Infosys | Data Privacy Office

# Privacy Do's and Don'ts for Suppliers

With the ever-emerging privacy landscape fueled by the introduction of strict data privacy and data protection regulations across the world, it is mandatory for organizations to ensure that the privacy nature of the personal data being processed are compliant to the sentiments of the data subjects from whom they were collected. Suppliers/Vendors/Service Providers during their engagement with Infosys and its subsidiaries will be exposed to personal data as part of the service engagements and it is crucial, that they adhere to strict legal obligations imposed both under contracts and from the applicable laws of the land.

**Our Objective:**

Infosys along with its subsidiaries ensures that it complies with all applicable data protection laws and contractual requirements and is committed to uphold highest data protection and privacy standards with respect to all supplier data and personal data. We expect our suppliers to adhere to similar standards and follow certain best practices to comply with the data privacy laws and regulations.

**DO's**

- **Set up Data Privacy Governance –** One of the key strongholds to demonstrate accountability on the data collection and processing practices within your organization. Where applicable, appoint a Data Protection Officer or a full-time, dedicated personnel for handling privacy matter.

- **Process personal data only on the written instructions of Infosys –** Processing should be subject to the scope, nature and purpose of such processing as permitted in writing only which is sacred in nature.

- **Execute written contracts/agreements –** Ensure appropriate written contracts/agreements are in place, including to your extended enterprises such as your subcontractors and subprocessor.

- **Maintain necessary records, including 'Register of Processing' –** These records provide visibility to the nature and scope of processing. For any support on Register of Processing, please reach out to Infosys.

- **Obtain prior written consent from Infosys before engaging any sub-processor –** For all parties who will be involved in processing of personal data exposed as part of the engagement. Where applicable, the scope of the work would need necessary amendments/changes that need to be assessed in line with applicable laws.

- **Guarantee confidentiality of Infosys data** - Ensure all project members sign confidentiality agreements to limit unauthorized access.

- **Notify Infosys if any processing is not compliant with the laws and regulations** - Notify Infosys without undue delay upon becoming aware of a personal data breach affecting personal data belonging to it and co-operate in the investigation, mitigation, and remediation of such breach/non-compliance. Maintain a documented data breach or incident management procedure.

- **Implement technical and organizational controls** - Based on categories of data processed, implement adequate safeguards in agreement with Infosys to ensure a level of security and protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the personal data. This includes but not limited to segregation of personal data from those of other clients, access control, encryption, etc.

- **Embed Privacy by Design** – Integrate privacy into design in your organization's operations to provide solutions, systems, services and platforms to Infosys while also meeting the requirements of privacy regulations.

- **Assist Infosys in fulfilling its privacy obligations -** Assist in responding to any Data Subject Rights request or carrying out Data Privacy Impact Assessment. Also assist where consultation with Data Protection Authority is warranted on any high-risk processing engagements. Allow carrying out audits/inspections by Infosys or auditors appointed by it.

- **Demonstrate accountability** - Maintain documentations demonstrating compliance and make them available for Infosys and Supervisory authorities.

- **Follow instruction on data retention and deletion -** Delete or return all data, including personal data, as per agreement with Infosys and when the purpose is over or upon request from Infosys, whichever is earlier, unless law requires it.

- **Integrate regular training and awareness on Privacy and Data Protection** - Provide training regarding the privacy, confidentiality, and security requirements to all personnel within your organization who have access to personal data and regularly monitor them for privacy compliance.

**DON'Ts**

- Do not use personal data for any purpose other than intended or as set out in the instruction from Infosys and its subsidiaries.

- Do not process, transmit or store any personal data in an unsecured form or in any other unauthorized location.

- Do not transfer personal data internally or externally for different purposes other than agreed and without instruction from Infosys.

- Do not allow third parties including sub-processors to process personal data without undergoing adequate assessments and due diligence wherever required.

- Do not modify, delete, aggregate or commingle, re-identify or de-anonymize any personal data, or attempt to do so, without knowledge of Infosys.

- Do not retain personal data any longer than necessary for purpose or after retention timeline set out by Infosys.

- Do not sell or otherwise commercially exploit or permit the sale or commercial exploitation of personal data belonging to Infosys, directly or indirectly.