



Evolving notion of privacy

Today, there is a much greater adoption of digital and emerging technologies in everything we do. The increased adoption of tools and technologies that we use at work have brought in a great deal of operational ease and efficiency, making life much simpler but at the same time, digital data processed as part of adoption of these tools and technologies is prone to data privacy threats and data leakages due to ease of information dissemination. This has led the authorities across the world to enforce stricter DP regulations demanding greater accountability from organizations, to ensure that the controls are not intrusive when deployed. At Infosys, the Data Privacy Office (DPO) an independent function, ensures right balance careful balancing before deploying them.

With AI evolving at rapid pace, various existing privacy laws already regulate AI systems to a considerable extent in applications processing personal information. Principles of AI like transparency, fairness and non-discrimination, explainability and human oversight are related to specific individual rights and provisions of corresponding privacy laws.



Approach to sustained DP compliance

Infosys established its independent Data Privacy function over a decade ago. Reporting directly to the Management, this function leverages the globally-recognized PIMS (Privacy Information Management System) framework. Through fiscal 2024, we ensured compliance with applicable DP regulations for all business enabling processes and applications, as well as client project execution.

Our Data Privacy Policy, published on the company intranet, clearly demonstrates the top management commitment to DP across all Infosys operations, including those involving service providers. To ensure complete transparency, we provide privacy notices at the point of data collection for both internal and external data subjects. Additionally, the privacy statement for external data subjects is readily available on the Infosys website. All privacy notices and statements are regularly updated to reflect any changes in personal data processing or applicable data protection regulations. [Personal Information Privacy Statement | Infosys](#)

DP governance framework

At Infosys, the Data Privacy Office plays the role of architect and checker, while business enabling functions and units are the makers, with independent audits being carried out periodically by our Quality team and external bodies. Quarterly senior management reviews ensure adequate oversight.

- **Privacy Sub-Council**
(Comprises nominated individuals from business enabling functions)
- **Data Privacy Council**
(Comprises heads of business enabling functions and business units)
- **Legal Compliance and Risk Council**
(General Counsel, CFO and CRO are key members)
- **Risk Management Committee**
(Chaired by an independent director)

Aspirations in data privacy

We make every effort to protect the personal information that comes under our purview. Our data privacy compliance framework is based on ISO 27701 with inputs that include convergence of international best practices, client-prescribed requirements, and applicable data privacy regulations across geographies.

Adopting internationally accepted protocols

We are among the first few organizations globally, to have our framework certified with accreditation, for ISO 27701 privacy information management standard. The coverage for this certification is being enhanced across Infosys centers worldwide in a phased manner.

The EPIC program

Anticipating the need to make privacy an integral part of any process or application dealing with personal data, an organization-wide strategic initiative named EPIC (Embedding Privacy by design into Infosys Culture) was rolled out in early 2022 by the Data Privacy Office in collaboration with quality and delivery functions. EPIC is a framework for embedding privacy in the architecture and design stage itself and then throughout the software development lifecycle while designing and developing digital solutions.

This EPIC program focuses on enabling the software development community at Infosys to engineer the 7 Privacy by Design principles into their software development process using privacy design strategies, design patterns and PETs (Privacy Enhancing Technologies).

Vendor DP guidelines

Vendor data privacy management of our extended entities has assumed strategic significance in the current scenario of third-party risks, given the increasing volume of data breaches, and enterprise dependency on outsourcing including cloud service providers. Suppliers present difficult and unique privacy and cybersecurity challenges. Compliance with diverse data protection laws across the world requires an effective mechanism for managing supplier-related risks to Infosys. We have published comprehensive guidelines for suppliers / vendors to ensure that they adhere to strict obligations imposed by contracts and applicable laws of the land, during their engagement with Infosys and its subsidiaries. The Infosys Supplier Code of Conduct is mandated across all essential suppliers involved in processing of personal data, along with necessary data processing clauses that are consented to prior to their onboarding. Assurance is further demonstrated through due diligence and annual assessments.

Incident and breach management

Infosys has implemented robust mechanisms to detect, assess, contain, and manage data privacy incidents and breaches, with well-defined processes and procedures to respond to them within defined timelines in accordance with the laws of the land. We have a dedicated team of data privacy professionals who oversee the incident management process and coordinate with the relevant stakeholders, such as the business units, the information security team, the legal team, the communications team, and the external service providers. We also have a network of data privacy champions and coordinators across the organization who act as the first point of contact for reporting and escalating any data privacy incidents or breaches. If an incident or a breach is determined to be of high impact, and / or if the law of the land mandates, such incidents or breaches are notified to the impacted data subjects and / or the supervisory authority. The notification includes the nature and extent of the incident or breach, the measures taken to mitigate the risks and prevent recurrence, and the contact details of the data privacy officer or the data protection officer. We also provide the data subjects with the necessary guidance and support to protect their rights and interests. We continuously monitor and evaluate the effectiveness of our data privacy incident management process and implement corrective and preventive actions to improve our

data privacy posture. We also incorporate key learnings from incidents in privacy awareness stories and tips sent to employees. Incidents of high and critical nature are reported to the incident disclosure committee, consisting of senior leaders including the CEO. Infosys has zero tolerance for any breaches, which, in addition to appropriate preventive measures, are controlled through effective deterrent mechanisms including stringent consequence management.

In fiscal 2024, there was one substantiated complaint received concerning breach of customer privacy by external parties.

Data subject rights management

Data subject rights, which have become an intrinsic part of data privacy laws in many countries, are legal rights enjoyed by the data subject. These rights are legally enforceable, but never absolute, with numerous interrelated and, at times, overlapping exceptions to be considered. This makes the fulfilment of data subject rights a complex exercise in the current enterprise setting, where data subjects as well as data in structured and unstructured formats are spread across systems and servers in multiple geographies with diverse regulatory regimes. Infosys has established necessary procedures and processes to optimally respond to such data subject rights requests within the legally stipulated timelines across Infosys locations, including subsidiaries.

Raising DP awareness through campaigns and events

Every year, we celebrate the Data Privacy Day by hosting engaging interventions and diverse online interactive events like crosswords, quizzes, Pictionary, chat with DPO and messages from senior leaders to spread awareness. The events span over several months and rewards are offered to promote employee participation. Additionally, monthly awareness mailers in the form of privacy tips and scenarios reflecting changing threats are also sent organization wide to strengthen awareness. We conducted International Privacy Symposium 2022, a virtual conference organized by the Infosys Data Privacy Office in association with IAPP and ACC, where participants included global privacy leaders, CPOs, experts from academia and global frontline practitioners to reflect on key trends, challenges, and best practices. Some of the sessions organized as part of this included privacy engineering, anonymization, privacy-preserving synthetic data, AI, data ethics and human behavior, privacy standards, data subject rights and other emerging areas. A similar symposium is proposed to be organized in 2024 in collaboration with international bodies.

All employees and sub-contractors must also mandatorily complete privacy awareness quiz annually, the questions and scenarios are tailored based on their respective roles.

Driving DP thought leadership

In this constantly changing privacy threat landscape, Infosys DPO recognizes the need for regular engagement with industry and government bodies to shape the future of data privacy. Towards this, it actively participates in various initiatives with industry forums and standard bodies globally, contributing to developing DP frameworks, policies, and standards. Infosys CPO is the co-editor for ISO and IEEE standards related to privacy engineering, management, and privacy in emerging technologies, some of which have been published while others are being developed. Such emerging technologies include AI, digital twins, Metaverse and ZKP (Zero Knowledge Proof).

Senior leaders from the DPO regularly speak in conferences of international repute, and actively engage with government bodies to help shape policy / regulations.