



Data Privacy at Wipro



About Wipro's Privacy team

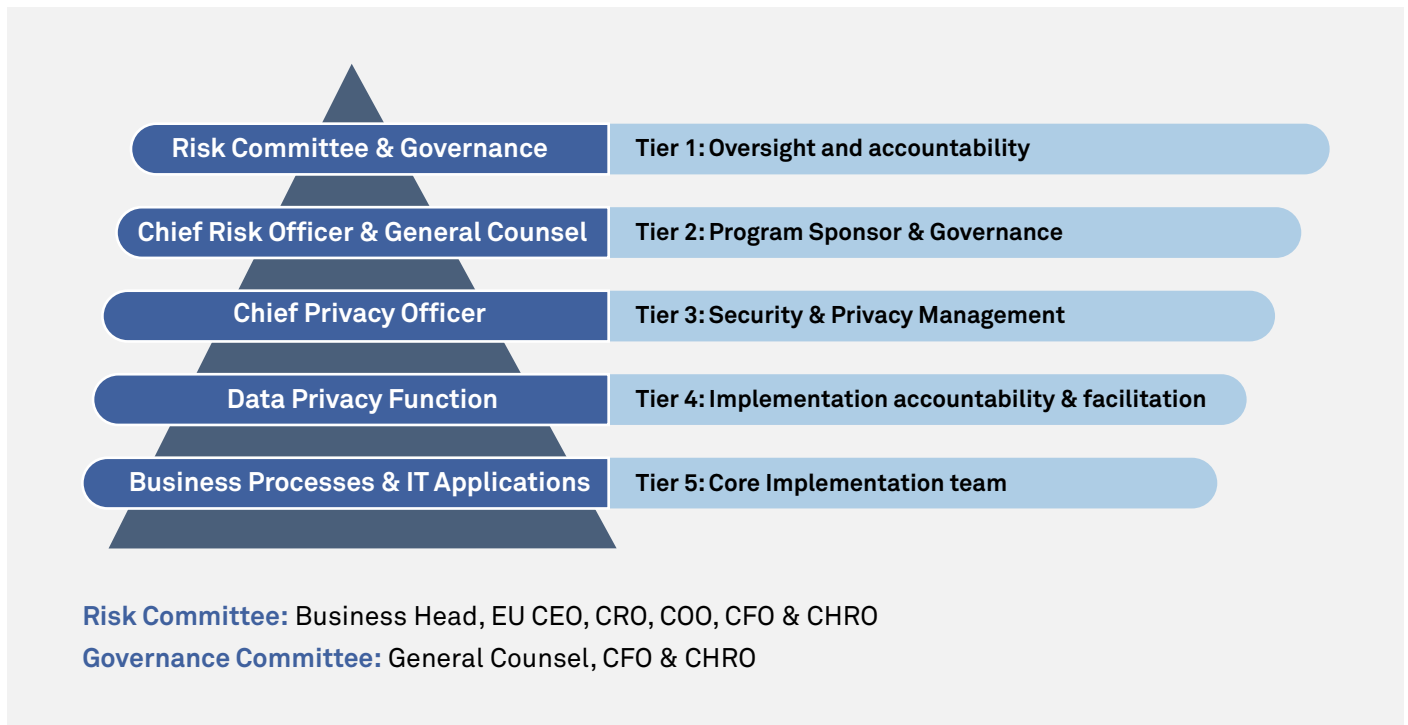
As a responsible global corporate enterprise, Wipro takes the processing of personal data very seriously and ensures adherence to global privacy principles. We promote a strong privacy culture through awareness, guidance, and mandatory processes.

Wipro has a dedicated central Global Data Privacy Team headed by the Chief Privacy Officer, who reports to the Chief Risk Officer and General Counsel.

The Data Privacy team at Wipro implements and manages all compliance measures with the privacy regulations applicable to Wipro as an organization.

The Team is also actively involved in supporting all client delivery functions, by leveraging Wipro's privacy-by-design approach to implement effective controls for customers' data.

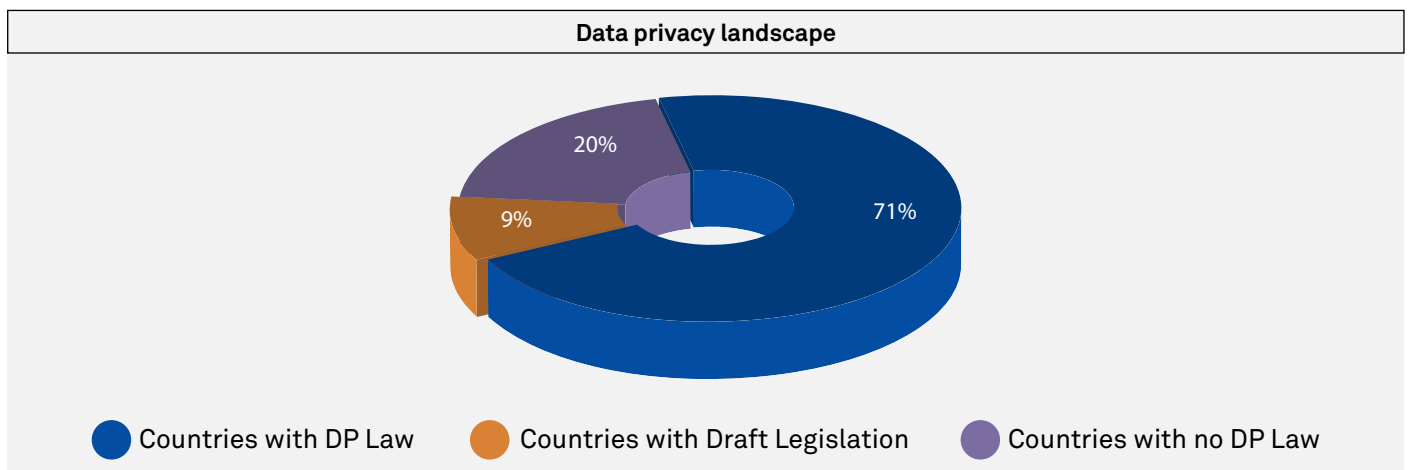
The diagram below represents the data privacy governance at Wipro.



Introduction to Data Privacy

Privacy is a fundamental right in many jurisdictions. Alongside data protection, it addresses the imbalance of power between the data subject (the individual) and the digital ecosystem by establishing

rules about the collection, storage, and sharing of personal information. Privacy and data protection law is generally technology neutral and interacts with sector or technology-related legislation, such as AI. Countries are increasingly equipping themselves with privacy and data protection legislation, as shown in the chart below:



Wipro Data Privacy Framework

Wipro's robust enterprise-wide Data Privacy Framework includes various governance mechanisms such as corporate policies, training and awareness programs, privacy impact assessments, privacy by design, data mapping, vendor due diligence, incident management, and awareness. Using this framework, Wipro ensures that data privacy remains agile and adapt to the international regulatory challenges and developments as well as ever-evolving customer expectations.

The dynamic, modular, risk-based Data Privacy Framework aligns with Wipro's Cybersecurity and Information Security frameworks, enabling Wipro to comply with regulations and industry best practices for privacy.

This means that Wipro customers get the best innovation with the best solutions for privacy, security, and ethics — a true competitive edge at a time when consumers and regulators are demanding more transparency and control.

The Global Data Privacy Office

Wipro's Data Privacy Office is a team of privacy professionals that proactively implement and manage Wipro's privacy portfolio to ensure compliance with privacy regulations as applicable.

The Data Privacy Office also supports all client delivery functions and facilitates compliance with the internally established privacy frameworks when personal data is processed for our customers. The team works with various business lines, integrating privacy principles and risk-based methodologies to ensure robust privacy compliance throughout the organization.

Key Principles of Wipro Privacy program

Wipro has a comprehensive privacy program and Code of Conduct designed to meet the requirements of all applicable laws and regulations globally. As part of this program, Wipro, acting as a data controller or data processor, shall follow global privacy principles.

Wipro identifies potential privacy risks while processing personal data and takes the appropriate actions to mitigate and remediate those risks. Wipro has documented, communicated, and assigned accountability for managing its data privacy framework. Wipro processes personal data for the purposes that are identified and are in accordance

with the consent received. Wipro has made available privacy notices as appropriate that explain the collection, usage, storage, sharing, and disposal of personal data. We take adequate measures to protect personal data from unauthorized access, data leakage, and probable misuse. Wipro has detailed processes for facilitating an access or correction request raised by the data subject and addresses it in line with the relevant regulatory requirement. Wipro has taken all the necessary steps to ensure that the personal data processed is accurate, complete, and up to date. Wipro does not retain the personal data any longer than it is required to fulfill the purpose for which it was collected, and after the purpose is met, the personal data is disposed securely. Wipro, where required, shall disclose data to third parties in a secure manner only if there is a purpose identified in the privacy notice.

Privacy by Design

Wipro has a specialized "privacy by design" center that has developed key guidelines, templates and resources to ensure "privacy by design" is maintained in various Wipro systems (both in-house and customer support). This team aims to provide teams and clients with support, knowledge, and the most efficient PET (Privacy Enhancing Technologies) solutions.

Privacy Impact Assessments (PIAs) are a key tenet of Privacy by Design so that privacy is not an afterthought but part of the design of a product.

Wipro's Privacy by Design Centre supports privacy implementation at the tactical and operational levels, and is essential in minimizing privacy and security risks, which helps in building trust and increase transparency with the data subjects and stakeholders. This team ensures that the PIA are performed in the early stages of the project's lifecycle and that the identified risks are addressed early to avoid unnecessary implications on the cost or the budget of the project. The risks thus identified and fixed aid in training purposes for the broader audience within Wipro.

These steps increase the likelihood of compliance with the applicable privacy regulations and minimize the chances of privacy intrusion that may negatively affect the data subjects and stakeholders. The risk mitigation efforts are also used for training purposes throughout Wipro to ensure our teams are keeping up with advancements in the field of data privacy.

Regulatory Compliance

Wipro understands the importance of the ever-evolving regulatory landscape and is committed to being a leader in data privacy in terms of demonstrating compliance with all the applicable regulatory requirements. Our continuous monitoring program ensures that Wipro stays up to date on the latest happenings by not just looking only at the actual new regulations but also reviewing and anticipating any potential changes that may adversely affect Wipro.

When we identify any significant developments likely to affect Wipro's operations, an analysis is sent to senior executives and key stakeholders in the respective jurisdictions, who then formulate a plan to prepare. Wipro also leverages support from external counsels and consultants to assist in some issues

Wipro has a global footprint with a presence in over sixty-five countries. To ensure compliance with all the country-specific data privacy requirements, Wipro conducts an in-depth country compliance activity.

End-User Privacy

Wipro's Privacy Statement on the website and internal Data Protection & Privacy Policy articulate the privacy and data protection principles followed by Wipro Limited and its entities worldwide. Parties covered by these policies include customers (including products, outsourcing, and other services), partners, current and former employees, trainees, applicants, contractors, prospects, vendors, and current or former members of the Board of Directors, whose personal information are processed by Wipro.

Wipro does not share personal information about customers with affiliates, partners, service providers, group entities, and non-affiliated companies except in cases where we have the end-users consent for a legitimate purpose or when legally required to do so. Refer to Wipro Privacy Statement for more details:

<https://www.wipro.com/privacy-statement/>.

Policy Review and Approach

The Data Privacy Office maintains the Wipro privacy policies and procedures such as our privacy incident management procedure, anonymization and pseudonymization guidelines, and HIPAA policy on a stipulated frequency. Significant modifications are made to the privacy policy or procedural documents only after seeking relevant approvals and then uploaded to the appropriate internal portals.

These changes are then communicated to required audience.



Privacy Incident Management

Wipro has a dedicated Data Privacy Team which proactively manages and implements appropriate and effective measures to ensure compliance with privacy requirements and industry standards applicable to the organization.

Wipro's Data Privacy Framework entails the integration of important aspects of data privacy (e.g. privacy principles and methodologies across the length and breadth of the organization) to strengthen privacy training and awareness within Wipro.

One of the most important aspects of Wipro's Privacy Framework is its systematic and strategic approach to managing potential privacy incidents and breaches. Privacy incidents and breaches are not only escalating in frequency along with their impact on a global scale, but the ramifications of these incidents are compounding as we move towards an increasingly connected digital society. Due to the enormity of the risks associated with such incidents, Wipro prioritizes the detection, response, and recovery processes in the highest possible manner to ensure effective and efficient management.

Wipro manages privacy incidents in a top-down approach, embedded in Wipro's overall Privacy Incident Management Framework. Wipro has industry-best solutions such as DLP to automatically detect incidents and technical vulnerabilities leading to leakages of personal data and trigger communication to all the required stakeholders.

Wipro also provides comprehensive training on privacy incident management and reporting to all employees on a stipulated frequency which encourages the employees to sincerely report any suspicious activity that could turn out to be a privacy incident. The Incident Management Team reviews the incident that is reported and validates if it is a privacy incident and engages the Data Privacy Team for support with any verified incidents. The Data Privacy Team is primarily engaged in reviewing the corrective, preventative, and remediation measures that must be deployed to address privacy incidents and prevent them from recurring. In addition to this, a specialized branch of the Data Privacy Team provides a great deal of sophistication in managing privacy incidents 24/7.

Wipro is cognizant of all the privacy incidents and related requirements arising from the applicable privacy laws and has developed processes and procedures to ensure we stay updated, implement and comply with the same.



Privacy Impact Assessments

Wipro's Data Privacy Framework advocates performing privacy impact assessments (PIAs) on all products and offerings, including but not limited to internal business-enabling functions, client-delivery engagements, shared-services platforms, products and platforms thereby ensuring a 360-degree view of all data processing activities.

PIAs are performed using a risk-based approach and follow industry-leading global standards. This methodology helps us challenge the traditional ways of managing privacy of the data through gap assessments and enable viewing data privacy from the lens of numerical risk score that are derived from carefully selected parameters like the probability of an incident that may occur or the potential financial impact of an incident. Furthermore, this methodology helps paint a comprehensive picture of the overall risk proposition for each of the elements included within.

Training & Awareness

Wipro's Data Privacy Office is constantly looking for new ways to enhance knowledge and awareness around data privacy topics and considerations across the length and breadth of the organization. Wipro takes special interest in encouraging and enhancing privacy learning and awareness throughout the organization. All employees, including contractors, must complete the mandatory privacy training to ensure that they understand key privacy concepts and principles, laws, best practices, and contractual obligations.

Training is designed to equip employees from all business lines with up-to-date information on data privacy in their respective fields. The Data Privacy Office has also developed interactive and focused training workshops, including awareness emails, podcasts, etc. that are relevant to Wipro business and are customized to cover any new developments in the privacy space.

Data Subject Requests

Wipro has an established and well-defined process to handle subject access requests related to personal data to cater to the SAR. Wipro respects every data subject's right and has a robust data subject request (DSR) program in place to address the requests from a data subject concerning their right to be informed, access, correct, request deletion or request restriction, portability, etc., as may be required under applicable law with timely resolution and highly efficient counsel support.

Cross-border Data Transfers

As a global business working with global clients, secure data sharing is a priority. We are at the forefront of the debate on data sharing. We believe our unique capabilities in privacy technology and engineering can support the safe global data handling.

We have a dedicated team to perform transfer impact assessments and support customers in this complex area. Our approach to cross-border data transfers post-Schrems II is available [here](#).

Data Security Management

We provide our customers with unparalleled data security expertise and a full suite of security measures. Wipro's Information Security Policy is articulated in our information security management system (ISMS), which is an ISO standard to provide management direction and information security support in accordance with business requirements and relevant laws and regulations to ensure confidentiality, integrity, and availability of customer assets, information, data, and IT services.



Wipro is certified under the ISO 27001:2013 standard for information security practices, inclusive of physical security & employee safety.



Technical (password protection) and organizational (user account management) measures with respect to user identification and authentication have been implemented.



Unauthorized activities outside of granted permissions are prevented. User access to IT infrastructure and applications is granted based on an individual's job responsibilities and business requirements on a need-to-know basis. Access restrictions are role-based, and authorizations will be obtained as defined in the access control matrix and their monitoring and documentation.



Through comprehensive physical and logical security controls, unauthorized persons are prevented from gaining access to data processing systems, thereby avoiding any kind of unauthorized access to personal data.



All aspects of transmitting personal data are regulated. Transmission and transfer or storage on data media (manual or electronic) are controlled as well as subsequent verification.



Data is protected against accidental destruction or loss by implementing adequate measures like encryption, pseudonymization etc.



Personal data processed on behalf of others are processed strictly in compliance with the controller's instructions dividing responsibilities between the contractor and the client.



Wipro has segregated processing (storage, alteration, deletion, transmission) of data for different purposes.



Wipro has processes for regularly testing and assessing the effectiveness of technical and organizational measures to ensure secure processing while strengthening the internal IT, IT security governance, and management.

Customer Compliance Support

Wipro's Data Privacy Team is engaged right from the time the request for proposal is made and throughout the complete sales lifecycle helping in responding to the queries and performing contract reviews. The team also helps conduct privacy assessments during onboarding and afterward, in line with the customers' privacy expectations.

Scheduled risk reviews on stipulated frequency are conducted as part of the regular compliance assessments. The Data Privacy Team requires relevant stakeholders to maintain the records of all the personal data processing activities along with all the appropriate documentation or agreement structure to maintain transparency. The team also helps in publishing Dos and Don'ts that are specific to personal data processing in processor context. The team also supports in keeping up with the ongoing regulatory requirements like Schrems II, UK IDTA, etc.

Vendor Compliance Support

Wipro takes into consideration various compliance factors that includes but not limited to privacy compliance right from the vendor selection stage.

The dedicated team here conducts vendor risk assessments prior to onboarding vendors into the corporate and delivery functions. Periodic reviews on vendor privacy compliance are also conducted.

Most importantly, the flow down of customer contractual obligations along with the regulatory requirements in accordance with the law of the land is executed with selected vendors, contractors, and subcontractors.



For more information, please contact:

Ivana Bartoletti
Global Chief Privacy Officer
data.privacy@wipro.com



Ambitions Realized.

Wipro Limited
Doddakannelli
Sarjapur Road
Bengaluru – 560 035
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading technology services and consulting company focused on building innovative solutions that address clients' most complex digital transformation needs. Leveraging our holistic portfolio of capabilities in consulting, design, engineering, and operations, we help clients realize their boldest ambitions

and build future-ready, sustainable businesses. With over 240,000 employees and business partners across 66 countries, we deliver on the promise of helping our customers, colleagues, and communities thrive in an ever-changing world.

For more information, please write to us at info@wipro.com