Wipro’s

Acceptable Data Collection and Usage Policy

## Document Control

|  |  |
| --- | --- |
| Function | General Counsel |
| Sub-function | Data Privacy |
| Policy Owner | Ivana Bartoletti, Head – Data Privacy & Chief Privacy Officer |
| Policy Effective Date | 1st July 2009 |

**Purpose**

This policy governs the collection, usage and disclosure of Personal Data or Confidential Data belonging to Wipro’s employees and clients. to perform the processing of such data in line with the intended purpose, contractual requirements, and as mandated by applicable laws and regulations. This document is intended to enable the delivery and functional support teams at Wipro to protect the privacy of Personal Data of Wipro’s clients, employees and any other individuals when processing such data.

## Audience

This policy is applicable to all employees, contractor, interns of Wipro Limited and its affiliates and subsidiaries**. Scope**

This policy is applicable to delivery and functional support teams involved in:

* Mass e-mail processing and communication (using Wipro's e-mail domain)
* Tele-calling activities either in-house or through Wipro's vendors/service providers.
* Collection and usage of data belonging to Wipro's clients’, employees’, vendors’, and any other individuals whose data is processed by Wipro.

## Policy Details

1. **Data Collection Notice**

Personal data may be collected online or offline. At the time of collection, a clear notification on the purpose of data collection, means of processing, and methods of data protection including disclosures to third-party must be provided to users. Further, wherever Personal Data is being collected through a webpage/application, a link to the privacy policy of Wipro shall be provided. Regardless of the method of collection, the same privacy protections shall apply to Personal Data. All privacy notices shall be drafted in clear and easy-to-understand language (bearing in mind the intended audience) and shall include, but not be limited to:

* + The identity of the Data Controller and its contact details;
  + A clear explanation of the purposes(s) why and method(s) for collecting Personal Data;
  + The notification on changes to data processing activities at reasonably frequent intervals, including but not limited to eventual secondary use of Personal Data;
  + The identity of the Data Controller’s nominated data protection officer and his/her contact details;
  + Details of cross border data transfers, if any;
  + Consequences, if any, should the data subject refuse to share the Personal Data;
  + Details of involvement of third parties, if any, in processing the Personal Data;
  + Details of any recipients of the Personal Data;
  + How data subjects can amend, update, request the deletion or restrict the processing of their Personal Data providing them the relevant notifications;
  + Safeguards implemented to secure Personal Data;
  + Details of how the Personal Data collected from data subjects is held within Wipro and the length of time it is stored;
  + The fact that Wipro may share customer and/or employee Personal Data with its business affiliates for accomplishing the business purpose identified;
  + Details of how data subjects who are concerned about how Wipro processes their Personal Data can express their concerns;
  + Clarification as to whether data subjects are required to provide their Personal Data as a requirement of contract or law;
  + A statement as to whether any automated decision making takes place on the basis of the Personal Data provided by data subjects;
  + Where applicable, information about how data subjects may lodge complaints with the relevant data protection authority when they believe that their Personal Data has been processed in a manner that is incompatible with applicable laws in the European Union; and
  + Contact details of Wipro personnel responsible, including Wipro’s nominated Data Protection Officer, for addressing queries regarding the collection, handling and use of customer and/or employee Personal Data.

## Data Protection

Personal data of a user, collected by Wipro, for carrying out business processes shall be protected against unauthorized access.

* + User's access to the application used for processing & storing of confidential data shall be granted based on business requirements on a "need to access" and "need-to-know" basis only. The authorization shall be obtained from the Information Owner as defined in the application access control matrix.
  + User shall be clearly notified on the purpose for which the data has been collected and how it should be protected including terms of use with Third parties, as applicable.
  + Wipro shall only collect Personal Data:
    - For the purpose(s) identified in the governing privacy policy or for Wipro’s legitimate business interests;
    - Proportionate to business purposes in accordance with applicable laws;
    - For any other purpose, if the Data Subject has consented (or has provided explicit Consent when Sensitive Personal Data is to be collected);
    - That has been examined for its correctness and completeness; and
    - In alignment with the necessity of its collection from data subjects on a periodic basis in order to minimize the risks associated with the collection of Personal Data
  + While collecting Personal Data of users (example- Wipro website or any other sites on behalf of Wipro), the above shall be considered.

Any additional purpose for which Personal data needs to be processed which has not been informed to the Data Subject at the time of collection will need to be notified to the Data Subject and consent shall be obtained where required prior to undertaking such processing.

1. **Data Usage Purpose Limitation**

Wipro shall use Personal Data collected according to the applicable laws pertaining to processing of Personal Data and in line with the defined purpose identified within the privacy policy provided to Data Subjects. A Privacy Notice stating what information is collected, the purpose of collection, potential information gathering technologies such as cookies and disclosures made, if any, shall be provided to Wipro customers, employees, and any other individuals whose data is processed by Wipro on all applications/platforms where data is being collected.

## Data Inventorization

Data processed by Wipro as a Data Controller and a Data Processor shall be inventoried in line with applicable requirements under relevant legislation. For performing such Data Inventorization or obtaining the template of the data inventory, advice/recommendation shall be sought from Global Data Privacy team.

## Data Retention

Personal data shall be retained in a form which permits identification of data subjects in line with the applicable Retention Period as stipulated in the Data Retention policy. It could also be subsequently modified as mandated by applicable law.

## Data Destruction

Personal data shall be destroyed at the end of the defined Retention Period. Destruction of data shall:

* + Be in a manner sufficient to prevent unauthorized access to that personal data; or
  + Be in a manner such that the personal data is anonymized.

## Third Party disclosure management

Wipro shall notify data subjects prior to disclosing personal data to any third parties. Any such disclosure made shall be for the purposes indicated in the privacy notice provided to the data subject.

Wipro shall further ensure that any third-party processing such personal data shall:

* + Not disclose the personal data without Wipro’s prior written consent
  + Where applicable, sign a Non-Disclosure Agreement (NDA) with Wipro before personal data is disclosed to the third-party
  + Enter into a Master Services Agreement with Wipro containing the relevant contractual obligations to ensure the protection of Personal Data that is disclosed to the third parties as per Wipro’s privacy practices (Data protection and privacy policy) and
  + Have adequate measures and comply with all applicable laws while personal data is transferred to another entity or country, and to facilitate such transfers.

Wipro may share personal data with third parties and/or vendors who may further engage with another organization (sub-contractor) to process personal data. In such scenarios, Wipro shall undertake at least the following measures:

* + Maintain a list of sub-contractors to whom personal data is being shared,
  + Assess the adequacy and appropriateness of security controls related to the protection of Personal Data as part of due diligence before any sub-contractor is engaged by the vendor or third-party.
  + Ensure that prior consent is required to be provided prior to any such third-party engagement.
  + Specifically require that the vendor flow down to the sub-contractor obligations to process the Personal Data in line with its instructions, and to always deploy appropriate technical and organizational security measures (measures and controls implemented by Wipro to protect personal data and ensure the ongoing confidentiality, integrity and availability of its products and services. e.g. Encryption, Pseudonymization, Anonymization, Data Masking, Access management) for Personal Data.
  + Ensure that when a contract between a third-party vendor and its sub-contractor is terminated, personal data is either destroyed or passed on to Wipro as per Wipro’s requirement. No copies of personal data should be retained by a sub-contractor on the termination or expiry of its contract.
  + The user shall be given option to opt out (whenever there is a change in purpose of processing activity or processing based on consent from the individual, a notice must be provided to the data subject and the individuals should be given a chance to unsubscribe) anytime either via e-mail or website.

## Processing and Communication

E-mails for broadcast shall contain accurate subject lines and shall not be deceptive in nature.

* + E-mails shall be sent to outside world only through company approved email system.
  + User's Personal Data shall be processed in segregated and secured physical area in the office.
  + Wipro employees and contractors engaged in processing of Users Personal Data shall undergo background check before commencing their job and also ensure relevant NDA is signed and stored for future reference.
  + The application/system in which User Personal Data is stored shall be protected against breach. Adequate measures should be taken before using the data for testing purpose
  + An internal database shall be maintained for reference and it shall be updated as and when contact information, subscription status changes happen.
  + E-mails shall be sent only to the intended recipient of such communication.
  + User data shall be classified as “Confidential” information and shall be shared on need-to-know basis only.
  + Individual teams sending bulk/follow-up/reminder/action request emails need to extract the Employees whose base location is EU and exclude them from such communications. Communications to EU employees, have to be routed through their respective HR/Reporting Managers. This is a legal requirement, and any non-compliance shall be leading to disciplinary action as per Wipro policy.

## Communications Management

There are several methods to establish a lawful basis for Data Privacy compliance, but the most likely mechanisms relied on when sending communications within Wipro is one of the following:

Consent – Most of the marketing/advertising communications will rely on “consent” that must be obtained by a “clear affirmative act”. For example, pre-checked boxes or implicit consent is inadequate to establish this lawful basis. The process for obtaining consent properly is one of the areas that is most impacted by the GDPR. It is advisable that the following criteria be met to show valid consent:

* + Consent must be freely given. This means giving Users genuine, ongoing choice and control over how Wipro uses their data.
  + Consent should be obvious and require positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise, user-friendly, and easy to understand.
  + Consent must specifically cover the controller’s name, the purposes of the processing, and the types of processing activity.
  + Explicit consent must be expressly confirmed in words, rather than by any other positive action.
  + There is no set time limit for consent. How long it lasts will depend on the context so that it is advisable to review and refresh consent as appropriate.
  + Consent obtained must be recorded so that it is easily audit-able. With each consent record, we recommend storing the identifier, timestamp, and location where consent was obtained.

**Contract** – if the processing of personal data is necessary for the performance of a contract, this lawful basis is used for processing of personal data. Password reset, billing notifications, and onboarding communication would likely fall under this lawful basis. Relevant teams involved in the creation , performance and compliance of the Contract have the responsibility for ensuring that the personal data collected is being processed in a lawful manner as described above.

**Message Bodies** – Wipro stores the bodies of messages for up to 72 hours for both incoming and outgoing messages. For outgoing messages, temporary storage allows Wipro systems to attempt to re-deliver messages that could not be delivered on the first attempt. Customers relying on Wipro’s parsing features use this feature to be able to retrieve messages that have been received as inbound messages.

For some customers, the message retention period may be selectively adjusted based on written instructions between the customer and Wipro. Additionally, features that prevent the retrieval of messages programmatically or allow the messages to be securely deleted after delivery are also in place.

Wipro personnel may access message bodies to assist customers in troubleshooting delivery issues or in

response to a potential violation. Employee access is routinely audited, and all employees are subject to our confidentiality provisions.

**Message Metadata** – The metadata of a message, which includes the sender, recipient(s), subject line, originating IP address and other routing data is indexed and maintained for 30 days.

**Recipient Data** – Wipro stores activity information of recipient email addresses in a hashed (Pseudonymized) format. This data allows it to pre-validate email addresses, detect potential risky senders who may damage IP reputation, and help customers optimize their delivery processes more accurately.

## Definitions

For the purpose of this policy,

User refers to both existing and potential set of customers/clients, vendor, employees and other individuals.

|  |  |
| --- | --- |
| **Definition** | **Description** |
| **Data** | refers to information in both, electronic and physical form. |
| **User Data** | refers to data such as but not limited to – name, contact information (office and mobile telephone numbers), address, organization name, areas of interest, title, e-mail address, country, etc. |
| **Personal Data/Personally Identifiable Information (PII)** | Is any data that could aid in potentially identifying a specific individual directly, or indirectly through the information provided. It includes, but not limited to name, date of birth, social security number, Government/National Identifier, address, telephone number, employee ID number, credit card number and password. |
| **Sensitive Personal Data** | Is any data that could aid in potentially identifying a specific individual’s racial or ethnic origin, political opinion, religious belief, physical or mental health etc through the information provided |
| **Confidential Data** | Refers to any information in any recorded medium which is not available in the public domain comprising or relating to WIPRO’s techniques; schematics; designs; contracts; financial information; sales and marketing plans; business plans; clients; client data; business affairs; operations; strategies; inventions; methodologies; technologies; employees; subcontractors; pricing; service proposals; methods of operations; procedures; products and/or services that an employee may be privy to in the course of employment with Wipro, This includes but not limited to Personal Data belonging to Wipro’s employees, customers, vendors and other third parties. |
| **Data Subject** | Means an individual who is the subject of personal data. In other words, the data subject is the individual about whom the particular personal data/ information belongs to |
| **Consent** | Is an unambiguous, specific and informed indication, given freely, of a Data Subject’s wishes for the processing of Personal Data relating to them. The Data Subject, by a statement or by a clear affirmative action, signifies consent to the processing of Personal Data relating to them. |
| **Data Controller** | Is an organization when it (either alone or jointly or in common with others) determines the purposes and means of the processing of Personal Data. |
| **Data Processor** | Is 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. The processing performed are under the direct authority of the Data Controller or Data Processor. |
| **Data Subject Request** | Is a written request made by the data subject to the data controller for information. |
| **Third Party** | Is a natural or legal person, public authority, agency or any other body other than the Data Subject, Data Controller, Data Processor |

Definitions above may vary between different jurisdictions, geographies etc. and the requirements of law / regulation will override these definitions as applicable.

## References

* + Mass E-Mail Processing and Transmission Standard
  + Information Classification Standard
  + Acceptable E-Mail and Internet Usage Policy
  + Information Security Management System (ISMS) Policy

# APPROVALS/ESCALATION MATRIX

Ivana Bartoletti, Chief Privacy Officer, [ivana.bartoletti@wipro.com](mailto:ivana.bartoletti@wipro.com)

# POC for queries

Harsha Chakravarthy K N, [harsha.neella@wipro.com](mailto:harsha.neella@wipro.com)

**Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | **Approved By** |
| 3.1 | 16-Mar-2022 | Periodic review – Minor Changes in verbiage | Harsha Chakravarthy K N | Durga Bharath Attaluri |
| 3.2 | 08-Dec-2022 | Adhoc change – Change in processing and communication section, point 9 taken off | Harsha Chakravarthy K N | Durga Bharath Attaluri |
| 4.0 | Sep 2023 | Periodic review | Harsha  Chakravarthy K N | Ivana Bartoletti |