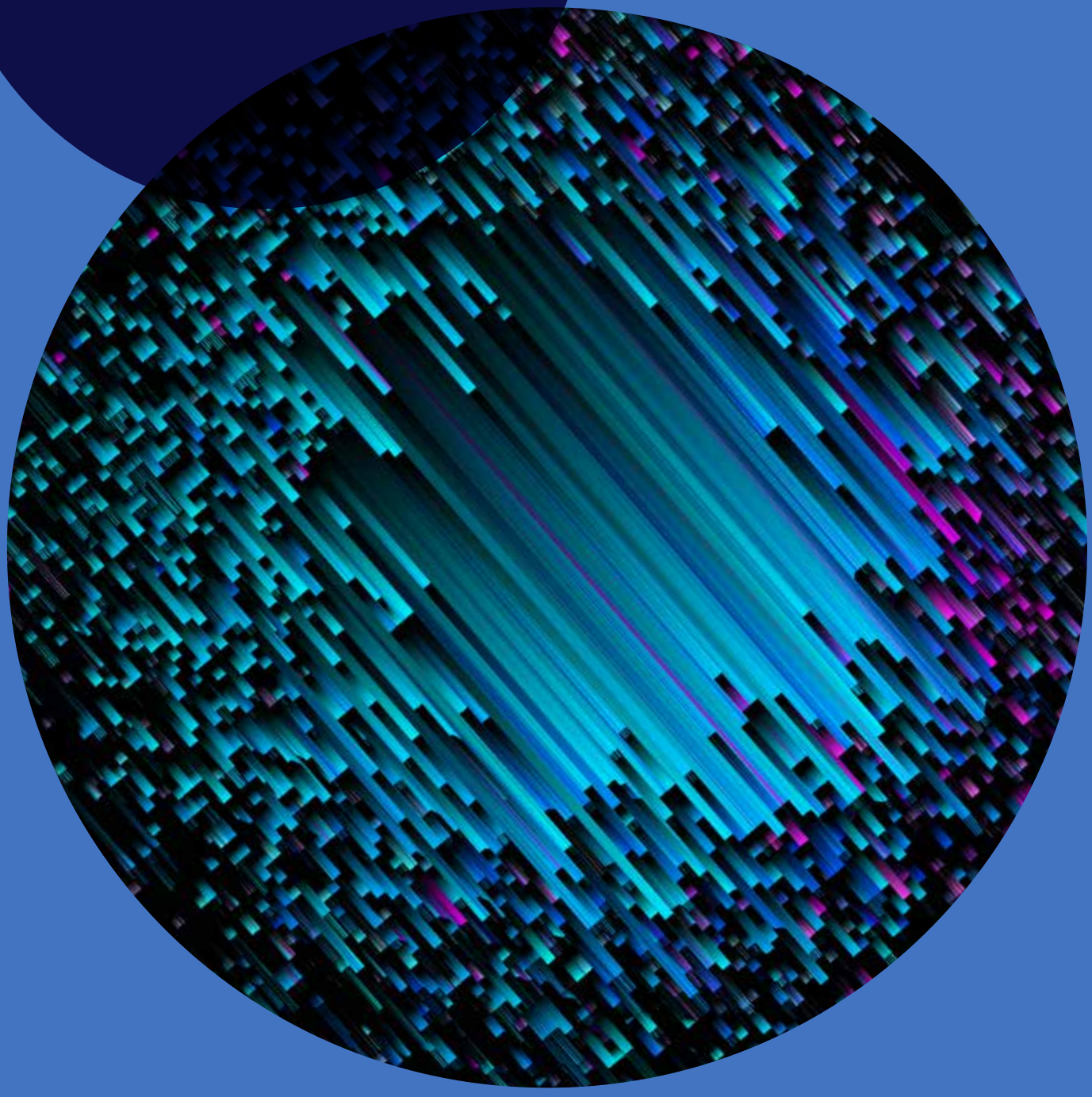
Cross-border data transfers:

Our point of view



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).

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).

In a nutshell, in the absence of a decision on adequacy, organisations may transfer data to a third country by providing appropriate safeguards, enforceable rights and effective legal remedies.

If necessary, with additional measures to compensate for gaps 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 is the data protection regime in India ?

The Personal Data Protection Bill, 2019 (the PDP Bill), is expected to be enacted in 2022-23. The PDP Bill focuses on setting up a robust 'Data Protection' regime in addition to setting out a more detailed 'Data Privacy' framework. 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'). Right to equality, Right to freedom of speech and expression and Right to protection of life and liberty have been enshrined in the Indian constitution as fundamental rights. Protection of an individual's privacy has been upheld in multiple decisions of the Courts in India and in 2017, the Supreme Court of India formally recognized "Right to Privacy" as a fundamental right. As for the Rights of the data subjects: In India, The 'right to privacy' and 'informational privacy' have been recognised, by the Supreme Court of India, as an intrinsic part of the 'fundamental right' of 'right to life' guaranteed under the Constitution of India. The right to Privacy is extended to non-citizens as well.

While the Telegraph Act deals with interception of 'communications', the IT Act deals with interception of 'data'. Existing surveillance laws in India require that the intercepting authorities must ensure the procedural and legal requirements including compliance to the proportionality tests while making such requests. This guarantees protection of an individual's privacy against unwarranted or unrestricted abuse by authorities.

The Indian supreme court's decisions suggest that monitoring, surveillance and disclosure requirements under both legislative and executive mechanisms, and any data collection and other actions under such mechanisms, would be subject to constitutional remedies and judicial review. Since, the Right to Privacy has been expressly recognized as a Fundamental right in India, it affords judicial recourse to citizens and non- citizens to approach the Court against unjust intrusion.

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.

Risk Committee: comprising of CRO, COO, CFO & CHRO
Governance Committee: comprising of General Counsel, CFO & CHRO

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

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:**

  o 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

  o 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 (Net work isolation policy to segregate handling of sensitive network areas and processing sensitive data. i.e., separate networks for test/development/production

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.

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 has a robust team of experts and internal SOPs to effectively handle government requests. Upon receipt of such a request, Wipro will:

- Review the request and its scope under appli cable local regulations, including relevant surveillance and disclosure laws
- Carry out an assessment to determine whether the request meets criteria for lawful disclosure in line with expected proportionality tests
- Refuse requests that are overbroad, not received under valid procedure or conflict majorly with EU data protection law
- Notify customers that their data is being requested where this is permissible, unless otherwise prohibited
- Review judicial remedies available and communicate the same to clients. Our inhouse and external litigations experts are fully equipped to challenge requests that don't meet procedural requirements under Indian laws and majorly conflict with international data protection laws
- 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

For more info, please contact:

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

Commercial office in Paris
(French headquarters)
Wipro Limited Tour Opus 12,
77 Esplanade du General de Gaulle,
92800 Puteaux, France.

Wipro Limited
Doddakannelli,
Sarjapur Road,
Bangalore-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 global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 220,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

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

IND/TBS/JAN 2022