Data Residency Policy

# Introduction

a. Purpose: The purpose of this Data Residency Policy is to establish guidelines and procedures for the storage, processing, and transmission of data, ensuring compliance with applicable privacy laws and regulations.

b. Scope: This policy applies to all employees, contractors, and third-party entities who handle or have access to data within the organization's infrastructure.

# Definitions

a. Data Residency: The physical or geographical location where data is stored or processed, subject to the laws and regulations of that jurisdiction.

b. Data Controller: The entity responsible for determining the purposes and means of data processing.

c. Data Processor: An entity that processes data on behalf of the data controller.

# Data Residency Requirements

a. Legal and Regulatory Compliance: Data residency decisions shall be made in compliance with applicable data protection laws, regulations, and industry standards in the jurisdictions where data is processed or stored.

b. Data Classification: Data shall be classified based on its sensitivity level to determine appropriate data residency requirements.

c. Informed Consent: Data subjects shall be informed about the location where their data will be stored or processed, and their consent shall be obtained when required by applicable laws.

# Data Transfer and Cross-Border Data Flows

a. Cross-Border Data Transfer: Data shall not be transferred to another country or jurisdiction unless it is permitted by applicable laws or if adequate safeguards are in place to protect the data.

b. Data Transfer Agreements: In the case of cross-border data transfers, data controllers shall establish data transfer agreements with data processors or recipients in compliance with relevant regulations.

# Vendor and Third-Party Compliance

a. Vendor Due Diligence: When engaging third-party vendors or data processors, the organization shall conduct due diligence to ensure they comply with relevant data residency requirements.

b. Contractual Obligations: Data residency requirements shall be included in contractual agreements with third-party vendors, specifying the jurisdictions where data can be processed or stored.

# Data Storage and Processing

a. Data Security Measures: The organization shall implement appropriate technical and organizational measures to safeguard data stored or processed in its systems or third-party infrastructure.

b. Regular Audits: Periodic audits shall be conducted to ensure compliance with data residency policies and to assess data security measures.

c. Data Minimization: Data shall be stored and processed only for the duration required to fulfill the purpose for which it was collected.

# Incident Response and Data Breach Notification

a. Incident Response Plan: The organization shall have an incident response plan in place to address data breaches or incidents related to data residency.

b. Data Breach Notification: In the event of a data breach affecting data stored or processed in a specific jurisdiction, data subjects and relevant regulatory authorities shall be notified as required by applicable laws.

# Training and Awareness

a. Privacy Training: Employees and relevant stakeholders shall receive training on data residency policies and data protection practices.

b. Privacy Awareness: The organization shall promote privacy awareness to reinforce the importance of data residency compliance.

# Policy Review and Updates

a. Regular Review: This policy shall be reviewed periodically to ensure its relevance and alignment with changing legal requirements and organizational needs.

b. Updates: Any updates or revisions to this policy shall be communicated to all relevant stakeholders.

# Non-Compliance

a. Violations of this policy may result in disciplinary action, up to and including termination, in accordance with the organization's policies and procedures.

By implementing this Data Residency Policy, the organization ensures the responsible handling of data while complying with privacy laws and regulations, thereby maintaining the trust and confidence of data subjects and stakeholders.