

Wipro’s

Data Protection and Privacy Policy (Personally Identifiable Information)

**Document Control**

|  |  |
| --- | --- |
| Function | General Counsel |
| Sub-function | Global Data Privacy |
| Policy Owner | Ivana Bartoletti |
| Policy Effective Date | 31-Jan-2024 |

**Purpose**

This policy governs the lifecycle of Personally Identifiable Information (PII) data and compliance with the applicable laws, regulations, contractual and business requirements across geographies.

**Audience**

Wipro employees, retainers, contractors, and service providers involved in the processing activities of PII data.

**Scope**

This policy applies to PII data owned or managed by Wipro.

**Policy Details**

**DPP.1**Wipro shall establish a Data Privacy Governance team and assign responsibilities.

**DPP.2**Wipro shall prepare a Data Privacy Plan and communicate it to all relevant stakeholders.

**DPP.3**Wipro shall comply with the globally accepted Data Principles.

**DPP.4**The Data Protection and Privacy Policy shall be applicable uniformly, irrespective of the PII data collection method.

**DPP.5**Relevant data subjects’ personal data shall be retained and disposed as per applicable laws, regulations, contractual and business requirements in respective geographies.

**DPP.6**Customer's personal data processed from Wipro's delivery centers shall be governed through data transfer and processing agreements with the customers.

**DPP.7**Wipro shall provide the intent of data collection, assurance of protection, and option for subscription or un-subscription to end users.

**DPP.8**Website visitors’ privacy shall be governed by   privacy policy statements.

**DPP.9**Information owner and data custodian shall protect the confidentiality of PII data.

**DPP.10**Data security and privacy requirements shall be defined in third-party contracts.

**DPP.11**Data protection requirements shall be reviewed and updated periodically as per the changes in the country-specific laws, regulations, and business requirements.

**DPP.12**Confidential data, including PII data, shall be protected throughout the data lifecycle using appropriate data obfuscation techniques, including data masking, as per business requirements.

**DPP.13**Data Leakage Prevention (DLP) methods shall be implemented to protect against unauthorized disclosure, extraction, modification, and misuse of PII data.

**DPP.14**The user and data custodian shall ensure that the data is reliable, accurate, complete, and current for its intended use.

**DPP.15**Information security risk assessment and Data Privacy Impact Assessment (DPIA) shall be performed periodically as per the DPIA standard, business requirements, and applicable laws.

**DDP.16**Workplaces shall be monitored to protect the PII data as per the applicable laws, regulations, contractual and business requirements.

**DPP.17**Wipro’s policies and procedures on processing PII data shall be communicated and made accessible to the Data Subject.

**DPP.18**Wipro shall issue notice to the Data Subjects upon major changes in the PII handling procedures.

**DPP.19**Wipro shall obtain the opt-in or explicit consent of the Data Subject for collecting or processing PII data, except where applicable law allows the processing of PII data without the  Individual’s consent.

**DPP.20**Provisions shall be made to provide Data Subject with the opportunity to choose how their Personal Data is handled and to allow them to withdraw consent easily and free of charge. Data Subject shall have the ability to withdraw consent, and the PII data shall be exempted from processing for any purpose not legally mandated.

**DPP.21**Collection Limitation - PII data shall be minimized, quantitatively and qualitatively, in accordance with the Data Minimization principle, and the data shall be collected only for its intended use.

**DPP.22**Data Minimization - Wipro shall ensure that the usage of PII data is minimized throughout the PII data lifecycle.

**DPP.23**PII data shall be de-identified or anonymized to minimize risk exposure.

**DPP.24**Wipro shall establish a mechanism to allow access, erase, correct, amend, update, portability, and restriction of further processing of PII data by the Data Subjects.

**DPP.25**Access to PII data shall be granted based on the authentication of the Data Subject’s identity and as per the laws, regulations, and business requirements.

**DPP.26**Wipro shall notify Data Subjects before disclosing personal data to third parties. Wipro shall ensure disclosure is made for the purposes indicated in the Data Protection and Privacy Standard provided to the Data Subject.

**DPP.27**Security controls shall be developed, documented, approved, and implemented to protect PII data and specific categories of PII from loss, misuse, unauthorized access, disclosure, alteration, and destruction.

**DPP.28**Wipro shall maintain the integrity, reliability, and quality of PII data to ensure accuracy and completeness.

**DPP.29**Wipro shall retain PII as per the contractual requirements or in line with legal and regulatory requirements as per the geography defined in the Data Retention Policy. Wipro shall delete and dispose PII whenever the purpose for PII processing has expired, there are no legal requirements to keep the PII, or whenever it is practical to do so, such as the data being inaccurate.

**DPP.30**Wipro shall have mechanisms to maintain the integrity of transmitted privacy attributes by ensuring PII data has not been modified in an unauthorized manner throughout the data processing lifecycle.

**DPP.31**PII data in transit, in process, and at rest shall be encrypted.

**DPP.32**Wipro shall resolve data privacy grievances in a timely manner and as per the applicable laws, regulations, contractual and business requirements.

**DPP.33**Wipro shall identify a third-party arbitrator for dispute resolution as per business requirements.

**DPP.34**The Data Privacy team shall involve relevant stakeholders to identify appropriate resolutions to address grievances or disputes.

**DPP.35**Data Protection and Privacy Policy shall be reviewed annually, and the changes shall be communicated to relevant stakeholders.

**DPP.36**Wipro shall develop a process to address and manage issues related to conflicting applicable laws, regulations, contractual and business requirements.

**DPP.37**Wipro shall conduct periodic privacy training and awareness sessions for employees, contractors, and service providers having access to the PII Data

**DPP.38**Wipro shall have mechanisms and representatives who shall oversee the implementation of privacy policies and liaise as points of contact on relevant policies and documents, including for applicable supervisory authorities.

**DPP.39**Wipro shall define and document the processes of handling privacy incidents and breaches concerning Personal Data.

**DPP.40**Cloud Privacy – In addition to the above obligations, Wipro shall abide by the below Cloud specifics:

* Wipro shall capture the information security and privacy requirements as part of the Cloud Service Provider (CSP) contract to protect PII data and Data Subject’s rights.
* PII data processed by the CSP shall not be used for marketing and advertising purposes without express consent from Wipro.
* The CSP shall notify Wipro regarding a legally binding request for disclosure of PII data as per applicable laws, regulations, contractual and business requirements unless such a disclosure is otherwise prohibited.
* Security incidents related to PII shall be reported by the CSP.
* Annual Information Security audits shall include applicable PII data compliance checks to evaluate the effectiveness of security controls implemented to protect PII data.
* Logging and monitoring shall be enabled as per the logging and monitoring standard.
* Security incidents related to PII data shall be reported as per the Security Incident Management Procedure.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| Consent | Consent is a freely given, specific, informed, and unambiguous indication of a Data Subject’s wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them. |
| Data Controller | An organization when it (either alone, jointly, or in common with others) determines the purposes and means of the processing of personal data. |
| Data Processor | A person or an organization (other than an employee of the Data Controller), who processes personal data based on the instructions from the Data Controller. |
| Data Subject | An identified or identifiable living individual natural person. |
| Data Custodian | Responsible for the safe custody, transport, data storage, and implementation of business rules. |
| Information Systems | Set of applications, services, information technology assets, or other information handling components. |
| PII | Data that could potentially identify a specific individual directly, or indirectly. It includes, but is not limited to name, date of birth, social security number, Government/National Identifier, address, telephone number, employee ID number, credit card number, and password. |
| Processing | Any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, including, but not limited to, collection, recording, accessing, organizing, structuring, storing, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction. |
| Sensitive Personal or Specific Categories of PII Data | Any data that could potentially identify a specific individual, which includes but is not limited to racial or ethnic origin, political opinion, religious belief, and physical or mental health. |

**References**

* Information Classification labelling and Handling Policy
* Encryption Policy
* Asset Management Policy
* Intellectual Property Rights Policy
* Backup and Restoration Policy
* Supply Chain Cyber Risk Management Policy
* Acceptable Usage Policy
* Physical Security Policy
* Information Security (IS) Policy
* Acceptable Data Collection and Usage Policy
* Mass E-mail Processing and Transmission Standard
* Data protection and Privacy Standard
* Logging and Monitoring Standard
* Security Incident Management procedure

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | **Approved By** | **Date Approved** |
| 6.0 | June 2022 | Periodic review (Changes in terminology for dependent teams) | Harsha Chakravarthy K N | Ivana Bartoletti | Jun, 2022 |
| 6.2 | Jan 2023 | Updated Definitions and scope. Modified DPP.1, DPP.5.1, DPP.5.3, DPP.5.4, DPP.5.7, DPP.5.10, DPP.5.11, DPP.5.13.Incorporated verbiage changes throughout the policy. | Chandrashekar M/ Harsha Chakravarthy K N | Ivana Bartoletti | Jan, 2023 |
| 6.3 | 25-May-23 | Updated Roles and Responsibilities for the Data Privacy Team.Updated DPP.3 section | Chandrashekar M/ Harsha Chakravarthy K N | Ivana Bartoletti | 25th May, 2023 |
| 6.4 | 18-Jul-23 | Updated the policy with the Cloud Privacy requirements and new Wipro document format. | Tanzeem Amjed / Harsha Chakravarthy K N | Ivana Bartoletti | 18th Jul, 2023 |
| 7.0 | 17th Nov 2023 | Reviewed and updated the policy as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5.Updated the policy to retain salient features/requirement from PIMS standard. | Chandrashekar M / Tanzeem Amjed | Harsha Chakravarthy K N | 20th Nov 2023 |
| 8.0 | 31st Jan 2024 | Change to the new Policy Format | Chandrashekar M / Tanzeem Amjed | Harsha Chakravarthy K N | 31st Jan 2024 |