

# OnMobile Bangladesh Private Limited

## PRIVACY POLICY

*(Bangladesh Personal Data Protection Ordinance, 2025)*

Document Release Date: 2026

Document Version: 1.0

Document classification: External / Important

### Document Control:

<b>Document Status</b>	Final
<b>Document Classification</b>	External / Important
<b>Document Owner</b>	Legal
<b>Effective Date</b>	01/03/2026
<b>Version</b>	1.0

### Approval and authorization:

<b>Name</b>	<b>Designation &amp; Department</b>	<b>Date</b>
Manu Sharma	AVP - Information Technology • CITS	01/03/2026
Harish B N	Director - Compliance	01/03/2026

## **1. PREAMBLE AND PURPOSE**

1.1 This Privacy Policy (“Policy”) is adopted by **OnMobile Bangladesh Private Limited**, a private limited company incorporated under the laws of Bangladesh (“Company”), in compliance with the **Personal Data Protection Ordinance, 2025 (PDPO 2025)**.

1.2 The purpose of this Policy is to:

- Ensure lawful, fair, and transparent processing of personal data
- Protect the privacy rights of individuals
- Establish internal controls, safeguards, and accountability mechanisms
- Define responsibilities relating to data processing, storage, transfer, and protection

## **2. SCOPE OF APPLICATION**

2.1 This Policy applies to:

- All personal data processed by the Company within Bangladesh
- Processing activities conducted by:
  - Employees
  - Directors
  - Contractors
  - Third-party processors

2.2 This Policy also applies to:

- Processing carried out outside Bangladesh where such processing relates to individuals located in Bangladesh

2.3 This Policy covers all data in:

- Digital format
- Physical records
- Structured and unstructured datasets

## **3. LEGAL BASIS AND COMPLIANCE COMMITMENT**

3.1 The Company acknowledges its status as a **Data Fiduciary** under PDPO 2025 and undertakes to comply with all applicable obligations.

3.2 The Company shall ensure that all processing of personal data is:

- Lawful
- Necessary
- Proportionate
- In accordance with PDPO principles and requirements

## 4. DEFINITIONS

For the purposes of this Policy:

- **“Personal Data”** means any information relating to an identifiable individual.
- **“Sensitive Personal Data”** includes, but is not limited to:
  - Health data
  - Biometric and genetic information
  - Financial data
  - Religious, political, or sexual orientation information
- **“Restricted Data”** means data relating to national security, public order, or critical infrastructure.
- **“Data Fiduciary”** means the Company determining the purpose and means of processing.
- **“Data Processor”** means any person processing data on behalf of the Company.
- **“Data Subject”** means the individual to whom personal data relates.

## 5. PRINCIPLES GOVERNING PROCESSING

5.1 The Company shall adhere to the following principles:

### **(a) Lawfulness, Fairness, and Transparency**

Data shall be processed only in accordance with law and in a transparent manner.

### **(b) Purpose Limitation**

Data shall be collected for specific, explicit, and legitimate purposes and shall not be further processed in a manner incompatible with such purposes.

### **(c) Data Minimization**

Only data necessary for the intended purpose shall be collected.

### **(d) Accuracy**

The Company shall take reasonable steps to ensure that data is accurate and up to date.

### **(e) Storage Limitation**

Data shall not be retained beyond the period necessary for the purpose for which it is collected.

### **(f) Integrity and Confidentiality**

Data shall be processed in a manner that ensures appropriate security.

## 6. COLLECTION OF PERSONAL DATA

6.1 The Company may collect personal data through:

- Direct interactions

- Employment processes
- Contracts and transactions
- Digital platforms and systems

6.2 The Company shall provide clear and adequate notice at the time of data collection, specifying:

- Purpose of processing
- Categories of data
- Rights available to the data subject

## **7. LAWFUL BASIS OF PROCESSING**

7.1 Personal data shall be processed based on:

### **(a) Consent**

- Explicit, informed, specific, and freely given
- Capable of being withdrawn at any time

### **(b) Non-consent grounds (where applicable):**

- Performance of contractual obligations
- Compliance with legal obligations
- Protection of vital interests
- Employment and social security obligations
- Publicly available information

## **8. CONSENT MANAGEMENT**

8.1 The Company shall:

- Maintain verifiable records of consent
- Provide mechanisms for withdrawal
- Ensure consent is purpose-specific

8.2 Withdrawal of consent shall not affect:

- Lawful processing carried out prior to withdrawal

## **9. DATA SUBJECT RIGHTS**

9.1 Data subjects shall have the right to:

- Access personal data
- Rectify inaccuracies
- Request erasure or restriction of processing
- Withdraw consent
- Obtain portability, where applicable

9.2 The Company shall:

- Establish a defined process for handling requests
- Respond within a reasonable timeframe
- Maintain records of such requests

## **10. PROCESSING OF SENSITIVE PERSONAL DATA**

10.1 Sensitive personal data shall be processed only where:

- Explicit consent has been obtained; or
- Processing is permitted under law

10.2 The Company shall implement:

- Enhanced security safeguards
- Restricted access controls
- Strict purpose limitation

## **11. CHILDREN'S DATA**

11.1 A child shall mean an individual below **18 years of age**.

11.2 The Company shall:

- Obtain verifiable parental or guardian consent
- Implement additional safeguards for children's data
- Avoid processing unnecessary child data

## **12. DATA SECURITY AND PROTECTION MEASURES**

12.1 The Company shall implement appropriate technical and organizational measures, including:

- Encryption
- Access control mechanisms
- Authentication protocols
- Data anonymization / pseudonymisation
- Secure storage systems
- Periodic vulnerability assessments

12.2 The Company shall ensure:

- Confidentiality, integrity, and availability of data

## **13. DATA BREACH MANAGEMENT**

13.1 The Company shall maintain a **Data Breach Response Framework**, including:

- Identification and containment procedures
- Risk assessment
- Internal escalation protocols

13.2 Where required:

- The Company shall notify the competent authority (NDGA)
- Appropriate remedial action shall be taken

## **14. DATA RETENTION AND DESTRUCTION**

14.1 Personal data shall:

- Be retained only for necessary periods
- Be reviewed periodically

14.2 The Company shall implement:

- Data retention schedules
- Secure deletion mechanisms
- Archival controls where required by law

## **15. CROSS-BORDER DATA TRANSFER**

15.1 Personal data shall not be transferred outside Bangladesh unless:

- Permitted under PDPO 2025
- Required safeguards are implemented
- Regulatory approvals (if applicable) are obtained

15.2 The Company shall:

- Maintain records of cross-border transfers
- Ensure contractual protections with recipients

## **16. DATA LOCALIZATION**

16.1 The Company shall comply with all requirements relating to:

- Storage of restricted or confidential personal data within Bangladesh

16.2 Cross-border transfer of such data shall be:

- Subject to regulatory approval
- Restricted where mandated

## **17. ENGAGEMENT OF DATA PROCESSORS**

17.1 The Company shall ensure that:

- Data processors are bound by written agreements
- Processors comply with applicable legal requirements

17.2 Such agreements shall include:

- Confidentiality obligations
- Security requirements
- Audit rights
- Liability provisions

## **18. ACCOUNTABILITY AND RECORD-KEEPING**

18.1 The Company shall maintain:

- Records of processing activities
- Consent logs

- Data breach records
- Data transfer records

18.2 The Company shall demonstrate compliance at all times.

## **19. DATA PROTECTION GOVERNANCE**

19.1 The Company shall appoint:

- A **Data Protection Officer / Chief Data Officer**, where required

19.2 Responsibilities shall include:

- Monitoring compliance
- Advising management
- Acting as point of contact with authorities

## **20. AUDITS AND COMPLIANCE REVIEWS**

20.1 The Company shall conduct:

- Periodic internal audits
- Risk assessments

20.2 Independent audits shall be undertaken where required by law.

## **21. DISCLOSURE OF PERSONAL DATA**

21.1 Personal data may be disclosed:

- To regulators
- To law enforcement authorities
- For legal proceedings

21.2 Such disclosures shall be:

- Limited to necessary scope
- Documented and justified

## **22. EXEMPTIONS**

22.1 Processing without consent may be carried out where permitted under law, including:

- National security
- Crime prevention
- Legal compliance
- Research and statistical purposes

## **23. REGULATORY AUTHORITY**

23.1 The Company shall comply with directions issued by the:

- **National Data Governance Authority (NDGA)**

23.2 The Company shall cooperate fully with regulatory inspections and inquiries.

## **24. POLICY REVIEW AND AMENDMENT**

24.1 This Policy shall be:

- Reviewed periodically
- Updated as required

24.2 Amendments shall be:

- Approved by management
- Communicated to stakeholders

## **25. CONTACT AND GRIEVANCE REDRESSAL**

For any data protection-related concerns:

**Email id :** [Privacy@onmobile.com](mailto:Privacy@onmobile.com)