Performance on Governance Goals | Corporate Governance | **Data Privacy** | Information Management

Data Privacy

Thought Leadership in Data Privacy

We understand that staying ahead in a dynamic privacy landscape requires leadership and advocacy beyond the organization. The Infosys Data Privacy Office is deeply engaged with global industry bodies, regulatory groups, and standard-setting organizations. Through these partnerships, we help shape the development of data protection frameworks, policies, and international standards, particularly in emerging areas such as artificial intelligence. Senior leaders from the DPO frequently represent Infosys at international conferences and collaborate with governments and institutions to inform regulatory direction. These contributions underscore our role not just as a compliant entity, but as a driver of best practices in data privacy across industries and borders.

> First India-headquartered Company to receive Binding Corporate Rules (BCR) approval from EU data protection authorities.

Evolving notion of privacy

At Infosys, we recognize that the rapidly evolving digital landscape has reshaped the very meaning of privacy. With the proliferation of technologies such as artificial intelligence, the Internet of Things, and big data, we are seeing transformative benefits across society. However, these same technologies introduce greater risks related to data privacy and security. Our business model involves the seamless global flow of data, which must comply with regulations that often have extraterritorial reach. That's why we emphasize the importance of consistent and effective data protection

practices across every country we operate in. Our independent Data Privacy Office (DPO) is central to this effort, ensuring that privacy is balanced with innovation. As AI continues to evolve, we are mindful that many existing privacy regulations already apply to AI systems that process personal data, and we closely align our practices with key principles like transparency, fairness, non-discrimination, explainability, and human oversight.

To effectively manage these evolving risks and regulatory expectations, we have built a strong internal governance structure that supports our privacy objectives across the organization.

Governance and Organizational Structure

A well-defined governance model forms the backbone of our privacy framework. The Data Privacy Office at Infosys functions as both architect and checker of privacy controls, while business-enabling functions and delivery teams serve as makers. Periodic audits by internal and external entities reinforce accountability, and quarterly reviews by senior management provide strategic direction. Our multi-tiered governance is further

enhanced by three dedicated councils: the Privacy Sub-Council, comprising representatives from delivery and enabling functions; the Data Privacy Council, which includes business unit and function heads; and the Legal Compliance and Risk Council, featuring senior leadership such as the General Counsel, Chief Financial Officer, and Chief Risk Officer.

This governance model supports our broader compliance strategy, which is focused on aligning operational practices with regulatory mandates and internal standards. Sustained Approach to Data Privacy Compliance.

Sustained Approach to Data Privacy Compliance

Infosys has long recognized the importance of a strategic and structured approach to privacy compliance. More than a decade ago, we established our Data Privacy function as an independent group reporting directly to top management. This function is built on the globally recognized Privacy Information

Management System (PIMS) framework and is responsible for ensuring compliance with data protection regulations across business processes, applications, and client engagements. Our Data Privacy Policy—accessible to all employees via the intranet—reflects top management's commitment to privacy. This commitment extends beyond internal operations to include third-party service providers. In line with our values of transparency and accountability, we provide privacy notices at data collection points for both internal and external data subjects. The privacy statement for external stakeholders is also publicly available on our website and is routinely updated to reflect changes in data handling practices or applicable laws. Read more.

As we continue to build on this foundation, embedding privacy into the design of our systems and services has become a key enabler of both compliance and innovation.

Cross-Jurisdictional Compliance

At Infosys, we maintain a robust, enterprise-wide data privacy and compliance framework designed to meet the complex and evolving regulatory requirements across jurisdictions. A dedicated compliance team actively monitors legal and regulatory developments globally, leveraging inputs from multiple sources, including regulatory databases, industry bodies, law firm alerts, and consulting advisories. This monitoring enables near real-time identification of changes and facilitates timely compliance actions.

To operationalize compliance tracking, Infosys employs specialized tools while drawing on memberships with professional organizations including the International Association of Privacy Professionals (IAPP) and the Association of Corporate Counsel (ACC). A centralized compliance repository maps regulatory requirements to business-enabling functions, ensuring consistent implementation across the enterprise.

We conduct Data Protection Impact Assessments (DPIAs) prior to initiating new data processing activities or deploying technologies involving personal data. This ensures that privacy-by-design principles are embedded from the outset. Our incident response protocols include predefined procedures for notification, assessment, mitigation, and documentation, supporting

adherence to cross-border data breach notification obligations.

In jurisdictions with data transfer restrictions, Infosys adopts appropriate legal mechanisms such as Standard Contractual Clauses (SCCs) and Joint Controller Agreements to legitimize international data transfers. Wherever possible, we aim to minimize or avoid such transfers in alignment with local regulatory expectations.

Demonstrating our commitment to global data privacy standards, Infosys became the first India-headquartered Company to receive Binding Corporate Rules (BCR) approval from EU data protection authorities—an internationally recognized framework for safeguarding personal data transferred outside the EU.

As we continue to build on this foundation, embedding privacy into the design of our systems and services has become a key enabler of both compliance and innovation.

EPIC — Embedding Privacy by Design into Infosys Culture

Integrates *privacy by design* into every stage of the software development lifecycle—from architecture to deployment

Privacy by Design Enablement

We believe that privacy should be integrated at the design stage of any process or application that handles personal data. To embed this principle into our organizational DNA, we launched the EPIC initiative—Embedding Privacy by Design into Infosys Culture. Rolled out by the Data Privacy Office in collaboration with quality and delivery teams, EPIC is a company-wide strategic program. It incorporates privacy considerations into the architecture, development, and deployment phases of the software lifecycle. Through this initiative, our development teams are trained to apply the seven foundational principles of Privacy by Design using privacy design strategies, patterns, and privacy-enhancing technologies (PETs). This not only supports regulatory compliance but also fosters a privacy-first mindset among our engineers.

Our ability to design and deliver privacy-conscious solutions is further bolstered by adherence to global benchmarks and certifications.

Privacy Performance Metrics

We are continuously strengthening our data privacy measurement framework under the oversight of our Data Protection Office (DPO). Various metrics are regularly analyzed, reviewed for trends, and presented to senior leadership during the cross-functional Quarterly Data Privacy Council Meetings. Insights from these reviews guide continuous improvement initiatives across the organization.