OnMobile Bangladesh Private Limited

DATA PROTECTION POLICY

(Bangladesh Personal Data Protection Ordinance, 2025)

Document Release Date: 2026
Document Version: 1.0
Document classification: External / Important

Document Control:

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

Approval and authorization:

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

1. Introduction

OnMobile Bangladesh Private Limited ("Company", "we", "our", or "us") is committed to protecting the privacy, confidentiality, integrity, and security of personal data processed by it. This Data Protection & Privacy Policy ("Policy") has been prepared in accordance with the principles, obligations, and standards envisaged under the Bangladesh Personal Data Protection Ordinance, 2025 ("PDPO"), including principles of lawful and consent-based processing, purpose limitation, data minimization, storage limitation, accountability, transparency, protection of data subject rights, implementation of appropriate security safeguards, and regulation of cross-border data transfers. This Policy explains how personal data is collected, used, stored, disclosed, protected, retained, and deleted by the Company.

2. Scope of the Policy:

This Policy applies to all employees, contractual staff, consultants, vendors, processors, service providers, customers, website visitors, mobile application users, business partners, and any other individual whose personal data is processed by the Company. It covers the processing of personal data in all forms, including electronic and physical records, and applies to both automated and manual processing systems used by the Company.

3. Definitions

3.1 Personal Data:

"Personal Data" means any information relating to an identified or identifiable natural person, including information that can directly or indirectly identify an individual. This may include, without limitation, a person's name, national identification number, passport number, email address, phone number, financial information, location data, IP address, biometric data, health-related information, and employment-related details.

3.2 Sensitive Personal Data

Sensitive Personal Data includes personal data that is of a more sensitive nature and requires a higher level of protection, including data relating to an individual's health, biometric identifiers, genetic information, religion, ethnicity, political opinions, sexual orientation, criminal records, financial credentials, and personal data of children.

3.3 Data Subject

A natural person to whom the personal data relates.

3.4 Data Controller / Data Fiduciary

Any entity that determines the purpose and means of processing personal data.

3.5 Data Processor

Any person or entity processing personal data on behalf of the Company.

3.6 Processing

"Processing" means any operation or set of operations performed on personal data, whether by automated or manual means, including the collection, recording, storage, organization, use, transfer, disclosure, deletion, or destruction of such personal data.

4. Principles of Data Protection
The Company shall process personal data in accordance with the following principles.

4.1 Lawfulness, Fairness & Transparency
Personal data shall be processed lawfully, fairly, and transparently.

4.2 Purpose Limitation
Personal data shall only be collected for specified, explicit, and legitimate purposes.

4.3 Data Minimization
Only the minimum necessary personal data shall be collected.

4.4 Accuracy
Reasonable steps shall be taken to ensure personal data remains accurate and updated.

4.5 Storage Limitation
Personal data shall not be retained longer than necessary.

4.6 Integrity & Confidentiality
Appropriate technical and organizational security measures shall be implemented.

4.7 Accountability
The Company shall maintain records, policies, controls, audit trails, and compliance mechanisms demonstrating compliance with applicable data protection obligations.

5. Categories of Personal Data Collected:
The Company may collect and process various categories of personal data depending on the nature of its relationship with the individual. This includes identity information such as full name, date of birth, national identification details, and passport information; contact information such as residential address, phone number, and email address; and employment-related information including designation, employee identification number, and payroll data. The Company may also collect financial information such as bank account details and payment history, as well as technical information including device identifiers, browser type, cookies, IP address, and login credentials. Any sensitive personal data, wherever applicable, shall be processed strictly on the basis of explicit consent of the data subject or where processing is otherwise permitted under applicable law.

6. Legal Basis for Processing:
The Company processes personal data only where it has a valid and lawful basis to do so. Such processing may be carried out where the data subject has provided free, informed, specific, and unambiguous consent. Personal data may also be processed where it is necessary for the performance of a contract to which the data subject is a party, or in order to comply with applicable legal or regulatory obligations. In certain circumstances, the Company may process personal data to pursue its legitimate business interests, provided that such interests do not override the fundamental rights and freedoms of the data subject. Additionally, personal data may be processed where

necessary for employment-related purposes, including employee administration and compliance with employment and labour laws.

7. Consent Management:
The Company ensures that consent obtained for the processing of personal data is free, informed, specific, explicit, and capable of being withdrawn at any time. Data subjects have the right to withdraw their consent by contacting the Company at privacy@onmobile.com

Any withdrawal of consent shall operate prospectively and shall not affect the lawfulness of processing carried out prior to such withdrawal.

8. Purposes of Data Processing:
The Company may process personal data for a variety of legitimate purposes, including account creation and management, provision of customer support, delivery of products and services, processing of payments, and administration of employment-related matters. Personal data may also be processed to ensure compliance with applicable laws and regulatory requirements, prevent fraud, conduct analytics, strengthen cybersecurity measures, manage legal claims or proceedings, send marketing and promotional communications where permitted, carry out internal audits, and ensure business continuity and operational resilience.

9. Data Subject Rights
Subject to applicable laws and regulations, data subjects are entitled to exercise the following rights in relation to their personal data:

9.1 Right to Information
The right to be informed about the manner in which their personal data is collected, used, and processed by the Company.

9.2 Right of Access
The right to request confirmation as to whether personal data is being processed and to obtain access to such personal data.

9.3 Right to Correction
The right to request correction or rectification of inaccurate, incomplete, or outdated personal data.

9.4 Right to Erasure
The right to request deletion or removal of personal data, where such erasure is permitted under applicable law.

9.5 Right to Withdraw Consent
The right to withdraw consent previously given for the processing of personal data, at any time.

9.6 Right to Restrict Processing
The right to request restriction or limitation of processing of personal data under specific circumstances.

9.7 Right to Grievance Redressal
The right to raise complaints or seek redressal in case of misuse, unauthorized processing, or violation of rights relating to personal data.

10. Data Retention Policy:
The Company shall retain personal data only for as long as it is necessary to fulfill legitimate business purposes, comply with applicable statutory retention requirements, address dispute resolution needs, and meet regulatory and legal obligations. Upon the expiry of the applicable retention period, personal data shall be securely deleted, anonymized, or otherwise irreversibly destroyed in accordance with the Company's data retention and disposal procedures and applicable law.

11. Security Measures:
The Company shall implement appropriate and reasonable technical and organizational safeguards to protect personal data against unauthorized access, loss, misuse, alteration, or destruction. Technical safeguards include measures such as encryption, firewalls, antivirus solutions, multi-factor authentication, role-based access controls, system logging and monitoring, and secure data backup mechanisms. In addition, the Company adopts organizational safeguards such as execution of confidentiality agreements, regular employee awareness and training programs, restriction of access on a need-to-know basis, vendor and third-party risk management practices, and periodic security audits to ensure the continued effectiveness of these security controls.

12. Data Breach Management:
The Company maintains procedures to manage personal data breaches effectively. Employees are required to immediately report any actual or suspected data breach. All reported incidents shall be investigated promptly, and where required under applicable law, the Company shall notify affected individuals and relevant regulatory authorities.

13. Cross-Border Data Transfers:
Where personal data is transferred outside Bangladesh, the Company shall ensure that such transfers are carried out in accordance with applicable law and are subject to appropriate safeguards, including contractual protections, adequacy mechanisms, encryption measures, and lawful transfer assessments. The Company shall take reasonable steps to ensure that personal data transferred across borders continues to receive an adequate level of protection.

14. Children's Data
The Company does not knowingly collect children's personal data without lawful authorization and parental/guardian consent where applicable. Additional safeguards shall apply to processing children's data.

15. Cookies & Tracking Technologies
The Company may use:

- cookies,
- analytics tools,
- session trackers,
- web beacons.

Users may manage cookie preferences through browser settings.

16. Third-Party Processors

Third-party service providers processing personal data on behalf of the Company shall:

- sign data processing agreements,
- implement security safeguards,
- process data only on instructions,
- maintain confidentiality.

17. Employee Privacy

Employee personal data shall be processed solely for:

- recruitment,
- payroll,
- benefits,
- attendance,
- performance management,
- compliance,
- workplace safety.

Employee monitoring shall be lawful, proportionate, and transparent.

18. Data Protection Governance:

The Company may appoint a Data Protection Officer or Privacy Officer responsible for overseeing compliance with applicable data protection laws, implementing this Policy, conducting audits and training, and coordinating with regulatory authorities. In addition, the Company may establish a Privacy Governance Committee to monitor ongoing compliance, assess data protection risks, and support effective data protection governance.

19. Vendor & Third-Party Risk Management

The Company shall conduct due diligence before onboarding vendors handling personal data.

Assessments may include:

- security posture,
- confidentiality controls,
- breach history,
- subcontractor usage,
- compliance certifications.

20. Privacy by Design & Default

The Company shall incorporate privacy safeguards into:

- systems,
- applications,
- products,
- business processes.

Privacy settings shall default to the most protective option wherever feasible.

21. Training & Awareness
Employees handling personal data shall receive periodic training on:

- privacy obligations,
- cybersecurity,
- phishing awareness,
- incident reporting,
- confidentiality.

22. Audits & Compliance Monitoring
The Company may conduct:

- internal audits,
- compliance assessments,
- vulnerability assessments,
- penetration testing,
- vendor reviews.

Corrective actions shall be implemented promptly.

23. Policy Violations
Violation of this Policy may result in:

- disciplinary action,
- termination,
- legal proceedings,
- contractual penalties.

24. Amendments to the Policy
The Company reserves the right to amend this Policy from time to time to reflect:

- legal developments,
- regulatory updates,
- technological changes,
- operational requirements.

Updated versions shall be published appropriately.

25. Contact Information
For questions, complaints, or requests regarding this Policy:
OnMobile Bangladesh Private Limited
Email: privacy@onmobile.com

26. Effective Date
Effective Date: 01/03/2026
Version: 1.0

Annexure A – Data Subject Request Form

The Company may provide forms for:

- access requests,
- correction requests,
- deletion requests,
- consent withdrawal,
- grievance submissions.

Annexure B – Data Retention Schedule

Data Category	Retention Period	Disposal Method
Customer Records	7 Years	Secure Deletion
Employee Records	6 Years after Exit	Secure Destruction
Financial Records	As per Law	Archival & Deletion
CCTV Footage	90 Days	Automatic Overwrite
Website Logs	12 Months	Secure Deletion