Deloitte. | Google Cloud

A billion minds, one vision: Data privacy as the pillar of Viksit Bharat

March 2025

Table of contents

Executive summary

As data becomes increasingly integrated into various aspects of decision-making, interactions and processes, effective data management and data privacy are paramount. Considering this, data privacy legislations play a critical role in today's digital landscape. These regulations are designed to safeguard individuals' privacy rights by ensuring that their personal data is managed in a fair, transparent and secure manner. By establishing clear guidelines and requirements for organisations, data privacy laws empower individuals to exercise control over their personal data and hold organisations accountable for its responsible use. This fosters trust between individuals and organisations, enabling a more secure and ethical data-driven society.

This white paper delves into the interconnectedness of digital transformation, data privacy and cloud computing. The rapid increase in data generation, fuelled by digital transformation and widespread technology adoption, has made data privacy regulations a major concern for businesses. The paper stresses the growing importance of complying with global data privacy laws to navigate this evolving landscape. It comprehensively overviews the complex relationship of digital transformation, cloud computing and data privacy.

The paper also highlights the importance of integrating data privacy principles into cloud-based strategies as businesses increasingly rely on cloud computing for digital transformation. It outlines how a privacy-first approach can benefit organisations by fostering transparency, accountability and customer trust in data management. Key regulatory impacts are also addressed, including data localisation, cross-border data transfers and data security assurance through encryption, access controls and compliance certifications. Furthermore, the paper highlights the pivotal role that Cloud Service Providers (CSPs) can play in simplifying compliance with privacy regulations by offering robust security features and adhering to best-in-class privacy standards. It proposes that using cloud computing can help organisations manage business operations while safeguarding privacy and citizens' rights, as outlined in the Act. By using cloud solutions, businesses can mitigate privacy risks while focusing on innovation. Adopting Privacy-by-Design (PbD) in cloud architectures can empower organisations to secure personal data and comply with global regulations, enhancing customer value and trust in the digital age.

Evolving privacy regulations across the globe

In today's hyperconnected world, we are generating approximately 402.74 million[1] terabytes of data each day. That is equivalent to 200 billion hours of HD video content generated daily. Increased internet and smartphone penetration, along with easily accessible infrastructure, has led to a boom in technology-enabled services, which is propelling the increase in 'data generation'.

Data privacy and data protection regulations enable individuals to exercise some control over their personal data. Currently, about 137 countries across the globe have legislation in place to secure the protection and privacy of data.[2] The European Union's General Data Protection Regulation (EU GDPR/GDPR) has been at the forefront of this movement. Following closely are regulations across the Asia-Pacific region. Australia's Privacy Act 1988 (Amended in 2022) establishes principles for handling personal information, provides the right to access it, and requires mandatory data breach notifications. New Zealand's Privacy Act 2020 strengthens data privacy protection and enhances the rights of individuals to access their data as well as mandatory breach reporting; Singapore's Personal Data Protection Act establishes a framework for personal data management as well as obligations around data breach management; Japan's Act on Protection of Personal Information, which has also received an adequacy decision from The European Commission, serves as a key reference for data protection standards. Similarly, India introduced the Digital Personal Data Protection Act (DPDPA) on 11 August 2023,[3] drawing inspiration from China's Personal Information Protection Law (PIPL), which came into force on 1 November 2021. While data privacy laws have their individual nuances reflecting their country's socio-economic and legal values, some fundamental principles are common across these legislations. Common themes include accountability through consent-based processing, detailed notices, data localisation and personal data security.

Digital transformation and the need for cloud

Digital transformation is changing how businesses operate, as it involves not just technology adoption but a fundamental transformation of the organisation, operations, team structures and culture. Digital transformation and cloud computing are inextricably linked. A hyperscale public cloud, driven by its massive infrastructure and distributed network capabilities, offers unique advantages, such as scalability, rapid resource allocation and global reach. As a result, it could be challenging to replicate these features fully in other cloud models, such as private or smaller-scale public cloud models. Cloud computing provides the infrastructure and platform necessary for digital transformation initiatives to succeed. Much of the value the cloud generates comes from increased agility, innovation and resilience, which are provided to businesses with sustained velocity. The cloud provides the foundation for digital transformation and is essential for businesses that want to succeed in the digital age, as outlined below:

Accelerated time-to-market: Organisations adopting cloud-native technologies can deploy code into production environments with increased frequency and heightened velocity.

Capacity for innovative business solutions: Prominent CSPs offer many native services and access to vibrant marketplaces featuring contributions from third-party ecosystems, collectively encompassing thousands of additional services.

Mitigated risk: Cloud computing reduces operational overhead for organisations capable of designing their platforms to use the cloud securely.

Unlocking customer value by using data privacy regulations

Transparency and accountability standards provide a competitive advantage. In the DPDPA, the notice and consent framework to secure an individual's consent is the bulwark on which data processing practices in the digital economy are founded. The introduction of consent managers in the DPDPA is a novel concept, positioning them as facilitators and custodians of the data principal's consent. This role allows individuals to express their choices and preferences to data fiduciaries effectively. The consent manager will operate through a technology interface, where any action requiring issuing, withdrawing or modifying consent about your personal data will be routed through them. This innovative mechanism seeks to empower individuals with greater control over their personal information while equipping organisations with the necessary guidance and tools needed to navigate the complex landscape of data protection and privacy. Moreover, the DPDPA bolsters the right to withdraw consent, empowering individuals to retract their agreement at any juncture.

As data privacy regulations have been enacted in most countries across the globe, the efforts required for organisation-wide compliance changes are bound to be substantial. At the same time, the aim of data privacy regulations is to empower individuals with rights for their personal data and ensure that standard guidelines for data protection are being implemented across all organisations in their respective regions.

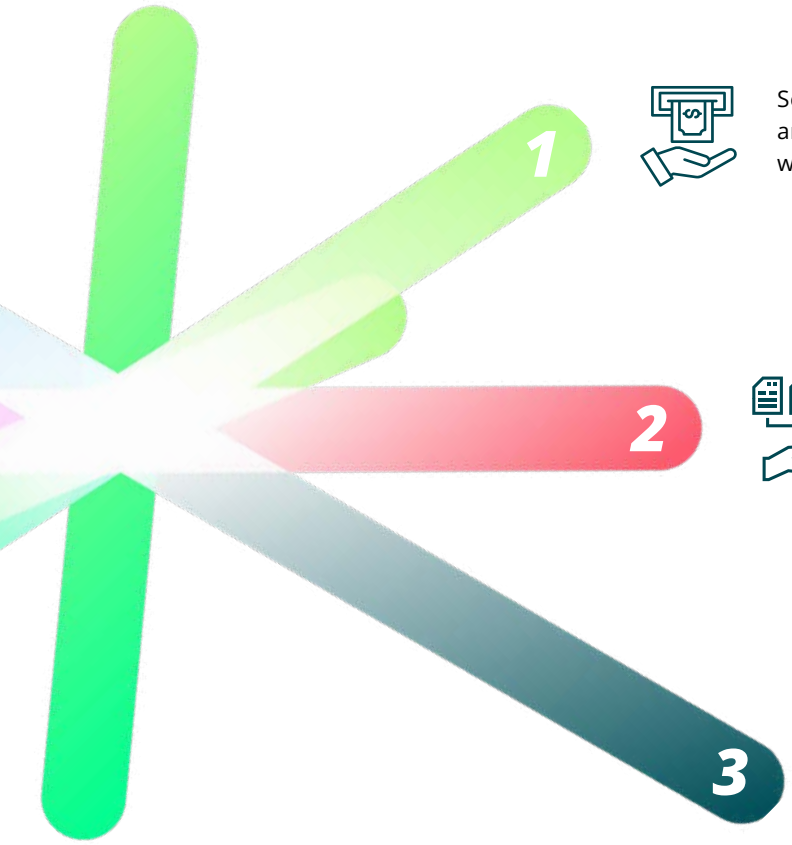
Organisations need to look at adopting a privacy-first culture while undertaking their cloud-driven digital transformation journeys to help them push the envelope and design better products and services for their customers with mature privacy practices. From a customer's perspective, service offerings enhanced with mature data privacy and protection controls will provide a secure value proposition and will reinforce a stronger trust in privacy-first brands. This will create a more secure data-sharing landscape, with appropriate controls where customers can provide their data with confidence and expect better services in return.

Organisations must implement adequate privacy controls to inform customers about how they ensure that their personal data is handled fairly and transparently. They must also ensure that such data is collected only after obtaining proper customer consent.

Cloud-based solutions reduce business risk and simplify compliance adherence by providing avenues for privacy-compliant data processing. This supports organisations in building digital trust, thereby enhancing consumer trust in their operations. They can use controls inherently available in cloud solutions to institute mechanisms that facilitate the rights of the data principals as envisaged in the Act.

Navigating privacy regulations in cloud-enabled organisations

Accountability: One of the fundamental principles across privacy regulations is accountability through 'lawfulness, fairness and transparency'. This translates into actionable obligations, such as:



Seeking explicit consent and its subsequent withdrawal

Providing accessible notice documenting the nature of personal data collected and the purpose of its processing

Ensuring the rights to access personal data

If organisations process personal data, individuals have a right to exercise control over its use. For organisations using cloud computing and services, the additional areas for regulatory impact are cross-border data transfers for analytics using AI models, data breach notifications and third-party vendor compliance engaged on backend services with CSPs.

Data localisation, data sovereignty and regulatory requirements: Cloud computing has fuelled the meteoric rise of digital businesses; therefore, it must also adapt and comply with these obligations to continue providing services to its clients. A survey showed that 84 percent of businesses feel affected by data privacy regulations, especially due to the General Data Protection Regulation (GDPR). Another 39 percent are relooking their data storage strategies to comply with data localisation requirements.[4] However, the localisation requirements do not outweigh the operational and efficiency benefits unlocked by adopting cloud-native technologies. Another study revealed that 80 percent of organisations are either using or migrating to multiple public or private clouds. CSPs face a challenge in balancing increasing demand for cloud computing services with regulatory obligations. The cloud computing market size is expected to grow from US$0.79 trillion in 2025 to US$1.69 trillion by 2030, at a CAGR of 16.4 percent.[5] Incentives to accommodate and comply with data privacy regulations across the globe, including those for data localisation, are very high. As a result, CSPs are exploring ways to design their services by collaborating with local/regional data centres.

A key principle is data localisation, where governments, through the legislation, wish to provide greater security and control over data. The push for data localisation stems from the belief that citizens' data, including their personal data, is more secure when governed by local laws and regulations. It also allows the citizens easier access to courts/redressal systems in case of a dispute or grievances.

Data sovereignty is connected with the concept of data localisation, which refers to the idea that data should be governed by the laws of the country in which it is collected or stored. This implies that a country exercises its sovereign control over its citizens' data usage, including aspects such as privacy, security and individual rights. While data localisation and data sovereignty may seem like two sides of the same coin, a closer inspection reveals that data localisation requirements are driven by principles of data sovereignty. Still, it may not necessarily embody all of them. For instance, one of the requirements of a 'Sovereign Cloud' is to support governments in their national initiatives. This, in turn, may translate into greater disclosures to authorities by the CSPs.

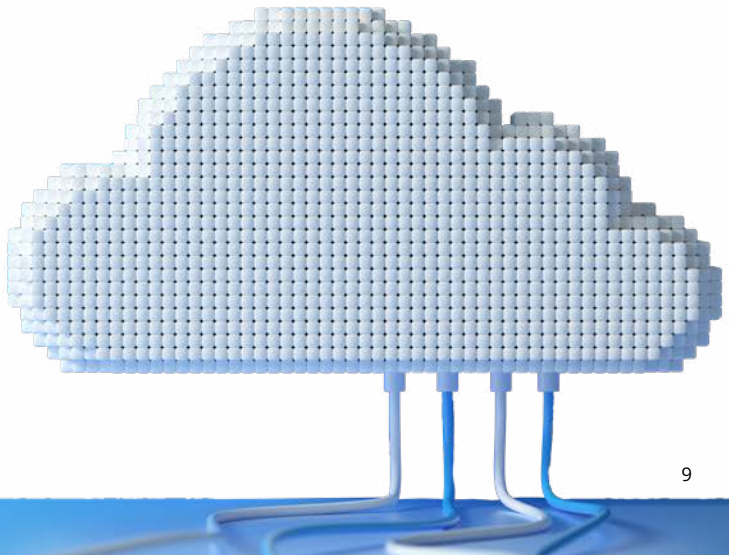
Cloud providers offer controls for data sovereignty, including storing and managing encryption keys outside the cloud, giving customers the power to only grant access to these keys based on detailed access justifications. Further, confidential computing solutions allow customers to protect data, complementing their ability to encrypt data at rest and in transit with keys independent of the cloud provider. These technologies use industry-proven encryption to enable businesses to fully control their data, making them the ultimate arbiter of access to their data.

Hyperscale cloud providers offer a wide range of regions across the globe, allowing customers to store their data in the specific geographical location required for compliance. Customers can select a region or group of regions when they create a new resource, such as a virtual machine or a storage bucket. This offers a significant advantage, as cloud provider regions give single-click, instant access to data centres in multiple locations that could otherwise take a business several years to build or acquire.

Cloud providers also offer several mechanisms, such as resource location controls, Identity and Access Management (IAM) configuration and organisational policy constraints, to ensure that resources can only be created in allowed regions. These mechanisms include tools that restrict the movement of data between regions. These controls are backed by contractual data residency commitments that require customer data to stay within the region they select.

The DPDPA clearly mandates that any sectoral regulation with a higher degree of protection or restriction on the transfer of data outside India will still apply. Any sector-specific regulations, such as the Reserve Bank of India's rule on storing payment system data in India or the Department of Telecommunications' Unified License Agreement (ULA), which prevents telecom service providers from transferring subscriber or user information outside of India, will still apply even after the DPDPA is enforced.

In an interconnected global landscape, threats can originate from anywhere. Therefore, organisations need to take an overarching, risk-based and principle-driven approach to data privacy regulations. By doing so, they can use these regulations as a differentiator to achieve their business goals while realising the full potential of technology and innovation.



Data security is one of the most important considerations for organisations when complying with data privacy and protection laws. Ensuring data safety and security against external and internal threats, maintaining availability, preventing unauthorised access, avoiding data leakage and protecting against accidental loss are crucial measures in processing personal data and complying with privacy regulations. Organisations need to demonstrate accountability with regard to data security by providing strong assurances through certifications and contractual obligations and allowing independent audits of their security controls. Implementing controls such as robust key management, encryption of data at rest and in transit, tokenisation, strong identity and access management tools, maintaining a global security operation centre, etc., are some of the controls that CSPs should implement. By doing so, they will demonstrate compliance and generate trust with respect to maintaining the security of personal data.

Most organisations have embraced the concept of cloud as a digital immune system, where cloud providers are incentivised to detect issues and then support their customers to help defend themselves. Businesses are increasingly looking to the public cloud for security, realising that cloud providers can invest more in technology, people and processes to deliver a more secure infrastructure.

For example, cloud providers have infrastructure that encrypts data at rest and in transit. Many use specialised hardware with built-in security features and manage the entire hardware lifecycle, including secure disposal. They regularly scan for vulnerabilities and apply security patches to their systems. They have dedicated security teams that monitor their infrastructure 24/7 and respond to security incidents. Global cloud providers undergo regular audits and certifications to demonstrate compliance with security and privacy standards at the global (e.g., ISO, SOC, PCI, NIST, etc.) and local (MeitY, etc.) level.

Businesses that embrace cloud technology can improve their security measures and reduce the risk of breaches by offloading some of their security responsibilities to a service provider who has the incentives, skills, resources and economies of scale to build and maintain a secure platform. They can then build on this solid foundation by taking advantage of various security features and tools offered natively by cloud providers — at little or no additional cost.

Considering the above regulations, organisations will need to be mindful of the location of processing (computing) and storage servers of technologies/tools/platforms deployed within their environment and the maintenance of security controls to prevent breach/loss.

Privacy by Design (PbD) in cloud: Based on Cloud Security Alliance's (CSA) and Cloud Controls Matrix (CCM), PbD in cloud is described as "Develop systems, products and business practices based on a principle of PbD and industry best practices. It ensures that systems' privacy settings are automatically configured according to all applicable laws and regulations.

Ensuring privacy is embedded throughout processes, applications, systems, frameworks and operations requires the implementation of PbD across all personal data touchpoints. PbD acts as a tollgate for i) a new process or technology or ii) a change to an existing process or technology that has an impact on personal data. This tollgate can be actualised by designing an organisation-wide PbD framework, with controls serving as an approval step for data privacy across all onboarding and change management channels.

In a cloud environment, such PbD tollgates can be embedded to validate privacy controls such as:

- Application level controls for data minimisation, data storage localisation, data retention schedules, audit logging and user access management
- Database level controls for personal data encryption at rest, data masking, pseudonymisation and anonymisation
- End-user privacy management features such as consent and preference management, data principal rights request portals and grievance redressal mechanisms
- At every stage of a technology-driven business process change, organisations need to evaluate whether customer privacy considerations are prioritised over organisational priorities or vice versa

The widespread integration of data privacy across cloud infrastructures, cloud-hosted platforms and end-user cloud services ensures comprehensive personal data protection, enabling customers to use services securely without being concerned about privacy fluctuations over time.

Why is it easier to comply with privacy on the cloud?

Migrating to the cloud can make it easier to follow privacy regulations because cloud providers typically offer robust built-in security features, data encryption options and robust access controls. These features significantly reduce the burden on organisations to manage these aspects themselves, allowing them to focus on data privacy compliance with less manual effort. Additionally, many cloud providers are already certified to meet various privacy standards, streamlining the compliance process for businesses.

Key reasons why cloud compliance is easier for privacy:

Dedicated security infrastructure

Cloud providers invest heavily in data centres and security measures that are regularly updated, making it easier to follow privacy regulations than managing your own on-premises infrastructure.

Data encryption

Most cloud providers offer robust data encryption options at rest and in transit, which helps protect sensitive information from unauthorised access.

Granular access controls

Cloud platforms allow for fine-grained user access controls, enabling organisations to restrict data access to authorised staff only.

Compliance certifications

Major cloud providers often hold certifications for various privacy regulations, which can simplify compliance audits.

Automated updates

Cloud providers automatically update their security patches and features, ensuring that organisations always use the latest privacy-focused technologies.

Comply with data subject rights

Cloud providers offer tools and APIs that can help organisations automate and streamline the processes required for addressing the rights of data principals.

Think differently about privacy, security and data protection

As information ecosystems become more complex, new threats and vulnerabilities emerge daily. Data-driven cloud security methods resolve these complex modern problems, allowing the organisation to efficiently secure information, mitigate risk and scale their services and user base. Constant verification, driven by automation, enhances information security against modern threats and allows the design of information systems without the constraints of an inflexible perimeter. The cloud provides a fresh approach to managing privacy risks. CSPs support this approach by offering and maintaining essential controls and tools to mitigate modern security and privacy threats.

Operationalising a data privacy framework

Many organisations store sensitive information so they can analyse data for a variety of business purposes. CSPs have various solutions that implement the Cloud Data Management Capabilities (CDMC) Key Controls Framework, managed by the Enterprise Data Management Council. The framework describes several key controls that providers can implement to let their customers effectively manage and govern sensitive data in the cloud in alignment with the data privacy principle. Some salient ones are data controls, understanding data provenance and lineage and data ownership. Additional considerations involve governing data sourcing and consumption accompanied by automation where applicable, managing and auditing cross-border movement of sensitive data, ensuring consistency in data cataloguing, enforcing and tracking data entitlements, and managing ethical access, use and outcomes of data throughout its lifecycle.

Leading CSPs have built-in tools for sensitive data discovery, which can be used to discover, scan and classify across a wide set of data and monitor sensitive data across a large set of assets. With the infusion of AI-enabled capabilities, targeted, focused inspection can help organisations identify every data element in storage systems. Synchronous, stateless inspection of data from anywhere, along with near real-time inspection or integration into custom workloads, applications, or pipelines, enables a data-centric approach to securing organisational data assets in line with established policies and regulatory requirements.

Customers are increasingly using AI in their day-to-day business functions and applications, as well as for their daily productivity and collaboration tools. Emphasis on data privacy with the advent and penetration of AI in an individual's everyday life is even more critical. It becomes the onus of AI technology providers to use and provide AI services in a manner that the organisation’s data remains within the company without any data leakage. Grounding the results from LLMs helps prevent hallucinations in responses, ensuring more accurate and expected outcomes. Prioritising customer privacy involves safeguarding their data with the help of CSPs. AI technology providers have developed robust security technologies and controls to ensure the safety of their services for customers. As AI continues to evolve and demand grows, the certification and compliance requirements for AI are also evolving. MITRE Atlas threat techniques, along with ISO 42001 standards, are helping companies that manage AI systems and AI providers meet compliance requirements, guaranteeing the security and privacy of their systems and data.

Furthermore, CSPs increasingly use GenAI to bolster privacy implementations. GenAI's Natural Language Processing (NLP) capabilities can identify and classify sensitive data within unstructured data sources such as text documents and emails, providing organisations with a comprehensive understanding of their data landscape. Additionally, GenAI can monitor data access and usage patterns in real time, detecting unauthorised access and potential data breaches. By offering insights into data privacy risks, such as identifying vulnerable data or assessing the effectiveness of existing controls, GenAI contributes to a more robust and proactive approach to data privacy.

Addressing the inherited and inherent vulnerabilities in systems helps protect customers' privacy and the organisation's sensitive information, preventing potential harm in the form of identity theft, financial loss, data leakage or even reputational damage.

As people have grown more conscious about using and sharing their data from cookie tracking, apprehensions surrounding third-party cookies have come to the forefront. This has spurred legislative changes in the form of data privacy legislation. Additionally, it has motivated technology players to announce plans to phase out third-party cookies. This shift will challenge organisations to evolve and adopt a more privacy-centric approach. It also opens doors for innovative alternatives, such as triangulating first-party [customer and enterprise data] with some third-party [environmental nudges, public sets, contextual data, etc.] in perhaps a cookie-less environment.

The cloud can function as a digital immune system; it can help reduce security and privacy threats as more organisations move to the cloud and undergo their digital transformations. Although direct responsibilities vary depending on the services used, privacy controls always remain in the hands of the business. Most CSPs actively collaborate to help customers deploy workloads and operate in a privacy-compliant manner, offering products and solutions for data life cycle management, access management, availability, data governance, etc.

Furthermore, because protecting data is core to CSP's business, they can make extensive investments in security, resources and expertise at scale. Their investment frees organisations to focus on their business and innovation.

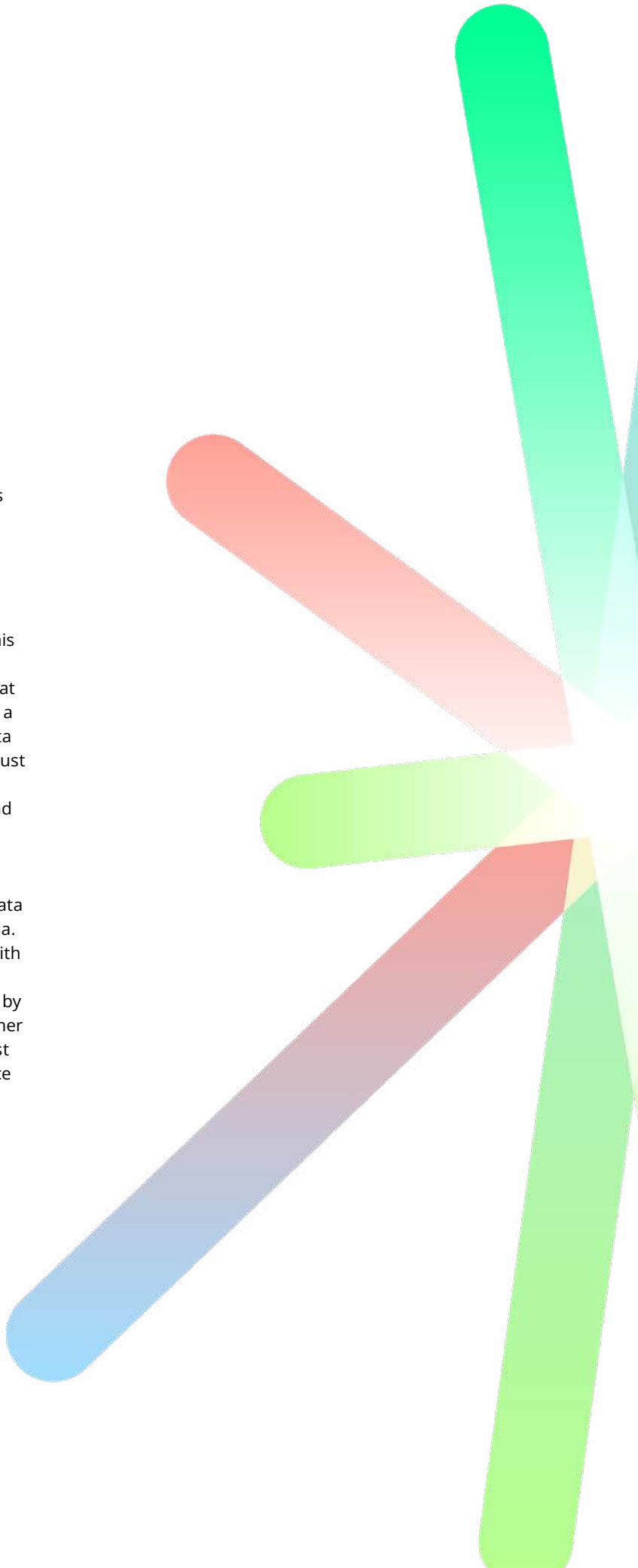
Digital India

A connected nation

India is on its way to becoming a digitally advanced nation. Novel digital ecosystems are already emerging, reshaping the country's socio-economic fabric. The government and private sector are rapidly expanding high-speed connectivity nationwide, providing the hardware and services needed to bring Indian consumers and businesses online. This highlights the emergence of a 'digital native, data-first' India, where data privacy and protection are integral to the broader digital transformation.

For the first time, India has a statutory framework for data protection in the form of the DPDPA, 2023. The presence of this framework will gradually lead to the development of minimal standards of behaviour and compliance among businesses that collect data. For Indian organisations, the DPDPA, 2023 offers a chance to optimise data collection, data management and data governance processes. However, achieving this requires a robust approach involving meticulous assessments, comprehensive strategies, strong execution, diligent monitoring, reporting and communication.

Against this backdrop, this whitepaper has discussed the intersection of digital transformation, cloud computing and data privacy regulations and what they entail for businesses in India. The paper highlights how cloud computing aids compliance with privacy regulations through its robust security features, data encryption options and granular access controls. It concludes by noting that cloud adoption provides businesses with a smoother path to aligning with data privacy laws, fostering a privacy-first culture and implementing PbD principles to ensure compliance and build customer trust.



References

1. www.techbusinessnews.com.au/blog/402-74-million-terrabytes-of-data-is-created-every-day/#google_vignette
2. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
3. Google Cloud whitepaper on New Zealand Privacy Act 2020
4. www.gartner.com/en/digital-markets/insights/importance-of-data-privacy
5. https://www.mordorintelligence.com/industry-reports/cloud-computing-market

About Deloitte

Deloitte is one of the world's largest and most diversified professional services organisations, providing assurance and advisory, tax, management consulting, and enterprise risk management services through more than 345,374 professionals in more than 150 countries. Our organization includes a unique portfolio of competencies integrated in one industry-leading organisation. Deloitte Touche Tohmatsu India LLP (DTTI LLP) also referred as Deloitte India is a member firm in India that provides non-audit consulting services. Our experienced professionals deliver seamless, consistent services wherever our clients operate.
In India, Deloitte is spread across 12 cities with over 12,000 professionals, who are proficient at delivering the right combination of local insight and international expertise to our clientele drawn from across industry segments. Deloitte is well-equipped to deliver solutions to the complex challenges faced by organisations across the public and private sectors. Our edge lies in our ability to draw upon a well-equipped global network and teaming this with customised services at a local office.
We have been consistently recognised as leaders by Gartner in Cybersecurity, the Data and Analytics space, as well for Public Cloud Infrastructure Managed and Professional Services and Oracle Cloud Application Services.

https://www2.deloitte.com/in/en.html

About Google Cloud

Google Cloud is the new way to the cloud, providing AI, infrastructure, developer, data, security, and collaboration tools built for today and tomorrow. Google Cloud offers a powerful, fully integrated and optimized AI stack with its own planet-scale infrastructure, custom-built chips, generative AI models and development platform, as well as AI-powered applications, to help organizations transform. Customers in more than 200 countries and territories turn to Google Cloud as their trusted technology partner.

https://cloud.google.com | https://cloud.google.com/security

Connect with us

Deloitte India

Sathish Gopalaiah
President - Technology & Transformation,
Deloitte South Asia
sathishtg@deloitte.com

Deepa Seshadri
Partner & Leader - Cyber
Deloitte South Asia
deseshadri@deloitte.com

Gaurav Shukla
Partner, Deloitte India
shuklagaurav@deloitte.com

Himanish Chaudhuri
Partner, Deloitte India
hchaudhuri@deloitte.com

Mayuran Palanisamy
Partner, Deloitte India
mayuranp@deloitte.com

Jignesh Oza
Partner, Deloitte India
jigneshoz@deloitte.com

Susmita Chaudhury
Partner, Deloitte India
susmitac@deloitte.com

P S Deepa
Executive Director, Deloitte India
psdeepa@deloitte.com

Google Cloud

Anant Gupta
Head – Financial Services
Google Cloud India
ganant@google.com

Chandra Sankholkar
Director – Partner Business
Google Cloud India
thechandra@google.com

Vineet Parameswaran
Head – Strategic Partnerships
Google Cloud India
pvineet@google.com

Yogesh Khadilkar
Global SI PDM
Google Cloud India
yogeshjk@google.com

Contributors

Deloitte India

Hiten Panchal

Google Cloud Security

Rohan Kanungo

Sandeep Agarwal

Sujata Dusi

This co-authored whitepaper applies to Google Cloud and Security products described in the Google Cloud Services Summary. The content contained herein is correct as of August 2024 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP) and Google Cloud India.