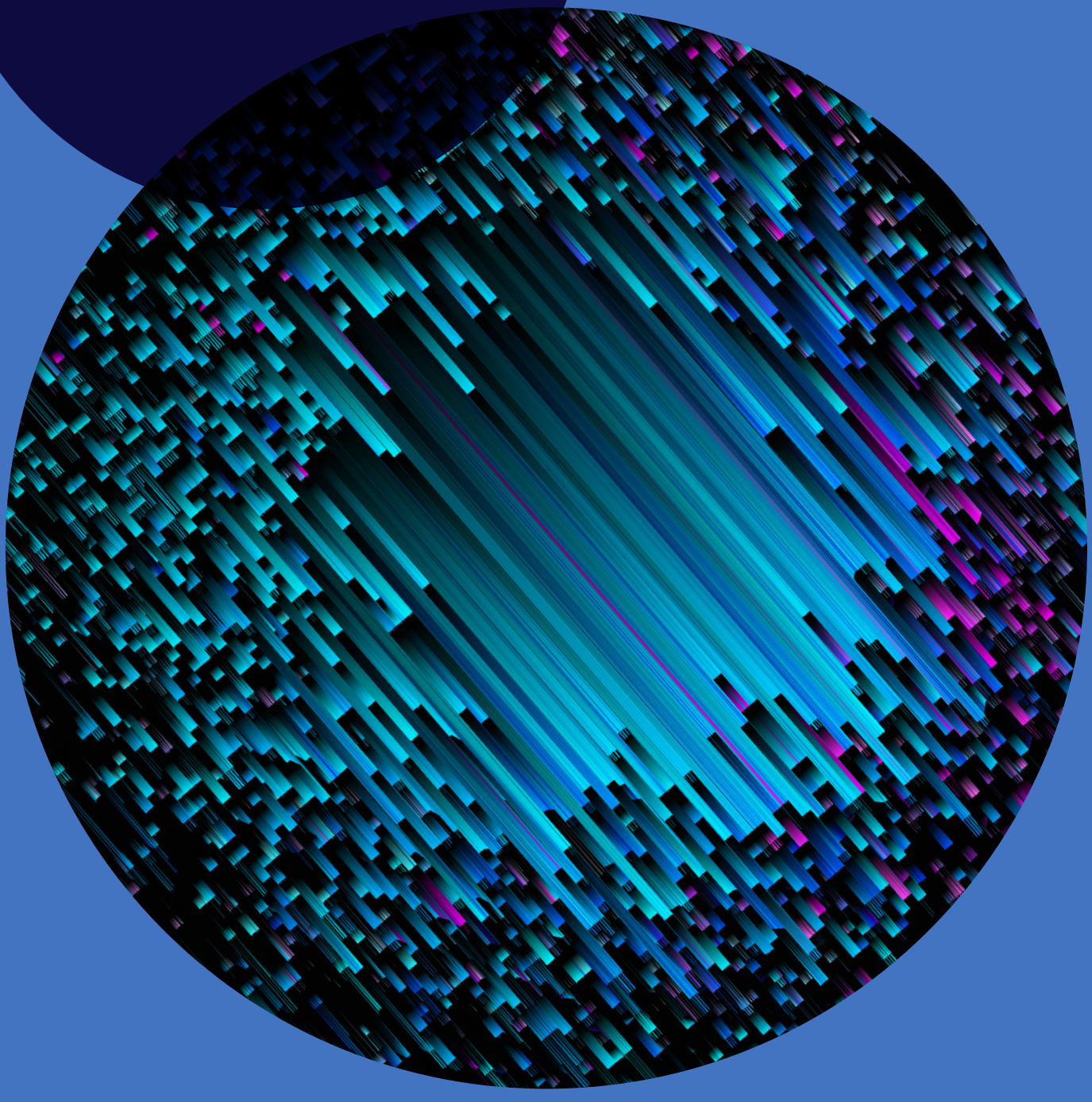
International Transfers of Data How we Work



What is Schrems II?

In July 2020, the Court of Justice of the European Union (CJEU) declared the European Commission's Privacy Shield Decision invalid on account of invasive US surveillance programs, thereby making transfers of personal data on the basis of the Privacy Shield Decision illegal.

Furthermore, the Court increased the requirements for the transfer of personal data based on standard contract clauses (SCCs). In a nutshell:

- Data controllers or processor who intend to transfer data based on SCCs must ensure that the data subject is granted a level of protection, essentially equivalent to that guaranteed by the General Data Protection Regulation (GDPR) and the EU Charter of Fundamental Rights (CFR).
- If necessary, with additional measures to compensate for lacunae in protection of third country legal systems.

How can Wipro help you?

The safety of our clients data is our utmost priority. At Wipro, we have an established GDPR compliance program and, in the aftermath of Schrems II, we have reviewed our own contracts and transfers by looking at the legal framework that applies in the receiving country, and taking into account relevant, objective, reliable, verifiable and publicly available or otherwise accessible information that reveals whether the transferred data will be appropriately safeguarded in practice.

This experience helps us understand what our clients need and we can work with you to establish any additional measure required. Our customers can rely on unparalleled data security expertise.

What should we do regarding transferring data to India?

India proposed the Personal Data Protection Bill in 2019. A Joint committee of Parliament was formulated to deliberate the bill in great detail. However, in the light of recent events the Ministry of Electronics & Information Technology (MeitY) has decided to work on a comprehensive legal framework and develop a bill that best fits this framework which will shortly be released for public consultation. In the meantime, India's data protection laws arise out of the Information Technology Act, 2000 ('the IT Act') and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('the SPDI Rules').
As for the rights of the data subjects: In India, the rights to equality, life and personal liberty, and privacy apply to all the people regardless of citizenship. The surveillance laws in India, as they exist today, do authorize the government to monitor information and/or data only if it adheres to the procedural and proportionality tests put in place by various legislations and judicial recourse is the effective remedy available for negating unlawful monitoring/surveillance efforts by government bodies.

Does Wipro have Data Privacy governance framework in place?

As a responsible global corporate enterprise, Wipro takes processing of personal data with the highest level of seriousness and ensures that processing follows globally accepted privacy principles. We promote a culture that values privacy through awareness and protects privacy of individuals through guidance, direction, and imposition.

Wipro has a dedicated central Global Data Privacy Team as well as Data Privacy Champions across all internal functions (Governance structure attached for reference). Below diagram represents the Data Privacy governance at Wipro.

Tier 1:
Oversight and Accountability

Tier 2:
Program Sponsor & Governance

Tier 3:
Strategy & Privacy Management

Tier 4:
Implementation accountability & facilitation

Tier 5:
Core Implementation team

Risk Committee: comprising of CRO, COO, CFO & CHRO

Governance Committee: comprising of General Counsel, CFO & CHRO

Our cross – functional Data Transfers Team (encompassing the Global Data Privacy Team, Legal and Security) is in charge of rolling out the new SCCs and implementing them through the inclusion of additional measures when necessary.

- **We assess the essential guarantees of the recipient country's surveillance/data access laws; and**
- **Wipro has adopted supplementary measures such as encryptions, pseudonymization of data, internal processes to respond to government data access requests etc.**
- **New SCCs are being implemented for customers and vendors**

Does Wipro have adequate measures in place to ensure compliance with Schrems II additional supplementary measures such as technical safeguards?

Yes. Our customers can rely on unparalleled data security expertise and a full suite of measures we offer. Highlights include:

- **Wipro is certified under the ISO 27001:2013 standard for information security practices inclusive of physical security & employee safety. Security practices of Wipro are governed by an established Information Security Management System (ISMS).**
- **Wipro's Information security policy is articulated in Information Security Management System (ISMS) which is an ISO standard to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations to ensure confidentiality, integrity, and availability of customer assets, information, data, and IT services.**
- **The Technical and Organizational Measures implemented at Wipro include:**
  - Unauthorized persons are prevented from gaining access to data processing systems for processing or using personal data through physical and logical security controls such as:
    - Access to Offshore Development: Center (ODC) and ODC devices, which is restricted and approved by an authorized approval authority as per Wipro Access control matrix
    - Perimeter Wall and Power fence (where permitted), both with 24 x 7 monitoring
    - Anti-pass back enabled in all ODC areas
    - Proximity/smart card-based physical access control and surveillance (CCTV)
    - Dual-layer firewalls and network-based intrusion prevention system at the Internet perimeter
    - Dedicated VLANs with strict ACLs
    - Hardware-based Internet proxy with blue-coat content filters. Internet browsing through AD authentication
  - Technical (password protection) and organizational (user account management) measures with respect to user identification and authentication include:
    - Password procedure (special characters, minimum password length, frequent change of passwords, etc.)
    - Automatic lock (e.g. lock screen or log-off)
    - User account management
    - Encryption of data media
  - **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-access" and "need-to-know" basis only. Access restrictions are role based and the authorizations will be obtained as defined in the access control matrix as well as their monitoring and documentation of what? (e.g. logs):**
    - Precise authorization (profiles, roles, transactions, and objects)
    - Frequent analysis and control of existing access rights
    - Timely update, respective deletion
    - Encryption of data
  - **All aspects of transmitting personal related data are regulated. Transport, transmission and transfer or storage on data media (manual or electronic) are controlled, as well as subsequent verification:**
    - Encryption/tunneling connections (VPN - Virtual Private Network)
    - Electronic signature
    - Network intrusion prevention and host-based intrusion detection system for internal critical applications
    - Uninterrupted Power Supply (UPS)
    - Protocols/log-files review

- **Personal data processed on behalf of others are processed strictly in compliance with the controller's instructions, dividing responsibilities between Contractor and Client:**
  - Precise contract design and wording
  - Formalized ordering procedure (order form)
  - Criteria for selecting contractors
  - Controlling contract execution
- **Data is protected against accidental destruction or loss. Measures of data backup (physical/ logical) include:**
  - Backup and restoration procedures
  - Mirroring of hard disk drives, e.g. RAID
  - Virus protection/firewall
  - Business continuity/disaster recovery plan
- **Separated processing (storage, alteration, deletion, transmission) of data for different purposes:**
  - Multi-client capabilities/physical separation
  - Function separation/production/test network isolation policy to segregate handling of sensitive network areas and processing sensitive data. i.e., separate networks for test/development/production

What will Wipro do in case of a request from law enforcement?

Wipro has not received any government access requests so far.

Wipro's priority is to protect customers and employees data should such a request arise.

Wipro will (where applicable):

- Assess the request completely and understand the surveillance law of the land
- Exhaust all available judicial remedies in its capacity before any lawful disclosure

How has Wipro Structured the DTA/SCC (Contracting)?

Wipro has completed the analysis of new SCCs and has started implementation with customers and vendors as applicable. Our team of Legal and DP experts is well equipped in procedures for handling the new SCCs.

- Notify customers that their data is being requested
- Challenge government request that prohibits notification to the customer
- Provide only such data to which the government agency has appropriate authority under applicable law which needs to be provided
- Challenge valid government agency requests in cases of a potential breach of applicable data protection laws in other country, which has authority over the customer data, and invoke mutual assistance mechanism as per the international law, as deemed appropriate
- Provide only such data which the requesting body has appropriate authority to ask for under applicable law and which is the minimum necessary to meet the disclosure request
- Invoke mutual assistance mechanism as appropriate

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 250,000 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**

IND/BRD/SEP2022-AUG2023