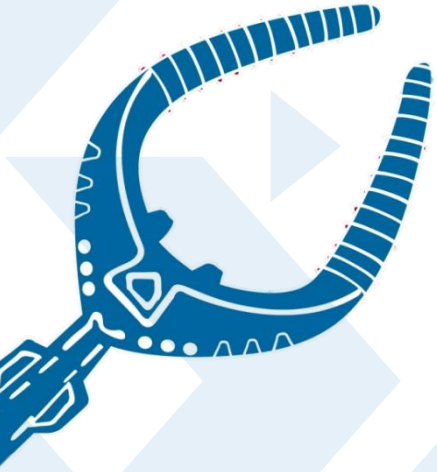

GUIDELINE 4

PROTECTION OF CONSUMER DATA & PRIVACY

FEBRUARY 2024

Disclaimer

This Guideline does not constitute legal advice. FSPs are encouraged to seek professional advice on how the requirements could be implemented within each institution. FSPs are responsible for determining the extent of each obligation. Examples outlined in this Guideline are purely for illustration; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

GUIDELINE ON THE PROTECTION OF CONSUMER DATA AND PRIVACY

A. Introduction

1. Pursuant to Section 5.4 of the *Financial Sector Development Policy Statement No. 3 for the Protection and Fair Treatment of Financial Consumers* ('Policy'), the following Guideline is issued to ensure that balanced rules are in place regarding the protection of consumer data and privacy provided to the FSPs.

2. This Guideline is intended to provide the minimum standards only to assist FSPs comply with Principle 4 of the Policy on the Protection of Consumer Data and Privacy.

3. The Guideline applies to all FSPs defined in the Policy.

4. The terms and expressions used in the Guideline have the same meaning as those expressed in the Policy unless stated otherwise.

5. This Guideline will be reviewed every 3 years from the implementation period, or whenever necessary.

B. Requirements of the Guideline

6. Every FSP should consider:

    a) **Data Privacy Policy -** developing a data privacy policy on the purpose of collection and/or processing of personal data and the legal basis for each personal data processing activity. The data privacy policy should be published on its website in addition to all customer-facing IT applications, including internet banking and mobile banking applications, through which personal data is being processed by the FSPs;

    b) **Consent Management Procedure -** developing and implementing a consent management procedure which should outline the procedures for obtaining consent from customers prior to processing personal data unless it is restricted by other laws, and recording of the time that the consent was obtained, the identification of the data subject and the consent statement;

    c) **Accountability -** being responsible and accountable for data privacy and data protection concerning the personal data it processes.

    d) **Data Breach Management Procedure -** establishing procedures for the identification and recording of breaches of personal data. As part of the

establishment of the data breach management procedures, the FSPs shall ensure coverage of all aspects of its operations including its branches and field operations; and should establish procedures for notifications to the data subject.

e) **Technical measures to protect personal data - e**nsure that employees are made aware of the personal data definition and how to recognize information that is personal data. In addition, FSPs must ensure that;

i. individuals operating under its control with access to personal data are subject to a confidentiality obligation. The confidentiality agreement of individuals, whether a part of a contract or separate, shall specify the length of time for which the obligations shall be adhered to;

ii. all access to personal data by employees as well as by data processors appointed by the FSPs shall be logged. Data access logs shall record access to personal data including who accessed, when, and which individual's personal data was accessed, and what changes, if any, were done to the data;

iii. any use of removable media and/or devices for the storage of personal data is documented well. For removable media on which personal data is/was stored, secure disposal methods shall be used;

iv. it documents a backup policy which addresses the requirements for backup, recovery, and restoration of personal data as well as for erasure of personal data contained in backup media;

v. personal data that is transmitted over untrusted data transmission networks is encrypted for transmission. Untrusted networks can include the public internet and other facilities outside the FSPs control;

vi. emails and any corporate communication platforms used to exchange documents or files containing personal data shall be encrypted and shall be secured with data leakage prevention;

vii. endpoint devices including laptops and PCs which are used for processing of personal data are secured with disk encryption and data leakage prevention tools;

viii. measures such as blocking the transfer of sensitive data, quarantining affected files, or automatically revoking access to compromised accounts are implemented; and

ix. key personnel must stay updated with technology trends and consider employing AI tools to combat data privacy leakage given the rise of cloud

computing, increased usage of mobile applications and evolving Internet of Things (IoT) devices.

Reserve Bank of Fiji
February 2024