AXIATA DIGITAL SERVICES SDN. BHD.

DATA PRIVACY POLICY

Effective Date: DD/MM/2020

Document No: ADS/DP/2020/XX

Version: 1.0

Classification: Private and Confidential

Document Revisions Record			
Version	**Release Date**	**Description/Summary of Changes**	**Approved and Reviewed by**
1.0	DD/MM/YY	Initial version	
2.0	DD/MM/YY		
3.0	DD/MM/YY		

Policy Owner

This Policy document is owned and maintained by Group Chief Risk and Compliance Officer.

Table of Contents

1. Abbreviation

Abbreviation	Description
BRCC	Board Risk and Compliance Committee
CEO	Chief Executive Officer
DPIA	Data Protection Impact Assessments
DPO	Data Privacy Officer
GCRCO	Group Chief Risk and Compliance Officer
GDPO	Group Data Privacy Officer

2. Definitions

"Data Privacy Policy" or ***"This Policy"*** is defined as this Data Privacy Policy.

"Axiata Group" or ***"the Group"*** is defined as Axiata Group Berhad and its subsidiaries and associates, owned directly or indirectly by Axiata Group Berhad as well as joint venture entities established.

"Applicable Privacy Laws" are defined as Privacy and Personal Data Protection laws specific to any jurisdiction or industry where the Company has a presence.

"Cross-Border Data Transfer" is defined as the transmission of personal data from one country (jurisdiction) to another.

"the Company" is defined as the subsidiaries and associates, owned directly or indirectly by Axiata Group Berhad as well as join ventures established.

"Data Privacy Officer ("DPO")" is defined as the designated individual responsible for ensuring the Company's compliance with applicable Privacy laws and Data Privacy Policy.

"Data Subject" is any individual who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

"Personal Data" is defined as any data that could potentially identify a specific individual directly, or indirectly. It includes, but is not limited to Name, Date of Birth, National Registration Identification Card Number, Telephone Number, Employee ID, credit card number.

"Privacy" is defined as the right to have some control over how personal information is collected and used.

"Privacy Notice" is defined as the written notice that the Company is required to provide to a data subject in compliance with applicable Privacy laws.

"Processing" means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data.

"Sensitive Personal Data" is defined as any data that could potentially identify a specific individual's racial or ethnic origin, political opinion, religious belief, physical or mental health etc.

"Stakeholders" *is* defined as all members of the Board of Directors, heads, senior managers, managers and individuals at all levels including permanent and contract employees and temporary employees and trainees or interns of Axiata Group. Additionally, suppliers, contractors, vendors, agents, consultants, representatives, distributors, joint venture partners and other external stakeholder(s) acting for or on behalf of Axiata Group.

3. Introduction

Axiata Group is committed to protecting the Privacy and data of our data subjects with utmost respect and due care.

This Data Privacy Policy (referred to as “Policy”) establishes the mandatory requirements of Axiata Group with respect to protection of personal data.

This is an overarching Policy and together with relevant underlying Privacy procedures, templates and guidelines provide the breadth and depth needed to meet Axiata Group’s Data Privacy requirements.

4. Guiding Principles

Axiata’s activities and Privacy practices are underpinned by the **T.R.U.S.T.** principles, which are laid out below:

TRANSPARENT	We are TRANSPARENT about what, why and how we collect and protect YOUR PERSONAL DATA so that YOU can make informed decisions.
RIGHTS	We respect YOUR RIGHTS as individuals, so YOU are in control of YOUR PERSONAL DATA.
USE	We USE YOUR PERSONAL DATA for specific and stated purposes and keep it for as long as required only.
SECURITY	We have established robust CYBER SECURITY PRACTICES in line with leading industry standards to protect YOUR PERSONAL DATA that YOU have shared with us.
TRANSFER	With YOUR CONSENT or in accordance with APPLICABLE LAWS we may TRANSFER YOUR PERSONAL DATA and will take appropriate steps to ensure it is adequately protected.

5. Purpose

The underlying premise to this Policy is that good Privacy is good business. Good Privacy practices are key component of corporate governance and accountability.

This Policy outlines the approach towards Data Privacy and to support Axiata Group's ambition in proactively enhancing customer digital trust and confidence.

6. Scope and Applicability

This Policy applies to all Stakeholders of Axiata Group, which includes subsidiaries and associated companies that the Group has a controlling stake or ownership. Companies or entities in which Axiata Group does not have a controlling stake are encouraged to adopt this Policy.

This Policy shall apply to the end-to-end processing of personal data of customers, employees and all other stakeholders (collectively referred to as "data subjects"), may it be in the form of digital, on paper or other materials. This Policy applies to all the employees, contract staff and vendors who process personal data on the Company's behalf.

The Company shall comply with applicable Privacy laws. To the extent this Policy contradicts or is inconsistent with requirements to any law, statute or regulation, the higher standards shall prevail.

7. Data Privacy Practices

In order to comply with and operationalize the T.R.U.S.T. principles, the Company shall implement the following Data Privacy Practices:

7.1 Lawfulness, Fairness, and Transparency

Data must be collected and processed from data subjects in a lawful, fair and transparent manner.

a) The Company shall process personal data lawfully, fairly and in a transparent manner. The Company shall provide the data subjects with a Privacy Notice which specifies details on the purpose for which the personal data is being collected and processed, source of the personal data, class of the third parties to which the personal data is disclosed or may be disclosed to, security measures towards protection of personal data, data retention requirements, rights available to data subjects and other relevant information in line with applicable Privacy laws.

Refer to Privacy Notice templates for Data Subjects for further details.

b) The Company shall process **Personal Data** when it is necessary and meets at least one of the following lawful bases for processing:
   i. where the data subject has given their consent for their personal data to be processed. Any processing shall be strictly within the purposes for which the consent is given
   ii. where the processing is necessary for the performance of a contract with the data subject
   iii. where steps are to be taken at the request of the data subject with a view to entering into a contract
   iv. where the processing is necessary to comply with legal obligations/regulatory requirement and for the exercise of any functions conferred on any person by or under any law
   v. where it required for administration of justice
   vi. to protect the vital interests of data subjects
   vii. any other lawful base for processing personal data as stated by applicable Privacy laws.

c) The Company shall also ensure that while processing **Sensitive Personal Data** explicit consent is required of data subjects except for other lawful bases stated below:
   i. exercising or performing any right or obligation which is conferred or imposed by law on the Company in connection with employment
   ii. any legal proceedings
   iii. obtaining legal advice
   iv. establishing, exercising or defending legal rights
   v. where the processing is necessary to protect the vital interests of the data subject or another person
   vi. any other lawful base for processing sensitive personal data as stated by applicable Privacy laws.

d) The Company shall take reasonable steps to maintain **accurate**, **complete**, **not misleading** and **up to date** personal data only for the purpose(s) identified in the Privacy Notice.

e) The Company shall ensure that personal data collected and processed shall be **adequate**, **relevant** and **not excessive** for the purpose(s) identified in the Privacy Notice.

Lawful bases for processing Personal Data:

- Consent
- Performance of Contract
- Entering into Contract
- Legal Obligations
- Administration of Justice
- Protection of Vital Interests
- Any other applicable lawful base

Lawful bases for processing Sensitive Personal data:

- Explicit Consent
- Employment purpose
- Legal proceedings, advice and defense
- Administration of Justice
- Protection of Vital Interests
- Any other applicable lawful base

7.2 Data Subject Rights

The Company respects the rights of data subjects and shall provide them with the opportunity and platform to exercise their rights. The Company shall establish processes for receiving, recording and responding to some or all of the below mentioned data subject rights in accordance with the applicable Privacy laws:

- Right to be informed
- Right to access
- Right to correct personal data
- Right to withdraw consent
- Right to prevent processing in certain circumstance (e.g. prevent direct marketing, processing that is likely to cause distress)
- Right to erasure (to be forgotten)
- Right to data portability.

Refer to Data Subject Rights Procedure for further details.

7.3 Retention and Disposal

Define and document data retention periods and securely dispose personal data post expiry of the retention periods.

The Company shall define and document retention periods for various categories of personal data in accordance with the stated purpose or as required by the law. The Company shall ensure that personal data is retained as per the defined retention periods. Post expiry of the retention period, personal data shall be securely disposed or de-identified.

Refer to Data Retention Procedure for further details.

7.4 Privacy by Design

Privacy by Design is a methodology that enables Privacy to be built in to the design and architecture of systems, products and processes.

The Company shall adopt Privacy by Design methodology by ensuring Data Privacy issues are considered at the design phase of any system, service, product or process and then throughout the personal data lifecycle.

Refer to Privacy by Design Guidelines for further details.

The Company shall conduct Data Protection Impact Assessments (DPIAs) to identify underlying Privacy risks in the high-risk personal data processing activities.

Refer to Data Protection Impact Assessment Procedure for further details.

Privacy by Design methodology is to be adopted and Privacy must be incorporated from the initial design phase.

Data Privacy Impact Assessments shall be conducted to identify the underlying Privacy risks of the high-risk processes.

7.5 Vendor Privacy Management and cross border data transfers

Key Vendor Privacy Management Activities:

- Due Diligence
- Contracts with adequate Privacy and Security clauses
- Periodic Vendor Assessments
- DPIAs to onboard new projects

The Company shall establish processes with respect to managing high-risk data processing vendors from a Data Privacy standpoint. The processes shall include the below tabulated activities:

Due Diligence	Conduct out **due diligence** on the prospective high-risk vendor's information security and Privacy posture prior to onboarding them
Data Processing Agreements	Include **adequate Privacy** and **information security clauses** in the contractual agreement executed with the vendors
Periodic Vendor Assessment	Carry out **periodic assessment** of the existing high-risk vendors' compliance with contractual and regulatory obligations
DPIAs for Projects	Carry out **DPIAs** prior to onboarding high-risk projects from existing vendors

Refer to Vendor Privacy Management Process Flows for further details.

The Company shall assess the permissibility of Cross-Border Data Transfers in accordance with applicable Privacy laws. Further, the Company shall also ensure that necessary safeguards (such as Data Transfer Agreements) are in place to protect all the Cross-Border Data Transfers.

7.6 Privacy Incident and Data Breach Management

The Company shall define and implement a process for reporting, assessing, resolving, communicating, escalating, notifying, and performing of any other actions required in the effective management of Privacy incidents and data breaches.

Refer to *Data Privacy Incident and Breach Management Procedure for further details.*

7.7 Security

The Company shall implement appropriate technical safeguards and organizational measures to maintain the confidentiality, integrity and availability of personal data.

Refer to Information Security Policy for further details.

7.8 Audit, Review and Reporting

The Company shall carry out periodic Privacy audits on their data processing environment to monitor its compliance against this Policy, Group Privacy standards and applicable Privacy laws.

7.9 Training and Awareness

The Company shall mandate annual Data Privacy awareness trainings for their employees and contract staff. The Company shall also raise awareness through knowledge sharing sessions, e-mailers, posters, Privacy campaigns and other such means.

Mandate Data Privacy Awareness trainings for all employees and contract staff.

8. Communication and Implementation

The Company's CEO is responsible for ensuring that this Policy is duly published, communicated and implemented throughout the organization.

CEO shall ensure that relevant and adequate organizational resources are available to ensure the implementation of this Policy. The CEO shall appoint a DPO to ensure adherence to the requirements in this Policy. This includes managing Privacy risks and concerns through operationalizing Privacy practices and processes. The DPO shall act as the liaison between the GDPO and key stakeholders in the Company.

9. Deviations and Exceptions

Any deviations and exceptions to this Policy shall be made in writing and presented to the Company's BRCC for approval and shall be further validated by the Group BRCC.

10. Breaches to the Policy

The Company shall have processes in place to enable the identification, recording, reporting and rectification on a timely basis of:

- Breaches of this Policy
- Non-compliance with any relevant requirements and/or standards
- Risk control failures, issues and other shortcomings.

The Company shall require all breaches to the Policy to be mandatorily notified and reported to their CEO, GDPO and GCRCO within a period of 48 hours from it being first detected.

Any failure to comply with this Policy can lead to disciplinary action, suspension or dismissal. Negligent or deliberate breaches can result in personal criminal liability. Additionally, the Company's employees and contract staff are subject to loss of access privileges, letter of reprimand, unsatisfactory performance evaluation, sanction, accountability in a court of law, civil, and criminal prosecution.

Breaches to the Policy are required to be notified to the CEO within 48 hours of detection.

Non-compliances to the Policy can lead to disciplinary action, suspension, dismissal or personal criminal liability.

11. Reference Documents

- Privacy Notice Templates
- Data Retention Procedure
- Data Subject Rights Procedure
- Privacy by Design Guidelines
- Data Protection Impact Assessment Procedures
- Privacy Incident and Data Breach Management Procedure
- Vendor Privacy Management Process Flows
- Information Security Policy

12. Review and updates to this Policy

- This Policy shall be monitored and reviewed by the Group Risk and Compliance Division on an annual basis or as the need arises. The required updates and modifications shall be recommended by the GCRCO to the BRCC for concurrence and the Board for approval before the amendments or updates are made accordingly. All Stakeholders shall be informed of any revisions made to this Policy.
- Axiata Group reserves the right to vary and/or amend the terms of the Data Privacy Policy from time to time.

Guidance for the Company to localize/update the Policy

Guidance for the Company to update and localize the Policy are tabulated below:

Area	Instructions
Section 1	The Company may localize/update.
Section 2	Definitions of data subjects, personal data and sensitive personal can be updated by the Company in line with what is stated in the applicable Privacy laws. In the absence of the same, the Company to retain the contents as is.
Section 3-Section 5	To be retained as is. Do not localize/update.
Section 6	To be retained as is. Do not localize/update.
Section 7.1	The Company to localize 7.1 b and 7.1 c depending on the lawful basis stated in the applicable Privacy laws. In the absence of an applicable Privacy law, the Company to remove the last subpoint under 7.1 b(vii) and 7.1 c(vi) and retain the remaining content as is.
Section 7.2	The Company to localize this section depending on the list of data subject rights called out in the applicable Privacy laws. Right to be informed, right to access and right to correct personal data are the minimum basic rights that the Company should provide to their data subjects even if they do not have an applicable Privacy law to comply with.
Section 7.3 - 7.9 Section 8 - Section 10	These sections should be retained as is. Do not localize/update.
Section 11 - Section 12	These sections should be retained as is. Do not localize/update.

The Company shall register the localizations with Group Risk and Compliance Division.

▶ END OF DOCUMENT