Guidelines on Data Privacy and Data Protection 2021

Preliminary

Pursuant to Section 210 of the Financial Services Act of Bhutan 2011 and Section 166 of the Royal Monetary Authority Act 2010, Authority hereby has adopted the Guidelines on Data Privacy and Data Protection 2021 in order to provide standard guidelines to the Financial Service Providers (hereafter refer to as FSPs) including but not limited to, in collecting, sharing, dessiminating, disposing data while ensuring the confidentiality and integrity of data so that the data obtained by the FSPs could be submitted to the Authority.

1 Short title, commencement and extent

1.1 These guidelines shall:

1.1.1 Be called "Guidelines on Data Privacy and Data Protection 2021"

1.1.2 Come into force on …..… 2021(with transitional period of 6 months); and

1.1.3 Apply to Authority and all FSPs as specified and defined under these Guidelines.

2 Purpose

2.1 FSPs to collect and furnish on such dates, terms and conditions, such data with regard to monetary and credit systems, balance of payments, and banking and provide the same to the Authority as mandated by Section 166 of the RMA Act 2010;

2.2 To continue to instill the public confidence in the financial and economic data and to ensure the integrity of the data, a robust data privacy and data protection ecosystem is mandatory in the financial sector in view of the rapid evolution of digitization in Bhutan;

2.3 To guide the FSPs in collecting, processing, analyzing and disseminating the confidential data as processing confidential data creates privacy risks to the data-subjects; and

2.4 To guide the overall data management, the FSPs are required to follow the standard practices for collecting and processing, including use, disclosure, retention, transmission and disposal broadly in line with the principle of *Privacy by Design and Default*.

3 Privacy by design and default

3.1 Privacy by design is approach in which privacy is considered at the initial design stage and throughout the complete lifecycle of products, digital platforms, processes or services that involve processing personally identifiable information and sensitive economic and financial data.

3.2 Privacy by default implies:

3.2.1 No coupling of service to additional and over-shooting data collection;

3.2.2 Providing clear information to the data-subject/s on how data will be processed and what rights they have relating to their data; and

3.2.3 Complete protection for the data-subject/s without any pre-adjustments in all information systems used to process personal data.

4 Obligations of FSPs

4.1 The FSPs shall be responsible and accountable for data privacy and data protection with respect to the personal data processed by them; and

4.2 Under the direction and supervision of the competent authority of the FSPs, the FSPs shall establish a Data Privacy Management Committee (DPMC) headed by a Data Protection Officer.

4.3 Roles and Responsibilities of the Data Privacy Management Committee the following shall be the roles and responsibilities of DPMC:

4.3.1 The DPMC shall provide the direction and resources necessary to implement the Data Privacy and Protection Guidelines.

4.3.2 The DPMC shall:

4.3.2.1 Approve the FSPs' data privacy policy document/s;

4.3.2.2 Review and approve exceptions to the data privacy policy, if any are necessary;

4.3.2.3 To oversee the effective implemntation of the Guidelines on Data Privacy Privacy and Data Protection;

4.3.2.4 Designate a Data Protection Officer for the FSPs who will implement the Guidelines on Data Privacy Privacy and Data Protection;

4.3.2.5 Review privacy risks identified in privacy impact assessment and approve the mitigation measures of the FSPs proposed by the Data Protection Officer; and

4.3.2.6 Provide guidance to the Data Protection Officer in executing the data privacy incident/s of the FSPs, whenever a breach is detected.

4.4 Appointment of Data Protection Officer

4.4.1 The FSPs shall appoint a Data Protection Officer who will report to the DPMC;

4.4.2 The Data Protection Officer shall be an employee of FSPs with the necessary knowledge and skills on data privacy and protection practices; and

4.4.3 The FSPs shall submit the contact details of the Data Protection Officer to the Authority.

4.4.4 The roles and responsibilities of the Data Protection Officer amongst others shall be to :

4.4.4.1 Ensure the organization's compliance with the Data Privacy and Data Protection guidelines issued by the Authority;

4.4.4.2 Develop the FSPs Data Privacy and Data Protection Policies and procedure and submit for review and approval by the DMPC;

4.4.4.3 Establish the Personal Data Inventory and review it on a periodic basis;

4.4.4.4 Ensure that record of processing operations is maintained, based on the information provided to his office;

4.4.4.5 Conduct Data Privacy Impact Assessment and develop mitigation measures for privacy risks identified;

4.4.4.6 Provide advice regarding incorporation of data privacy and data protection measures for Information Systems being developed or enhanced by the FSPs;

4.4.4.7 Develop and oversee the roll-out of the organization-wide data privacy training programme;

4.4.4.8 Develop and implement data privacy incident management system;

4.4.4.9 Provide assistance to data-subject/s whose data is being managed by the FSPs in the role of data controller in resolving their data access requests and any other queries they may have with pect to their data privacy and data protection; and

4.4.4.10 Plan and executive information, education and communication initiatives to inform and educate the customers of the FSPs and the public at large on the steps and precautions they need to take to protect their personal data and what rights and obligations they have with respect to the data privacy and data protection.

4.5 Develop and publish a Data Privacy Policy by FSPs

4.5.1 FSPs shall develop and publish internal data privacy policy in line with these guidelines including the following:

4.5.1.1 The purpose of collection and processing of personal data;

4.5.1.2 The legal basis for each personal data processing activity, which can include one or more of the following;

4.5.1.3 Compliance with a legal or regulatory obligations;

4.5.1.4 Consent from the personal data-subject/s;

4.5.1.5 Performance of a contract/s with data-subject/s;

4.5.1.6 Protection of vital intets of personal data ; and

4.5.1.7 Performance of a task carried out in the public interest.(for example)

4.5.2 The data privacy policy shall be published on the website of the FSPs.

4.5.3 The data privacy notice shall also be published via all customer facing IT applications, including internet banking and mobile banking applications, through which a data-subject/s's personal data is being processed by the FSPs.

4.6 Develop and implement a consent management procedure by the FSPs:

4.6.1 They shall develop and implement a consent management procedure;

4.6.2 They shall obtain consent of the data-subject/s for processing of personal data, unless it is restricted by other laws;

4.6.3 They shall process personal data for the purpose for which an explicit consent from the data-subject/s has not been obtained and shall be treated as an exception to the Guidelines on Data Privacy and Data Protection; and

4.6.4 They shall record the date on which the consent was obtained, idenitfy the data subject/s and consent statement as per the consent management procedure.

4.7 Develop and maintain Personal Data Inventory

4.7.1 FSPs shall document all the personal data processed by them for delivery of financial services in the form of a Personal Data Inventory;

4.7.2 The personal data inventory shall provide, via Data Flow Diagrams, a view of who, where, how and why personal data is being processed at various stages of the personal data lifecycle;

4.7.3 Personal data inventorization shall cover both structured and unstructured data:

4.7.3.1 Structured data: Metadata shall be obtained from the application databases which shall be recorded in the personal data inventory; and

4.7.3.2 Unstructured data: Data discovery techniques shall be used to identify the personal data and sensitive personal data residing in end-usersystems, file storage and email and messaging servers, etc .

4.7.4 Exclusions of devices or systems: A comprehensive list of systems/devices not included in data discovery for developing the Personal Data Inventory shall be maintained by the DPO, highlighting the reason for exclusion. The list shall be reviewed semi-annually by Privacy Management Committee.

4.8 Perform Data Privacy Impact Assessment

4.8.1 Personal data processing creates risks for data-subjects. These risks shall be assessed through a privacy impact assessment and mitigation measures shall be identified and documented by the FSPs.

4.8.2 Privacy impact assessment shall be mandatorily carried out if personal data processing by the FSPs involves:

4.8.2.1 Automated decision making which produces legal effects on data-subject/s; and

4.8.2.2 Processing of personal data using data warehouses and analytics platforms.

4.8.3 On an ongoing basis, the FSPs shall assess the need for, and implement where appropriate, a privacy impact assessment whenever processing new personal data or changes to existing personal data processing is planned.

4.9 Maintain records related to processing of personal data

4.9.1 The FSPs shall maintain records of processing of personal data, inter alia, the following:

4.9.1.1 Type and purpose of processing;

4.9.1.2 Description of categories of personal data and the data-subject/s;

4.9.1.3 The categories of recepients to whom the personal data will be disclosed or has been disclosed including recepients in other countries or international organizations;

4.9.1.4 A general description of the technical and FSPs security measures; and

4.9.1.5 A privacy impact assessment report.

4.9.2 The inventory of records of processing shall have one or more owners within the FSPs who is responsible for its accuracy and completeness.

4.9.3 Data-subject shall be provided with appropriate information about the processing of their personal data.

4.9.4 A nodal person from the FSP, which can be the Data Protection Officer or any of his nominees, shall be appointed whom data-subjectss can approach to resolve their requests.

4.9.5 The information to be provided to data-subject/s shall include:

4.9.5.1 Information about the purpose of processing;
4.9.5.2 Contact details of the Data Protection Officer;
4.9.5.3 Information about the lawful basis of processing;
4.9.5.4 Information on where the personal data was obtained, if not directly from the data-subjects;
4.9.5.5 Information on how the data-subjects can withdraw consent;
4.9.5.6 Information about transfers of personal data (eg. from FSPs to Authority/CIB);
4.9.5.7 Information about recepients or categories of recepients of personal data; and
4.9.5.8 Information about the period for which the personal data is retained.

4.9.6 When an FSP is making use of automated decision -making using personal data, the data-subject/s shall be explicitly notified of the existence of automated decision -making.

4.9.7 A mechanism shall be provided to data-subject/s to withdraw their consent or objection to the automated/system generated decision making and requesting for manual intervention.

4.10 Incorporate guidelines in contracts with outsourced data processors

4.10.1 FSPs which are making use of third party vendors to perform personal data processing on their behalf shall have fol contracts addressing the requirements of data privacy and data protection. In such scenarios, the third party to whom the personal data processing is outsourced shall be treated as a ‘data processor’.

4.10.2 These contracts shall contain a minimum of the following:

4.10.2.1 Conditions for collection and processing;
4.10.2.2 Obligations to data-subject/s;
4.10.2.3 Measures to ensure privacy by design and default;
4.10.2.4 Disposal of files created during processing;
4.10.2.5 Return, transfer or disposal of personal data;
4.10.2.6 Personal data transmission controls;
4.10.2.7 Personal data sharing, transfer and disclosure;
4.10.2.8 Basis for data transfer between jurisdictions;
4.10.2.8.1 Countries and international organizations to which personal data can be transferred;
4.10.2.8.2 Records of personal data disclosure to third parties;

4.10.2.8.3 Notification to data-subjects in case of any legally binding requests for disclosure;
4.10.2.8.4 Legally binding personal data disclosure;
4.10.2.8.5 Disclosure of sub-contractors used for processing personal data;
4.10.2.8.6 Engagement of a sub-contractor to process personal data; and
4.10.2.8.7 Change of sub-contractor to process personal data.

4.11 Implement data breach management procedure

4.11.1 As a part of the overall infotion security incident management process, an FSP shall establish procedure for identification and recording of breaches of personal data;

4.11.2 As a part of establishment of the data breach management procedure, an FSP shall ensure coverage of all aspects of its operations including its branches and field operations;

4.11.3 An FSP shall establish procedure for notifications to the data-subject/s as well as to Authority regarding the data breach;

4.11.4 FSPs shall report personal data breaches to Authority within 48 hours of becoming aware of the data breach; and

4.11.5 Reporting of data breach to Authority shall be performed prior to any other public or media disclosure regarding the data breach by the FSP.

4.11.6 Data breach notifications shall clearly state:

4.11.6.1 A contact point where more infoAuthoritytion can be obtained;
4.11.6.2 A description and likely consequences of the breach;
4.11.6.3 A description of the breach including number of individuals concerned and number of associated records; and
4.11.6.4 Measures taken or planned to be taken.

4.11.7 Where a breach involving personal data has occurred, a record shall be maintained with sufficient information to provide a report for regulatory and/or forensic purposes such as:

4.11.7.1 A description of the incident;
4.11.7.2 The time/date of the incident;
4.11.7.3 The consequences of the incident;
4.11.7.4 Name of the reporter;
4.11.7.5 To whom the incident was reported;
4.11.7.6 The steps taken to resolve the incident; and
4.11.7.7 The fact that the incident ulted in unavailability, loss, disclosure or modification of personal data.

4.12 Updates to existing information security policy, if any

4.12.1 While the domain of information security pertains to ensuring confidentiality, integrity and availability, the domain of data protection requires FSPs resilience and traceability also to be ensured in addition to confidentiality, integrity and availability. Therefore, updates to existing information security policy and associated procedures will be essential/mandatory.

4.12.2 FSPs which have information security policies in place shall either develop separate privacy policies or augment information security policies by producing a statement concerning support for and commitment to achieving compliance with the Data Privacy and Data Protection Guidelines.

4.13 Implement technical measures to protect personal data

4.13.1 An FSP's information classification system shall explicitly consider personal data as a separate category of data;

4.13.2 For encryption of personal data at FSP and in transit, any of the encryption mechanisms specified in and approved for use as per "*NIST Special Publication 800-175B Revision 1 - Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms"* or its latest revision shall be used;

4.13.3 Encryption keys pertaining to personal shall be managed using Hardware Security Modules;

4.13.4 All internet communications involving personal data shall use latest Transport Layer Security version standard;

4.13.5 An FSP shall ensure that employees are made aware of the personal data definition and how to recognize information which is personal data;

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

4.13.7 All access to personal data by employees as well as by data processors appointed by the FSP 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;

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

4.13.9 If physical media is used for data transfer, a process shall be put in place to record incoming and outgoing media containing personal data. Such physical media transfer shall have an authorization procedure. Following shall be recorded regarding usage of physical media for data transfer type of media, authorized sender and receiver, date and time of entry or exit and number of physical media;

4.13.10 The FSP shall ensure that the use of mobile devices does not lead to compromise of personal data. To enable this, data loss prevention solutions are recommended to be installed on mobile devices used by employees or vendors to process personal data;

4.13.11 An FSP shall have a documented 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;

4.13.12 An FSP shall ensure that 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 organization's control;

4.13.13 Email 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;

4.13.14 Endpoint devices including laptops and PCs which are used for processing of personal data shall be secured with disk encryption and data leakage prevention tools;

4.13.15 Public cloud platforms may be used for storage and processing of personal data provided the public cloud platform meets the following requirements:

4.13.15.1 ISO 27001 – standard for information security management;

4.13.15.2 ISO 27017 – standard of practice for information security controls based on ISO/IEC 27002, specifically for cloud services; and

4.13.15.3 ISO 27018 - standard of practice for protection of personally identifiable information (PII) in public cloud services.

4.13.16 In all such cases of usage of public cloud platforms for processing personal data, a Virtual Private Cloud environment shall be set up on the public cloud.

4.14 Incorporate data protection by design and default in information systems

4.14.1 Data protection by design and by default helps ensure that the information systems fulfil data protection principles, and that the systems safeguard the rights of data-subjectss;

4.14.2 Minimum requirements for data protection which shall be considered in design and development of information systems are:

4.14.2.1 The system must only use personal data as planned, and all data must be deleted when storage is no longer lawful according to the legal basis for its processing or is no longer necessary to fulfil the intended purpose;

4.14.2.2 If the system is working as intended without identifiable data, no identifying data must be collected;

4.14.2.3 Personal data must be available to those authorised to use it when necessary;

4.14.2.4 The system must be developed with default settings that protect the rights of data-subjectss and safeguards privacy;

4.14.2.5 The system shall guide the user to the most privacy-friendly manner of use;

4.14.2.6 If the system operates based on consent, the consent must be explicit, voluntary, and informed;

4.14.2.7 The users must be able to withdraw consent at any time and as easily as they give it; and

4.14.2.8 The system must pseudonymise personal data when there is no longer any need to have identifying personal data and anonymise or delete personal data when the purpose of processing is fulfilled.

4.14.3 The system must contain safeguards preventing the linking of personal data about the data-subjects to other personal data in other systems, or to personal data collected for other purposes;

4.14.4 Personal data shall not be communicated, processed, or stored in plain text;

4.14.5 Database tables containing personal data shall have shorter storage times and a deadline for automatic deletion, while tables without personal data can be stored for longer. The duration of storage shall be consistent with the purpose for which the personal data was collected and the consent obtained from the data-subjects;

4.14.6 Personal data shall be gathered and processed in as aggregated or pseudonymised manner as possible to ensure the enforceability of the data-subject's rights;

4.14.7 All settings shall, by default, be configured in the most privacy-friendly setting. The user shall have to make a conscious choice to change any settings that would result in a less privacy-friendly configuration;

4.14.8 Testing must ensure that users only gain access to the information and functions they are authorised for;

4.14.9 Personal data shall not be used for testing purposes. Synthetic or false personal data shall be used. Where usage of personal data for testing is unavoidable, the necessity shall be reviewed and approved by the FSP's Data Privacy Management Committee;

4.14.10 Testing must verify that unauthorised attempts to acquire information are logged as security and personal data breaches; and

4.14.11 Penetration tests must be performed on newly developed software before release, or at regular intervals, to uncover vulnerabilities. Different testers shall be used every time a penetration test is performed.

4.15 Specific technical measures to be adopted for data warehousing and analytics

4.15.1 An FSP implementing data warehousing and analytics platforms need to adopt specific measures to protect data privacy and enable data protection;

4.15.2 The design and measures to enable privacy and data protection shall be reviewed and approved by the DPMC established by the FSPs;

4.15.3 Anonymization shall be used to mitigate three risks associated with personal data processing using a data warehousing and analytics platform, namely:

4.15.3.1 Singling out , which corresponds to the possibility to isolate some or all records which identify an individual in the dataset;

4.15.3.2 Linkability, which is the ability to link, at least, two records concerning the same data-subjects or a group of data-subjectss (either in the same database or in two different databases); and

4.15.3.3 Inference, which is the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes.

4.15.4 Anonymisation techniques shall be built into the design to enable data privacy;

4.15.5 Anonymisation itself shall be considered as a further processing of personal data;

4.15.6 One or more anonymization techniques shall be applied to a dataset based on the intended use and the level of risk associated with the dataset. These may include:

4.15.6.1 Randomization: a family of techniques that modifies the veracity of the data in order to remove the strong link between the data and the individual; and

4.15.6.2 Generalization: this approach consists of generalizing, or diluting, the attributes of data-subjectss by modifying the respective scale or order of magnitude (i.e. a region rather than a city, a month rather than a week).

4.15.7 Additional technical solutions may be provisioned in the data warehousing and analytics platform to:

4.15.7.1 Automatically crawl all the data as well as metadata and develop a personal data inventory; and

4.15.7.2 Enable automated data anonymization using various techniques and configurable rules by the data owner within the FSP.

5 Audit and Certification

5.1 The Authority may conduct onsite/offsite inspections to oversee the implementation of the guidelines by the FSPs.

5.2 Notwithstanding the above clause 5.1, the compliance of the FSP with these guidelines shall be audited by a third-party auditor on an annual basis. An annual compliance statement with respect to the data privacy and data protection guidelines shall be submitted to the Authority.

5.3 FSPs which have obtained ISO 27001:2013 certifications may consider obtaining ISO/IEC 27701:2019 – security techniques – extension to ISO/IEC 27001 certification.

6 General Provisions

6.1 Rules of Construction

6.1.1 Unless the context clearly otherwise requires, wherever used in the Guidelines, the singular includes the plural.

6.1.2 A pronoun in the masculine gender will be considered as including the feminine gender and vice versa unless the context indicates otherwise.

6.2 Interpretation

6.2.1 The Authority shall have the power to interpret any provision under this Guideline and its interpretation shall be final and binding upon all parties.

6.3 Transitional period

6.3.1 These guidelines shall come into force within a period of 6months from the date of issue of the guidelines.

6.4 Amendment

6.4.1 The additions, changes, or repeal of any provision of these Guidelines shall be made by the Board based on the recommendation of the Management.

7 Definitions

7.1 Authority: the term authority denotes as defined by the RMA Act of Bhutan 2010.

7.2 Data privacy is defined as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information".

7.3 Data protection is defined as "the implementation of appropriate administrative, technical or physical means to guard against unauthorized intentional or accidental disclosure, modification, or destruction of data".

7.4 FSPs means the Financial Service Providers regulated by the Authority in accordance with the Financial Services Act of Bhutan 2011.

7.5 Personal data processing is defined as "any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, modification, retrieval, consultation, use".

7.6 "Personal Data" or "Personal information" is defined as "any data or information which relates to a person who can be identified from that data".

7.7 Sensitive Personal Data or Information includes:

7.7.1 Password(s), location data and IP add FSPs;

7.7.2 financial infoAuthoritytion such as bank account, loan account, insurance account, credit card or debit card details;

7.7.3 physical, physiological and mental health condition;

7.7.4 medical records and history;

7.7.5 biometric information; and

7.7.6 other information that may be legally deemed to be private.

7.8 Provided that, any information that is freely available or accessible in public domain or available under any other existing national laws shall not be regarded as sensitive personal information."

7.9 Data-subjects means an identified or identifiable natural person, which is the subject of personal data.

7.10 Authority means as defined in the RMA Act of Bhutan 2010 or amendment thereof.

7.11 Financial Service Providers (FSPs) means an individual or an entity who/which is given the registration certificates or licenses by the Authority to provide the financial services to the public.

7.12 Data controller means natural or legal person, public authority, agency or any other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.

7.13 Data processor means natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller.

7.14 Data-subject’s consent means any freely given specific and informed indication of his/her wishes by which the data-subjects signifies his/her agreement to personal data relating to him/her being processed.

7.15 A virtual private cloud (VPC) is a secure, isolated private cloud hosted within a public cloud.

7.16 Destruction of data is an unplanned incident leading of loss of data due to failure of storage media, software errors, hacking attacks, etc.

7.17 Disposal of data is a planned activity at the last stage of the data lifecycle.

7.18 Identified person is one whose identity is already known.