



Evolving notion of privacy

Today, there is a much greater adoption of digital and emerging technologies in everything we do. The tools and technologies that we use at work have brought in a great deal of operational ease and efficiency, making life much simpler. Often, the incentives to use these are so compelling, that choice is only notional. On the other hand, Data Privacy (DP) regulations around the world are demanding greater accountability from us, to ensure that these are not intrusive when deployed. Many of these tools, platforms and processes have the propensity to breach privacy if not deployed with due diligence. Hence, at Infosys, the Data Privacy Office (DPO) an independent function, ensures careful balancing before deploying them.



Approach to sustained DP compliance

At Infosys, we constituted the data privacy function over a decade ago as an independent business enabling function reporting to the management and using the globally recognized PIMS (Privacy Information Management System) framework. We complied with all applicable data privacy regulations in fiscal 2023 in building applications and platforms, or while executing client projects, by introducing appropriate privacy safeguards. Our Data Privacy Policy published in the Company intranet, demonstrates our the Management's commitment to privacy and applies to the entire operations including service providers. To ensure complete transparency, we provide privacy notices at

the time of data collection to both internal and external data subjects and the privacy statement for external data subjects is also made available in the public domain. These are constantly updated to reflect the changes in personal data processing or applicable DP regulations.

Privacy Statement

Infosys does not do behavioral advertising. Infosys also does not use personal data for secondary purposes. Whenever there is a change in the purpose, data subjects are notified of the new purpose through privacy notices.

[Infosys - Privacy Statement.](#)

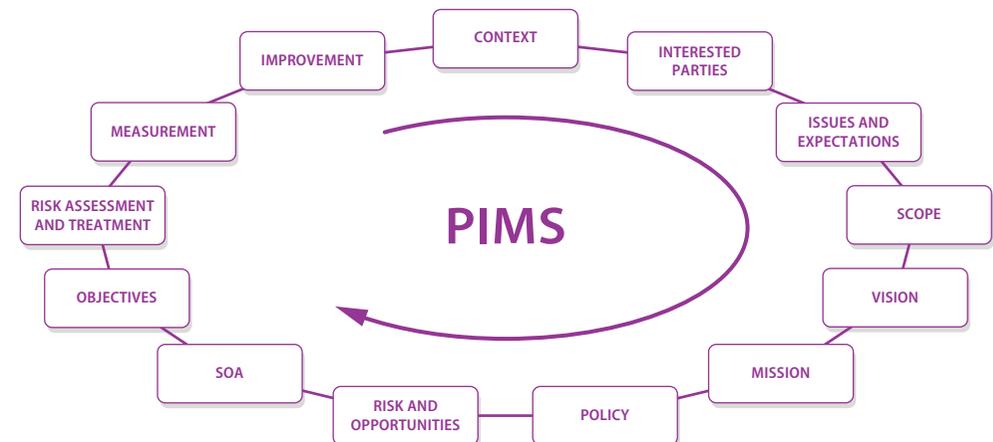
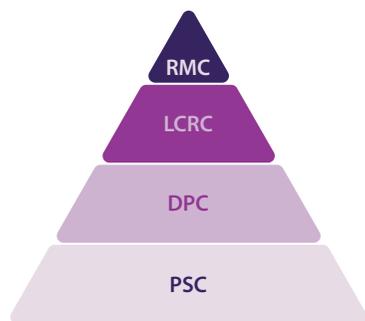


Diagram 1: A robust framework to continuously improve data privacy

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.



■ Risk Management Committee ■ Data Privacy Council
 ■ Legal Compliance and Risk Council ■ Privacy Sub-Council

- **Privacy Sub-Council**
 (Comprises nominated individuals from business enabling functions and Delivery)
- **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 DP

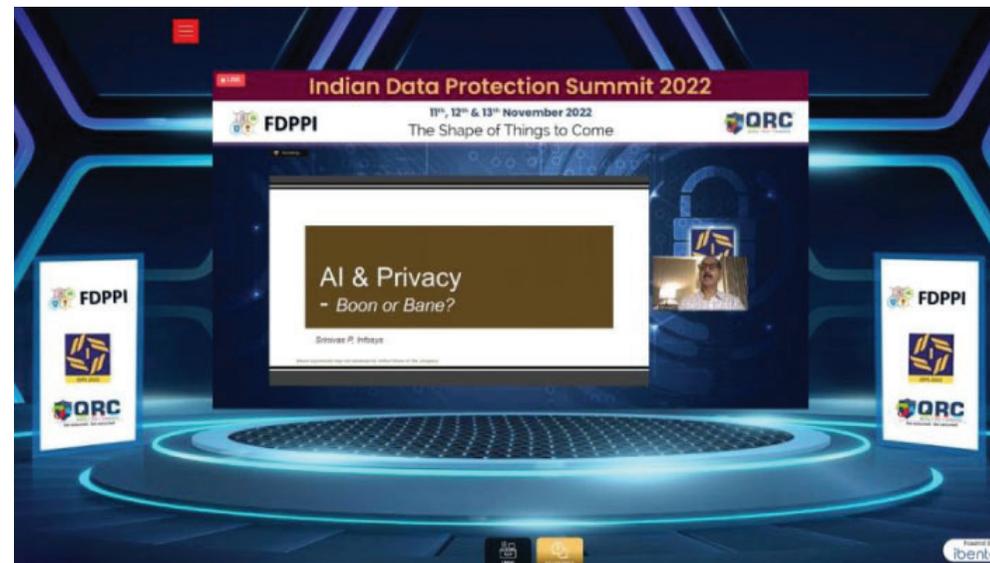
We make every effort to protect the personal information that comes under our purview. Our data privacy compliance framework is based on ISO 27701 with inputs that include convergence of international best practices, client-prescribed requirements and applicable data privacy regulations across geographies.

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. We intend to increase the coverage of the certification across the enterprise in phases.

Privacy by Design (PbD) 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 DPO in collaboration with Quality and Delivery functions. EPIC embeds PbD into the solution development process at Infosys to enable responsible data-centric innovation



that complies with DP regulations, leading to market differentiation. The program focuses on introducing PbD strategies, patterns and guidelines to integrate privacy principles and requirements into solutions and platforms development. To institutionalize privacy by design, a two-phased enabling program is under way. In phase one, foundational and intermediate courses on privacy by design were designed and enabled for all employees globally. Phase two is focusing on taking the privacy by design implementation to clients.

Vendor DP guidelines

Vendor DP 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 cyber security 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 which are agreed prior to their onboarding. Assurance is further demonstrated through due diligence and annual assessments.

Robust incident management and breach handling

At Infosys, we have robust mechanisms to detect, assess, contain and manage data privacy breaches and incidents with well-defined processes and procedures to respond to breach notifications within defined timelines in accordance with the laws of the land. If an incident or a breach is determined to be of

high impact, and / or if the law of the land mandates, such breaches are notified to the impacted data subjects and /or supervisory authority. 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 & MD. 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 2023, there were no substantiated complaints received concerning breaches of customer privacy from outside parties and regulatory authorities.

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, which makes the fulfilment complex in the current enterprise setting with data spread across systems and servers in multiple geographies with diverse regulatory regimes. Infosys has established necessary tools and processes to cater 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, 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 to everyone in the organization 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 2023 in collaboration with international bodies.

All employees and sub-contractors have to also mandatorily complete privacy awareness quizzes annually, the questions and scenarios for which are tailored based on the their respective roles.

Driving DP thought leadership

In this constantly changing privacy threat landscape, the 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. The Infosys DPO 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).

Recently, AI-based tools and technologies have proliferated across the digital industry, bringing in rich dividends both for consumers and businesses. However, this has also introduced hitherto unknown privacy threats, particularly on decisional autonomy, basic to individual data empowerment. At Infosys, data privacy and data ethics are an integral parts of the responsible AI framework and all AI-based solutions and platforms are subjected to privacy assessments before deployment, to balance business value derived with data privacy.