Personal Data Protection Act, 2023



Further, holistic steps that to be followed in addition to the above for an effective data privacy program.

Step 1 Conduct a Data Privacy Risk Assessment

A thorough data privacy risk assessment is crucial for identifying weaknesses in compliance and protection efforts. This assessment aims to identify the data collected, stored, and processed by the organization, assess privacy risks associated with that data (e.g., confidentiality, security), evaluate existing controls addressing those risks, and identify any gaps or residual risks. This process helps leadership understand critical data privacy regulations, determine compliance obligations, and strengthen the organization's overall data privacy framework.

Step 2 Establish a Baseline

Baselining is a zero day approach to privacy compliance in any organization. It covers invading the totality of an organization's privacy commitments; determining exactly what the company has promised its customers regarding how the business collects, processes, stores and transfers their data; and, most important, whether or not the company is honoring those commitments. It is imperative to ensure that these commitments are honored. Extending privacy commitments to contracts, third-party vendor relationships, and training can further strengthen data privacy practices.

Step 3 Adopt Privacy-Enhancing Technologies

To protect data privacy, organizations should adopt privacy-enhancing technologies that provide robust safeguards. These include encryption, Data loss prevention tools, Anonymization Techniques, Privacy Governance Tools, Data Mapping/ Cataloging and Privacy Rights Automation, Privacy Impact Assessment/ Data Protection Impact Assessment Automation, Consent/ Preference Management Automation Tools, AI Privacy Governance Tools, Third Party Privacy Risk Management Tools, Privacy Training Tools, Identity Management Platforms and Secure Data Storage Solutions. These technologies help safeguard sensitive information, minimize the risk of unauthorized access or data breaches and assist in managing the regulatory requirements in a structured way.

Step 4 Manage Change

Organizations must continuously assess how privacy decisions, changes to services and products, and data sharing with third parties can impact data privacy commitments and compliance requirements. This can be challenging, particularly for large companies where changes occur at a rapid pace. Establishing a sustainable change-management program is critical. Leaders should prioritize data privacy as a strategic business objective and foster a "culture of compliance" and also ensure privacy awareness across the organization Effective change management ensures the honoring of privacy commitments to customers and helps maintain trust. Further, ensure that the tone at the top is clear and the board supports the privacy initiatives.

Step 5 **Documentation and Awareness**

Two essential documentation approaches are vital for building a successful data privacy program. First, organizations should document privacy procedures, processes, risks, and controls comprehensively. This at times is a deficiency in companies, requiring investment in time and effort. Second, the processes that handle customer information or covered information within the business must be documented. Understanding existing processes helps capture the impact of changes on privacy risks. Maintaining clearly verifiable and readily accessible documentation of plans and processes is crucial for managing the program effectively. Assigning an employee responsible for document security, compliance, and maintaining updated records is highly recommended.

Adopt Privacy by design and Integrate privacy considerations into the design of systems, products, and services from the outset. Implement privacy-enhancing technologies and practices to minimize the collection and storage of personal data, and ensure data protection measures are in place throughout the data lifecycle. Embedding data privacy and protection as an integral part of organizational processes requires time, focus, and resources. By following the fundamental steps outlined above, businesses can establish a comprehensive data privacy program that upholds customer confidence, meets regulatory expectations, and fosters trust in an evolving landscape of data privacy and protection.

In conclusion, in today's digital landscape, safeguarding personal data and prioritizing privacy protection are crucial. By embracing privacy-by-design principles, obtaining informed consent, implementing robust security measures, and fostering transparency and accountability, organizations can build trust, mitigate risks, and uphold the privacy rights of individuals. Overall, the outlook for data privacy in India indicates a growing focus on protecting individual privacy rights, strengthening regulatory measures, and adapting to evolving technological landscapes. The introduction of the Digital Personal Data Protection Act, 2023 will be a significant milestone in establishing comprehensive data protection regulations, aligning India with global privacy standards and fostering a privacy-conscious environment to ensure that the objective of Digital India initiative are met.

About CII - CDT

Confederation of Indian Industry

The Confederation of Indian Industry (CII) works to create and sustain an environment conducive to the development of India, partnering Industry, Government, and civil society through working closely with Government on policy issues, interfacing with thought leaders, and enhancing efficiency, competitiveness and business opportunities for Industry.

For more than 125 years, CII has been engaged in shaping India's development journey and works proactively on transforming Indian Industry's engagement in national development. The premier business association has around 9000 members, from the private as well as public sectors, and an indirect membership of over 300,000 enterprises from around 286 national and regional sectoral industry bodies.

With 62 offices, including 10 Centres of Excellence in India, and 8 overseas offices in Australia, Egypt, Germany, Indonesia, Singapore, UAE, UK, and USA, as well as institutional partnerships with 350 counterpart organizations in 133 countries, CII serves as a reference point for Indian Industry and the international business community.

Confederation of Indian Industry
The Mantosh Sondhi Centre, 23, Institutional Area
Lodi Road, New Delhi – 110 003, India
Phone: 91 11 45771000/ 24629994-7
Email: info@cii.in
Web: www.cii.in

As organizations navigate their business through Digital Transformation (DX), they face multiple challenges, and seek a platform of trust to handhold their digital journey. To help organizations leverage the technology changes, Confederation of Indian Industry (CII) has created a focused Centre for Digital Transformation (CDT). The centre operates with Tata Communications as principal partner and other Industry members.

CDT aims to emerge as leading authority in guiding and enabling organizations to building intelligent systems and help in personal computing, cloud and reinventing their productivity and business processes. Vision is to be a Centre of international repute that provides role model products and services for continuous betterment of organizations, industries and society through digital transformation. Ultimate goal is to evolve and leverage a Digital Transformation Movement that transforms India and make Indian industry globally competitive.

The CDT plays a pioneering role in introducing latest concepts in DX and establish systems of intelligence. The services include Assessment & Advisory, Technology seminars, Awards, Best Practices, Training & Development, Cyber Security, Technology Missions, etc.

CII – Tata Communications Centre for Digital Transformation
249-F, Sector 18, Udyog Vihar, Phase IV
Gurugram, Haryana 122 015, India
Phone: +91 124 401 4060 – 67
Email: contact.cdt@cii.in
Web: ciicdt.com

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, governance, risk and internal audit through its network of more than 85 offices in over 25 countries.

Named to the 2023 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Acknowledgement:
Arindam Pal, Nagesh Akula, Nitin Sinha, Sahil Chander, Sarita Padmini and Shobhit Singhal contributed to the publication, led by Vaibhav Koul.

Contacts:

Sandeep Gupta
Managing Director
Email: sandeep.gupta@protivitiglobal.in
Mobile: +91 9702730000

Vaibhav Koul
Managing Director
Email: vaibhav.koul@protivitiglobal.in
Mobile: +91 9819751715

Aju Sebastian
Managing Director
Email: aju.sebastian@protivitiglobal.in
Mobile: +91 9818286225

Dhrubabrata Ghosh
Managing Director
Email: dhrubabrata.ghosh@protivitiglobal.in
Mobile: +91 9739546661

Amit Lundia
Managing Director
Email: amit.lundia@protivitiglobal.in
Mobile: +91 9836922881

Our India Offices:

Bengaluru
Umiya Business Bay - 1, 9th Floor
Cessna Business Park, Outer Ring Road
Kadubeesanahalli, Varthur Hobli
Bengaluru – 560 049
Karnataka, India
Phone: +91.80.6780.9300

Chennai
10th Floor, Module No. 1007
D Block, North Side, Tidel Park
No. 4, Rajiv Gandhi, Salai,
Taramani, Chennai - 600 113
Tamil Nadu, India
Phone: +91.44.6131.5151

Gurugram
15th Floor, Tower A,
DLF Building No. 5, DLF Phase III
DLF Cyber City, Gurugram – 122 002
Haryana, India
Phone: +91.124.661.8600

Hyderabad
Q City, 4th Floor, Block B, Survey No.
109, 110 & 111/2 Nanakramguda Village
Serilingampally Mandal, R.R. District
Hyderabad – 500 032
Telangana, India
Phone: +91.40.6658.8700

Kolkata
PS Srijan Corporate Park, Unit
No. 1001, 10th Floor, Tower - 1,
Plot No. 2, Block - EP & GP
Sector-V, Bidhannagar,
Salt Lake Electronics Complex,
Kolkata –700 091
West Bengal, India
Phone: +91.33.6657.1501

Mumbai
1st Floor, Godrej Coliseum
A & B Wing
Somaiya Hospital Road
Sion (East) Mumbai – 400 022
Maharashtra, India
Phone: +91.22.6626.3333

Noida
Windsor Grand, 16th Floor
1C, Sector - 126 Noida
Gautam Buddha Nagar- 201313
Uttar Pradesh, India
Phone: +91.120.697.2700

protiviti®


protiviti®
Global Business Consulting