DATA RESIDENCY POLICY FOR PAYMENT SYSTEMS DATA 2021

In exercise of the powers conferred by Section 4 (Section 4.1.1-4.1.2) of the Payment and Settlement Systems Rules and Regulations 2018, the RMA hereby issues Data Residency Policy for Payment Systems Data 2021.

PART I: PRELIMINARY

Short Title, Commencement, and Application

1. This Policy shall be called the Data Residency Policy for Payment Systems Data 2021;
2. This Policy shall come into effect from May 2021;
3. This Policy shall apply to any licensed national or international payment service providers which include payment systems, payment systems operators and payment system participants, operated or controlled from within the territories of the Kingdom of Bhutan.

Scope of Activities

4. This policy shall define:
    i. Processing and storing of payment data that has been collected, disclosed, or shared within the territory of Bhutan; and
    ii. Processing and storing of cross border payment data that has a connection with foreign leg of the transaction with any business carried from the territory of Bhutan.

Objectives

5. The primary objective of this policy is to:
    i. Ensure that a payment service provider licensed/approved by the authority store its payment data on Premise in Bhutan or on Cloud;
    ii. To provide necessary checks and balances to ensure security and sovereignty of the payment system data;
    iii. For effective monitoring and supervisory access to data stored with Payment Service Providers in Bhutan which include payment systems, payment systems operators and payment system participants licensed by the Authority; and

iv. To safeguard the integrity, authenticity, and confidentiality of data and operating processes while promoting growth in digital payments.

PART II: SERVICE UPTIME ARCHITECTURE

Service Uptime Architecture of On Premise and Cloud (IaaS, PaaS, and SaaS)

Infrastructure	On Premise	Cloud		
		Infrastructure as a Service (IaaS)	Platfrom as a Service (PaaS)	Software as a Service (SaaS)
Application				
Data				
Runtime				
Middleware				
Operating System				
Virtualization				
Servers				
Storage				
Networking				

	Managed by Payment Service Provider
	Managed by Cloud Provider

PART III: SYSTEM REQUIREMENTS

A payment service provider licensed/approved by the authority may store its payment data on Premise or on Cloud subject to fulfillment of the following general and specific technical requirements based on the type of data service adopted:

General:

6. Industry standard methods and levels of data encryption at any given period:

i. Encryption Algorithms

(a) Advanced Encryption Standards (AES)

The Advanced Encryption Standard (AES) is the algorithm trusted as the standard by the government and payment industries. AES 128-bit, 192- and 256-bits forms should be used as the standard for data encryption.

(b) Triple DES Encryption

To produce a more secure encryption using the Triple DES (3DES) algorithm, the CSP shall be able to provide solutions that use hardware dependent 3DES encryption for financial services.

(c) RSA Encryption

RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in PGP and GPG programs and therefore shall be adopted wherever necessary.

ii. **Encryption Methods** - Must implement any one of the following:

(a) Full Disk: encryption of data at the disk level shall include the operating system, applications, and the data the applications use on a disk that is encrypted.

(b) Directory Level (or Filesystem): encryption and decryption of entire data directories as a container with access to files requiring use of encryption keys. The same approach shall be used to segregate data of identical sensitivity or categorization into directories that are individually encrypted with different keys.

(c) File Level - encryption of individual files.

(d) Application Level - encryption and decryption of application managed data.

7. PCI DSS/ISO/IEC 27001/SOC standards for information security management;

8. Information Technology and Data Recovery Plan in conjunction with the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP);

9. Maintain ownership of the payments data to provide unfettered accessibility and availability of data to the Authority;

10. Transfer Payments data abroad with prior written approval from the Authority. The Authority shall prescribe specific terms and conditions for approval;

11. Payments application and data breaches and/or loss must be reported immediately to the RMA including the affected individual/parties**;**

12**.** Sign Service-Level Agreement (SLA) with the Internet Service Provider (ISP) to ensure 99.9 percent uptime of network connectivity and a minimum level of service maintenance, reliability, and availability; and

13. Ensure redundancy on network connectivity with a secondary ISP, in case the primary network fails and vice versa.

On premise:

14**.** Payment service providers shall ensure that the entire payments data are stored in a system in Bhutan.

15. For cross-border transactions, the foreign leg of the transaction, if any, the copy of the encrypted data can also be stored in the foreign country subject to annual third-party system assessment/audit for critical and core systems by a certified external auditor.

On Cloud:

16. A payment service provider shall sign a cloud service level agreement (cloud SLA) with a cloud provider and ensure that following risk mitigating measures are specified/included in the agreement:

i. **Performance Service Level Objectives** - the performance of the cloud service and the performance of related aspects of the interface between the PSP and the cloud service provider -

(a) Availability: the cloud services are easily accessible and usable upon demand.

(b) Response time- minimum time interval between initiated event (stimulus) by the PSP and initiated response to that stimulus by CSP.

(c) Capacity - On demand computing capacity (scalable) and interoperable with other CSP's including flexibility to modify applications and services live without service interruptions.

(d) bandwidth- Support any bandwidth requirements of the client and be flexible to meet future demands while maintaining an acceptable response time.

ii. **Data Management Service Level Objectives:**

(a) Demarcation- the data stored in the cloud are segregated either electronically or physically from other client's data and applications. CSP may provide cage services for housing the computing devices that require separate keys or biometric access.

(b) Data Replication- the data is replicated and restored as part of the CSP's data recovery plan in case of service disruptions.

(c) Data Ownership- ownership of the data and the format remains with the PSP.

(d) Termination terms- all internal memory, buffers and/or other reusable memory to be cleared to effectively deny access to previously stored information. Further, all data shall be sanitized and removed from the cloud

before they are released from the classified information controls or released for use at a lower classification level.

(e) Support- Metrics and responsibilities among the pirates involved in cloud configuration shall be clearly outlined, such as the specific amount of response time for reporting or addressing system failures.

PART IV: MISCELLANEOUS

Transitional Provision

17. Timeline of one year shall be given to the payment service providers through issuance of directives to ensure smooth shift to and successful implementation of the new Policy.

Reporting

18. Payment service providers shall submit the System Audit Report (SAR) certifying adherence to requirements stipulated in this Policy to the Authority annually.

Review of Policy

19. The RMA reserves the right to review/amend the policy regularly in context to developments in new technology.

Penalty

20. Failing to comply with any provision of this policy shall be dealt as per the Penalties Rules and Regulations 2019 to the extent pursuant.

Definitions

21. In this Policy, unless the context indicates otherwise, the words are defined as follows:

i. **Cloud** means software and computing services that run on a remote computer and are available over the internet using a web browser or applications on your computing device;

ii. **Data Residency** means collecting, processing, storing of payments data on premise or cloud, with data protection standards in place;

iii. **On Premise** means a software that is installed and runs on a computer on the premise of the organization. The entire software/infrastructure resides at the organization's premises;

iv. **Participant** means the system provider and any institution or party authorized by the Authority to participate in a system in the Kingdom of Bhutan;

v. **Payment** means the payer's transfer of a monetary claim through a party acceptable to the payee;

vi. **Processing** means collecting, structuring, organizing, using, storing, sharing, disclosing, erasing and destruction of data;

vii. **Payment System Data** means the data should include end-to-end transaction details and information pertaining to payment or settlement transaction that is gathered / transmitted / processed as part of a payment message / instruction. This may, include - Customer data (Name, Mobile Number, email, PAN number, etc. as applicable); Payment sensitive data (customer and beneficiary account details); Payment Credentials (OTP, PIN, Passwords, etc.); and, Transaction data (originating & destination system information, transaction reference, timestamp, amount, etc.);

viii. **Payment Institution** means an entity licensed by the Authority under these rules and regulations to provide payment services;

ix. **Payment Service Provider** means a payment institution, a bank and a DMFI;

x. **Payment System** mean a system that enables payments to be effected between a player and a beneficiary, involving a clearing, payment or settlement service, on a gross settlement – real time transfer or a net - deferred settlement basis; and

xi. **Payment services** shall include:

a) Services enabling cash to be placed on a payment account or enabling cash withdrawals from a payment account and all of the operations required for operating a payment account;

b) The execution of the following types of payment transactions: (i) Direct debits, including one-off direct debits; (ii) Payment transactions executed through a payment card or a similar device; (iii) Credit transfers, including standing orders;

c) Issuing payment instruments or acquiring payment transactions;

d) Money remittances; and

e) Issuance of electronic money (including mobile money), as further specified and notified by the Authority.
