

Data Protection Office

DATA PROTECTION IN THE MAURITIAN FINANCIAL SECTOR

Issued By: Data Protection Office

Date: October 2026

DATA PROTECTION

IN THE

MAURITIAN FINANCIAL SECTOR




SUCCESS
100.000.0
100,000,
PRODUCTION
70000
WEB
MEDIA
WORK GROUP
STORAGE
SERVER
SERVER
WORK STATION
SUCCESS
PRODUCT
RESULT
?
PROCCESS
TEAM
COMMUNITY
GROUP
IDEA

TABLE OF CONTENTS

1.0 Introduction 1

2.0 Governing legislations, regulations, policies and guidelines in the financial sector 3

3.0 Data Protection Office 4

4.0 Mauritius Data Protection Framework 4

4.1 Data Protection Act 2017 4

4.2 Data Protection (Fees) Regulations 2020 5

4.3 Data Protection (Designation, Tasks and Position of Data Protection Officers) Regulations 2026 5

4.4 Necessity and proportionality principles 5

4.5 Case Law 9

5.0 Powers of the Data Protection Commissioner 10

6.0 Personal data and special categories of personal data processed in the financial sector 12

7.0 Mandatory Registration and Appointment of Data Protection Officer 14

8.0 Principles relating to processing of personal data 15

8.1 Duties of controller 16

8.2 Collection of personal data 20

8.3 Conditions for consent 21

8.4 Notification of personal data breach and communication to the data subject 22

8.5 Duty to destroy personal data and retention period 23

8.6 Lawful processing 23

8.7 Special categories of personal data 24

8.8 Personal data of child 26

8.9 Security of processing 26

8.10 Record of processing operations 27

8.11 Data Protection Impact Assessment 28

8.12 Prior Authorisation and Consultation 29

8.13 Transfer of personal data 30

8.14 Rights of individuals 31

8.14.1 Right of access 31

8.14.2 Right to rectification, erasure or restriction 31

8.14.3 Right to object 32

9.0 Cloud Computing 32

10.0 Direct Marketing 34

11.0 Unlawful disclosure of personal data 35

12.0 Potential consequences of non-adherence to rules and regulations in the financial sector 36

13.0 Processing of personal data for anti-money laundering/ countering financing of terrorism or proliferation purposes 37

14.0 Fintech 44

14.1 The VAITOS Act 2021 47

14.2 Other initiatives 48

15.0 Artificial Intelligence 48

16.0 Management Companies 51

17.0 Some examples of oversight bodies in the financial sector 54

17.1 Ministry of Financial Services and Economic Planning 54

17.2 Bank of Mauritius 55

17.3 Financial Services Commission 103

17.4 Securities Exchanges 104

17.4.1 Stock Exchange of Mauritius Ltd 104

17.4.2 AFRINEX Limited 105

17.4.3 MINDEX Limited 105

17.5 Financial Intelligence Unit 105

17.6 Mauritius Revenue Authority (MRA) 105

17.7 Mauritius Financial Reporting Council (FRC) 106

17.8 The Financial Crimes Commission 106

17.9 Ombudsperson for Financial Services (OFS) 108

18.0 MOU with Bank of Mauritius 109

19.0 The Mauritius National Data Strategy and Data Governance 109

20.0 General Recommendations 110

21.0 Specific Recommendations for the Banking Sector 114

Non-Exhaustive Safeguards To Promote The Security of Personal Data (Annex 1) ... 119


11010
10101010
AI



1.0 Introduction

In an era of digital transformation and innovation, the financial industry finds itself at the crossroads of opportunities and risks. With the rapid growth of data-driven technologies, data privacy and protection have become intrinsic to the financial landscape. The collection, storage, and processing of massive amounts of personal data must be regulated to ensure that data protection meets financial stability with responsible data handling. Indeed, data protection is a fundamental requirement for resilient international financial centers (IFCs), not only to meet legal obligations but also to uphold their reputation and maintain the trust of clients, investors and the global financial community.

In this guide, the Data Protection Office will delve into the critical importance of data protection in the financial sector amidst data breaches and cyber threats having consequences which can be financially devastating and reputationally catastrophic. This guide will impart knowledge, best practices, and insights on data protection for institutions (public and private) in the financial sector. It is also aimed at providing guidance on the processing of personal data performed by financial entities in order to ensure compliance with data protection principles under the Data Protection Act 2017 (DPA) of Mauritius.

A financial institution, public or private, within the scope of the guide, relates to all organizations which handle financial personal data, directly or indirectly and not only to institutions which are defined as such under specific legislation/s.

Any controller[1] and/or processor[2] , whether it falls or not within the definition of a financial institution, which processes personal data relating directly or indirectly to the finances of the data subject, shall comply with the principles explained in this guide.

This guide is of a non binding legal nature. However, it is to be considered as an authoritative source providing legal clarity on the provisions of the Data Protection Act.

It has also been made after consultation with relevant stakeholders in the financial sector : - Bank of Mauritius (BoM), Financial Crimes Commission (FCC), Financial Services Commission (FSC) , Ministry of Financial Services and Economic Planning, Mauritius Fintech, Afrinex, Mauritius Finance, State Bank of Mauritius (SBM) Group and The Stock Exchange of Mauritius.

As part of Mauritius' endeavour to obtain an adequacy decision from the European Union, Cabinet agreed that the Ministry of Information Technology, Communication and Innovation conveys drafting instructions to the Attorney General's Office for amendments to be brought to the DPA. The principal areas under consideration are summarised below:

1 "controller" means a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing;

2 "processor" means a person who, or public body which, processes personal data on behalf of a controller;

(a) **Financial independence of the Data Protection Office** to make it financially self-sustaining.

(b) **Strengthening of enforcement powers** through the introduction of administrative fines for breaches of the DPA. This would provide a faster, proportionate and deterrent means of responding to non-compliance. The proposed approach would place greater emphasis on the issuance of enforcement notices, with administrative fines potentially following where an organisation fails to comply, rather than relying primarily on criminal penalties.

(c) **Establishment of a dedicated Prosecution Unit** to support effective enforcement. The Unit would strengthen the handling of offences, the collection and preservation of evidence, including digital evidence and the preparation of cases for prosecution before the courts.

(d) **Review of the investigative powers of the Data Protection Commissioner** to support more effective inquiries, inspections and enforcement action.

(e) **Written contracts between controllers, processors and subprocessors** would reinforce the requirement for clear written contractual arrangements throughout personal data-processing chains.

(f) **Direct appeals to the Supreme Court** for an aggrieved person to appeal directly to the Supreme Court, thereby providing an effective and appropriate avenue for judicial redress.

(g) **Introduction of a right to data portability** to obtain personal data which they have provided in a structured and usable format or to request that the data be transmitted to another service provider where technically feasible.

The Guide highlights the proposed reforms where appropriate in footnotes. Should there be any aspects relating to the financial sector not directly covered in this guide or new developments or future legislations in the financial sector, the relevant data protection principles explained will still apply in all relevant scenarios under the DPA.

2.0 GOVERNING LEGISLATIONS, REGULATIONS, POLICIES AND GUIDELINES IN THE FINANCIAL SECTOR

Mauritius has a well-developed financial sector with a robust regulatory framework designed to ensure stability and transparency. The regulatory framework comprises:

A. The various legislations enacted include the following:

The Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA), The Prevention of Terrorism Act (POTA) 2002, the Convention For The Suppression Of The Financing Of Terrorism Act 2003, Mutual Assistance In Criminal And Related Matters Act 2003, The Bank of Mauritius Act 2004, The Banking Act 2004, The National Payment Systems Act 2018 ("the NPS Act"), Companies Act 2001 (Corporate and Business Registration Department), Financial Reporting Act 2004, Financial Services Act 2007, The Mauritius Revenue Authority Act 2004, The Financial Crimes Commission Act 2023, Competition Act 2007, Virtual Asset and Initial Token Offering Services (VAITOS) Act 2021, Securities Act 2005, United Nations (Financial Prohibitions, Arms Embargo And Travel Ban) Sanctions Act 2019.

B. A comprehensive Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) Framework

Mauritius has demonstrated its commitment to combat money laundering, terrorism financing and proliferation financing by implementing a comprehensive AML/CFT/CPF regime.

Indeed, Mauritius has developed a strong and innovative legislative framework. In this respect, more than 60 pieces of legislation have been amended or introduced since 2018. These have played a crucial role in strengthening various aspects of its AML/CFT/CPF legal framework, reinforcing the nation's commitment to combat money laundering and the financing of terrorism. Mauritius is now amongst the top-tier jurisdictions which are "compliant" or "largely compliant" with all the 40 Financial Action Task Force (FATF) Recommendations.

Mauritius has also ratified and acceded to numerous international conventions, protocols, and treaties to express its commitment towards the international community to combat this scourge.

C. Various regulations/rules issued as follows:

Banking Regulations, the National Payment Systems (Authorisation and Licensing) Regulations 2021, Financial Intelligence and Anti-Money Laundering Regulations (FIAMLR) 2018, Financial Services Regulations, Insurance Regulations, Prevention of Terrorism (Special Measures) Regulations 2003, Protected Cell Companies Regulations, Securities Regulations, Stock Exchange Regulations, Guidance issued on AML/CFT/CPF Handbook.

3.0 Data Protection Office

The Data Protection Office is an independent public office, established by the Data Protection Act which implements the provisions of the DPA.

The Data Protection Office became operational since 16 February 2009. The office acts with complete independence and impartiality and is not subject to the control or direction of any other person or authority. The head of the office is known as the Data Protection Commissioner, who is a barrister of not less than 5 years' standing, as stipulated under the DPA.

The Data Protection Commissioner is assisted by such public officers as may be necessary. The Commissioner may delegate any investigating or enforcement power conferred on her by the DPA to an officer of the office or to a police officer designated for that purpose by the Commissioner of Police.

The mission of the office is to safeguard the processing of personal data in the present age of information and communication. The office lays down an annual report of its activities before the National Assembly each year. Annual reports can be downloaded on the link
https://dataprotection.govmu.org/Pages/Downloads/Annual-Reports.aspx

4.0 Mauritius Data Protection Framework

4.1 Data Protection Act 2017

The DPA governs the processing of personal data across all sectors, including personal data held by financial institutions. Mauritius enacted its first data protection legislation in 2004 which was proclaimed in 2009 and was later replaced by a new and improved legislation which came into force on 15 January 2018[3].

The rationale of the DPA is to provide for a new modernised legislation to strengthen the control and personal autonomy of data subjects over their personal data, in line with current relevant international standards. The DPA has been brought at par with international best practices including the European Union General Data Protection Regulation (GDPR) and the Council of Europe Convention 108 and 108+.

The DPA is available on the website link
https://dataprotection.govmu.org/Documents/DPA_2017_updated.pdf?csf=1&e=0rlrff

3 Please consult the Data Protection (Amendment) Act for the latest provisions.

Mauritius has taken various international commitments on data protection namely:

i. Mauritius is the first African State to ratify the Council of Europe Convention 108 since 01 October 2016.
ii. Mauritius is also the first non-european State to ratify Convention 108+ on 04 September 2020.
iii. Ratification of the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) on 14 March 2018.

4.2 Data Protection (Fees) Regulations 2020

The Data Protection (Fees) Regulations 2020[4] came into force on 01 August 2020 and caters for the fees payable under the Data Protection Act 2017 for:

i. The registration/ renewal of registration certificates as controllers and processors under sections 16(2) and 18(2) of the DPA on a three-year validity period.
ii. A certified copy of, or an extract from, an entry in the register under section 20(3)(b) of the DPA.
iii. The right of access for manifestly excessive requests under section 37(7) of the DPA.
iv. Appeal under section 52(4) of the DPA.

The Data Protection (Fees) Regulations 2020 is available on the website link https://dataprotection.govmu.org/Pages/The%20Law/152%20The%20Data%20Protection%20Fees%20Regulations%202020.pdf

4.3 Data Protection (Designation, Tasks and Position of Data Protection Officers) Regulations 2026

The Data Protection (Designation, Tasks and Position of Data Protection Officers)Regulations 2026, which come into operation on 1 January 2027, set out the requirements governing the designation, tasks and position of Data Protection Officers. Further details are provided in section 8.1 of this Guide.

4.4 Necessity and proportionality principles

Any law enforcement agency or regulatory body in the financial sector such as the Police, Financial Crimes Commission, amongst others, that can initiate enforcement actions, has to act in compliance with the DPA. They are defined as controllers under the DPA and will have to abide with the DPA subject to exceptions catered for under law, i.e., they have to abide to all provisions of the DPA that are not exempted. For example, a law enforcement agency has to comply with section 22(2)(e) of the DPA regarding the appointment of a data protection officer.

4 The fees are being reviewed. Please consult amendments to Data Protection (Fees) Regulations.

5 Please consult the Data Protection (Amendment) Act for the latest provisions.

Enforcement agencies may rely on the exemptions under section 44(1)(b)[5] of the DPA as required by law for prevention, investigation, detection, or prosecution of an offence suffice that they also meet the **necessity and proportionality** test in a democratic society, which are constitutional principles. If section 44 of the DPA has been breached, a data subject or the Data Protection Commissioner may apply for a Judge's order to protect the rights of individuals as per section 44(3) of the DPA.

"44. Exceptions and restrictions

(1) No exception to this Act shall be allowed except where it constitutes a necessary and proportionate measure in a democratic society for –

(a) subject to subsection (4), the protection of national security, defence or public security;
(b) the prevention, investigation, detection or prosecution of an offence, including the execution of a penalty;
(c) an objective of general public interest, including an economic or financial interest of the State;
(d) the protection of judicial independence and judicial proceedings;
(e) the protection of a data subject or the rights and freedoms of others; or
(f) issue of any licence, permit or authorisation during the COVID-19 period.

(2) The processing of personal data for the purpose of historical, statistical or scientific research may be exempt from the provisions of this Act where the security and organisational measures specified in section 31 are implemented to protect the rights and freedoms of data subjects involved.

(3) Where this section has been breached, a data subject or the Commissioner may apply for a Judge's order to protect the rights of individuals."

Necessity

Necessity requires a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive in comparison with other options to attain the same goal.

Test for necessity

The diagram below shows a series of steps that can be followed in order to ensure that any national security project complies with the necessity principle in relation to the objective(s) pursued.

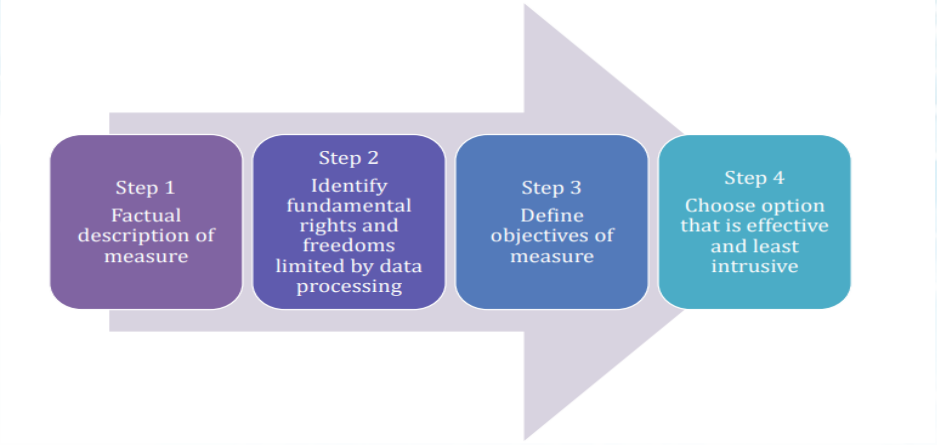


Diagram from EDPS (2017)[6]

A controller cannot proceed to the test of proportionality if the test of necessity fails.

Proportionality

Proportionality is a general principle in law which "restricts the authorities in the exercise of their powers by requiring a balance to be struck between the means used and the intended aim (or result reached)".

Test for proportionality

The diagram below provides the steps to be considered when determining whether any measure adopted for a project will be proportionate in relation to the objective(s) pursued.

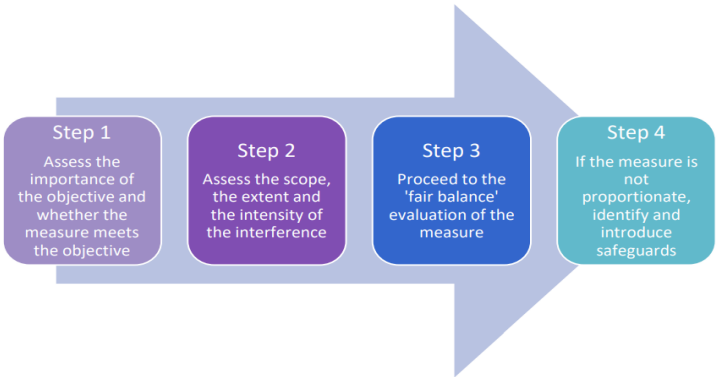


Diagram from EDPS (2019)[7]

Summary of the Data Protection Commissioner's Decision Based on Necessity and Proportionality Principles

The office investigated a complaint on the use of fingerprint for attendance of employees without their consent against their employer. The decision of the Data Protection Commissioner is outlined as follows:

By definition, any biometric collection of personal information has implications for privacy. These initiatives can also affect privacy in other ways, including affecting people's human dignity or expectations

6 European Data Protection Supervisor (2017), 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit'https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf (last visited on 21.05.2020)

7 European Data Protection Supervisor (2019),' EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data' https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf (last visited on 10.04.2020)

of anonymity. Therefore, before deploying a new biometric system with implications for privacy, an organisation should be able to clearly justify the prospective privacy intrusions. Many countries have rejected the imposition of fingerprint technology as a mandatory means to secure attendance. To guide this analysis, our office applies a four-part test which represents the international standards applicable at European level and is also reflected in a 1986 Supreme Court of Canada decision, R. v. Oakes. The test weighs the appropriateness of a potentially privacy-invasive measure in light of four questions:

"1. Is the measure demonstrably necessary to meet a specific need?
2. Is it likely to be effective in meeting that need?
3. Would the loss of privacy be proportionate to the benefit gained?
4. Is there a less privacy-invasive way of achieving the same end?"

Necessity: - Because there are privacy issues associated with all biometric systems, a proposed system should not be adopted simply because it appears to be the most convenient or cost-effective option. Instead, organisations proposing a biometric solution have to determine what specific problem they hope to solve, and whether the proposed system is essential for satisfying the need.

Effectiveness: - A second consideration is whether the proposed biometric system is likely to be effective in meeting the identified need. Different biometric characteristics have attributes that can make them more or less appropriate for specific purposes. For example, facial recognition systems are popular, in part because of the wide availability of passport photos and other facial images in databases - not to mention pictures that can be captured covertly. And yet, because facial features are neither permanent nor unique, facial recognition systems cannot be counted on to identify people with a high degree of certainty.

Proportionality: - All biometric systems involve some loss of privacy because personal information is stored and used for authentication. In analysing the appropriateness of a proposed biometric measure, a third consideration is whether the resulting loss of privacy would be proportional to any anticipated benefit. If the benefit is relatively minor, such as an increase in convenience or a slight cost saving, then the loss of privacy may not be appropriate.

In testing for proportionality, organisations should bear in mind that certain biometric characteristics are more privacy-sensitive than others. Fingerprints, for example, are especially sensitive because they can be collected covertly, linked across applications and databases, and used in law enforcement. Any proposal to use fingerprints in a biometric initiative would, therefore, have to promise extraordinary benefits.

It was thus proven beyond reasonable doubt, applying the above principles that the use of fingerprints for attendance purposes by the employer in this case regarding those who have not expressly consented to it cannot be deemed to be in strict compliance with the Data Protection Act and cannot fall within the purview of the employment contract.

The fact that many public and/or private organisations are using fingerprinting technology for attendance purposes because it represents a cost-effective and convenient means to record attendance should not

potentially and materially undermine in any way whatsoever the right of the data subject not to consent to this method and further be prejudiced or discriminated for not conforming to it. This case illustrates the modern flow of sacrificing privacy rights at the altar of technology without understanding and measuring the negative consequences which technology can also give rise to. Technology is certainly to be used but not abused. The matter was thus referred to the police for prosecution against the employer's Chief Executive Officer.

4.5 Case Law

(i) *In Stanford Asset Holdings Ltd (SAH) and another (Appellants) v AfrAsia Bank Ltd (Respondent) (Mauritius),* as a result of an alleged fraud, over USD 11 million was transferred from an account belonging to Stanford Asset Holding Limited at AfrAsia Bank Limited ("AfrAsia") to the bank account of Key Stone Properties Limited ("Key Stone"). Approximately USD 4 million remained in the account of Key Stone and was frozen. The remainder was transferred into the accounts of unknown third parties. The Appellants brought an application seeking to compel AfrAsia to disclose information about the identity of the recipients of any of the allegedly misappropriated funds. The objective of their application was to trace, freeze and recover the funds.The Supreme Court of Mauritius refused the relief sought, setting aside the Appellants' application. The Appellants have been granted final leave to appeal to the Judicial Committee of the Privy Council.The Judicial Committee of Privy Council concluded that the appeal should be allowed, and it ordered the disclosure of information sought by the appellants. The Privy Council emphasized that despite differences in the analysis of section 64 of the Banking Act 2004, the outcomes were not expected to differ substantially. The Bank was directed to disclose, in the form of an affidavit within seven days, the full names, addresses, account numbers and particulars of the recipients of the USD 11 Million transferred from SAH's account.

(ii) *In Michaud v. France,* the applicant, a French lawyer, challenged his obligation under French law to report suspicions regarding possible money-laundering activities by his clients. The ECtHR observed that requiring lawyers to report information concerning another person, which had come into their possession through their professional exchanges, to the administrative authorities constituted an interference with the lawyers' right to respect for their correspondence and private life under Article 8 of the ECHR, as that concept covered activities of a professional or business nature. However, the interference was in accordance with the law and pursued a legitimate aim, namely the prevention of disorder and crime. Given that lawyers are subject to the obligation to report suspicious activity only under very specific circumstances, the ECtHR held that this obligation was proportionate. It concluded that there had not been a violation of Article 8 (right to privacy).

(iii) *In M.N. and Others v. San Marino,* the applicant, an Italian citizen, concluded a fiduciary agreement with a company under investigation. The company was subject to the search and seizure of copies of (electronic) documentation. The applicant filed a complaint with the San Marino court, claiming that there was no link between him and the alleged crimes. However, the court declared his complaint inadmissible, as he was not an "interested party". The ECtHR held that the applicant had been at a

significant disadvantage regarding judicial protection compared to an "interested party", yet his data were still subject to the search and seizure operations. Thus, the Court held that Article 8 was violated (right to privacy).

(iv) *In G.S.B. v. Switzerland,* the applicant's bank account details were sent to the US tax authorities on the basis of the administrative cooperation agreement between Switzerland and the US. The ECtHR held that transmission was not in violation of Article 8 ECHR because the interference with the applicant's right to privacy was prescribed by law, pursued a legitimate aim, and was proportionate to the public interest at stake[8].

5.0 Powers of the Data Protection Commissioner

The Data Protection Act provides a wide range of powers to the Data Protection Commissioner in carrying out her functions and enforcing the provisions of the DPA. The powers are stipulated under sections 6, 7, 8, 9, 10, 11, 13, 32 and 46[9] of the DPA and are as follows:

i. Investigation of complaints (section 6 of DPA)
Where a complaint is made to the Commissioner that the DPA or any regulations made under it, has or have been, is or are being, or is or are about to be, contravened, the Commissioner shall –

(a) investigate into the complaint or cause it to be investigated by an authorised officer, unless she is of the opinion that the complaint is frivolous or vexatious; and

(b) where he is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the complaint, notify, in writing, the individual who made the complaint of his decision in relation to it so that the individual may, where he considers that he is aggrieved by the decision, appeal against it under section 51 of the DPA[10] .

ii. Power to require information (section 7 of DPA)
The Data Protection Commissioner may, by written notice served on a person, request from that person such information as is necessary or expedient for the discharge of the functions prescribed under the DPA subject to section 26 of the Bank of Mauritius Act, section 64 of the Banking Act, section 83 of the Financial Services Act, section 30 of the Financial Intelligence and Anti-Money Laundering Act and section 161 of the Financial Crimes Commission Act[11].

Where the information requested by the Commissioner is stored in a computer, disc or cassette, or on microfilm, or preserved by any mechanical or electronic device, the person named in the notice must produce or give access to the information in a form in which it can be taken away and in which it is visible and legible.

iii. Preservation order (section 8 of DPA)

8 Handbook on European data protection law , 2018 edition, page 243 – 244 https://www.jcpc.uk/cases/jcpc-2023-0011.html

9 Please consult the Data Protection (Amendment) Act for the latest provisions.

10 Please consult the Data Protection (Amendment) Act for the latest provisions.

11 Please consult the Data Protection (Amendment) Act for the latest provisions.

The Data Protection Commissioner may apply to a Judge in Chambers for a preservation order for the expeditious preservation of data, including traffic data, where he/she has reasonable ground to believe that the data are vulnerable to loss or modification.

iv. Enforcement notice (section 9 of DPA)

Where the Data Protection Commissioner is of the opinion that a controller or a processor has contravened, is contravening or is about to contravene the Data Protection Act, the Commissioner may serve an enforcement notice on him requiring him to take such steps within such period as may be specified in the notice.

v. Power to seek assistance (section 10 of DPA)

For the purpose of gathering information or for the proper conduct of any investigation under the DPA, the Data Protection Commissioner may seek the assistance of such person or authority as he/she thinks fit and that person or authority may do such things as are reasonably necessary to assist the Commissioner in the discharge of his/her functions.

vi. Power of entry and search (section 11 of DPA)

An authorised officer may enter and search any premises for the purpose of discharging any function or exercising any power under the Data Protection Act upon the production of a warrant. Subject to section 26 of the Bank of Mauritius Act, section 64 of the Banking Act, section 83 of the Financial Services Act, section 30 of the Financial Intelligence and Anti-Money Laundering Act and section 161 of the Financial Crimes Commission Act[12], an authorised officer may, on entering any premises:

a) request the owner or occupier to produce any document, record or data;
b) examine any such document, record or data and take copies or extracts from them;
c) request the owner of the premises entered into, any person employed by him, or any other person on the premises, to give to the authorised officer all reasonable assistance and to answer all reasonable questions, orally or in writing.

Furthermore, where any information requested by the authorised officer is stored in a computer, disc or cassette, or on microfilm, or preserved by any mechanical or electronic device, the person to whom the request is made must produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

vii. Delegation of power by Data Protection Commissioner (section 13 of DPA)

The Data Protection Commissioner may delegate any investigating or enforcement power conferred on him/her by the Data Protection Act to an officer of the office or to a police officer designated for that purpose by the Commissioner of Police.

12 Please consult the Data Protection (Amendment) Act for the latest provisions.

viii. Prior security check (section 32 of DPA)

Where the Data Protection Commissioner is of the opinion that the processing or transfer of data by a controller or processor may entail a specific risk to the privacy rights of data subjects, she may inspect and assess the security measures taken under section 31 prior to the beginning of the processing or transfer. The Commissioner may, at any reasonable time during working hours, carry out further inspection and assessment of the security measures imposed on a controller or processor under section 31 of the DPA.

ix. Compliance audit (section 46 of DPA)

The Commissioner may carry out periodical audits of the systems of controllers or processors to ensure compliance with the Data Protection Act.

x. Power to require Data Protection Impact Assessment (DPIA)

Controllers must carry out a DPIA for high risk processing operations and submit it to the Data Protection Office.

xi. Certification

Section 48(1) of the DPA stipulates that:

"The Office may, in order to encourage compliance of processing operations by controllers and processors with this Act, lay down technical standards for data protection certification mechanisms and data protection seals and marks."

The purpose of certification is to enhance transparency and compliance with the DPA and is voluntary.

It has been introduced to help controllers or processors to demonstrate accountability and compliance with the Act, build confidence and trust in the organization, as well as with the wider public, allow data subjects to quickly assess the level of data protection of relevant products and services, and give legal certainty for cross-border data transfers.

Any organisation willing to be certified must fill the certification form online on the eDPO system.

6.0 Personal Data and Special Categories of Personal Data Processed in the Financial Sector

Under section 2 of the DPA, personal data is defined as any information relating to an identified or identifiable individual, in particular 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.

The Data Protection Act applies to both physical and electronic form of documents containing personal data.

The following are examples, amongst others, of personal data processed by financial institutions:

- Name of individuals (such as customers, employees, suppliers, contractors, guarantors, directors, shareholders, authorised signatories, amongst others)
- Date of birth
- National Identity Card Number
- Citizenship status
- Residential Address
- Phone numbers
- Email addresses
- Bank account numbers
- Credit/debit card numbers
- Investment account details
- Income and employment information
- Records of purchases, withdrawals, deposits, and transfers
- Payment history
- Insurance policy details
- Mortgage and loan applications
- Utility bills or other proof of address documents
- KYC (Know Your Customer) Information

Special categories of personal data, in relation to a data subject, means personal data pertaining to –

(a) his racial or ethnic origin;
(b) his political opinion or adherence;
(c) his religious or philosophical beliefs;
(d) his membership of a trade union;
(e) his physical or mental health or condition;
(f) his sexual orientation, practices or preferences;
(g) his genetic data or biometric data uniquely identifying him;
(h) the commission or alleged commission of an offence by him;
(i) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings; or
(j) such other personal data as the Commissioner may determine to be sensitive personal data;

The following are examples, amongst others, of special categories of personal data processed by financial institutions:

- Health Data
- Biometric Data
- Criminal Records

7.0 Mandatory Registration and Appointment of Data Protection Officer

Section 2 of the DPA further provides for the following definitions:

"processing" means an operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"controller" means a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing;

"processor" means a person who, or public body which, processes personal data on behalf of a controller;

Under section 14 of the DPA, subject to section 44, no person shall act as controller or processor unless he or it is registered with the Commissioner. Therefore, all financial institutions must register with the Data Protection Office.

A registration certificate issued is valid for a period of 3 years and under section 18 of the DPA, the holder of a registration certificate may apply for the renewal of the certificate not later than 3 months before the date of its expiry.

Financial institutions must submit their registration or renewal on the online portal of the Data Protection Office available at the following link:
https://dataprotection.govmu.org/Documents/Pages/eDPO.aspx.

The following guides are available on the office website to facilitate registration and renewal:

- Basic Steps to follow for using the eDPO system
- Data Protection Office's Portal User Guide
- Guide on registration and renewal

8.0 Principles relating to processing of personal data

Financial institutions, as controllers and/or processors under the DPA, have a legal obligation under section 21 of the DPA to ensure that the following principles are being observed in the processing of personal data:

- Transparent and lawful processing: Personal data must be processed lawfully, fairly and in a transparent manner in relation to any data subject. It can be achieved by applying the following rules:
  * 'lawful' by meeting the conditions under section 28 of the DPA,
  * fair' by informing data subjects of any potential risks to ensure that the processing does not have unforeseeable negative effects,
  * transparent' by informing data subjects on the requirements for processing (section 23 of the DPA)

- Purpose Limitation: Personal data must be collected for explicit, specified and legitimate purpose(s) and not further processed in a way incompatible with those purpose(s).

- Data minimisation: Personal data must be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed. Excessive data must not be processed. For example, when completing an application form for the opening of a bank account, the mandatory requirement for an individual to provide the names of other members of the individual's family to the bank (other than in the context of providing an emergency contact) would be excessive in relation to the purpose of opening an account.

- Accuracy: Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- Storage limitation: Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the personal data are processed.

- Data subjects' rights: Personal data must be processed in accordance with the rights of data subjects.

8.1 Duties of controller

Financial institutions must adopt policies and implement appropriate technical and organisational measures to demonstrate that the processing of personal data is performed in accordance with section 22 of the DPA.

The measures mentioned above must include the following:

- Implementing appropriate data security and organisational measures.
  Upon the development of policies and procedures, financial institutions are required to put in place appropriate training and/or awareness mechanisms for their employees, ensuring a clear understanding of the relevance of these policies and procedures to their respective roles.

- Keeping a record of all processing operations as per the template provided on the website of the Data Protection Office on the link
  https://dataprotection.govmu.org/Pages/Home%20-%20Pages/Document%20%26%20Forms/Records-of-processing-operations.aspx

- Performing data protection impact assessments whenever required on high-risk operations as per the guideline provided on the website of the Data Protection Office on the link
  https://dataprotection.govmu.org/Pages/Home%20-%20Pages/Document%20%26%20Forms/Data-Protection-Impact-Assessment-and-High-Risk-Operations.aspx

- Complying with requirements of prior authorisation and consultation as per section 35 of the DPA.

- In accordance with section 22(2)(e) of the DPA, financial institutions must designate a data protection officer responsible for data protection compliance. Regulations for Data Protection Officers have been enacted to strengthen and clarify the roles of data protection officers as elaborated below:

Regulations	Explanations:
1	These regulations may be cited as the Data Protection (Designation, Tasks and Position of Data Protection Officers) Regulations 2026.
2	In these regulations: "Act" means the Data Protection Act; "data protection officer" means the person designated under regulation 3(1); "lead data protection officer" means the person designated under regulation 3(3).
3	(1) Subject to paragraph (2) and regulations 5 and 6, every controller shall, for the purpose of section 22(2)(e) of the Act, designate, from a staff member of the organisation, a data protection officer for the purpose of carrying out the tasks specified under regulation 4. (2) The controller may designate more than one data protection officer having regard to its organisational structure, size and scale, complexity and sensitivity of the processing of such personal data. (3) Where the controller has appointed more than one data protection officer, the controller shall designate a lead data protection officer, who shall be the primary point of contact with the Office and the data subjects. (4) The controller shall: a. communicate the particulars of the data protection officer or lead data protection officer to the Office, within 14 days of such designation; and b. where any change occurs to the identity or particulars of the officers referred to in sub-paragraph (a), notify the Office of such change and provide their updated particulars within 14 days of such change.

4	The data protection officer or lead data protection officer shall: (a) carry out the data protection functions in the organisation, namely: (i) ensuring that personal data is processed by the organisation in accordance with the principles of data processing; (ii) protection of data subject rights; (iii) data protection impact assessment; (iv) ensuring that security and organisational measures are implemented; (v) maintaining the record of processing operations; (vi) notification to the Office and communication to the data subjects of data breaches; (vii) the registration of the organisation as controller or processor or both with the Office; (viii) facilitating the investigation by the Office of breaches of the Act by the controller; (ix) inform and advise the controller, processor, or employees who carry out processing of personal data within the organisation, of their obligations under the Act; (x) monitor compliance of the organisation with the Act and its data protection policies, including the assignment of responsibilities, the conduct of internal audits, awareness raising and training of employees involved in processing operations at such intervals as may be required; (xi) assist the Office in the carrying out of compliance audits under the Act; (xii) facilitate security checks and inspections by the Office; (xiii) provide advice, where requested by the controller with regard to data protection impact assessments; (xiv) provide advice and issue recommendations to the controller to ensure that Parts II, III IV, V, VI and VII of the Act are complied with; (xv) cooperate with the Commissioner as and when required; (xvi) act as the liaison officer with the Commissioner on matters relating to processing of personal data; (xvii) perform any other such tasks which may involve data protection compliance within the organisation; and (xviii) in the performance of the above duties, report to the highest management level of the organisation.

5	The data protection officer or lead data protection officer shall be designated by the controller on the basis of his professional qualifications and, in particular– (a) expert knowledge of data protection laws and practices applicable in Mauritius; (b) the proven ability to fulfil the tasks specified in regulation 4; (c) an in-depth understanding of the operational requirements of the organisation and the specific regulatory environment of its business sector; and (d) evidence of certification issued by: (i) the Office, following the successful completion of the training conducted by the Office and on payment of such fees, as the Office may determine, for the training; or (ii) a duly registered and accredited training institution approved by the Office for its expertise in data protection laws.
6	The controller shall – (a) ensure that the duties assigned to the data protection officer or lead data protection officer are compatible with the duties referred to under regulation 4 and do not result in any conflict of interest; (b) ensure that the data protection officer or lead data protection officer is involved, in a timely manner, in all issues related to the protection of personal data; (c) adequately support the data protection officer or the lead data protection officer in the performance of his duties under regulation 4 by providing necessary resources and training to the data protection officer or lead data protection officer; (d) ensure that the data protection officer or lead data protection officer carries out his functions in an independent manner without any unlawful interference; (e) not dismiss or suspend or otherwise penalise a data protection officer or lead data protection officer for lawfully performing the duties under these regulations.
7	(1) Subject to paragraph (2), the data protection officer or lead data protection officer shall not be personally liable for any non-compliance by the controller with the provisions of the Act. 2) The data protection officer or lead data protection officer may be held accountable by the organisation for any failure to perform the duties and tasks specifically assigned to him under regulation 4.
8	The controller shall publish the contact details of the data protection officer or lead data protection officer at a conspicuous place on its premises or, where applicable, on the website of the controller. (1) A data subject may contact the data protection officer or lead data protection officer in respect of any matter related to the processing of his personal data or the exercise of his rights under the Act.
9	Any person who contravenes regulations 3(4) or 8(1) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100, 000 rupees and to imprisonment for a term not exceeding 5 years. These regulations shall come into operation on 1 January 2027.

Regulation 3(2) further permits an organisation to designate several Data Protection Officers, having regard to its structure, size, scale of activities, complexity of operations and the sensitivity of the personal data processed. Where several Data Protection Officers are designated, regulation 3(3) requires the appointment of a Lead Data Protection Officer who will act as the principal point of contact with the Data Protection Office and with data subjects.

The certification programme conducted by the Data Protection Ofiice comprises of online training, face-to-face training, a written examination and, upon successful completion, the issuance of a certificate by the Office.

The Guidance Notes on Data Protection Officers further provide practical guidance on the designation, training and certification of Data Protection Officers. They also address a number of queries and practical issues received by the Data Protection Office in relation to the implementation of the Data Protection Officer requirements.

Financial institutions must also implement suitable mechanisms to verify the effectiveness of the technical and organisational measures implemented as per section 22(3) of the DPA.

8.2 Collection of personal data

Financial institutions must ensure that the collection of personal data: -

- is done for a lawful purpose connected with a function or activity of the organisation; and
- is necessary for that purpose.

Financial institutions as controllers must comply with section 23(2) of the DPA when collecting personal data. The information provided must be clear and effective to individuals to promote transparency and compliance with data protection principles. Clear communication with data subjects, explaining the organisation's data processing practices, legal basis for processing, data retention policies, data subject rights, and other relevant information are essential. Financial institutions must further be coherent in application forms on the contractual terms and conditions and/or privacy notices about the purpose(s) for which they collect and hold personal data of a customer. Financial institutions must indicate in their application forms whether the individual fields of personal data requested are mandatory.

It is important that the information provided are in plain language that is easily understandable by any person when describing data collection practices. Legal jargon or technical terms should be avoided whenever possible. It is also essential to periodically review and update the information to ensure ongoing compliance with changing laws and practices.

The required information should also be provided and updated at appropriate times. Notifications may be displayed on websites or through direct communication channels and must be accessible to all individuals. Employees must also be trained to adhere to the organisation's data protection information requirements and policies. Financial institutions should ensure that customer-facing staff are knowledgeable about data protection and can address customer inquiries.

If a financial institution uses third-party services or partners that collect personal data on its behalf, it is recommended that financial institutions clarify how data subjects can access the data protection information requirements of these third parties.

A financial institution may sometimes record by law the contents of certain phone calls made with regard to certain orders and instructions by customers, because the recording may be used to provide proof of and defend a judicial claim. This is in line with specific sector-related regulations, in particular those applying to stock exchange orders for example. It is important to note that the data subject must be informed via the agreement it has with the organisation about the recording in accordance with section 23 of the DPA under such circumstances.

8.3 Conditions for consent

The DPA defines consent as *"any freely given specific, informed and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which he signifies his agreement to personal data relating to him being processed."*

The elements of a valid consent:

- 'freely given' – a data subject must have the choice to accept or refuse to the processing of his/her personal data;
- 'specific' – consent of the data subject must be given in relation to "one or more specific" purposes and that a data subject has a choice in relation to each of them. The requirement that consent must be 'specific' aims to ensure a degree of user control and transparency for the data subject.
- 'informed' – Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make an accurate judgment, understand what they are agreeing to, and for example exercise their right to withdraw their consent.
- 'unambiguous indication' - by statement or a clear affirmative action. Implied form of actions by the data subject must be avoided such as pre-ticked opt-in boxes.

Financial institutions should clearly explain the purpose(s) for which consent is sought using clear and unambiguous language that is easy for individuals to understand. However, consent is one of the lawful basis for processing under the DPA. Other conditions under sections 28 or 29 of the DPA may be relied upon for processing.

When the lawful ground of processing is based on consent, then the document seeking consent should be as detailed as possible to include all potential scenarios which are consent-based. Bundled or vague consent requests should be avoided. Opt-in mechanisms (e.g., checkboxes) should be provided to allow individuals to actively indicate their consent. In accordance with section 24 of the DPA, financial institutions must:

- Obtain, maintain and be able to demonstrate valid consent and
- Ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time.

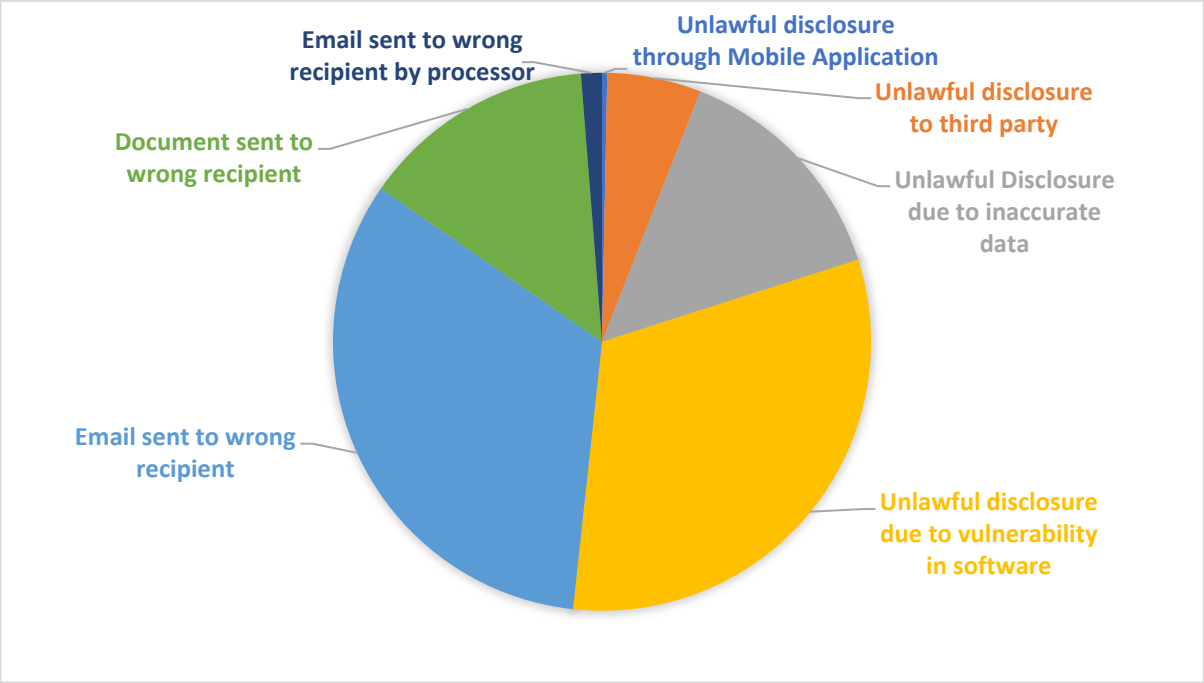
8.4 Notification of personal data breach and communication to the data subject

Section 25 of the DPA stipulates that in case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Commissioner.

Examples of personal data breaches are:

a) A hacker obtains unauthorised access to a financial institution's database to steal credit card information.
b) An employee within a financial institution who intentionally leaks sensitive client data to third party.
c) An attacker who intercepts the email addresses of clients due to vulnerabilities and security flaws in a mobile banking app.
d) An e-mail containing personal data sent to incorrect e-mail addresses.
e) Unauthorized disclosure of sensitive/confidential data.

For the cumulative period of 2023 to March 2026, the Data Protection Office received personal data breach notifications from financial institutions for the following categories:



Financial institutions must submit their notifications for personal data breaches on the online portal of the Data Protection Office available at the following link:
https://dataprotection.govmu.org/Pages/eDPO.aspx.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the controller shall, after the notification referred to in section 25, communicate the personal data breach

to the data subject without undue delay in accordance with section 26(1) of the DPA, in clear language and also set out the required information and recommendations under sections 25 and 26 (2).
As per section 26(3) of the DPA, the communication of a personal data breach to the data subject shall not be required where –

a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the breach, in particular, those that render the data unintelligible to any person who is not authorised to access it, such as encryption;
b) the controller has taken subsequent measures to ensure that the high risk to the rights and freedoms of the data subject referred to in subsection (1) is no longer likely to materialise; or
c) it would involve disproportionate effort and the controller has made a public communication or similar measure whereby data subject is informed in an equally effective manner.

8.5 Duty to destroy personal data and retention period

Section 27 of the DPA requires all controllers to destroy personal data as soon as is reasonably practicable where the purpose for keeping personal data has lapsed and to notify any processor holding the data.

The DPA does not specify the retention periods for keeping personal data. The retention period has to be determined by the financial institution taking into consideration the purpose(s) for keeping the data and such other applicable laws.

Personal data that are physically archived are still subject to the provisions of the DPA until they are destroyed or completely anonymised.

8.6 Lawful processing

As per section 28(1)(a) of the DPA, consent of individuals concerned is one of the lawful grounds on which personal data processing may be based. However, consent of the individuals is not required if the processing falls under **any one** of the exceptions of section 28(1)(b)[13].
(1) No person shall process personal data unless –
(a) the data subject consents to the processing for one or more specified purposes; **or**
(b) the processing is necessary –
(i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract; **or**
(ii) for compliance with any legal obligation to which the controller is subject; **or**
(iii) in order to protect the vital interests of the data subject or another person; **or**
(iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; **or**
(v) he performance of any task carried out by a public authority; **or**
(vi) the exercise, by any person in the public interest, of any other functions of a public nature;**or**
(vii) for the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; **or**
(viii) or the purpose of historical, statistical or scientific research.

13 Please consult the Data Protection (Amendment) Act for the latest provisions.

The lawful grounds under sections 28(1)(a), 28(1)(b)(i) to (viii) are non-cumulative, implying that each provision within these subsections is distinct and operates on its own and does not build upon the others.

Some non-exhaustive examples to illustrate the application of section 28 of the DPA are as follows:

-- *Lawful ground: consent*
An individual who provides his consent to receive marketing offers from a financial institution for new financial products or services, such as credit cards, loans, or investment opportunities.

-- *Lawful ground: for the performance of a contract with the data subject*
Where an individual enters into an agreement with a bank in order to secure a loan or open a bank account.

-- *Lawful ground: for compliance with any legal obligation to which the controller is subject*
Financial institutions in Mauritius are obligated by law under FIAMLA to identify and report certain transactions to the Financial Intelligence Unit of Mauritius (FIU) as part of their AML/CFT/CPF compliance obligations. Hence, section 28(b)(ii) of the DPA will apply, i.e., for compliance with any legal obligation to which the controller is subject and thus consent of individuals is not required for this type of processing.

-- *Lawful ground: legitimate interests*
The factsheet on legitimate interests published by this office provides examples which is available at the following link
https://dataprotection.govmu.org/Documents/Factsheet%20legitimate%20interest.pdf

Any person who contravenes section 28(1)[14] of the DPA shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 5 years. Accordingly, financial institutions should ensure that their processing operations are lawful.

8.7 Special categories of personal data

Special categories of personal data, often referred to as sensitive data, are subject to stricter data protection and privacy regulations due to their sensitive nature. Section 29 of the DPA provides the following:

Special categories of personal data shall not be processed unless[15] –

(a) section 28 applies to the processing; ***and***

(b) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for- profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; ***or***

(c) the processing relates to personal data which are manifestly made public by the data subject; ***or***

14 Please consult the Data Protection (Amendment) Act for the latest provisions.

15 Please consult the Data Protection (Amendment) Act for the latest provisions.

(d) the processing is necessary for –

(i) the establishment, exercise or defence of a legal claim; ***or***

(ii) the purpose of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to a contract with a health professional and subject to the conditions and safeguards referred to in subsection (2); ***or***

(iii) the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; ***or***

(iv) protecting the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.

(2) The personal data referred to in subsection (1) may be processed for the purposes referred to in subsection (1)(d)(ii) where the data are processed by or under the responsibility of a professional or other person subject to the obligation of professional secrecy under any enactment.

The lawful grounds under subsections 29(1)(b) to 29(1)(d) are non-cumulative, implying that each provision within these subsections is distinct and operates on its own and does not build upon the others.

For example, processing special categories of personal data by a financial institution can occur when it is necessary for the establishment, exercise, or defense of a legal claim. The following scenario may be considered:

XYZ, an insurance company, is involved in a legal dispute with one of its policy holders, Mr A. The latter has filed a lawsuit against XYZ , claiming that XYZ wrongfully denied his disability insurance claim.

In the course of defending itself against this legal claim, XYZ needs to process special categories of personal data. In this case, the special categories of personal data involved could be medical information about Mr A's health and disability status. This data is essential for XYZ to assess the validity of Mr A's claim and defend itself in Court.

The lawful ground for processing this special category of personal data (i.e., health-related data) in this scenario is the establishment, exercise, or defense of a legal claim. According to data protection regulations, processing sensitive data is generally prohibited unless there is a specific legal basis for doing so, and defending against legal claims is one such basis.

8.8 Personal data of child

According to section 30[16] of the DPA, no person shall process personal data of a child below the age of 16 years unless the child's parent or guardian provide his/her consent. Secondly, where the personal data of a child below the age of 16 years is involved, a financial institution shall make every reasonable effort to verify that consent has been given or authorised, taking into account available technology.

Section 30 needs to be interpreted together with section 28(1)(a) of the DPA.

8.9 Security of processing

Pursuant to section 31 of the DPA, appropriate technical and organisational measures should be implemented for the protection of personal data whether it is stored in manual or automated data filing systems against unauthorised access, alteration, disclosure, accidental loss and destruction. The financial institutions are not exempt from these security obligations. Financial institutions should take reasonable steps to store personal data securely such that it is not stolen, lost or used deliberately or accidentally.

Financial institutions should consider their:

- Technical (electronic) security
  This includes log-on controls, firewalls, encryption, remote wiping facilities, suitable back-ups, multifactor authentication and proper disposal of old equipment. Consider both office computer systems and any mobile devices used out of the office (e.g. smartphones, laptops or tablets). Organisations are recommended to establish their BYOD (Bring Your Own Devices) guidance policy if employees are allowed to use their own mobile devices.

- Physical security
  This includes locks, alarms, supervision of visitors, disposal of paper waste, and how to prevent notebooks and mobile devices being lost or stolen when staff are out of the office.

- Management and organisational measures
  For example, ensuring that a person with the necessary authority and resources has a day to day responsibility for ensuring information security, and putting in place robust policies and procedures, including a breach management plan.

- Staff training and supervision
  Organisations should train new staff to a level appropriate to their position (including regular refresher training) on key security risks, procedures and responsibilities.

Section 31 also states at subsection 4[17] that where a controller is using the services of a processor –

(a) he or it shall choose a processor providing sufficient guarantees in respect of security and organisational measures for the purpose of complying with subsection (1); and

(b) the controller and the processor shall enter into a written contract which shall provide that –

16 Please consult the Data Protection (Amendment) Act for the latest provisions.

17 Please consult the Data Protection (Amendment) Act for the latest provisions.

(i) the processor shall act only on instructions received from the controller; and
(ii) the processor shall be bound by obligations devolving on the controller under subsection (1).

For instance, if a financial institution is using the service of a cloud provider for its processing activities, section 31 (4) will apply.

In determining the appropriate security measures, in particular, where the processing involves the transmission of data over an information and communication network, a financial institution shall have regard to –

(a) the state of technological development available;
(b) the cost of implementing any of the security measures;
(c) the special risks that exist in the processing of the data; and
(d) the nature of the data being processed.

For example, some financial institutions comply with the following commonly used standards to promote trust and confidence in their processing operations:

- Payment Card Industry Data Security Standard (PCI DSS): PCI DSS is a security standard developed by major credit card companies to protect payment card data during transactions. It sets security requirements for organisations that handle credit card information.
- ISO 27001: The International Organization for Standardization (ISO) publishes ISO 27001, which is a globally recognised standard for information security management systems (ISMS). Financial institutions use ISO 27001 to protect sensitive data and manage cybersecurity risks.
- National Institute of Standards and Technology (NIST) Cybersecurity Framework: The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organisations to better manage and reduce cybersecurity risks. It was also designed to foster risk and cybersecurity management communications amongst both internal and external organisational stakeholders.
- Control Objectives for Information and Related Technologies (COBIT) by ISACA: The framework allows for bridging the gap between business risks, technical issues, and control requirements.

The examples listed above are non-exhaustive. Financial institutions must perform regular testing, assessing and evaluating the effectiveness of technical and organisational measures. Other credible and trustworthy practices may also meet the requirements under section 31 of the DPA although not mentioned in the guide. Furthermore, this office may also be consulted.

8.10 Record of processing operations

Since the rule is the same for all controllers, financial institutions must maintain a record of all processing operations under their responsibility according to section 33 of the DPA. The Data Protection Office has designed a template to assist organisations in complying with this obligation which is available on the office website at the following URL:
https://dataprotection.govmu.org/Pages/Home%20-%20Pages/Document%20%26%20Forms/Records-of-processing-operations.aspx
This template provides for a comprehensive general overview of the processing activities to be carried out.

8.11 Data Protection Impact Assessment

As per section 34 of the DPA, where processing operations are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature, scope, context and purposes, every controller or processor must, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

A DPIA must be carried out prior to processing, in other words, the DPIA must be started as early as practically possible in the design of the processing activities even if some of the processing operations are still unknown.
A DPIA is not required:

- where the processing operation is likely to present lower levels of risk;
- if special categories of data, such as medical records, are not processed systematically and on a large scale, then, such processing operations may not automatically present high risks to the rights and freedoms of individuals;
- if you are organising a corporate event and you need to know what kind of food the invitees are allergic to, you do not have to carry out a DPIA.
- when the nature, scope, context and purposes of the processing are very similar to the processing for which a DPIA have already been carried out. In such cases, results of the DPIA for similar processing can be used;
- where the provisions under section 44 of the Data Protection Act 2017 are met.

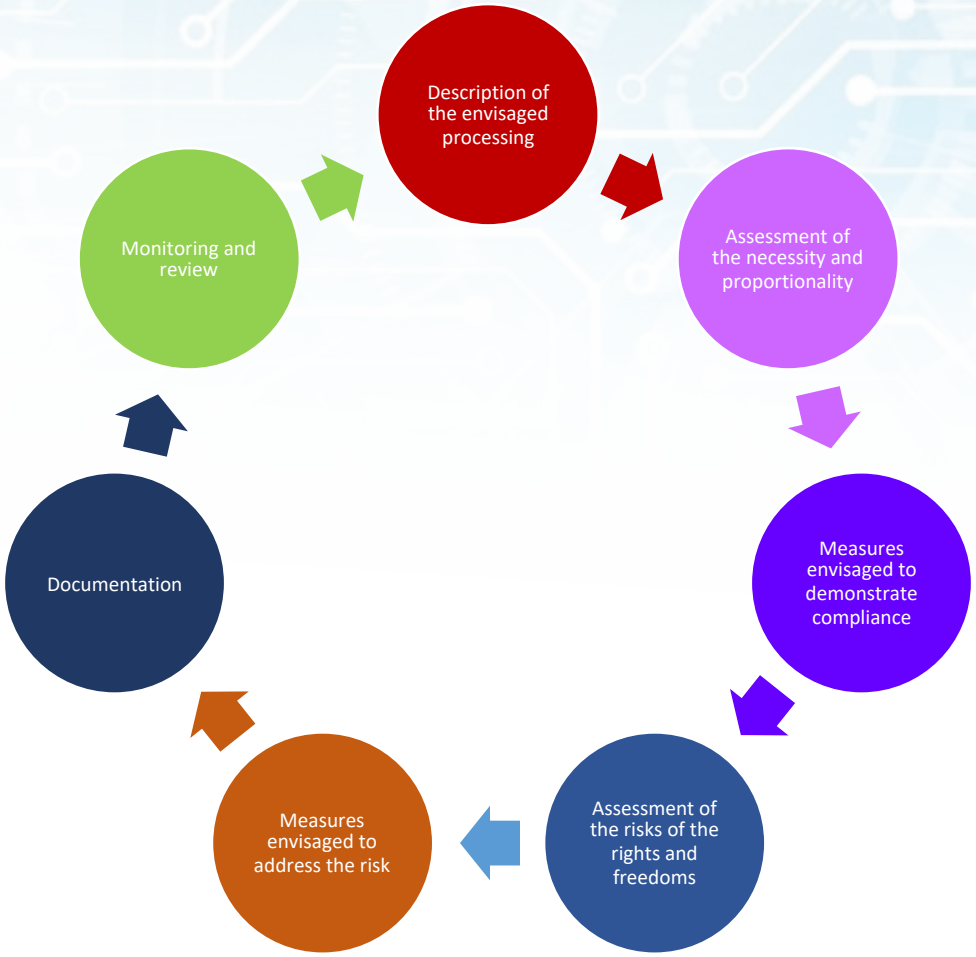
Nonetheless, in cases where it is not clear whether a DPIA is required, the Data Protection Office recommends that a DPIA is performed as it is a useful tool to help controllers or processors comply with data protection law.

The Data Protection Act 2017 sets out the minimum features of a DPIA:

- a description of the envisaged processing operations and the purposes of the processing;
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged must address:

(i) the risks and the safeguards, security measures, mechanisms to ensure the protection of personal data
(ii) demonstrate compliance with the Data Protection Act 2017.

The following figure demonstrates the iterative process for carrying out a DPIA:



DPIA form may be submitted online on the eDPO system and a list of criteria to evaluate high risk processing are available on the website of the Data Protection Office on the link below:
https://dataprotection.govmu.org/Pages/Home%20%20Pages/Document%20%26%20Forms/Data-Protection-Impact-Assessment-and-High-Risk-Operations.aspx

8.12 Prior Authorisation and Consultation

Subject to section 35, every controller or processor must obtain authorisation from the Office prior to processing personal data in order to ensure compliance of the intended processing with the Data Protection Act and in particular to mitigate the risks involved for the data subjects where a controller or processor cannot provide for the appropriate safeguards referred to in section 36 in relation to the transfer of personal data to another country.

Authorisation must be sought from the Data Protection Office when a processing operation is likely to result in a high risk to the rights and freedoms of an individual or where a controller or processor cannot provide for the appropriate safeguards referred to in section 36 in relation to the transfer of personal data to another country.

8.13 Transfer of personal data

The controller or processor may transfer personal data abroad in any one or more of the following circumstances according to section 36(1)[18] of the Data Protection Act 2017 (DPA) which reads as follows:

"A controller or processor may transfer personal data to another country where –

(a) he or it has provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data; or

(b) the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards; or

(c) the transfer is necessary –

(i) for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

(ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person; or

(iii) for reasons of public interest as provided by law; or

(iv) for the establishment, exercise or defence of a legal claim; or

(v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(vi)for the purpose of compelling legitimate interests pursued by the controller or the processor which are not overridden by the interests, rights and freedoms of the data subjects involved and where –

(A) the transfer is not repetitive and concerns a limited number of data subjects; and

(B) the controller or processor has assessed all the circumstances surrounding the data transfer operation and has, based on such assessment, provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data; or

(d) the transfer is made from a register which, according to law, is intended to provide information to the public and which is open for consultation by the public or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down by law for consultation are fulfilled in the particular case."

A transfer pursuant to subsection 36(1)(d) shall not involve the entirety of the personal data or entire categories of the personal data contained in the register and, where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or in case they are to be the recipients.

Subsection 36(1)(a) and 36(c)(i), (ii) and (vi) shall not apply to activities carried out by a public authority in the exercise of its functions.

The Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the safeguards or the existence of compelling legitimate interests and may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as he may determine.

18 Please consult the Data Protection (Amendment) Act for the latest provisions.

If the controller will rely on section 36(1)(a) above, then the controller is required to submit the transfer of data abroad on the online portal of the Data Protection Office available at the link https://dataprotection.govmu.org/Pages/eDPO.aspx.
Controllers are requested to refer to the section on "Transfer of Personal Data Abroad" in the user guide for the dpo portal which is available on the DPO website.

When filling the online form, the controller must provide the description of the types of data transferred only without divulging the actual data of individuals.
Should the controller rely on any one of the other exceptions, no authorisation from the Data Protection Commissioner is required.

The Data Protection Office recommends the use of Standard Contractual Clauses issued by the European Commission as proposed by :

(a) the Council of Europe available at
https://rm.coe.int/t-pd-2022-1rev10-en-final/1680abc6b4%E2%80%8B
and/or
(b) the European Union available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en and Binding Corporate Rules for multinational companies.

8.14 Rights of individuals

Part VII[19] of the DPA elaborates on the rights of individuals.

8.14.1 Right of access

Individuals have the right to obtain confirmation of whether personal data relating to him are kept as well as a copy of such data free of charge following a written request.

The controller should consider whether information (or some of it) can be provided without undermining its financial activities. The request may be refused if the disclosure of the information would impair the financial activities, or would infringe the rights of third parties. In case of refusal to comply with a request, the financial institutions should record the reasons for this decision and communicate them to the person concerned.

8.14.2 Right to rectification, erasure or restriction

Similarly, an individual has the right to request for correction of personal data which he/she believes is inaccurate or incomplete. Or, he/she may also request that his/her personal data are erased if the continued processing of those data is not justified, for example where the data is no longer needed in relation to the purpose for which it was originally collected, the individual withdraws consent, individual objects to processing and there is no overriding legitimate interest for it continuing or data is processed unlawfully.

19 Please consult the Data Protection (Amendment) Act for the latest provisions.

In addition, an individual may request that the processing of his/her personal data is restricted for example, where the individual contests accuracy of the data (processing is restricted until the accuracy is verified), objects to its processing(and consideration is being given to whether legitimate grounds override those of the individual), processing is unlawful or data is no needed but the individual requires it for a legal claim.

Under section 39(3) of the DPA, where the controller has made the personal data public, he shall take all reasonable steps to inform third parties processing such data, that the data subject has requested the erasure of any links to, or copy or replication of, that personal data.

8.14.3 Right to object

Likewise, an individual has the right to object in writing at any time to the processing of personal data relating to him/her free of charge, unless the controller demonstrates compelling legitimate grounds for the processing which override the data subject's interests, rights and freedoms or for the establishment, exercise or defence of a legal claim.

9.0 Cloud Computing

In the rapidly evolving digital landscape, businesses are increasingly relying on cloud services to streamline operations, enhance collaboration, and ensure scalability. However, with the multitude of cloud service providers available, selecting the right one is crucial for the success and security of an organization. Choosing a trusted cloud service provider involves evaluating various factors to ensure that data is handled with the utmost care.

Some non-exhaustive important considerations when selecting a trusted cloud service provider are: -

Data Encryption	**In-Transit Encryption:** Ensure that data is encrypted during transmission between your systems and the cloud provider's infrastructure. **At-Rest Encryption:** Confirm that data stored on the cloud provider's servers is encrypted to protect it from unauthorized access.
Compliance with Data Protection Regulations	Verify that the cloud provider complies with relevant data protection regulations, such as GDPR in Europe or other applicable local laws. Check if the provider undergoes regular audits and assessments to demonstrate compliance.
Data Location	Understand where the cloud provider stores your data and ensure it aligns with legal and regulatory requirements.
Access Controls and Identity Management	Evaluate the access control mechanisms to restrict and monitor who can access your data. Ensure robust identity and access management tools are in place to manage user permissions effectively.

Data Portability and Interoperability	Assess the ease of migrating data in and out of the cloud platform. Ensure compatibility with your existing systems and the ability to transfer data without vendor lock-in.
Data Backup and Recovery	Verify the cloud provider's data backup policies and procedures. Assess the capabilities for data recovery in case of accidental deletion or data loss.
Incident Response and Notification	Understand the cloud provider's incident response plan and how they handle security breaches. Confirm their commitment to timely and transparent communication in the event of a data breach.
Audit and Monitoring Tools	Check if the provider offers tools for monitoring and auditing data access and activities. Ensure that you have visibility into who is accessing your data and when.
Security Certifications and Standards	Look for certifications and adherence to security standards, such as ISO 27001, SOC 2, or others relevant to your organisation. Consider whether the cloud provider undergoes third-party security audits.
Data Deletion and Retention Policies	Understand the provider's data retention policies and mechanisms for permanent data deletion. Ensure compliance with your organization's data retention requirements.
Terms of Service and Legal Agreements	Review the cloud provider's terms of service and contractual agreements. Ensure that data protection and privacy terms are clearly outlined and meet your organization's standards.
Customer Support and Training	Assess the level of support provided by the cloud provider, especially concerning data protection queries. Consider the availability of training resources to educate your team on data protection best practices.

Cloud computing has become ubiquitous especially with financial institutions. As per section 36(1) of the DPA, in case personal data is transferred abroad (in cloud), the requirements for the transfer abroad must be fulfilled irrespective of the type of data flow involved as per paragraph 8.13.

It is legally required to have a written contract between the financial institution and the cloud provider. Open-ended provisions are found in the DPA to ensure flexibility.
The contract may cover the following points amongst others:

a. Continuity of service, backups and integrity,
b. Certification such as ISO 27001 compliant (which is not mandatory, but essential),
c. Auditing of the cloud provider by third party,
d. Appropriate access rights are provided to authorised officers for creation, amendment and deletion of data with audit trails,
e. For termination of contract, to ensure that all personal data are returned to controller and no copies are kept at the cloud provider.

Financial institutions should pay particular attention to the sub-sections of section 31 of the DPA on security of processing. The choice of a cloud provider should be made carefully to protect the personal data at risk, as the primary responsibility for processing lies with the controller.

In case the controller cannot provide proof of appropriate safeguards with respect to the protection of the personal data or cannot rely on any of the exceptions provided in section 36(1) of the DPA, then, according to section 35 of the DPA, the controller must seek authorisation and consult the Data Protection Office prior to processing personal data. This will ensure compliance of the intended processing with the DPA and in particular to mitigate the risks involved for data subjects (individuals) where the controller intends to transfer personal information to another country.

10.0 Direct Marketing

By virtue of section 28 of the DPA, controllers must have a lawful basis for processing personal data for direct marketing purposes.

Prior consent from data subjects (i.e. individuals/customers) is required before processing their personal data for marketing purposes. Financial institutions must, therefore, be able to demonstrate that they have obtained valid consent as per section 24 of the DPA. They must keep records of those who consented, indicating when, how and what information was provided for this purpose.

Section 40(2) of the DPA provides individuals with the right to object, at any time, to the processing of their personal data for the purpose of direct marketing. The right to object to direct marketing is absolute and financial institutions must stop the processing of the data subjects' personal data whenever they object. Generally, it is good practice to acknowledge the request and confirm that the marketing will stop.

According to Section 23 of the DPA, a financial institution must always be able to identify itself. It has to provide contact details for individuals to contact them, particularly if they want to opt-out/unsubscribe from the marketing list.

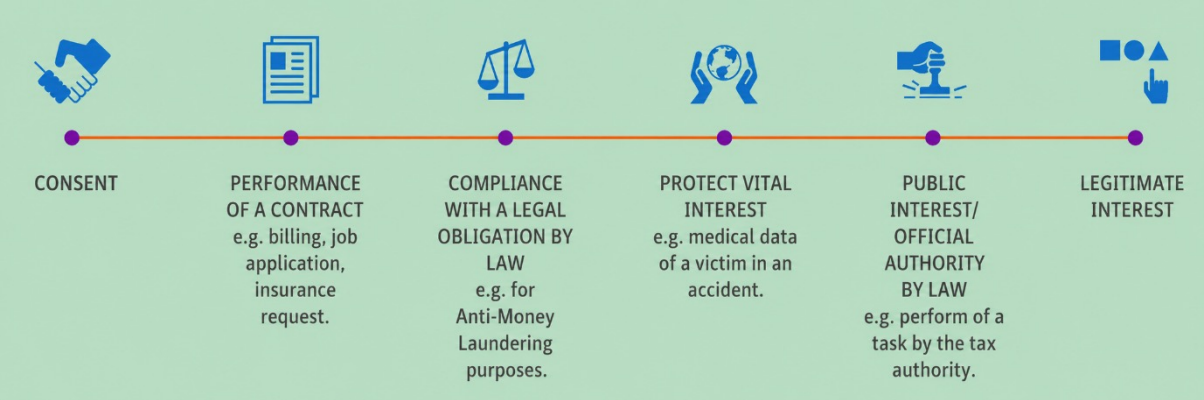
Financial institutions should also implement a privacy policy explaining clearly how the data will be collected and processed for marketing purposes. A template is available on our website at the following URL:

https://dataprotection.govmu.org/SitePages/ViewAllReports.aspx?RType=Templates

11.0 Unlawful disclosure of personal data

Any financial institution who, without lawful excuse, discloses personal data in any manner that is incompatible with the purpose(s) for which such data has been collected shall commit an offence.

Personal data must not be disclosed unless condition(s) under section 28 of the DPA apply.



For instance, if a financial institution shares customers' information without a lawful basis or without the individual's consent with a marketing company for the purpose of targeted advertising in order to generate revenue from marketing partnerships, then this disclosure is deemed unlawful.

However, a financial institution is legally obligated to disclose details of a suspected customer to the police following a court order during criminal investigation.

It is recommended that financial institutions put in place a disclosure policy elaborating the various circumstances where disclosure is permitted or otherwise, as well as the process and procedures that must be adhered to when handling third party requests for disclosure of personal data.

12.0 Potential consequences of non-adherence to rules and regulations in the financial sector

There are various offences and criminal penalties under the DPA which, in general if committed, are sanctioned by a court of law.

Where no specific penalty is provided, any person who does not comply or contravenes this Act shall, on conviction, be liable to a fine not exceeding 200,000 rupees and to imprisonment for a term not exceeding 5 years.

Other Offences and Penalties[20]

Offences under the DPA	Penalties
Section 6: Investigation of Complaints Any person who fails to attend a hearing or to produce a document or other material when required to do so.	Liable to a fine not exceeding 50,000 rupees and to imprisonment for a term not exceeding 2 years.
Section 7: Power to require information Any person who fails or refuses to comply with a requirement specified in a notice, or who furnishes to the Commissioner any information which he knows to be false or misleading in a material particular.	Liable to a fine not exceeding 50,000 rupees and to imprisonment for a term not exceeding 2 years.
Section 15: Application for registration Any controller or processor who knowingly supplies any information, during registration, which is false or misleading in a material particular.	Liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 5 year.
Section 17: Change in particulars Any controller or processor who fails to notify a change in particulars.	Liable to a fine not exceeding 50,000 rupees
Section 28: Lawful processing Any person who process personal data unlawfully.	Liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding 5 years.

20 Please consult the Data Protection (Amendment) Act for the latest provisions.

13.0 Processing of personal data for anti-money laundering/ countering financing of terrorism or proliferation purposes[21]

The AML/CFT/CPF framework which often involves specific investigations into suspicions of or actual Money Laundering and Financing of Terrorism (ML/FT) activities, provides for situations where the customer is not or only partially informed of the data processing, particularly in relation to suspicious transaction reporting obligations by the Obliged Entities[22] (OE), the provision of personal data in response to requests for information by Financial Intelligence Units and Law Enforcement Agencies (LEAs) and the application of monitoring orders. In those cases, prior information of the customer would contravene to AML/CFT/CPF prohibitions, in particular to tipping-off.

Processing of personal data by public authorities can be based on the lawful ground of public interest, given they are entrusted with the mandate to combat AML/CFT/CPF and are entrusted with specific tasks in this area with appropriate safeguards. Checks and balances as well as oversight are also implemented. The same does not extend necessarily to private sector institutions which are obliged entities and have a different legal status and mandate.

Processing of personal data by OEs in the AML/CFT/CPF context should be based on a clear and detailed legal basis that provides for the principles of necessity and proportionality to which the controllers are subject. Failure by OE to comply with those obligations would entail risks of measures taken by supervisory authorities, including administrative and criminal sanctions. Failure by customers to provide the requested data could, in turn, result in that the transaction or customer relationship is not being concluded or in the restriction of services.

For example, data processing is required to prevent the misuse of legal persons for ML or TF by ensuring that there is adequate, accurate and up-to-date information on beneficial ownership and control of legal persons. Beneficial Ownership Information should be accessible in a timely manner by a competent authority through either a register of beneficial ownership or an alternative mechanism. Competent authorities should handle such data in accordance with their powers and responsibilities under the law.

21 Guidelines from Council of Europe https://rm.coe.int/t-pd-2021-8rev8-aml-cft-guidelines-en-final-2772-7823-8984-1/1680abdb4d

22 An "obliged entity" typically refers to an individual or organization that is legally obligated or required to comply with certain regulations or laws, often in the context of financial transactions and anti-money laundering (AML) measures. Obliged entities are usually subject to specific rules and regulations that aim to prevent activities such as money laundering, terrorist financing, and other illicit financial practices.

Case WM (C 37/20), Sovim SA (C 601/20) v Luxembourg Business Registers

In the case of *WM (C 37/20), Sovim SA (C 601/20) v Luxembourg Business Registers*, the Court (Grand Chamber) ruled that "Member States must ensure that information on the beneficial ownership of companies and of other legal entities incorporated within their territory is accessible in all cases to any member of the general public."[23] In the judgment, reference was made to Recitals 34, 36 and 38, amongst others, of Directive 2018/843 as follows:

"(34) In all cases, both with regard to corporate and other legal entities, as well as trusts and similar legal arrangements, a fair balance should be sought in particular between the general public interest in the prevention of money laundering and terrorist financing and the data subjects' fundamental rights. The set of data to be made available to the public should be limited, clearly and exhaustively defined, and should be of a general nature, so as to minimise the potential prejudice to the beneficial owners. At the same time, information made accessible to the public should not significantly differ from the data currently collected. In order to limit the interference with the right to respect for their private life in general and to protection of their personal data in particular, that information should relate essentially to the status of beneficial owners of corporate and other legal entities and of trusts and similar legal arrangements and should strictly concern the sphere of economic activity in which the beneficial owners operate. ...

...

(36) Moreover, with the aim of ensuring a proportionate and balanced approach and to guarantee the rights to private life and personal data protection, it should be possible for Member States to provide for exemptions to the disclosure through the registers of beneficial ownership information and to access to such information, in exceptional circumstances, where that information would expose the beneficial owner to a disproportionate risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation. It should also be possible for Member States to require online registration in order to identify any person who requests information from the register, as well as the payment of a fee for access to the information in the register.

...

(38) [The GDPR] applies to the processing of personal data under this Directive. As a consequence, natural persons whose personal data are held in national registers as beneficial owners should be informed accordingly. Furthermore, only personal data that is up to date and corresponds to the actual beneficial owners should be made available and the beneficiaries should be informed about their rights under the current Union legal data protection framework ... and the procedures applicable for exercising those rights. In addition, to prevent the abuse of the information contained in the registers and to balance out the rights of beneficial owners, Member States might find it appropriate to consider making information relating to the requesting person along with the legal basis for their request available to the beneficial owner."

23 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62020CJ0037

The first question raised concerned the validity of Directive 2018/843, specifically Article 1(15)(c), which mandates public access to beneficial ownership information of legal entities. This raised concerns about potential interference with fundamental rights guaranteed by Articles 7 and 8 of the Charter, particularly regarding privacy and protection of personal data. The referring court sought clarification on whether this provision aligns with the Charter's principles. Article 7 of the Charter guarantees everyone the right to respect for his or her private and family life, home and communications, while Article 8(1) of the Charter expressly confers on everyone the right to the protection of personal data concerning him or her. Directive 2015/849, as amended, mandates Member States to enforce requirements for corporate and legal entities within their jurisdiction to gather and maintain precise, up-to-date information on their beneficial ownership. This information must be stored in a central register within each Member State. Under Article 3(6) of that directive, beneficial owners mean any natural person (or persons) who ultimately owns or controls the customer and/or the natural person (or persons) on whose behalf a transaction or activity is being conducted. Directive 2015/849, as amended, mandates Member States to ensure that information on beneficial ownership is accessible to the general public, including details like name, month and year of birth, country of residence and nationality, and the extent of beneficial interest. Additionally, Member States can permit access to further identifying information, such as date of birth or contact details, under national law conditions and in compliance with data protection regulations.
The existence of information sharing initiatives through Public-Private Partnerships (PPPs) has been noted in several jurisdictions. While the opportunities they provide in the fight against financial crime are significant, there are remaining challenges which are also of a legislative nature and of compliance nature (e.g. legislative amendments may be needed to ensure a proper legal basis and allow partners to achieve their objectives).

Due regard has to be given to the mandate with which public authorities are entrusted and can be held accountable for non-compliance with their legal obligations. Public interest as a legal basis for data processing emerging initiatives by private sector entities subject to AML/CFT/CPF obligations should be properly substantiated and carefully scrutinised.

Effective information sharing is one of the cornerstones of the FATF Recommendations. As such below are the extract of Recommendations 2 and 40 which focuses on the protection of information sharing[24].

Recommendation 2: National cooperation and coordination
Countries should ensure that policy-makers, the financial intelligence unit, law enforcement authorities, supervisors and other relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. Countries should have inter-agency frameworks in place to enable policy makers, the Financial Intelligence Unit (FIU), law enforcement authorities , supervisors and other

24 FATF (2012-2025), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Financial Action Task Force (FATF), Paris, France, last updated October 2025.

relevant competent authorities to co-operate and where appropriate, co-ordinate and exchange information domestically with each other concerning the development and implementation of AML/CFT/CPF policies.

Countries should have co-operation and co-ordination between relevant authorities to ensure the compatibility of AML/CFT/CPF requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localization).

Recommendation 40: Other forms of International Co-operation

Competent authorities shall provide the widest possible range of international cooperation in relation to money laundering, terrorist financing and the financing of proliferation, in a rapid, constructive and effective manner.

Such cooperation shall include, where appropriate, the exchange of information, supervisory cooperation, investigative assistance and other forms of collaboration between competent authorities.

Competent authorities shall maintain strict confidentiality of any request for cooperation and any information exchanged, in accordance with applicable data protection and privacy obligations.

At a minimum, exchanged information shall be protected to a standard equivalent to that applied to similar information obtained domestically and shall be used solely for the purpose for which it was requested, unless prior consent is obtained from the providing authority.

Cooperation shall not be refused on unreasonable or disproportionate grounds. However, competent authorities may refuse to provide information where the requesting authority is unable to ensure adequate protection and confidentiality of the information in accordance with applicable legal and data protection requirements.

As a founder member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), Mauritius has committed to adhere to the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation issued by the Financial Action Task Force.

The Financial Crimes Commission Act (FCC Act) 2023 requires financial institutions to implement measures as are reasonably necessary to ensure that neither it nor any service offered by it, is capable of being used by a person to commit or to facilitate the commission of a money laundering offence or the financing of terrorism offence.

FIAMLA and FIAMLR made thereunder, prescribe the preventive measures to be put in place by financial institutions to effectively protect their businesses, sectors and financial systems from misuse and abuse by criminal networks through:

- Sound identification and understanding of ML/TF risks; and
- Strong and appropriate application of customer due diligence (CDD), record-keeping, internal control and reporting requirements.

Financial institutions are thus required to collect and process personal data of their customers to ensure compliance with the AML/CFT/CPF requirements.

Disclosure of personal data to competent authorities, such as the Financial Intelligence Unit and Law Enforcement Authorities, is also required under these enactments, for intelligence or investigation purposes.

Such processing would fall under the remit of section 28 of the Data Protection Act.

The Bank of Mauritius is designated as the AML/CFT/CPF supervisory authority for the banking sector. The Financial Services Commission is the integrated regulator in Mauritius for the financial services sector (other than banking) and global business.

Section 26 of the Bank of Mauritius Act provides that the duty of confidentiality imposed under that section shall not preclude the exchange or disclosure of any information, under conditions of confidentiality, between the Bank and any public sector agency, foreign supervisory institution or authority, international organisation or law enforcement agency, where the Bank is satisfied that the public sector agency, foreign supervisory institution or authority, international organisation or law enforcement agency has the capacity to protect the confidentiality of the information imparted, or between the Bank and any other foreign regulatory agency performing functions similar to those of the Bank under the Bank of Mauritius Act or the National Payment Systems Act 2018, pursuant to any existing or future treaty, or agreement or memorandum of understanding entered into by the Bank or the State of Mauritius.
The Bank may also disclose any information to the Financial Intelligence Unit pursuant to section 22 of the FIAMLA.

Section 64 of the Banking Act provides that the duty of confidentiality imposed under that section shall not apply where the financial institution is required to make a report or provides additional information on a suspicious transaction to the Financial Intelligence Unit under the FIAMLA. Also, the disclosure of information by the Bank of Mauritius, under conditions of confidentiality, and subject to the satisfaction of such conditions as it may determine, is permitted to a domestic or foreign supervisory authority where the information is required by the supervisory authority for the sole purpose of carrying out its supervisory functions in respect of money laundering or terrorism financing.

The duty of confidentiality is also lifted where the information is required to be disclosed by the financial institution for the purpose of discharging its responsibilities under Part VIIIA of the Banking Act, pertaining to the prevention of money laundering and terrorism financing.

Similarly, disclosure of information is permissible -

- with respect to payable-through accounts, where the customer due diligence information is required to be disclosed, upon request, by the financial institution to another institution with which it maintains a correspondent banking relationship, provided that the institution has given to the financial institution a written undertaking regarding the confidentiality of the information provided.
- the customer due diligence information is required to be disclosed by the financial institution for the purpose of meeting the requirement set out by the central bank with respect to domestic or cross-border wire transfers or reliance on a third party.

Furthermore, under section 64A of the Banking Act, financial institutions and holders of licences, including its branches and subsidiaries, are required to implement programmes against money laundering and terrorism financing, which are commensurate with the money laundering and terrorism financing risks to which it or he is exposed and the size of its or his business. The programmes include the following internal policies, procedures and controls: (a) compliance management arrangements, including the appointment of a compliance officer at management level, (b) screening procedures to ensure high standards when hiring officers, (c) ongoing training programmes for its or his directors and officers, and (d) an independent audit function to test the programme.

Every financial institution and every holder of a licence, including its branches and subsidiaries, operating in a group structure shall implement group-wide programmes against money laundering and terrorism financing. The group-wide programmes shall include: (a) the internal policies, procedures and controls referred to above, (b) policies and procedures for sharing information required for the purposes of customer due diligence and money laundering and terrorism financing risk management, (c) procedures to ensure that group level compliance, audit and anti-money laundering and combating the financing of terrorism functions shall have the power to request customer, account and transaction information from branches and subsidiaries, as necessary to perform their functions in order to combat money laundering and terrorism financing, (d) the provision at group level functions from branches and subsidiaries, of information and analysis of transactions or activities which appear unusual when relevant and appropriate to risk management and (e) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

Furthermore, the Bank of Mauritius may, from time to time, issue such guidelines, directives or instructions to any financial institution, class of financial institutions or holder of a licence, as it considers necessary for the prevention of money laundering or terrorism financing, which may provide for: (a) customer due diligence measures to be undertaken by financial institutions or holders of a licence to prevent money laundering and the financing of terrorism, (b) an on-going duty to keep customer due diligence information up to date in respect of both new and existing customers, and (c) the keeping of records for the purpose of paragraphs (a) and (b).

Guideline on Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation	The Bank of Mauritius issued the Guideline on Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation ('Guideline') to financial institutions, in order to set out the broad parameters within which financial institutions should operate in order to ward off money laundering, terrorist financing and proliferation financing risks. The Guideline outlines the relevant requirements of the FIAMLA, the FIAMR, FCC Act, Banking Act 2004 and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019. The Guideline provides guidance and assistance to financial institutions in order to assist them to understand and effectively perform their statutory obligations under the legal and regulatory framework. It sets out the minimum expectations of the Bank regarding the factors that should be taken into consideration by financial institutions when identifying, assessing and mitigating the risks of money laundering and the financing of terrorism and proliferation. In complying with statutory requirements and in applying the provisions and requirements of the Guideline, financial institutions should as far as possible adopt an appropriate and intelligent risk-based approach and always consider additional measures that could be necessary to prevent its exploitation, and that of its products and services, by persons seeking either to launder money or to finance terrorism or proliferation. The Bank of Mauritius, in the exercise of its supervisory duties, will monitor adherence to the Guideline and failure to measure up to the standard contained in the Guideline will be dealt with, as appropriate, by the Bank of Mauritius. Regulatory actions may entail the imposition of non-monetary sanctions, monetary penalties and in very serious instances, may lead to the revocation of the licence of the financial institution. It is a criminal offence for financial institutions to fail to take measures to prevent their institutions or the services their institutions offer from being used to commit or to facilitate the commission of money laundering.
The National Payment Systems Act 2018	Section 22 of the National Payment Systems Act prescribes that the AML/CFT/CPF obligations of section 64 A of Banking Act shall be applicable for the Payment Service Providers licensed under the NPS Act.

Section 83 of the Financial Services Act provides that the duty of confidentiality imposed under that section shall not preclude the exchange or disclosure of any information in the following cases:

(a) the obligations of Mauritius under any international treaty, convention or agreement, and to the obligations of any public sector agency under any international arrangement or concordat;
(b) such disclosure as is necessary for the purpose of administering the relevant Acts, and of discharging a function under those Acts;
(c) disclosure, pursuant to an agreement or arrangement for the exchange of information and under condition of confidentiality, for the purpose of exercising its functions, in relation to a corporation holding a Global Business Licence or in relation to a financial institution carrying out any services or business activities under any of the relevant Acts –
  (i) to a public sector agency; or
  (ii) to any other institution which performs in a foreign country functions similar to those of the Commission under this Act.
(d) the duty of the Commission to pass on information to the FIU established under the Financial Intelligence and Anti-Money Laundering Act 2002, pursuant to section 22 of that Act;
(e) disclosure to the Ombudsperson for Financial Services, pursuant to an agreement or arrangement for the exchange of information.

14.0 FINTECH

Fintech refers to technologically enabled financial innovations which could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services.

Fintech uses various innovative technologies to revolutionalise the financial services industry such as:

- Artificial Intelligence
- Blockchain
- Big data
- Cloud computing

One of the most dynamic areas within fintech is the emergence of cryptocurrencies and blockchain-based assets. These technologies are gaining momentum through applications such as digital wallets, decentralized finance (DeFi) platforms, tokenized assets and blockchain-powered payment systems. However, alongside these innovations come significant data protection challenges, especially in the context of cryptocurrencies and blockchain systems namely:

a) Pseudonymity versus Anonymity: While blockchain transactions are pseudonymous, the integration of off-chain data can potentially re-identify individuals thereby compromising privacy.

b) Immutability of Blockchain: Information recorded on a blockchain is often permanent, posing conflicts with legal rights such as the "right to erasure" under the DPA.

c) Cross-border Data Transfers: The inherently global nature of blockchain networks can lead to unauthorized international transfers of personal data, raising compliance concerns.

Given these risks, ensuring data protection compliance is essential to ensure the protection of the privacy rights and security of individuals' personal information.

The following points should be considered for data protection and Fintech compliance:

Regulatory Framework: Depending on the jurisdictions and markets in which a Fintech operates, there may be numerous data protection laws and regulations that must be adhered to.

Blockchain: Ensure that no personal data is stored on a permissionless blockchain — whether in plain text, encrypted, or anonymised. Instead, any processing involving personal data should be carried out on a permissioned blockchain network, where participation is restricted to known and authorised entities.

User Consent: Fintech organisations collect a large amount of user data to provide personalised financial services. If the legal basis for processing is user consent, then organisations must ensure that they obtain valid consent from users. Individuals should be informed about the type(s) of data collected, the purpose(s), relevant information on how their data would be processed and the option to withdraw consent.

Data Minimisation: Fintech companies should ensure that only minimum data would be collected with respect to the purpose(s) for the execution of the service.

Data Security: Fintech organisations must safeguard data and processing operations against cybersecurity threats. Security and organisational measures such as encryption, anonymisation, secure authentication, regular security audits, and employee training are some of the measures that Fintech companies should implement. All transfers of data across jurisdictions must be secured with appropriate security measures. The organisation is required to ensure that its system/platform is tested at a predetermined timeframe for reliability and adequate data security.

Limit access to sensitive information by implementing strong access controls. Make sure employees only access the data they need for their specific tasks. By restricting access to only authorised personnel and implementing multi-layered authentication protocols, Fintech firms can fortify their defenses against potential security breaches. Simultaneously, a robust data protection framework, including encryption and secure storage protocols, is essential to ensure the confidentiality and integrity of customer data.

Third-Party Service Providers: Fintech organisations often depend on third-party service providers for diverse functions. Thus, it is crucial that third-party service providers abide with data protection laws and implement adequate organisational and technical measures to protect data. Fintech organisations which rely on biometrics, including fingerprints and facial recognition, data, must handle and store those data securely.

Cross-Border Data Transfers: If a Fintech organisation operates across different jurisdictions, it must ensure that cross border transfers comply with relevant data protection laws and regulations. Safeguards such as Standard Contractual Clauses (SCCs) have to be considered.

Data Breach Response: Fintech organisations must implement a data breach response plan to promptly identify when a data breach occurs, take appropriate actions to mitigate the impact of the breach and notify relevant authorities and communicate with affected data subjects when required.

Privacy Policies and Transparency: Clearly written privacy policies using plain and simple language which explain how user data is collected, used, and protected and which inform of any potential privacy risks during the processing are important. Transparency builds trust with users and demonstrates the organisation's commitment to data protection.

Fairness: Assurance must be given by Fintech organisations that only minimum data will be collected with respect to the purpose/s for the execution of the service.

Privacy by design: Fintech organisations must incorporate built-in privacy protections using data protection by design, data protection impact assessments and default techniques to ensure that these systems do not pose risks to the rights and freedoms of individuals. Systems must be developed and also work in tandem with people's privacy expectations and rights.

Rights of individuals: Fintech organisations must respect the privacy rights of individuals. For instance, data protection laws recognise a right to erasure which enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Regular Compliance Audits: Fintech organisations should conduct regular assessments and audits to ensure the effectiveness of policies, procedures, and security measures and ensure ongoing compliance with data protection regulations.

In general, data protection compliance is an essential part of Fintech operations, and companies in this industry must prioritise the importance of privacy and security of user data to maintain trust and adhere to legal requirements.

Employee Training: Fintech firms should train their staffs on data protection security policies on a regular basis. They must prioritise comprehensive training programs for their employees to ensure a deep understanding of evolving industry regulations, cybersecurity best practices, and the responsible handling of sensitive financial data. Rigorous training not only cultivates a workforce equipped to navigate the intricacies of Fintech but also reinforces a culture of compliance and security.

Fintech leverages blockchain and distributed ledger technology (DLT), driving innovations like virtual assets, non-fungible tokens (NFTs) and spot commodity markets. In Mauritius, the VAITOS Act 2021 regulates virtual assets.

14.1 The VAITOS Act 2021

The FSC came up with the VAITOS Act which came into force on 07 February 2022 to regulate and supervise Virtual Asset Service Providers (VASPs) and issuers of Initial Token Offerings (ITOs) in the non-bank financial services sector in Mauritius.

The VAITOS Act enables any company which intends to conduct business activities in relation to VASPs or issue of ITOs, in or from Mauritius, to apply for a licence or registration from the FSC and operate within a sound prudential and market conduct regime. The Act provides for timely, accurate and transparent disclosures by the issuers of ITOs.

A Virtual Asset (VA) is a digital representation of value (such as Bitcoin, Ether and other blockchain-based tokens) that can be digitally traded or transferred, and may be used for payment or investment purposes. However, VAs (including cryptocurrencies) are not legal tender in Mauritius, unlike fiat currencies and digital representations of fiat currency (like e-money).

An ITO refers to an offer for sale, to the public, of a virtual asset in exchange for fiat currency or another VA by an issuer of ITOs. ITO is a means of raising funds for projects through innovative and digital platforms.

The Act regulates two main categories of activities:
A. VASP, meaning a person who conducts, as a business activity, for or on behalf of another person one or more of the following activities or operations, namely:

(i) exchange between VAs and fiat currencies;
(ii) exchange between one or more forms of VAs;
(iii) transfer of VAs;
(iv) safekeeping of VAs or instruments enabling control over VAs;
(v) administration of VAs or instruments enabling control over VAs; or
(vi) participation in, and provision of, financial services related to an issuer's offer and sale of a VA; or an issuer's offer or sale of a VA.

B. Issuers of ITOs, are companies registered under the Act and making issuance of ITOs. An ITO is an offer for sale to the public of a VA in exchange for fiat currency or another VA.

14.2 Other initiatives

In addition to VAITOS, the FSC introduced the following initiatives:

- The issuance of Guidance Notes on the regulatory treatment of Non-Fungible Tokens (NFTs);
- The release of a regulatory framework for the Spot Commodity Market and intermediaries, which allows these markets to inter-alia be operated through electronic systems or platforms incorporating emerging technologies, such as distributed ledger technology;
- The issuance of Consultation Papers addressing topics such as the impact of the Metaverse on the financial services sector and regulatory considerations arising from financial collateralization in decentralized finance (DeFi).

15.0 Artificial Intelligence

Emerging digital technologies and services including Artificial Intelligence (AI) creates an unprecedented promise to the world with limitless benefits in terms of enhanced efficiency, accuracy and timeliness.

For instance, AI presents significant challenges and concerns in the realm of privacy and data protection. *"AI is not just about technology but delves into fundamental and interdisciplinary human rights and freedoms"*.
Not only does AI force us to better understand its impact on human rights and fundamental freedoms, but it also entails in-depth reflection on who is responsible for its harmful consequences.

The Ministry of Information Technology, Communication and Innovation has launched the National Artificial Intelligence Strategy which sets out a clear national vision for positioning Mauritius as a trusted jurisdiction for responsible and inclusive AI. The Strategy emphasises a people-centred, innovation-friendly and risk-proportionate approach ensuring that AI systems enhance public service delivery, strengthen economic competitiveness and support evidence-based decision-making while safeguarding fundamental rights. It recognises that AI must be developed within a robust governance framework anchored in transparency, accountability and trust, supported by strong data foundations, institutional coordination and investment in human capital. The Strategy further underscores the importance of collaboration across Government, private sector, academia and civil society to ensure that AI contributes to sustainable development and shared prosperity. The link to access the AI Strategy is available at:
https://mitci.govmu.org/mitci/wp-content/uploads/2026/04/aistrategy.pdf

This Strategy is complemented by the FAIR (Fairness, Accountability, Inclusiveness and Integrity and Responsibility) Guidelines which provide a practical and flexible governance framework for the responsible development and use of AI systems across their entire lifecycle. The Guidelines are grounded in core principles that ensure AI systems operate without unjustified bias, maintain clear lines of accountability, promote inclusiveness and integrity and are subject to continuous monitoring and responsibility over time. They adopt a risk-based approach, recognising that governance and oversight must be proportionate to the potential impact of AI systems, while reinforcing alignment with existing legal frameworks, including data protection requirements. Together, these instruments provide a coherent national approach to AI governance, promoting trust, safeguarding individual rights and supporting innovation across sectors. The FAIR Guidelines may be accessed at:

https://mitci.govmu.org/mitci/wp-content/uploads/2026/04/FINAL-GUIDELINES-15AVRIL.pdf

Financial institutions worldwide including banks, insurance firms, asset managers and Fintech startups and companies are increasingly utilizing AI-driven personas. These virtual agents deliver services, offer guidance and manage tasks with a level of responsiveness and realism that closely mimics human behaviour. These digital personas go far beyond basic chatbots or scripted automation. They are powered by advanced neural networks capable of recognizing emotional cues demonstrating empathy and adapting to each user's behaviour over time. By integrating large language models with contextual financial data and user history, they can personalize conversations, recall previous interactions and even align with cultural expectations. In finance, such AI personas can fulfill a variety of roles namely:

- Serve as investment advisors that adjust portfolios based on changing client risk profiles.
- Deliver highly personalized client service thereby strengthening relationship management.
- Detect and prevent fraud through nuanced behavioural analysis.

However, the rise of AI personas also raises several critical ethical concerns:

1. Sensitive Data Handling: AI personas usually process personal and financial data, raising risks of misuse or breaches.
2. Over-Reliance and Misrepresentation: Customers may perceive AI personas as human advisors, creating a risk of undue dependence on their guidance and blurring lines of accountability.
3. Accountability and Responsibility Gaps: When AI-generated advice results in financial loss, it's unclear who is legally liable, raising complex regulatory questions.
4. Bias and Discrimination: Without stringent oversight, these systems may inherit and reproduce biases from their training data, potentially leading to unfair financial decisions.

To address these issues, it is essential that proper principles of data protection are followed."The foundational principles of any AI system should rely on transparency, fairness and accountability". This will ensure that processing operations are not opaque to individuals and that they are informed of the identity of the AI institutions processing their data as well as how their data is used, decisions that are made on this basis and the logic behind those decisions to prevent any unfair bias against them. AI institutions must establish the provenance of data and ensure the quality and relevance of the data entered into the algorithms.

Additionally, adopting a risk-based approach to AI is of paramount importance. Robust data security measures and the use of pseudonymisation and anonymisation techniques should be advocated to prevent personal data from being easily linked to specific individuals. Since AI systems process huge amounts of data, they are often the target of cyber threats. Therefore, deploying the necessary organisational and technical measures will prevent data control from falling into the wrong hands. Regular audits and assessments are also necessary to identify and mitigate data privacy and security issues. Privacy design should be embedded at the heart of technology development.

The essence of all technological developments, including AI, should be based on user consent and control. Users should have the right to understand and control how their data is used in AI systems. This perspective strengthens the idea that individuals should be active participants in the data-driven AI ecosystem. The caution line in this environment is: *"If it is not you who control the parameters of your data, then it's someone else controlling you!"*

The rapid development of AI has transformed the current business landscape. Businesses leverage AI solutions for a variety of purposes, including automating customer service, improving business intelligence, and facilitating strategic decision-making. While AI has the potential to drive innovation by automating many digital tasks, it is also seen as a potential threat that requires regulation.
The European Union introduced a groundbreaking initiative by the formulation of the EU AI Act and paved the way for comprehensive AI regulation. It is the first legislation of its kind in the world, which regulates the use of AI in Europe, respects the values and rules, and harnesses the potential of AI for industry. The gist of the AI Act is a classification system that determines the level of risk an AI technology could pose to the health and safety or fundamental rights of a person. The framework incorporates four risk tiers: unacceptable, high, limited and minimal.

Our Mauritius Data Protection Act 2017 caters for strong and robust principles applicable in the AI sphere, covering amongst others:

- ***Principles relating to processing of personal data (section 21)***
- ***Automated individual decision making (section 38)***
- ***Duties of controller (section 22)***
- ***Collection of personal data (section 23)***
- ***Notification of personal data breach (section 25)***
- ***Duty to destroy personal data (section 27)***
- ***Lawful processing (section 28)***
- ***Special categories of personal data (section 29)***
- ***Security of processing (section 31)***
- ***Data protection impact assessment (section 34)***
- ***Right of access (section 37)***
- ***Rectification, erasure or restriction of processing (section 39)***
- ***Right to object (section 40)***

Setting up the right data governance, legal and ethical framework is crucial to contain the risks associated with AI. This requires a multi-faceted approach to AI, including robust data governance, privacy-preserving AI techniques, responsible AI development practices, transparency in AI decision-making, and adherence to relevant legal and ethical frameworks. AI organisations and policymakers need to collaborate to strike a balance between harnessing the potential of AI and safeguarding individuals' rights and interests regarding their data.

16.0 Management Companies

This Office has issued the following guidance to provide greater clarity on the application of the DPA and Data Protection (Designation, Tasks and Position of Data Protection Officers) Regulations 2026 to Management Companies and managed entities. The guidance is also published on the Data Protection Office website.

Advice to Management Companies (MCs)

16.1. Relevant provisions and definitions under the DPA

16.1.1 Application of the Act – section 3(5), (6) and (7) of the DPA

Section 3(5)
"Subject to section 44, this Act shall apply to a controller or processor who –
(a) is established in Mauritius and processes personal data in the context of that establishment; and
(b) is not established in Mauritius but uses equipment in Mauritius for processing personal data, other than for the purpose of transit through Mauritius."
Section 3(6)
"Every controller or processor referred to in subsection (5)(b) shall nominate a representative established in Mauritius."
Section 3(7)
"For the purpose of subsection (5)(a), any person who –
(a) is ordinarily resident in Mauritius; or
(b) carries out data processing operations through an office, branch or agency in Mauritius,
shall be treated as being established in Mauritius."

16.1.2 Definitions – section 2 of the DPA

Controller
"controller" means a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing;

Processor
"processor" means a person who, or public body which, processes personal data on behalf of a controller;

Personal data
"personal data" means any information relating to a data subject;

25 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62020CJ0037

the processing.

Processing

"processing" means an operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

16.1.3 Registration – section 14 of the DPA

"Subject to section 44, no person shall act as controller or processor unless he or it is registered with the Commissioner."

16.1.4 Data Protection Officer

Section 22(2)(e) of the DPA

Section 22(2) provides that the measures referred to in section 22(1) shall include –

"(e) designating an officer responsible for data protection compliance issues."

Data Protection (Designation, Tasks and Position of Data Protection Officers) Regulations 2026

"3. (1) Subject to paragraph (2) and regulations 5 and 6, every controller shall, for the purpose of section 22(2)(e) of the Act, designate, from a staff member of the organisation, a data protection officer for the purpose of carrying out the tasks specified under regulation 4."

16.2. Interpretation: registration as controller and processor

16.2.1 Controller registration. A person or entity that determines the purposes and means of the processing of personal data and has decision-making power in respect of that processing acts as a controller and is required to register under the DPA.

16.2.2 Processor registration. A person or entity that processes personal data on behalf of a controller acts as a processor and must register as a processor. Registration as a processor is therefore a separate obligation from registration as a controller. The Data Protection (Fees) Regulations 2020 prescribe the fees applicable to registration and renewal as controllers and processors.

16.2.3 Dual capacity. An entity may act as a controller and as a processor. Where this occurs, it must register in each capacity in which it acts.

16.2.4 Internal departments. An internal department of an organisation is not a separate processor merely because it processes personal data for another department of the same legal entity. Processor status concerns processing carried out on behalf of a separate controller.

16.3. Management Companies

16.3.1 Registration as controller. Every Management Company must register as a controller. A Management Company processes personal data for its own purposes and determines the purposes and means of such processing, including, as applicable, personal data relating to its employees, directors, shareholders, clients, suppliers, compliance functions, statutory obligations and its own administration.

16.3.2 Registration as processor. A Management Company must additionally register as a processor where it processes personal data on behalf of one or more managed entities and does not determine the purposes and means of that processing. This may include processing undertaken under a management, administration, company secretarial or other service arrangement where the managed entity remains the controller and the Management Company acts on its instructions.

16.3.3 Separate capacities. Registration of the Management Company as a controller does not replace its obligation to register as a processor where it also carries out processing on behalf of managed entities. Likewise, registration of the Management Company does not, by itself, remove the separate registration obligations of any managed entity.

16.3.4 Data Protection Officer. Each Management Company must have its own Data Protection Officer in accordance with the applicable provisions of the DPA and the Data Protection Officers Regulations 2026. The Data Protection Officer of the Management Company is not, merely by reason of that appointment, the Data Protection Officer of each managed entity. Kindly consult the Guidance Notes under the Data Protection Officers Regulations 2026 for further information.

16.4. Managed Entities - General rule

16.4.1 Separate registration

Each managed entity is a separate legal entity and must be assessed on its own processing activities. Where the managed entity acts as a controller or processor within the scope of the DPA, it must register separately in the relevant capacity. The fact that its activities are administered by a Management Company does not, by itself, dispense with the managed entity's registration obligation.

16.4.2 No automatic exemption

A managed entity should not assume that it is exempt from registration or from the requirement to have a Data Protection Officer merely because it has no employees, no physical premises, limited activities or because its records are maintained by a Management Company. These circumstances are relevant factors but are not determinative on their own.

16.4.3 Data Protection Officer

A managed entity must have its own Data Protection Officer. Where the circumstances fall within the categories addressed in the Guidance Notes on the designation and certification of Data Protection Officers, the managed entity may submit its special circumstances for consideration in accordance with the Guidance Notes. The appointment of the Management Company's Data Protection Officer does not automatically satisfy the obligation of the managed entity.

16.5. Managed Entities - Case-by-case approach

16.5.1 When the case-by-case approach may be requested.

Where a Management Company or managed entity considers that, having regard to its particular structure and processing arrangements, the ordinary registration and/or Data Protection Officer requirements may require individual determination, the matter shall be submitted to the Data Protection Office for a case-by-case assessment. Until a determination is made, no general exemption should be presumed.

16.5.2 Individual determination. Each case will be considered on its own facts and circumstances. No generalisation should be made from the determination for one managed entity to another.

16.5.3 Criteria and information for assessment

The Data Protection Office may consider, among other relevant matters, the following criteria:

1. Nature of the business and the activities of the managed entity.
2. Whether the managed entity has any employees or other staff members and the functions performed by them.
3. The identity and role of the directors, owners or partners.
4. Whether the managed entity has premises, an office, branch, agency or other operational presence in Mauritius.
5. Whether personal data relating to the managed entity are centralised and held by the Management Company, and if so, the extent of that centralisation.
6. Whether the Management Company is taking all legal responsibilities related to the processing of

Example: A management company is administering a GBC. The MC has decision making power with regard to the processing of the personal data and all the data are centralised at the MC. The GBC does not personal data.

7. The categories and approximate volume of personal data processed and the categories of data subjects concerned.
8. Whether special categories of personal data or other higher-risk personal data are processed.
9. The systems and applications used to collect, access, process, transfer or store the personal data, and who controls those systems.
10. Whether processing activities are carried out in Mauritius.
11. Who gives instructions to the Management Company concerning the processing of personal data.
12. Any other fact or circumstance which the Data Protection Office considers relevant to the determination.

Where deemed appropriate, a site visit inspection may be undertaken by the Data Protection Office.

16.5.4 Submission to the Data Protection Office

A request for case-by-case assessment should identify the managed entity/ies concerned and provide complete supporting information addressing the criteria above. Important: This guidance does not create a blanket exemption for any category of managed entity. Registration and Data Protection Officer obligations are determined by the DPA, the applicable Regulations and Guidance Notes and the particular facts of each entity.

17.0 Some examples of oversight bodies in the financial sector

17.1 Ministry of Financial Services and Economic Planning

The Ministry of Financial Services and Economic Planning was established in December 2014 with a view to giving a new impetus to the financial services sector which is a key sector of our economy and has a huge potential for growth. Besides the promotion of financial services, this Ministry provides guidance and support for the enforcement of good governance practices in order to restore the national values in Mauritius through the eradication of fraud, corruption, malpractices and irregularities in all aspects of public life[26].

Further, since 2021, a permanent AML/CFT/CPF unit has been set up at the Ministry of Financial Services and Economic Planning for planning and implementing policies, strategies, systems and processes in line with FATF Standards. It is also involved in coordinating risk assessments exercise, drafting technical compliance re-rating applications, preparing reports for relevant international bodies to ensure continuous compliance with evolving AML/CFT/CPF standards.

26 https://financialservices.govmu.org/Pages/TheMinistry.aspx

17.2 Bank of Mauritius

The Bank of Mauritius is a statutory body established under the Bank of Mauritius Act to act as the central bank of the Republic of Mauritius. In the pursuit of its objects set out in the Act, the Bank is required to perform its functions independently.

The general policy of the affairs and business of the Bank, other than the formulation and determination of monetary policy, is entrusted to a Board of Directors.

The Governor is the principal representative of the Bank of Mauritius and is responsible for the execution of the policy of the Board and the general supervision of the Bank. She is assisted by two Deputy Governors who are responsible for the day-to-day administration of the Bank under the general supervision of the Governor.

Section 5 of the Bank of Mauritius Act 2004 prescribes several functions that are necessary for the Bank to attain its objects, some of which are the following:

(i) to regulate and supervise financial institutions and any other Institution which the Bank of Mauritius may license or authorise under the banking laws to carry out activities in, or from within, Mauritius;
(ii) to regulate and supervise ultimate and intermediate financial holding companies, incorporated in Mauritius, which have, within the group, at least one subsidiary or joint venture, or such other ownership structure as the Bank may determine, which is a bank or non-bank deposit taking institution licensed by the Bank of Mauritius;
(iii) to manage, in collaboration with other relevant supervisory and regulatory bodies, the clearing, payment and settlement systems of Mauritius; and
(iv) to collect, compile, disseminate, on a timely basis, monetary and related financial statistics.

The Bank of Mauritius also derives its licensing and supervisory powers for the banking sector and the national payment systems under the Banking Act and NPS Act. As part of its functions, the Bank of Mauritius is thus required to -

(i) ascertain and promote the soundness of financial institutions and their compliance with governing laws, rules and regulations;
(ii) ensure the adoption by financial institutions of policies and procedures designed to control and manage risks effectively;
(iii) adopt policies to safeguard the rights and interests of depositors and creditors of financial institutions, having due regard to the need for financial institutions to compete effectively in the market and take reasonable risks;
(iv) monitor system-wide factors that might have or potentially have a negative impact on the financial condition of financial institutions;
(v) promote public understanding of the financial system, including awareness of the benefits

and risks associated with different financial products regulated by the Bank, which are offered by financial institutions;

(vi) carry out investigations and take measures to suppress illegal, dishonourable and improper practices, market abuse and any potential breach of the banking laws.

The Bank is also the designated AML/CFT/CPF supervisor for institutions operating in the banking sector and ensures that these institutions comply with the AML/CFT/CPF requirements set out under the banking laws which include, the Convention for the Suppression of Financing of Terrorism Act, FIAMLA, POTA, Financial Crimes Commission Act 2023, the Prevention of Terrorism (International Obligations) Act and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 as well as regulations and guidelines made thereunder.

The Bank may also, from time to time issue such guidelines, directives or instructions to its licencees, as it considers necessary for the purposes of the banking laws and the NPS Act.

The following measures, amongst others are undertaken by the Bank of Mauritius:
The Bank has, as part of the supervisory process, issued various guidelines on both prudential and AML/CFT/CPF matters and requires its licensees to comply with the provisions contained therein. The Bank monitors and ensures compliance of the various guidelines/directives/instructions by its licencees through on-site and off-site supervision in line with the requirements of the Banking Act 2004.

The Guidelines issued by the Bank are available at:
https://www.bom.mu/financial-stability/supervision/guideline

The Bank conducts regular examinations of the operations and affairs of every financial institution at least once every 2 years or within such other period as the central bank may determine in order to cater for a risk-based approach. Where in relation to any financial institution, a special examination appears to be necessary or expedient in order to determine whether the financial institution is in a sound financial condition and whether the banking laws or any enactment relating to anti-money laundering or prevention of terrorism or directives, guidelines and instructions issued by the central bank, as the case may be, are being complied with, the central bank may appoint one or more of its officers or such other duly qualified person to conduct a special examination in respect of the affairs of the financial institution and of its affiliates and overseas branches and affiliates, if any.
The Bank further verifies compliance with the banking laws, the NPS Act and Regulations made thereunder during off-site and also during the course of on-site inspections for institutions falling under its purview.

The Bank may also impose administrative sanctions, where a financial institution has failed to comply with the provisions of the Banking Act or any condition attached to its licence.

The NPS Act and the National Payment Systems (Authorisation and Licensing) Regulations 2021 (NPS

Regulations) provide for the regulation, overseeing and supervision of the national payment systems and payment systems being operated in Mauritius primarily for the purpose of ensuring their safe, secure, efficient and effective operation and accessibility to the public and designates the Bank of Mauritius as the authority for that purpose. The NPS Act sets the framework for the regulation, oversight, and supervision of payment systems in Mauritius.

Governing legislations and regulations

The Bank of Mauritius Act 2004	The banking sector in Mauritius is governed primarily by the Bank of Mauritius Act 2004, the Banking Act 2004, the National Payment Systems Act 2018 and Regulations made thereunder. The Bank of Mauritius was established in September 1967 as the central bank of the country under the Bank of Mauritius Act 1966. The Bank of Mauritius Act 1966 was repealed with the enactment of a new Bank of Mauritius Act in 2004. The 2004 Act enhances the independence of the Bank of Mauritius, moved towards the adoption of the primary objective of the Bank as being to maintain price stability and to promote orderly and balanced economic development. The Bank further regulates credit and currency in the best interests of economic development of Mauritius, to ensure the stability and soundness of the financial system of Mauritius. The Bank of Mauritius is also the prudential and the designated AML/CFT/CPF regulator and supervisor of financial institutions under its purview, i.e., banks, non-bank deposit taking institutions, and cash dealers (money changers and foreign exchange dealers) which it licenses under the Banking Act 2004, as well as payment service providers and payment system operators which are licensed/ authorised under the National Payment Systems Act 2018.

The Banking Act 2004	The Banking Act 2004 is the enabling legislation for all the financial institutions falling under the purview of the Bank. The basic objectives of the Banking Act 2004 are to maintain a sound banking system in Mauritius and to protect the interests of depositors. The Banking Act 2004 incorporates general principles of prudential regulation and supervision of licensed financial institutions, including licensing requirements.
The National Payment Systems Act	The National Payment Systems Act 2018 ("the NPS Act") and the National Payment Systems (Authorisation and Licensing) Regulations 2021 (NPS Regulations) provide for the regulation, oversight and supervision of the national payment systems and payment systems being operated in Mauritius primarily for the purpose of ensuring their safe, secure, efficient and effective operation and accessibility to the public and designates the Bank of Mauritius as the authority for that purpose. The NPS Act designates the Bank as the authority which may issue a license to a person to act as a payment service provider and authorize a person to operate a payment system. Payment Service Providers and Payment System Operators are, respectively licensed and authorized by the Bank under the NPS Act.
Web links	The Bank of Mauritius Act 2004, the Banking Act 2004, the National Payment Systems Act 2018 and the National Payment Systems (Authorisation and Licensing) Regulations 2021 are available on the following web links. https://www.bom.mu/about-bank/legislations/bank-mauritius-act-2004 https://www.bom.mu/about-bank/legislations/banking-act-2004 https://www.bom.mu/about-bank/legislations/national-payment-systems-act-2018

Powers of the Bank of Mauritius

As the regulator for the Banking Sector, the Bank of Mauritius is entrusted with extensive regulatory and supervisory powers to ensure that its licensees operate in a sound manner thereby contributing in maintaining the stability of the financial system.

Amongst others, the Bank of Mauritius may undertake the following :

The Bank of Mauritius Act 2004	The Bank of Mauritius also regulates credit and currency in the best interests of the economic development of Mauritius, ensures the stability and soundness of the financial system of Mauritius and acts as the central bank for Mauritius. The main functions of the Bank are:- (i)Conducting monetary policy and managing the exchange rate of the rupee. (ii)Regulating and supervising banks, non-bank deposit taking institutions and cash dealers. (iii)Management of the clearing, payment and settlement systems. (iv)Collecting, compiling, disseminating monetary and related financial statistics. (v)Management of foreign exchange reserves. <u>Power to issue instructions</u> Section 50 of the Bank of Mauritius Act 2004 empowers the Bank of Mauritius to, for the efficient achievement of the purposes of the Act, by notice in writing to banks or to other financial institutions, issue instructions or guidelines or impose requirements on or relating to the operations and activities of and standards to be maintained by the banks and other financial institutions. <u>Power to make rules</u> Section 50A of the Bank of Mauritius Act 2004 empowers the Bank of Mauritius to make such rules as it may determine for the purpose of the banking laws. <u>Power to impose administrative penalty</u> The Bank may impose an administrative penalty on any financial institution which refrains from complying, or negligently fails to comply, with any instructions or guidelines issued by the Bank or requirement imposed under the banking laws, or where the financial institution has failed to comply with the requirements imposed under a code or guideline issued by the Bank under the FIAMLA.

	Power to impose monetary penalty The Bank may, with the consent of the Director of Public Prosecutions (DPP) compound any offence committed by a person under the Banking Act and Bank of Mauritius Act which is prescribed as a compoundable offence, where the person agrees in writing to pay such amount not exceeding the maximum penalty specified for the offence, acceptable to the Bank. Information from banks and other financial institutions Section 51 of the Bank of Mauritius Act 2004 empowers the Bank of Mauritius to require any financial institution to furnish, at such time and in such manner and form as may be approved by the Bank of Mauritius, such information and data as the Bank of Mauritius may require for the proper discharge of its functions and responsibilities under the banking laws. Also, the Bank may examine the accounts, books, records and other documents, whether they are in written form or are kept on microfilm, magnetic tape, or any other form of mechanical or electronic data retrieval mechanism, of any financial institution, in order to verify its compliance with any requirement under the banking laws. Application to the Court The Bank of Mauritius may apply to a Judge in Chambers for an order in respect of any matter relating to any of its functions under section 5 of the Bank of Mauritius Act 2004. The order of the Judge in Chambers may direct a person to do a specified act or refrain from doing a specified act, for the purposes of – (i) preventing a contravention of the banking laws; (ii) compelling any person to comply with a lawful request, direction or instruction made, issued or given by the Bank under the banking laws; (iii) remedying the effects of a contravention; (iv) ensuring that the person does not commit further contraventions of the banking laws; (v) preserving the assets of a financial institution; or (vi) compensating any person who has suffered loss because of a contravention. Under section 5 of the Bank of Mauritius Act 2004, the Bank also has the right to institute and conduct proceedings in any Court of law against any financial institution for the proper application of the banking laws, ask for and obtain declaratory orders from the Supreme Court of Mauritius, seek guidance and directions from the Supreme Court of Mauritius on any point of law or as to the interpretation of any provision of the banking laws and intervene in any proceedings in which a financial institution is a party.
The Banking Act 2004	The Banking Act 2004 consolidates the laws relating to the business of banking and other financial institutions. The Bank has broad powers under this Act for the effective regulation and supervision of its licensees. In cases of necessity, the Bank is also empowered to revoke a banking licence , where: (i) a bank has been convicted by a court of an offense under any enactment relating to anti-money laundering or prevention of terrorism; or (ii) a bank is carrying on business in a manner which is contrary or detrimental to the interests of its depositors or the public, fails to comply with any directive or instruction issued by the central bank under the banking legislation or contravenes any provision of the banking legislation.

	The Banking Act incorporates general principles of prudential regulation and supervision of licensed financial institutions such as: (i) Licensing of banks and other financial institutions; (ii) Capital structure and other financial requirements; (iii) Limitation on operations; (iv) Audit and supervision including on-site examinations and off-site surveillance; (v) Administration of financial institutions; (vi) Compliance with AML/CFT/CPF; and (vii) Conservatorship, voluntary and compulsory liquidation of financial institutions. <u>Power to grant banking licenses</u> The Bank has the power to grant licenses to applicants to engage in banking business, Islamic banking business, digital banking business or private banking business in Mauritius. It may also at any time, amend, vary or cancel any condition attached to, or impose new conditions on, the licence. Regular and special examinations Section 42 of the Banking Act 2004 empowers the Bank of Mauritius to conduct regular examinations of the operations and affairs of every financial institution at least once every 2 years or within such other period it may determine, including, where the Bank of Mauritius so specifies, of affiliates and overseas branches and affiliates of the financial institution. The examinations may be conducted by the officers of the Bank or such other duly qualified person as it may appoint. Such examinations may be of a scope as the Bank deems necessary to assess that the financial institution is duly observing the provisions of the banking laws, directives, guidelines, and instructions issued by the Bank and is in a sound financial condition. The Bank of Mauritius may, in addition, under section 43 of the Banking Act 2004 appoint one or more of its officers or such other duly qualified person to conduct a special examination in respect of the affairs of the financial institution and of its affiliates and overseas branches and affiliates, if any where it appears to be necessary or expedient in order to determine whether the financial institution is in a sound financial condition and whether the banking laws or any enactment relating to anti-money laundering or prevention of terrorism or directives, guidelines and instructions issued by the Bank of Mauritius, as the case may be, are being complied with.

	Where the Bank of Mauritius has reason to believe that any person who, either as a principal or as an agent, carries on, advertises or holds himself out in any way as carrying on banking business, deposit taking business, business of foreign exchange dealer or money changer or accepting deposits from the public, without a licence or written authorisation from the Bank of Mauritius, it: (i) shall require the person to produce for examination its books, accounts, records and financial statements and such other information and certified copies of all relevant documents as it may require to ascertain whether the person is carrying on that business; (ii) may cause a notice in writing to be issued, calling upon any person who is suspected to be involved in engaging in activities under the banking laws without holding the appropriate licence, to attend the Bank of Mauritius for the purpose of being examined orally in relation to any matter which may assist in its investigation and calling upon the person to produce any book, document or information in his possession within the period specified in the notice; and (iii) may issue a warning alert to caution the public that the person specified in the alert may be engaging in activities under the banking laws without holding the appropriate licence issued by the Bank of Mauritius. For the purposes of the examination, the examiners and special examiners have the power to: (i) examine all books, minutes, accounts, records, cash, securities, vouchers and any other document, in the possession or custody of the financial institution or of its affiliates in Mauritius or its branches and affiliates outside Mauritius, (ii) have access to any program or data and take extracts of any file, document or record held electronically in any computer or other electronic device of the financial institution or of its affiliates in Mauritius or its branches and affiliates outside Mauritius, (iii) request a financial institution to provide it with an off-site or remote access to such information and system as may be required for the conduct of the examination; and (iv) require, within such time as may be specified, such information and copies of all relevant documents, that he may reasonably require concerning its business, or that of its affiliates in Mauritius, or that of its branches and affiliates outside Mauritius, if any, as appear necessary. <u>Power to issue Directives, guidelines or instructions</u> Under section 100 of the Banking Act 2004, the Bank of Mauritius may make such directives, guidelines or instructions as it thinks fit for the purposes of this Act. The directives, guidelines or instructions shall apply to all financial institutions or to one or more categories of financial institutions. The Bank of Mauritius may also issue specific instructions to any financial institution. The Bank of Mauritius may also issue such guidelines, instructions or directives as it may determine to ultimate and intermediate financial holding companies incorporated in Mauritius which have, within the group, at least one subsidiary or joint venture or such other ownership structure as the Bank of Mauritius may determine, which is a bank or a non-bank deposit-taking institution.

	The Bank of Mauritius may, by guidelines, instructions or directives issued require the ultimate and intermediate financial holding companies incorporated in Mauritius which have, within the group, at least one subsidiary or joint venture or such other ownership structure as it may determine, which is a bank or a non-bank deposit-taking institution, to comply with such specific provision of this Act as it considers appropriate so as to ensure effective supervision of the institution.
The National Payment Systems Act and the National Payment Systems (Authorisation and Licensing) Regulations 2021	The Bank of Mauritius has powers and duties under the National Payment Systems Act to - (i) formulate and adopt a national payment system policy for Mauritius; (ii) issue a licence to payment service providers or grant an authorisation to operators of payment systems; (iii) determine general or individual conditions, standards, rules and procedures in accordance with this Act and any other implementing measures applicable to any entity to which it has issued a licence or granted an authorisation and their activities and ensure that the conditions, standards, rules and procedures are applied; (iv) establish a forum for the consideration of matters of policy and mutual interest concerning the national payment systems; (v) issue directives, instructions and guidelines for the operation of the national payment systems; (vi) collect, compile, disseminate, on a timely basis, monetary and related financial statistics related to the national payment systems; and (vii) perform such other duties relating to payment systems, clearing systems and settlement systems or the issue of payment instruments for the accomplishment of its duties. The Bank has the power - (i) to issue a license or authorization to payment service providers or operators; (ii) to suspend or revoke an authorisation granted under this Act in such manner as may be prescribed. The Bank has the power take administrative actions with respect to a payment service provider, an operator, a participant or its directors where it determines that one or more entities has or have contravened the National Payment Systems Act or any directives, instructions or guidelines issued by the central bank.

Personal data and special categories of personal data processed by the Bank of Mauritius

The type and amount of personal data that the Bank of Mauritius and financial institutions in the banking sector may collect would depend on the purpose and intention for processing.

Personal data collected at the Bank of Mauritius are processed lawfully and according to rules of fairness and confidentiality, in compliance with the requirements of the DPA. The Bank of Mauritius use confidential information and documents for lawful purpose in fulfilling its obligations.

Section 52 of the Bank of Mauritius Act provides that the Bank may, for the purpose of ensuring the operation of a sound credit information system in, and maintaining the stability and soundness of the financial system of Mauritius, establish a Credit Information Bureau and require, on such terms and conditions as it may determine, any institution offering credit, including leasing facilities and hire purchase or, any crowdlending platform or any utility body, to furnish at such time and in such manner such credit information or such other information as it may require for the purpose of –

(a) maintaining a database on recipients of credit facilities and guarantors and such other information as may reasonably assist in ensuring the soundness of the credit information system;
(b) collecting, consolidating and collating trade, credit and financial information on recipients of credit facilities, whether fund-based or non fund-based;
(c) storing the information so collected, amongst others.

Personal Information collected by the Bank of Mauritius	The following are examples, amongst others: - Name - Address - National Identity Card/ Passport Number/ Company or Registration Number - Residential Address/Physical business address, - Telephone/Mobile/contact Nos. - Marital Status - Date of Birth - Gender - Medical History - Signature - Citizenship/Nationality - Professional positions - VAT Registration number - TAN No, Address, PAYE details and Bank details - Press cards - Vehicle registration numbers,

Special categories of personal data	- CCTV Footage - Legal Convictions - Biometric data: For Security Access Control to specific users - Commission or alleged commission of an offence: For Recruitment of employees/ Fit & Proper Test (Certificate of character).

Registration Obligation and mandatory appointment of Data Protection Officer

"bank"	"bank" means a company incorporated under the Companies Act, or a branch of a company incorporated abroad, which is licensed under section 7(5) of the Act to carry on any or all of the following – (a) banking business; (b) Islamic banking business; (c) private banking business; (d) digital banking business;
"banking business"	"banking business" – (a) means – (i) the business of accepting sums of money, in the form of deposits or other funds, whether or not such deposits or funds involve the issue of securities or other obligations howsoever described, withdrawable or repayable on demand or after a fixed period or after notice; and (ii) the use of such deposits or funds, either in whole or in part, for – (A) loans, advances or investments, on the own account and at the risk of the person carrying on such business; (B) the business of acquiring, under an agreement with a person, an asset from a supplier for the purpose of letting out the asset to the person, subject to payment of instalments together with an option to retain ownership of the asset at the end of the contractual period; (iii) paying and collecting cheques drawn by or paid in by customers and making other payment instruments available to customers; and (b) includes such services as are incidental and necessary to banking;
"banking licence"	"banking licence" means a banking licence, an Islamic banking licence, a digital banking licence or a private banking licence granted under section 7;

"deposit taking business"	"deposit taking business" means the business of accepting – (a) deposits of money for the purpose of - (i) financing the specific activities of the non-bank deposit taking institution receiving such deposits or such other activities as may be approved by the central bank; and (ii) investment in Government securities, Bank of Mauritius Bills issued under the Bank of Mauritius Act 2004 or such other investment as may be approved by the central bank; or (b) Islamic deposits for the purposes of financing the activities of the non-bank deposit taking institution receiving such deposits or such other activities as may be approved by the central bank, the aims and operations of which are, in addition to the conventional good governance and risk management rules, in consonance with the ethos and value system of Islam;
"digital banking business"	"digital banking business" means banking business carried on exclusively through digital means or electronically;
"financial institution"	"financial institution" means any bank, non-bank deposit taking institution or cash dealer licensed by the central bank;
"foreign exchange dealer"	"foreign exchange dealer" means any body corporate licensed as such by the central bank to carry on the business of - (a) buying and selling foreign currency, including spot and forward exchange transactions and wholesale money market dealings; and (b) a money-changer; (c) money or value transfer services;
"Islamic banking business"	"Islamic banking business" means any financial business, the aims and operations of which are, in addition to the conventional good governance and risk management rules, in consonance with the ethos and value system of Islam;
money-changer"	"money-changer" means any body corporate licensed as such under this Act to carry on solely the business of - (a) buying and selling of foreign currency notes, coins and travellers' cheques; (b) replacement of lost or stolen travellers' cheques; and (c) encashment under credit cards;
"private banking business"	"private banking business" means the business of offering banking and financial services and products to high-net-worth customers, including but not limited to an all-inclusive money-management relationship;

An applicant may be granted with either:

- a banking licence;
- an Islamic banking licence;
- a digital banking licence; or
- a private banking licence

Licensing Requirements for a Banking Licence as set out in the Banking Act

The licensing process for a banking licence	1. Applicants are required to submit an application for a banking licence. In terms of section 5 of the Banking Act, no person may engage in banking business in Mauritius without a banking licence issued by the central bank. Every application for a banking licence shall be made in such medium and in such form as the central bank may determine and shall be accompanied by a set of documents prescribed in the Banking Act, listed hereunder, and such other information or document as the Bank of Mauritius may specify in the form of application. (a) a copy of the certificate of incorporation of the applicant; (b) in the case of a foreign bank wishing to establish a branch, subsidiary or joint venture in Mauritius, by a written confirmation from the banking supervisory authority in the applicant's country of incorporation that the supervisory authority has no objection to the applicant's proposal to carry on banking business in Mauritius; (c) a copy of the constitution of the applicant; (d) a certified list of the full names and address of the directors, beneficial owners, chief executive officer and other senior officers of the applicant and a list of its shareholders owning 10 per cent or more of its shares; (e) a copy of the financial statements of the applicant, as of a date within 60 days preceding the date of application; (f) a business plan giving the nature of the planned business, organisational structure and internal control, projected financial statements including cash flow statements for each of the next 3 financial years; (g) in respect of the directors, chief executive officer, other senior officers and shareholders holding a significant interest, of the applicant, an identification and a certificate of good conduct, in such form as may be specified by the central bank, from a competent authority or an affidavit duly sworn stating any convictions for crimes and any past or present involvement in a managerial function in a body corporate subject to insolvency proceedings or having declared personal bankruptcy; (h) payment of the appropriate non-refundable processing fee as may be determined by the central bank by regulations made by the central bank, with the approval of the Minister; and

	(i) such other information or document as the central bank may specify in the form of application. 2. The application also includes an authority from the applicant authorising any regulatory body, law enforcement body or financial institution, in Mauritius or in a foreign country, to release to the central bank, for use in relation to the application and the enforcement of the Banking Act, any information about the applicant, and any of its directors, shareholders, beneficial owners, chief executive officer or other senior officers as may be applicable. 3. Under section 7 of the Banking Act, no banking license shall be granted by the Bank of Mauritius unless it is satisfied, amongst others,: (a) that the applicant has: (i) demonstrated that the directors or senior officers of the applicant have technical knowledge, experience in banking or finance and are fit and proper persons to carry on the proposed banking business; (ii) sufficient financial resources and an adequate capital structure to serve as a continuing source of financial support for the proposed bank; (iii) demonstrated the soundness and feasibility of the applicant's plans for the future conduct and development of the business of the proposed bank, including accounting and internal control systems; (iv) the ability and willingness to comply with such other conditions as the central bank may impose under the banking laws; (b) as to the history and character of the business and management of the applicant; (c) as to the convenience and needs of the community or market to be served; and (d) as to the fitness and suitability of the applicant's shareholders, particularly shareholders holding a significant interest. 4. An applicant is required to notify the Bank of Mauritius of any material change which may have occurred before or after the issue of a license in the information provided in the application.

The Bank of Mauritius and its licensees are registered as controllers as required by the DPA and have a data protection officer. Financial institutions have to comply with the provisions of the DPA regarding registration and appointment of a data protection officer.

Principles relating to processing of personal data

The National Payment Systems Act 2018	The NPS Act provides for confidentiality and record-keeping procedures for data processed by Payment Service Providers and Payment Service Operators. The express written consent of the customer of a Payment Service Provider or Payment Service Operator or participant has to be sought before disclosure in any form whatsoever, of any information relating to the affairs of the customer, except for the instances outlined at section 18(1), section 18 (1A) of the National Payment Systems Act and section 64 (1B) (3) to (7) of the Banking Act where the duty of confidentiality imposed under the section shall not apply.

Duties of Controller

The Bank of Mauritius Act 2004	Section 26 of the Bank of Mauritius Act requires every Director, officer or employee of the Bank of Mauritius or any person appointed by the Bank of Mauritius pursuant to the banking laws, to take an oath of confidentiality/make a declaration of confidentiality and proscribes such persons, during and after their relationship with the Bank of Mauritius, from disclosing directly or indirectly to any person any information, amongst others, relating to the affairs of the customers of any other bank or financial institution, which they have acquired in the performance of their duties or the exercise of their functions. They may only disclose such information for the purposes of (a) the performance of their duties or the exercise of their functions under the banking laws or meeting the requirements of an agreement or understanding reached by the Bank with any other relevant supervisory body or (b) when lawfully required to do so by an order of a Judge in Chambers or any Court of law or under any enactment. Every person appointed by the Bank for the purposes of carrying out regular examinations or special examinations under section 42 and 43 of the Banking Act 2004, are required under section 44 of the Act, to comply with the provisions of confidentiality under the banking laws.

	Under section 66 of the Bank of Mauritius Act 2004, the Bank of Mauritius keeps every record of the Bank for a period of at least 7 years after the completion of the transaction to which it relates, or the date of the record, as the case may be.
The Banking Act 2004	Section 64 of the Banking Act 2004 requires every person, including a service provider, having access to the books, accounts, records, financial statements or other documents of a financial institution to take an oath of confidentiality/make a declaration of confidentiality as applicable and proscribes such persons, during and after their relationship with the financial institution, from disclosing, directly or indirectly to any person, any matter or information relating to the affairs of any of its customers, including any deposits, borrowings, or transactions or other personal, financial or business affairs without the written consent of the customer or his personal representative. However, they may disclose such information for the purposes of the performance of their duties or the exercise of their functions under the banking laws or when lawfully required to do so by a Judge in Chambers or any court of law or under any enactment. Alternatively, a service provider may provide a financial institution with a written undertaking signed by its officer in charge and all its employees to the effect that they shall not, during and after their relationship with the financial institution, disclose, directly or indirectly to any person, any information relating to the affairs of any of its customers, including any deposits, borrowings, or transactions or other personal, financial or business affairs, without the written consent of the customer or his personal representative, and the financial institution requires the officer in charge of the service provider to make, on behalf of the service provider and all its employees, the declaration of confidentiality. It should be noted that section 64 provides instances where the duty of confidentiality does not apply. Regarding record keeping obligations, section 33 of the Banking Act 2004 requires every financial institution, for the purposes of the banking laws, to keep in relation to its activities, a full and true written record of every transaction it conducts. As regards risk, financial institutions, are required by section 54 of the Banking Act 2004, to maintain adequate internal control systems, commensurate with the nature and volume of its activities and various types of risks to which they are exposed.

The National Payment Systems Act 2018	Section 18 of the National Payment Systems Act requires every person who has access to the books, accounts, records, financial statements or other document, whether electronically or otherwise, to take an oath of confidentiality/make a declaration of confidentiality, before he begins to perform any duties under this Act. Such person shall not, during or after his relationship with the operator, participant or payment service provider, disclose to any person any information relating to the affairs of a customer of a participant or payment service provider, except (a) with the written authorisation of the customer or his personal representative; (b) for the purpose of the performance of his duties within the scope of employment or appointment in compliance with this Act; (c) as directed in writing by the Bank of Mauritius; or (d) when required to do so by a Court or under any enactment.
Guideline on Internet Banking	Under the Guideline on Internet Banking issued by the Bank of Mauritius in February 2001, the internet banking service should be designed and operated in such a manner that it always complies with all relevant laws and guidelines. Every institution should state clearly in its terms and conditions for internet banking services and on its website that the governing law is the Mauritian law.
Guidelines on Outsourcing by Financial Institutions	The Bank of Mauritius issued the Guidelines on Outsourcing by Financial institutions to set out a broad framework for financial institutions that have entered into outsourcing or are planning to outsource their business activities to service providers. Under the said Guidelines, financial institutions should abide by all relevant provisions of section 64 of Banking Act 2004 when entering into an outsourcing agreement, i.e., when they have recourse to third-party service providers to perform activities (which are normally undertaken by the financial institutions themselves) on a continuing basis. The Bank of Mauritius prescribes that outsourcing agreements should contain a clause that would address the service providers' responsibility for confidentiality and security. Financial institutions that engage in outsourcing should take appropriate steps to protect confidential customer information. Financial institutions should expressly prohibit service providers from disclosing confidential customer information to any third-party except for regulatory purposes.

Guideline on Mobile Banking and Mobile Payment Systems	The Bank of Mauritius has issued the Guideline on Mobile Banking and Mobile Payment Systems to regulate the mobile banking and mobile payment systems. The service providers and the retail agents shall maintain the confidentiality of all documents and information pertaining to their customers at all times and shall not, on any account and at any time, disclose directly or indirectly to any person, any matter or information relating to their customers unless legally authorised to do so.
Guideline for Digital Banks	Under the Guideline for Digital Banks issued by the Bank in December 2021, a digital bank has the obligation to duly inform and educate its customers of the financial products and financial services and the appropriate security measures to be taken in this respect. A digital bank shall ensure compliance with the relevant data protection laws and regulations.
Guideline on Use of Cloud Services	The Bank of Mauritius issued the Guideline on Use of Cloud Services to provide the necessary guidance to financial institutions engaging in the use of cloud services such that the risks are duly identified and managed. The said Guideline sets out the general requirements for the use of cloud services and the additional minimum requirements for the use of material cloud services and for cloud services which involve customer information. Material cloud service includes a service which involves customer information or other sensitive information and, in the event of any unauthorised access or disclosure, loss or theft of customer information, may have a material impact on the financial institution or its customers. The Bank of Mauritius issued the Guideline on Use of Cloud Services to provide the necessary guidance to financial institutions engaging in the use of cloud services such that the risks are duly identified and managed. The said Guideline sets out the general requirements for the use of cloud services and the additional minimum requirements for the use of material cloud services and for cloud services which involve customer information. Material cloud service includes a service which involves customer information or other sensitive information and, in the event of any unauthorised access or disclosure, loss or theft of customer information, may have a material impact on the financial institution or its customers.

	The Bank of Mauritius issued the Guideline on Use of Cloud Services to provide the necessary guidance to financial institutions engaging in the use of cloud services such that the risks are duly identified and managed. The said Guideline sets out the general requirements for the use of cloud services and the additional minimum requirements for the use of material cloud services and for cloud services which involve customer information. Material cloud service includes a service which involves customer information or other sensitive information and, in the event of any unauthorised access or disclosure, loss or theft of customer information, may have a material impact on the financial institution or its customers. In the Guideline, the Bank of Mauritius has prescribed that financial institutions shall ensure that all agreements for material cloud services and cloud services involving customer information (a) do not consist of clauses that would hinder the Bank of Mauritius from exercising its supervisory powers, (b) contain appropriate provisions to ensure compliance with the Mauritian data protection laws (Data Protection Act 2017, Information and Communication Technology Act) or to data protection laws which are equivalent to the Mauritian data protection laws at all times, and (c) impose confidentiality obligations on the cloud service provider which are in line with the underlying objective of section 64 of the Banking Act 2004 or section 18 of the National Payment Systems Act 2018.
Guideline on Cyber and Technology Risk Management	The Bank of Mauritius issued the Guideline on Cyber and Technology Risk Management in May 2023 to provide for the minimum requirements which banks and payment service providers are expected to implement with respect to cyber and technology risk management to ensure that the risks are well understood and managed appropriately. A financial institution shall put in place a robust and effective set of security controls that will enable it to fulfil its security objectives, which should include ensuring the continuity and availability of its information systems and the confidentiality, integrity and availability of information stored in its information systems, amongst others.

Collection of personal data

The Bank of Mauritius Act 2004	Also, the Bank of Mauritius has established the Mauritius Credit Information Bureau (MCIB) under section 52 of the Bank of Mauritius Act 2004 and requires institutions offering credit, including leasing facilities and hire purchase or, any crowdlending platform or any utility body, to furnish credit information or such other information as it may require for the purpose of: (a) maintaining a database on recipients of credit facilities and guarantors and such other information as may reasonably assist in ensuring the soundness of the credit information system, (b) collecting, consolidating and collating trade, credit and financial information on recipients of credit facilities, (c) storing the information so collected, (d) disclosing, or allowing access, to such institutions as it may approve, the information so collected, (e) assisting the Bank of Mauritius in the discharge of its functions under section 5(1) of the Bank of Mauritius Act, and (f) providing credit scores. Personal information on recipients of credit facilities and guarantors are collected by the MCIB, for the purpose of ensuring the operation of a sound credit information system in, and maintaining the stability and soundness of the financial system of Mauritius. The credit information so collected is used for the purpose of meeting the objectives of the MCIB and is kept confidential between the Bank of Mauritius and the participating institutions. Information maintained in the MCIB may be imparted by the Bank of Mauritius to specific institutions only, as provided in the Bank of Mauritius Act 2004. For the purposes of the MCIB, a utility body (including the Central Electricity Board, the Central Water Authority, the Waste Water Management Authority, etc) may, for the purposes of providing credit information to the MCIB, require any of its customers to provide it with the necessary identification details.

The Banking Act 2004	As per section 55 of the Banking Act, a financial institution shall only open accounts for deposits of money and securities, and rent out safe deposit boxes, where it is satisfied that it has established the true identity of the person in whose name the funds or securities are to be credited or deposited or the true identity of the lessee of the safe deposit box. Every financial institution shall require that each of its accounts be properly named, at all times, so that the true owner of the accounts can be identified by the public and no name shall be allowed that is likely to mislead the public. Furthermore, the Bank of Mauritius may issue guidelines, directives or instructions to any financial institution, class of financial institutions or holder of a licence, as it considers necessary for the prevention of money laundering or terrorism financing, under section 64B of the Banking Act, which may provide for (a) customer due diligence measures to be undertaken by financial institutions or holders of a licence to prevent money laundering and the financing of terrorism, (b) an on-going duty to keep customer due diligence information up to date in respect of both new and existing customers, and (c) the keeping of records for the above purposes. Also, per the Guideline on Anti-Money Laundering and Combating the Financing of Terrorism for Financial institutions issued by the Bank of Mauritius, it is mandatory for financial institutions to verify the true identity of their customers before opening any account, accepting any deposit of money and securities and renting a safe deposit box.
The Financial Intelligence And Anti-Money Laundering Act 2002 (FIAMLA)	The Banking Act includes the FIAMLA as the "banking laws" in Mauritius. The FIAMLA requires every financial institution to verify, in such manner as may be prescribed, the true identity of all customers and other persons with whom they conduct transactions, including when opening an account for, or otherwise establishing a business relationship with, a customer. The manner of verification of identity and address of customers is prescribed in the Financial Intelligence and Anti-Money Laundering Regulations 2018.
Guideline for Digital Banks	Under the Guideline for Digital Banks issued by the Bank of Mauritius in December 2021, a digital bank shall apply appropriate measures to authenticate and verify the identity of the customers.
The National Payment Systems Act	Collection of personal data is subject to the provisions of confidentiality and record-keeping outlined at sections 18 and 23 of the National Payment Systems Act.

Conditions for consent

A controller may process personal data, amongst others, for the performance of a contract to which a data subject is a party, and/or for compliance with any legal obligation, and/or for legitimate interests

The Bank of Mauritius Act 2004	Section 52(2A) of the Bank of Mauritius Act provides that the Bank of Mauritius may impart information maintained in the MCIB to such bodies as it considers appropriate for credit rating purposes, any public sector agency or law enforcement agency to enable the agency to discharge, or assist it in discharging, any of its functions, or such institutions and for such purpose as it may determine, where the person from whom the information is being sought has given his written consent for the information to be disclosed to the institution. Furthermore, any participating institution processing an application for credit facilities for its customer, having recourse to the information from the MCIB for this purpose, shall inform the customer that all available information will be used for the processing of the application.
The Banking Act 2004	As mentioned above, section 64 of the Banking Act 2004 provides, amongst others, that a person has access to the information or records of a financial institution shall take an oath/declaration of confidentiality. Except for the purpose of the performance of their duties or the exercise of their functions under the banking laws or as directed in writing by the Bank of Mauritius, such persons shall not during or after his relationship with the financial institution, disclose to any person any information relating to the affairs of any of its customers including any deposits, borrowings or transactions or other personal, financial or business affairs, without the prior written consent of the customer or his personal representative. The section further provides that any person who publishes information relating to the affairs of a customer or financial institution without the express written consent of the customer or financial institution shall commit an offence. Also, there are instances provided by section 64 of the Banking Act, where the duty of confidentiality imposed under this section shall not apply. Some of these instances are where: (a) a customer who had been issued a credit card or charge card by a financial institution, has his card suspended or cancelled by the financial institution by reason of his default in payment, and the financial institution discloses information relating to the customer's name and identity, the amount of his indebtedness and the date of suspension or cancellation of his credit card or charge card to other financial institutions issuing credit cards or charge cards in Mauritius;

	(b) the information is required by another financial institution for the purpose of assessing the credit-worthiness of a customer, provided that the information is being sought for commercial reasons and is of a general nature; (c) with respect to payable- through accounts, the customer due diligence information is required to be disclosed, upon request, by the financial institution to another institution with which it maintains a correspondent banking relationship, provided that the institution has given to the financial institution a written undertaking regarding the confidentiality of the information provided; (d) the customer due diligence information is required to be disclosed by the financial institution for the purpose of meeting the requirement set out by the central bank with respect to domestic or cross-border wire transfers or reliance on a third party; (e) in respect of credit information, the information is required for transmission to the guarantor of a credit facility contracted by the customer.
Guideline on Internet Banking	Under the Guideline on Internet Banking issued by the Bank of Mauritius in February 2001, prior to the offering of Internet banking services to their customers, each institution is required to ensure that the customers have agreed to the terms and conditions for internet banking services.
The National Payment Systems Act 2018	As mentioned above, section 18 of the National Payment Systems Act provides for the duty of confidentiality on persons who have access to the books, accounts, records, financial statements or other document, whether electronically or otherwise. Such persons shall not, during or after their relationship with the operator, participant or payment service provider, disclose to any person any information relating to the affairs of a customer of a participant or payment service provider. Exceptions are: (i) with the written authorization of the customer or his personal representative; (ii) for the purpose of the performance of his duties within the scope of employment or appointment in compliance with this Act; (iii) as directed in writing by the central bank; or (iv) when required to do so by a Court or under any enactment. (1A) The duty of confidentiality imposed under subsection (1) of section 18 shall not apply where the Ombudsperson requires information, documents and particulars to enable him to discharge, or assist him in discharging, any of his functions under the Ombudsperson for Financial Services Act 2018.

Notification of personal data breach and Communication to the data subject

The Banking Act 2004	Upon an application for a banking licence, section 5 of the Banking Act provides that the applicant shall notify the Bank of any material change which may have occurred, before or after the issue of a licence, in the information provided in his application. Section 54A on protection of whistleblowers provides that "Where a director, a senior officer, an employee or an agent of a financial institution – (a) discloses to the central bank that the financial institution or a customer of the financial institution may have been involved in an act which constitutes a breach of the banking laws; and (b) at the time he makes the disclosure, has reasonable grounds to believe that the information he discloses may be true, he shall incur no civil or criminal liability as a result of such disclosure and no disciplinary action shall be initiated against him by reason of such disclosure. (2) The central bank shall not, without the consent of the person making the disclosure, disclose the identity of that person.

While there are no specific requirements set out in the Banking Laws in respect of notification of data breach, the Bank of Mauritius has provided the following guidance to its licensees through its Guidelines:

Guideline on Internet Banking	As per the Guideline on Internet Banking, the institution's security policy should provide that its responsible officers should report security breaches promptly to the Bank of Mauritius.

Guideline on Mobile Banking and Mobile Payment Systems	The Guideline on Mobile Banking and Mobile Payment Systems requires that the mobile banking or mobile payment service provider (non-bank led models) to submit to the Bank of Mauritius on a monthly basis, any system security lapses and any loss of confidential data.
Guidelines on Outsourcing by Financial Institutions	Under the Guidelines on Outsourcing by Financial Institutions, the Bank of Mauritius has prescribed that a financial institution should report to the Bank of Mauritius immediately about any unauthorised access or breach of confidentiality and security, directly or indirectly, by an outsourced service provider and the action/s it is proposed to take in consequence.
Guideline on Use of Cloud Services	The Guideline on Use of Cloud Services issued by the Bank in September 2022 applies to all cloud-based arrangements entered by any financial institution licensed by the Bank of Mauritius under the Banking Act 2004 and the National Payment Systems Act 2018. Thereunder, financial institutions have a duty to report promptly to the Bank of Mauritius any incident including unauthorised access or breach of confidentiality and security, directly or indirectly, by a cloud service provider.
Guideline on Cyber and Technology Risk Management	The Guideline on Cyber and Technology Risk Management issued by the Bank of Mauritius in May 2023 provides that financial institutions shall report cyber and technology events and incidents to the Bank.

Duty to destroy personal data and retention period

There are, in Mauritius, sector-specific record keeping requirements.

Section 66 of the Bank of Mauritius Act provides that records of the Bank shall be kept in written form, or on microfilm, magnetic tape, optical disk or any other form of mechanical or electronic data storage and retrieval mechanism, for a period of at least 7 years after the completion of the transaction to which it relates, or the date of the record, as the case may be.

Under the Banking Act, a financial institution is required to keep a record for a period of at least seven years after the completion of the transactions to which it relates.

The personal data collected and processed by the Bank (e.g for unsuccessful tenderers, unsuccessful candidates during recruitment processes, applicants who were unsuccessful for fitness and probity, retiring employees, etc) shall be retained for a minimum of seven years after the end of the particular process, for regulatory purposes.

The type and amount of personal data financial institutions in the banking sector may collect would depend on the purpose and intention for the processing. The customer financial institution relation is governed by contract which, as a minimum, sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of the data subjects and the obligations and rights of the parties.

The Banking Act creates the obligation for financial institutions, to keep in relation to their activities, a full and true written record of every transaction it conducts under Section 33.

Records kept under this section shall include, amongst others, (i) accounting records exhibiting clearly and correctly the state of its business affairs, explaining its transactions and financial position so as to enable the central bank to determine whether the financial institution has complied with all the provisions of the banking laws, (ii) the financial statements, (iii) account files of every customer, business correspondences exchanged with every customer and records showing, for every customer, at least on a daily basis, particulars of its transactions with or for the account of that customer, and the balance owing to or by that customer, (iv) proper credit documentation and (v) such other records as the central bank may determine.

It is highlighted that this section also requires that every record be kept for a period of at least 7 years after the completion of the transaction to which it relates at the principal office of the financial institution, or at such other place as may be approved by the central bank.

Given the pivotal importance of record keeping in relation to Anti Money Laundering and Combatting the Financing of Terrorism and Proliferation, the Bank's Guideline on this subject matter includes a dedicated chapter on record keeping, detailing the requirements of the FIAMLA and the FIAMLR, the Banking Act and other requirements for CDD Records and Transactional Records amongst others.

Lawful processing

We have a panoply of rules, guidelines and laws for the proper conduct of banking business in Mauritius.

During the AML/CFT/CPF on-site examinations of regulated entities, examiners are guided by the AML/CFT/CPF Supervision Procedures manual for a standardised approach. These include, amongst others, an assessment of AML/CFT/CPF risk management of financial institutions which includes compliance with AML/CFT/CPF legislation and guidelines in the areas of AML/CFT/CPF Governance, Compliance Programs, policies and procedures, internal audit reviews, third party reliance, suspicious transaction monitoring and reporting systems, internal controls and follow-up on recommendations of previous examinations. The Bank also carries out special (targeted) AML/CFT/CPF examinations, whenever it is alerted from internal or external sources on any AML/CFT/CPF issue that may arise in a financial institution under the purview of the Bank. Supervisory issues identified during the examinations are discussed with the management of the financial institutions during an exit meeting. Remedial actions taken on recommendations of the on-site examination reports are followed up by examiners to ensure their timely implementation.

The Bank of Mauritius processes personal data mainly where the processing is necessary for the performance of tasks that it is required to carry out under the Bank of Mauritius Act 2004, the Banking Act 2004 and the National Payment Systems Act 2018.

Financial institutions process personal data mainly where the processing is necessary for the performance of a contract to which the person is a party or in order to take steps at the request of the person before entering into a contract and for compliance with any legal obligation.

Special categories of personal data

The processing of special categories of personal data should be carried out in special circumstances for e.g in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

According to the data minimisation principle, the Bank of Mauritius shall limit the collection and processing of personal data to what is necessary for that purpose. The Bank shall assess the necessity with consideration to the purpose of the processing and will collect special category of personal data only where it is relevant.

The Banking Act 2004	Under section 46 of the Banking Act 2004, the Bank of Mauritius determines whether a person is fit and proper to be appointed or reappointed as senior officer in Mauritius. As part of the process, the Bank of Mauritius receives a certificate of character or an affidavit stating any convictions for crimes and any past or present involvement in a managerial function in a body corporate subject to insolvency proceedings or having declared personal bankruptcy duly executed by the person concerned. For the purposes of determining whether the person is fit and proper, the Bank of Mauritius has regard to whether the person not having been subject to any conviction of an offence involving fraud or other dishonesty. As per the Guideline on Fit and Proper Person Criteria issued by the Bank of Mauritius, consideration is also given to the mental condition of a person, which would affect the applicant's ability to perform the position.
The National Payment Systems Act 2018	Similarly, section 19(7) of the NPS Act provides that the central bank shall, for the purpose of determining whether a third-party service provider is a fit and proper person, have regard to – (a) its probity, integrity, diligence, competence and business experience; (b) its previous conduct and activities in business; and (c) any conviction for an offence involving fraud or dishonesty. Section 27A(1) of the NPS Act states that: No person shall be appointed or reappointed as the director of a licensee unless the appointment or reappointment is in accordance with the guidelines issued by the central bank in relation to fit and proper persons. Under section 27A(2) of the NPS Act the same requirements of section 46 of the Banking Act as mentioned in the previous section apply for the appointment or re-appointment of senior officers of persons licensed or authorized under the NPS Act.
The National Payment Systems (Authorisation and Licensing) Regulations 2021	Pursuant to Regulation 4(6) of the NPS Regulations, the central bank shall not grant an authorisation or a licence unless it is satisfied (a) that the applicant has demonstrated that its directors and senior officers are fit and proper persons to operate the system or act as a payment service provider; and (b) of the fitness and suitability of the applicant's shareholders, particularly shareholders holding a significant interest.

Guideline on Mobile Banking and Mobile Payment Systems	Under the Guideline on Mobile Banking and Mobile Payment Systems, a mobile payment system may conduct authentication by several methods, one of which is by a unique physiological, genetic or physical trait possessed by the customer such as fingerprint or voice.
Guideline on Cyber and Technology Risk Management	Under the Guideline on Cyber and Technology Risk Management, the Bank of Mauritius has prescribed that financial institutions shall ensure that the processing of special categories of data, such as the use of biometric data for authentication purposes, is in line with the requirements of the Data Protection Act 2017

Personal data of child

The DPA provides that a person shall not process the personal data of a child below the age of 16 years unless consent is given by the child's parent or guardian and where the personal data of a child below the age of 16 years is involved, a controller shall make every reasonable effort to verify that consent has been given or authorized.

In the banking industry, personal data of minors are collected from their guardian or legal representatives until the minors reach 18 years of age

Security of Processing

The Banking Act 2004	Section 50 of the Banking Act 2004 makes provision for security in the operations of Automated Teller Machines (ATMs) set up by banks for the use by customers to make deposits or cash withdrawals. The bank has the obligation to provide such security for their operation, and such systems for customer authentication, terminal receipts and periodic statements and for physical and logical protection against unauthorized access in any form. Also, under section 51 of the Banking Act 2004, where a bank provides computer access to its customers, i.e., remote access to their accounts through computers using proprietary software or the internet, it has the obligation to provide such security for their Internet or proprietary platforms, and such systems for customer authentication, appropriate documentation and for physical and logical protection against unauthorized external access in any form whether by individual penetration attempts, computer viruses, denial of service, and other forms of electronic access, as the Bank of Mauritius considers adequate.

	Furthermore, where banks provide services to customers through electronic delivery channels such as the internet, section 52 of the Banking Act 2004 requires banks to have such systems to identify, monitor, and control transactional risk from the bank's use of technology and shall provide such security for their internet platforms, including such systems for customer authentication and for physical and logical protection against unauthorized external access by individual penetration attempts, computer viruses, denial of service, and other forms of electronic access. Overall, under section 54 of the Banking Act 2004, every financial institution has the obligation to maintain adequate internal control systems, commensurate with the nature and volume of its activities and various types of risks to which it is exposed, regarding operations and internal procedures; the organisation of accounting and information processing systems; risk and result measurement systems; documentation and information systems; and cash flow transactions monitoring systems. Pursuant to section 100 of the Banking Act and section 50 of the Bank of Mauritius Act, the Bank may issue guidelines and instructions for the efficient achievement of the purposes of the banking laws. Further, the Bank has issued guidelines to ensure cyber and technology resilience of our financial institutions and the security of data (including personal data), such as, (i) Guideline on Cyber and Technology Risk Management; (ii) Guideline on Use of Cloud Services; (iii) Guideline on Cross-Border Exposure; (iv) Guideline for Digital Banks; (v) Guidelines on Outsourcing by Financial Institutions (vi) Guideline on Internet Banking (vii) Guideline on Mobile Banking and Mobile Payment Systems (viii) Guideline on Public Disclosure of Information (ix) Guideline on Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation Failure to comply with any guideline is an offence.
Guideline on Internet Banking	Under the Guideline on Internet Banking, it is provided that as part of its security requirements, each institution must have a security program providing for the security arrangements which should achieve the following objectives: data privacy and confidentiality, data integrity, authentication/ identification of counterparties, amongst others. Access controls should be designed to effectively restrict unauthorised individuals from entering sensitive data and retrieving confidential information. Each institution should put in place tested systems to securely authenticate the

identity of internet banking customers when customers access personal account information or engage in on-line transactions for products or services. Each institution should provide sufficient authentication for internet banking customers who access personal account information or engage in online transactions for products or services. Each institution should use a combination of access, authentication and other security controls to create a secure and confidential internet banking environment. These generally include passwords, firewalls, and encryption. Each institution should be aware of the privacy concerns and its obligations for any loss of control of customers' information when they outsource their internet banking systems.

Also, each institution should adopt a privacy policy which explicitly lays down its commitment to safeguard the privacy of customer personal information. The privacy policy statement must (a) identify the types of information the institution collects about customers and how the information is used, (b) provide a brief description on the kind of existing security procedures that are in place or clearly state that sufficient safeguards have been put in place to protect the loss, misuse or alteration of information under the institution's control including restricting employee access to information, including that respecting a customer who has terminated his relationship with the institution, (c) identify with whom the institution shares this information, including agents, affiliates and non-affiliated third parties and how the institution ensures that the confidentiality of information is maintained, (d) explain the choices available to customers regarding collection, use and distribution of the information including the customers' right to opt-out of disclosures that are not mandatory, (e) explain how the institution maintains the accuracy of information and how customers can correct inaccuracies in the information; and (f) explain how the institution handles customer questions or complaints about the handling of personal information. Each institution should at the minimum prompt customers to refer to its privacy policy statements prior to or at the time that individually identifiable information is collected.

Also, when an institution provides links to third party websites to enable customers to access other third party services or products, the institution should analyse the risks presented by these arrangements. As part of its overall management policy, an institution should adequately manage its linking practices and enter into linking agreements where appropriate. The linking agreement should include the use and control of user data generated by the links as well as privacy and data protection obligations.

Guidelines on Outsourcing by Financial Institutions	The Bank of Mauritius has therefore prescribed that financial institutions should, perform the necessary due diligence and apply sound governance and risk management practices when subscribing to cloud-based services. The Bank of Mauritius expects financial institutions to be fully aware of cloud-based services characteristics such as multi-tenancy, data commingling and the possibility for processing to be carried out in different locations. Financial institutions are required to take appropriate measures with respect to data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing. They should ensure that the service providers have the capacity to identify and segregate customer data using strong physical or logical controls. Also, financial institutions should strictly adhere to the Data Protection Act and also ensure compliance with the Banking Act including amongst others confidentiality provisions set out under Section 64 thereof, when storing customers' information on the cloud. Financial institutions are ultimately responsible and accountable for maintaining oversight of cloud-based services and managing the attendant risks of adopting cloudbased services, as in any other form of outsourcing arrangement.
Guideline on Mobile Banking and Mobile Payment Systems	The Guideline on Mobile Banking and Mobile Payment Systems provides the minimum technology standards (authentication and modularity of technologies) and security requirements that mobile payment systems shall comply with. Also, where private or personal data in the application are directly accessible through menu or user interface, the access shall be protected.

(a) they consider the risk of foreign authorities having access to their data and require the cloud service provider to advise of instances where it was legally bound to disclose clients' data to foreign authorities in the past and of any such potential disclosures in the future (if available) in their risk assessment;

(b) the governing law and jurisdiction chosen are suitable for enforceability of the contractual provisions in case of breach thereof on part of the cloud service provider;

(c) data protection laws in the foreign jurisdiction where the data is hosted and processed are in line with the Mauritian data protection laws or data protection laws which are equivalent to the Mauritian data protection laws;

(d) the foreign jurisdiction's laws or regulations do not place any restrictions regarding on-site examination audit and access rights of the Bank, the financial institution, its external auditors or any third party appointed by them; and access to the information by the Bank, the financial institution, its external auditors or any third party appointed by them;

(e) there are appropriate contractual provisions allowing the financial institution to terminate the agreement in case there is a change in location where their data is hosted and they have concerns with the new location;

(f) the authorities of countries where the data will be hosted, processed and managed or where the cloud service providers will be located, do not have access to the data of the financial institution. Where the cloud service provider is required to disclose data of the financial institution to an authority of the countries where the data is located, following an order issued by a court or regulatory authority of competent jurisdiction, the agreement entered with the cloud service providers should contain the following obligations to cater for such instances: the cloud service provider shall use reasonable efforts to notify the financial institution before any such disclosure is made so that the financial institution may seek by legal means to prevent or limit such disclosure, except to the extent that providing such prior notice to the financial institution is prohibited by law or regulatory authority; and where the cloud service provider is unable to give such prior notice due to legal or regulatory constraints, it should implement appropriate legal and protective measures in the interest of the financial institution; and

g) the Bank of Mauritius is duly informed by the financial institution of any disclosure made by the cloud service provider in the event the latter is required to disclose data of the financial institution to an authority of the countries where the data is located, following an order issued by a court or regulatory authority of competent jurisdiction.

	Financial institutions shall establish a pre-agreed list of locations where its data will be processed with the cloud service provider. Where data is processed in a location outside the pre-agreed list, the financial institution shall ensure that: (a) such instances are limited to cases involving processing of individual transactions initiated by end users of the financial institution; (b) it is promptly informed by the cloud service provider of the location (city and country) where its data has been processed including the rationale thereof; and (c) it obtains assurance from the cloud service provider that the processing of data was done in a secured environment and that its data has been permanently removed from that location and transferred to a pre-agreed location within a reasonable timeframe. The said Guideline provides that financial institutions shall comply with the requirements of this Guideline for new cloud-based services and that financial institutions shall ensure (a) the establishment of the requisite strategy, policy and processes within 6 months of the effective date of this Guideline; and (b) compliance with the remaining requirements of this Guideline for existing cloud services within 12 months from the effective date of this Guideline.
Guideline on Cyber and Technology Risk Management	Under the Guideline on Use of Cloud Services, the Bank of Mauritius has prescribed several measures that a financial institution shall take with respect to control implementation and design, network and infrastructure management, logical security management, encryption, physical security management, use of third-party service providers, hosting of customer information, information assets and information systems outside Mauritius, amongst others. Financial institutions are required to (a) put in place a robust and effective set of security controls that will enable it to fulfil its security objectives, which should include ensuring the continuity and availability of its information systems, and the confidentiality, integrity and availability of information stored in its information systems and (b) develop its security controls to address all aspects of security, including logical, physical, people and third-party security. Financial institutions shall ensure that multi-factor authentication for employees and authorised third-parties is implemented for all accounts for critical systems, services, infrastructures and other assets/applications which directly allow access to customer information through the internet (e.g. web-based applications, etc). Also, where the financial institution opts for the key management services and other cryptography related services of a third-party service provider, it shall ensure that there is appropriate segregation within the service provider between access to keys and, where applicable, access to customer information.

	Financial institutions shall conduct due diligence on third-party service providers before using their services. The due diligence on a third-party service provider in respect of material services shall, inter alia, include the third-party service provider's compliance with the requirements of this Guideline, the applicable data protection, confidentiality and information security regulations or other legislations and adherence to international IT standards. With respect to third-party service providers having access to its information assets or hosting its information assets, a financial institution shall, amongst others, ensure that the contracts with third-party service providers are duly executed, do not consist of any clause that would hinder the Bank from exercising its supervisory powers, and include relevant provisions (a) to ensure the continued effectiveness of its cyber and technology risk management framework, (b) to ensure compliance with relevant laws in Mauritius (e.g. The Cybersecurity and Cybercrime Act 2021, Data Protection Act 2017, ICTA, etc.) or to relevant and equivalent laws at all times, (c) to impose confidentiality obligations on the third-party service provider which are in line with the underlying objective of section 64 of the Banking Act 2004 or section 18 of the National Payment Systems Act 2018, as relevant, (d) to ensure compliance with the record keeping obligations as set out in the Banking Act 2004, and (e) on exit strategies which are comprehensive and well documented (the exit plan shall include agreed process and procedures including reasonable timeframe for deletion of all data (bank and customer data) of the financial institution), (f) conduct third-party risk assessment at the outset and on a periodic basis which shall, inter alia, include an assessment to ensure that data, including customer information, are logically segregated and encrypted, (g) be aware of the cybersecurity/information security measures established by thirdparty service providers having access to customer information and other critical information assets and ensure that such security measures are equivalent, if not more stringent, than the controls which are implemented on premise for similar information assets, (h) ensure that it is satisfied with the cyber and technology resilience capabilities of third-party service providers having access to customer information and other critical information assets, by periodically using tools such as certification, external audits, testing exercises such as vulnerability assessment, service level agreements and key performance indicators in this respect.

Record of processing operations

The Banking Act 2004	Section 33 of the Banking Act 2004 and Section 23 of the NPS Act requires every financial institution and licensee under the NPS Act, for the purposes of the banking laws, to keep in relation to its activities, a full and true written record of every transaction it conducts. Such records required to be kept by financial institutions under section 33 of the Banking Act include – (a) accounting records exhibiting clearly and correctly the state of its business affairs, explaining its transactions and financial position so as to enable the central bank to determine whether the financial institution has complied with all the provisions of the banking laws; (b) the financial statements; (c) account files of every customer, business correspondences exchanged with every customer and records showing, for every customer, at least on a daily basis, particulars of its transactions with or for the account of that customer, and the balance owing to or by that customer; (d) proper credit documentation; and (e) such other records as the Bank of Mauritius may determine. The above records shall be kept – (a) in written form or kept on microfilm, magnetic tape, optical disk, or any other form of mechanical or electronic data storage and retrieval mechanism as the central bank may agree to; (b) for a period of at least 7 years after the completion of the transaction to which it relates; (c) at the principal office of the financial institution, or at such other place as may be approved by the Bank of Mauritius; and (d) for identification purposes, in chronological order or sequential order, as appropriate, in batches of convenient size.
The National Payment Systems Act	Section 23 of the National Payment Systems Act prescribes the same requirements as section 33 of the Banking Act outlined above for Payment Service Providers and Payment Service Operators.
The Financial Intelligence and Anti Money Laundering Act	The Financial Intelligence and Anti Money Laundering Act, section 17A also requires every financial institution to maintain a record in writing of its policies, controls and procedures, any changes made thereto as a result of a review/update as well as the steps taken to communicate these changes internally.

	The Financial Intelligence and Anti Money Laundering Act, section 17A also requires every financial institution to maintain a record in writing of its policies, controls and procedures, any changes made thereto as a result of a review/update as well as the steps taken to communicate these changes internally. Under section 17F (Record keeping) of the FIAMLA, a reporting person has the obligation to maintain all books and records with respect to his customers and transactions in accordance with the below and shall ensure that such records and books are kept for such time as specified below. The books and records referred to in subsection (1) shall include (a) all records obtained through Customer Due Diligence (CDD) measures, including account files, business correspondence and copies of all documents evidencing the identity of customers and beneficial owners, and records and the results of any analysis undertaken in accordance with this Act, all of which shall be maintained for a period of not less than 7 years after the business relationship has ended, (b) records on transactions, both domestic and international, that are sufficient to permit reconstruction of each individual transaction for both account holders and non-account holders, which shall be maintained for a period of 7 years after the completion of the transaction, and (c) copies of all suspicious transaction reports made pursuant to section 14 or other reports made to FIU in accordance with this Act, including any accompanying documentation, which shall be maintained for a period of at least 7 years from the date the report was made.
Guideline on Internet Banking issued by the Bank of Mauritius in February 2001	The Guideline on Internet Banking requires that institutions maintain, at all times, books and records in Mauritius for inspection by the Bank. A digital bank shall comply with the requirement of section 33 of the Banking Act on records and ensure that its records are, at all times, readily accessible to the Bank of Mauritius.
Guideline on Mobile Banking and Mobile Payment Systems	Under the Guideline on Mobile Banking and Mobile Payment Systems issued by the Bank, all transaction records shall be retained for a period of at least seven years.
Guideline on Use of Cloud Services	Under the Guideline on Use of Cloud Services, the Bank of Mauritius has prescribed that financial institutions shall keep an updated register of information on all their cloud services, irrespective of their materiality. Also, financial institutions have a duty to submit to the Bank a Return on Use of Cloud Services, in such form and manner prescribed by the Bank of Mauritius.

	Under the Guideline on Use of Cloud Services, the Bank of Mauritius has prescribed that financial institutions shall keep an updated register of information on all their cloud services, irrespective of their materiality. Also, financial institutions have a duty to submit to the Bank a Return on Use of Cloud Services, in such form and manner prescribed by the Bank of Mauritius. For material cloud services, financial institutions shall ensure that comprehensive and well documented exit strategies are established and regularly reviewed to ensure that they remain adequate and effective. The exit plan shall, as a minimum, include the following: a. agreed process and procedures including reasonable timeframe for deletion of all data (bank and customer data) of the financial institution, b. assurance from the cloud service provider through relevant independent reports/certificates that all data of the financial institution (including any backup) is rendered permanently irrecoverable and inaccessible in a timely manner after termination of the contract, etc.
Guideline on Cyber and Technology Risk Management	Under the Guideline on Cyber and Technology Risk Management, with respect to third-party service providers having access to its information assets or hosting its information assets, a financial institution shall ensure that the contracts with third-party service providers are duly executed, do not consist of any clause that would hinder the Bank of Mauritius from exercising its supervisory powers, and include relevant provisions to ensure compliance with the record keeping obligations as set out in the Banking Act 2004.
Guideline on Anti Money Laundering and Combatting the Financing of Terrorism and Proliferation	Paragraph 6.35 of the Guideline on Anti Money Laundering and Combatting the Financing of Terrorism and Proliferation, provides that the enterprise-wide ML/TF risk assessments, the details of implementation and report to senior management as well as the frequency of review should be kept on record. The Guideline on Anti Money Laundering and Combatting the Financing of Terrorism and Proliferation also requires financial institutions to keep records of the actions taken under paragraph 6.50 of the aforementioned guideline regarding beneficial ownership information, as well as any difficulties encountered during the verification process. The Guideline on Anti Money Laundering and Combatting the Financing of Terrorism and Proliferation includes comprehensive sections on the identification procedures to be followed for individuals for both face-to-face and non face-to-face applications and record-keeping which reiterates the statutory requirements of the FIAMLA, FIAMLR and Banking Act. Section 23 of the National Payment Systems Act prescribes the same requirements as section 33 of the Banking Act outlined above for Payment Service Providers and Payment Service Operators.

Transfer of personal data

Banks have traditionally stored and protected their customer's data responsibly and at the same time abiding to the principle of confidentiality imposed under the banking laws. All data which are collected and processed by the Bank of Mauritius provide for the mandatory obligations related to our economic activity, for the purposes of management and conclusion of the contractual relationship which the Bank has with data subjects to be able to respond to their requests. The Bank has regulatory and supervisory powers under the banking laws that can involve the collection and processing of personal data. Such data may relate to both the Bank's employees and/or non-employees (e.g. members of the public, applicants for employment with the Bank, for fitness and probity of senior officers within the banking sector etc.).

The Bank is committed to protect the privacy of data subjects and ensure that personal data collected from them are processed according to the principles laid down in the data protection laws. The DPA ensures that personal data be collected for explicit, specific and legitimate purposes and processed lawfully, fairly and in a transparent manner. The Bank receives personal information from individuals directly or indirectly from other parties (e.g. from other regulatory bodies). Before the Bank processes personal data, the Bank determines if the processing is necessary and considers the impact of processing activities on the fundamental rights and freedoms of data subjects. Sharing of data is important but this has to be balanced with the protection of data subject's rights and privacy.

Section 64(8) and (8A) of the Banking Act 2004 provides that "Where an officer of a foreign financial institution or an officer of a central bank or banking regulator in a foreign country or any other entity or agency, by whatever name called, having the responsibility to supervise financial institutions or performing the functions of a central bank or a foreign supervisory authority having the responsibility of carrying out supervisory functions in respect of money laundering or terrorism financing, proposes to conduct an inquiry, audit or inspection of a branch or a subsidiary of such financial institution in Mauritius or to conduct such other action that would involve the duty of confidentiality imposed under this section, he shall obtain the prior written authorisation of the central bank and be subject to the duty of confidentiality imposed under this section and any conditions that the central bank may impose before information of a confidential nature be made available to him."

"A financial institution shall seek the prior approval of the central bank before providing any confidential information to any person who intends to carry out due diligence on the financial institution with a view to acquiring a shareholding in the financial institution.

Guideline on Internet Banking issued by the Bank of Mauritius in February 2001	Under the Guideline on Internet Banking, each institution may outsource its internet banking systems to resident and non-resident (i.e. located outside Mauritius) service providers and software vendors subject to the prior written approval of the Bank of Mauritius.

Guidelines on Outsourcing by Financial Institutions	Under the Guidelines on Outsourcing by Financial Institutions issued by the Bank of Mauritius in May 2006, the Bank of Mauritius prescribes that financial institutions should consider the possibility of notifying in advance their customers that customer data may be transmitted to a service provider as part of their contractual arrangement with the customers depending on the nature and materiality of the outsourcing arrangement.
Guideline on Cyber and Technology Risk Management	Under the Guideline on Cyber and Technology Risk Management, regarding the hosting of customer information, information assets and information systems outside Mauritius, the Bank of Mauritius has prescribed that financial institutions shall conduct relevant due diligence on the countries involved. Financial institutions shall be aware of the location (city and country) where their customer and other material information assets/systems will be hosted and shall ensure, amongst others, that: (a) they consider the risk of foreign authorities having access to their data and require the service provider to advise of instances where it was legally bound to disclose clients' data to foreign authorities in the past and of any such potential disclosures in the future (if available) in their risk assessment, (b) data protection laws in the foreign jurisdiction where the data is hosted and processed are in line with the Mauritian data protection laws or data protection laws which are equivalent to the Mauritian data protection laws. Financial institutions shall establish a pre-agreed list of locations where its data will be processed with the service provider. Where data is processed in a location outside the preagreed list, the financial institution shall ensure that: (a) such instances are limited to cases involving processing of individual transactions initiated by end users of the financial institution, (b) it is promptly informed by the outsourced service provider of the location (city and country) where its data has been processed including the rationale thereof; and (c) it obtains assurance from the service provider that the processing of data was done in a secured environment and that its data has been permanently removed from that location and transferred to a pre-agreed location within a reasonable timeframe. The Bank of Mauritius Guideline on Cyber and Technology Risk Management provides at paragraphs 43 to 46, the obligations on financial institutions under its purview on the hosting of customer information, information assets and information systems outside Mauritius. In addition to the due diligence on the host country, financial institutions are required to ensure that the governing law and jurisdiction chosen are suitable for enforceability of the contractual provisions in case of breach thereof on part of the service provider and data protection laws in the foreign jurisdiction where the data is hosted and processed are in line with the Mauritian data protection laws or data protection laws which are equivalent to the Mauritian data protection laws.

	The Bank should be duly informed by the financial institution of any disclosure made by the service provider in the event the latter is required to disclose data of the financial institution to an authority of the countries where the data is located, following an order issued by a court or regulatory authority of competent jurisdiction.

Rights of individuals

The Bank of Mauritius ensures compliance with the provisions on the rights of data subjects under the DPA. Where deemed necessary, compliance with the DPA is also included as a provision in the guidelines issued by the Bank.

Under the National Payment Systems Act Section 18 (1B) with reference to Banking Act section 64 (1A) (c), where the express written consent of the customer of a Payment Service Provider or Payment Service Operator or participant has to be sought before disclosure in any form whatsoever, of any information relating to the affairs of the customer, except for the instances outlined at section 18 (1A) of the National Payment Systems Act and section 64 (1B) (3) to (7) of the Banking Act where the duty of confidentiality imposed under the section shall not apply.

Guideline on Internet Banking	Also, as mentioned above, under the Guideline on Internet Banking, the privacy policy statement adopted by every institution must explain the choices available to customers regarding collection, use and distribution of the information including the customers' right to opt-out of disclosures that are not mandatory; explain how the institution maintains the accuracy of information and how customers can correct inaccuracies in the information; and explain how the institution handles customer questions or complaints about the handling of personal information. Furthermore, the Guideline requires that each institution discloses a procedure to enable customers to inquire about its personal information or inform the institution about the potential misuse of personal information in the online environment. Each institution should have a web page to educate customers on Internet banking particularly, with respect to their rights and responsibilities and the protection of their own privacy on the Internet.

Unlawful disclosure of personal data

The Bank of Mauritius Act 2004	The general rule is that no person referred to in section 26(1) of the Bank of Mauritius Act shall, during and after his relationship with the Bank of Mauritius, disclose directly or indirectly to any person any information relating to the affairs of the Bank, of any other bank or financial institution or of any of its customers, which he has acquired in the performance of his duties or the exercise of his functions. The exceptions are for the purposes of (a) the performance of his duties or the exercise of his functions under the banking laws or meeting the requirements of an agreement or understanding reached by the Bank with any other relevant supervisory body; or (b) when lawfully required to do so by an order of a Judge in Chambers or any court of law; or under any enactment. Any person who contravenes this section shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.
The National Payment Systems Act 2018	Section 18 of the NPS Act outlines the provisions for confidentiality (non-disclosure) of data held a Payment Service Provider, operator or participant and the exceptions as follows: Section 18(1) states that a person who has access to the books, accounts, records, financial statements or other document, whether electronically or otherwise, in his capacity as – (a) director, officer, employee, agent or service provider of an operator, a participant or a payment service provider; or (b) liquidator of an operator or a payment service provider, shall not, during or after his relationship with the operator, participant or payment service provider, disclose to any person any information relating to the affairs of a customer of a participant or payment service provider, except – (i) with the written authorisation of the customer or his personal representative; (ii) for the purpose of the performance of his duties within the scope of employment or appointment in compliance with this Act; (iii) as directed in writing by the central bank; or (iv) when required to do so by a Court or under any enactment. Section 18(1A) states that the duty of confidentiality imposed under subsection (1) shall not apply where the Ombudsperson requires information, documents and particulars to enable him to discharge, or assist him in discharging, any of his functions under the Ombudsperson for Financial Services Act 2018.

	Section 18(1B) of the NPS Act provides that Section 64(1A), (1B), (2) to (7), (7A), (8), (8A), (9) to (16) of the Banking Act shall apply to Payment Service Providers and Payment Service Operators, with such modifications, adaptations and exceptions as may be necessary. Section 29 (5) of the National Payment Systems Act provides that any person who contravenes any other provision under this Act, including section 18 thereof relating to 'Confidentiality', shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding one year.
The Banking Act Section 64 (1A) (1B)	(1A) Any person – (a) to whom any information pertaining to a customer or financial institution is disclosed and who knows or has reasonable grounds to believe, at the time of the disclosure, that the information was disclosed to him in contravention of this section; (b) who is in possession of information relating to the affairs of a customer or financial institution without just or reasonable grounds or in contravention of this section; or (c) who publishes, in any form whatsoever, any information relating to the affairs of a customer or financial institution without the express written consent of the customer or financial institution or in contravention of this section, shall commit an offence and shall, on conviction, be liable – (i) in the case of an individual, to a fine not exceeding 500,000 rupees and to imprisonment for a term not exceeding 3 years; or (ii) in any other case, to a fine not exceeding one million rupees. (1B) Where a person is prosecuted for an offence under subsection (1A)(a) or (b), it shall be a defence for the person to prove that – (a) the disclosure was made without his consent; (b) where the disclosure was made in a written form, he, as soon as practicable, surrendered or took all reasonable steps to surrender the information and all copies thereof to the central bank; and (c) where the disclosure was made in an electronic form, he, as soon as practicable, took all reasonable steps to ensure that all electronic copies of the information were deleted and that the information and all copies thereof in other forms were surrendered to the central bank. (1B) (2) Except for the purpose of the performance of his duties or the exercise of his functions under the banking laws or as directed in writing by the central bank, no person referred to in subsection (1) shall, during or after his relationship with the financial institution, disclose directly or indirectly to any person any information relating to the affairs of any of its customers including any deposits, borrowings or transactions or other personal, financial or business affairs, without the prior written consent of the customer or his personal representative.

Potential consequences of non-adherence to rules and regulations

Non compliance with the provisions of the Banking Laws, regulations made thereunder as well as guidelines, instructions or directives issued by the Bank of Mauritius also entail sanctions, which may be monetary, administrative, criminal or regulatory in nature as per below:

Monetary Penalty	Monetary penalty may be imposed with the consent of the Director of Public Prosecutions and agreement of the financial institution regarding offence which are prescribed as compoundable offences.
Administrative Penalty	The Bank may impose an administrative penalty on any financial institution which refrains from complying, or negligently fails to comply, with any instructions or guidelines issued by the Bank or requirement imposed under the banking laws, or where the financial institution has failed to comply with the requirements imposed under a guideline, instruction or directive issued by the Bank.
Non-Monetary, Regulatory And Disciplinary Actions	Following an examination made under section 42 of the Banking Act or a Special examination under section 43 of the Act or other information at its disposal, the Bank may be of the opinion that, inter alia, the financial institution has, or has knowingly or negligently permitted any of its directors or senior officers or employees or agents to violate any provision of the banking laws or any enactment relating to anti-money laundering or prevention of terrorism and the regulations, guidelines, or instructions issued by the central bank to which the financial institution is subject, or these actions or violations are about to occur, it may pursuant to Section 45 of the Banking Act, in the light of the nature, gravity, scale and recurrence of the breach, take any of the following steps which are commensurate and proportionate thereto - (i) impose or vary conditions attaching to the financial institution's licence in accordance with section 10 or 16 of the Banking Act, as the case may be, invoking in cases of urgency the procedure specified in section 17 of the Banking Act; (ii) require the financial institution forthwith to take such steps as may appear to the central bank to be necessary to remedy the situation and submit such reports on remedial actions taken to the central bank at such frequency and in such manner as the central bank may specify; (iii) appoint a person to advise the financial institution in the proper conduct of its business and fix the remuneration to be paid by the financial institution to the person so appointed;

	(iv) issue a cease and desist order that requires the financial institution and its directors, senior officers, employees or shareholders holding a significant interest, as the case may be, to cease and desist from the actions and violations specified in the order and may require affirmative action to correct the conditions resulting from any such actions or violations; (v) issue an order to the financial institution to suspend from office any director or senior officer or employee who has engaged in, or is otherwise responsible for, such actions or violations. (vi) take such action as may be warranted pursuant to section 50(6), (7), (8) and (9) of the Bank of Mauritius Act.
Revocation/ Suspension of Licence	The Bank may further in terms of sections 11 and 17 of the Banking Act revoke or suspend the licence of the financial institution where the seriousness of the non-compliance so warrants coupled with a deliberate or reckless disregard of regulatory requirements as well as weak controls and governance, or where criminal elements are present.
Criminal Liability	Any breach of the Banking Laws is a criminal offence for which the Bank may refer the matter to the Police for investigation. Section 50 of the Bank of Mauritius Act 2004 confers powers on the Bank to impose administrative penalties on regulated entities for non-compliance with any instructions or guidelines issued or requirement imposed by the Bank under the banking laws, which includes AML/CFT/CPF provisions. The FIAMLA has been amended in September 2018 to include provisions empowering the Bank to impose penalties, including an administrative penalty on banks and cash dealers, for failure to comply with the requirements of the Guideline on AML/CFT/CPF and Proliferation. The Bank may also impose administrative penalty on regulated financial institutions. The Bank is further empowered to suspend from office any director, senior officer, employee or agent whom it considers to have knowingly or negligently been permitted to violate AML/CFT/CPF laws and guidelines. The Director of the FIU also is empowered to impose administrative sanctions on persons for failure to comply with guidelines on filing of STRs. (i) outline the criminal sanctions for non –compliance with AML obligations, and (ii) quantify the penalties to be applied for such offences. The industry is aware that failure to take measures as are reasonably necessary to prevent or to facilitate ML constitutes an offence. Section 64A of the Banking

	Act creates the obligation on all financial institutions, including branches and subsidiaries to implement programmes against money laundering and terrorism financing risks commensurate to its size and the risks to which it is exposed. These programmes should include compliance management arrangements, screening procedures, ongoing training programmes and an independent audit function to test the programme. Section 11(1)(f) of the Banking Act provides that where a licence may be revoked by the central bank in cases where a bank has been convicted by a court of an offence under any enactment relating to AML/CFT/CPF related offences, or section 45 of the Act where following an examination or based on information at its disposal the central bank is of the opinion that the financial institution concerned has or any of its directors or employees have engaged in unsafe or unsound practices or violated any provision of the banking laws or any enactment relating to AML/CFT/CPF, the BoM may issue an order to the financial institution to suspend from office that director or employee. Moreover, the BoM maintains an internal blacklist of staff of banks who have been subject to disciplinary actions and/or referrals to Police by their respective banks. This list is used in the assessment procedures regarding the appointment of senior officers of banks, amongst others.
The Banking Act Section 64 (1A) (1B)	(1A) Any person – (a) to whom any information pertaining to a customer or financial institution is disclosed and who knows or has reasonable grounds to believe, at the time of the disclosure, that the information was disclosed to him in contravention of this section; (b) who is in possession of information relating to the affairs of a customer or financial institution without just or reasonable grounds or in contravention of this section; or (c) who publishes, in any form whatsoever, any information relating to the affairs of a customer or financial institution without the express written consent of the customer or financial institution or in contravention of this section, shall commit an offence and shall, on conviction, be liable – (i) in the case of an individual, to a fine not exceeding 500,000 rupees and to imprisonment for a term not exceeding 3 years; or (ii) in any other case, to a fine not exceeding one million rupees.

Fintech

Fintech, i.e technology-enabled innovation in the banking sector has been developing significantly over the past years and is impacting the way banking services are delivered.

Under the Banking Act, "Fintech" means technologically enabled financial innovations which could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services.

The Bank of Mauritius, as the regulator for the Banking Sector and also having been mandated to ensure the stability and soundness of the financial sector, has been following closely the evolution of Fintech and working on the issuance of the Central Bank Digital Currency (the Digital Rupee) with the aim of building new solutions in the banking sector. Through innovation, the banking sector can open new markets, increase operation efficiency and reduce costs (especially in payments), attract and build digital talent, while adhering to and strengthening compliance requirements.

The Bank of Mauritius has deemed it appropriate to explore the implementation of its CBDC for the various merits it offers. It has systematically upgraded its payments infrastructure taking into consideration risks that a CBDC will bring along in designing the Digital Rupee. Cybersecurity is one of the biggest risks associated with digitalization. A CBDC will open our systems to more participants and also more points of attack. The severity of frauds could be more significant given the ease with which data and large funds could be transferred electronically.

One of the criteria for the success of a CBDC is the degree of privacy it offers to its users. The Bank as a Controller will need to consider the appropriate degree of privacy of the end-users of the CBDC, while taking into account AML/CFT/CPF concerns and requirements.

The Bank of Mauritius Act defines "digital currency" as the central bank digital currency issued by the Bank of Mauritius under section 35(1) of the Act. Under section 35 of the Bank of Mauritius Act, the Bank shall have the sole right to issue Mauritius digital currency. The Bank of Mauritius may make rules to provide for the framework under which digital currency may be issued by the Bank of Mauritius and may be held or used by the public. Section 37 of the Bank of Mauritius Act also provides that currency issued by the Bank of Mauritius under this Act shall be legal tender in Mauritius - in the case of notes and digital currency, for the payment of any amount.

Under section 11C of the Banking Act, a financial institution, a licensee under the National Payment Systems Act or a body corporate may apply to the Bank of Mauritius for a regulatory sandbox authorisation. The Bank of Mauritius may grant a regulatory sandbox authorisation where it is satisfied that the applicant meets such requirements, including eligibility criteria for a specified period and subject to such terms and conditions, including appropriate safeguards to contain the consequences of failure and maintain the overall safety and soundness of the financial system, as it may determine.

Upon the Bank of Mauritius being satisfied of the successful experimentation of Fintech, regtech or such other relevant innovation driven financial service, as the case may be, the holder of a regulatory sandbox

authorisation may submit an application to the Bank of Mauritius for the relevant licence or authorisation under the Banking Act or the National Payment Systems Act.

All licensees of the Bank are required to adhere to the Data Protection Act. They are also required to ensure that any third party service provider, including Fintech companies, also ensure strict compliance with the domestic law or GDPR, if the service provider is a foreign company.

It is also important to note the following definitions from the Banking Act:

"regtech" or "regulatory technology" means the innovative technology solutions utilised by financial institutions and other regulated entities to facilitate compliance with regulatory rules and requirements;

"regulatory sandbox" means a controlled testing environment which allows a financial institution, a licensee under the National Payment Systems Act or a body corporate authorised by the central bank under section 11C to conduct experiments under the supervision of the central bank; and

"regulatory sandbox authorisation" means an authorisation granted under section 11C which allows a financial institution, a licensee under the National Payment Systems Act or a body corporate to enter a regulatory sandbox to experiment with Fintech, regtech or other innovation driven financial services falling under the purview of the central bank.

The Banking Act has also been amended to provide for the establishment of a Fintech innovation hub and digital lab, to foster innovation and the use of emerging technologies to facilitate the provision of banking and payment solutions and other related services falling under the purview of the central bank, to identify critical trends in technology affecting the banking and payment services sectors and develop in-depth insights into these technologies, to provide a testing environment for Fintech to develop, test, prototype and operate products or services and to establish an international networking platform for experts on innovative technologies related to the banking and payment services sectors to promote research, exchange of views and knowledge-sharing.

The Fintech innovation hub and digital lab is intended for usage by the financial sector as a whole as well as by the academia amongst other stakeholders. The Bank is ensuring, prior to implementation of the Fintech innovation hub and digital lab, that all cybersecurity measures are put into place such that data used to interact with the Fintech innovation hub and digital lab is safe.

17.3 Financial Services Commission

The FSC is the integrated regulator in Mauritius for the financial services sector (other than banking) and global business[27].

The FSC, through its legislative framework, is mandated to request, share and process data for AML/CFT/CPF purposes, while ensuring the necessary safeguards in terms of data protection and privacy. As a jurisdiction which is compliant and largely compliant with all the 40 FATF Recommendations, it is worth noting that the above is in line with Recommendation 40 which states that competent authorities should maintain appropriate confidentiality for any request for cooperation and the information exchanged, in order to protect the integrity of the investigation or inquiry, consistent with both parties' obligations concerning privacy and data protection.

Pursuant to Section 17C of the FIAMLA, financial institutions have the obligation to verify the identity of customers and any persons with whom they conduct transactions. The financial institutions are required to carry out customer due diligence ('CDD') and be satisfied with all the results obtained before carrying out any business transaction. They must ensure that all documents, data or information collected under the CDD process are kept relevant and up-to-date by undertaking reviews of existing records. For example, when collecting information for an individual, they are required to collect relevant identification data which includes name, current residential address, date and place of birth, nationality, and any occupation.

Financial institutions are required to maintain these records as the FSC has the right to request for any records and documents at any time. As such, Section 17F of the FIAMLA provides for record keeping whereby:

1. A reporting person shall maintain all books and records with respect to his customers and transactions in accordance with subsection (2) and shall ensure that such records and books are kept for such time as specified in, and in accordance with, subsection (2).
2. The books and records referred to in subsection (1) shall include –
    a) all records obtained through CDD measures, including account files, business correspondence and copies of all documents evidencing the identity of customers and beneficial owners, and records and the results of any analysis undertaken in accordance with this Act, all of which shall be maintained for a period of not less than 7 years after the business relationship has ended;
    b) records on transactions, both domestic and international, that are sufficient to permit reconstruction of each individual transaction for both account holders and non-account holders, which shall be maintained for a period of 7 years after the completion of the transaction; and
    c) copies of all suspicious transaction reports made pursuant to section 14 or other reports made to FIU in accordance with this Act, including any accompanying documentation, which shall be maintained for a period of at least 7 years from the date the report was made. The objective of keeping adequate records is to ensure that the Company can provide necessary information about Customers, and their transactions details at any given time or as per the request from Regulatory body.

27 https://www.fscmauritius.org/en/licensing/licensed-activities/securities

As per the Securities Act 2005, the FSC is the regulator of the non-bank financial markets in Mauritius which comprises Securities Exchanges, clearing and settlement facilities and securities trading systems on the one hand and Collective Investment Schemes and intermediaries on the other.

Therefore, as the regulator of the securities markets, the FSC strives to:

a) foster fair, efficient, transparent and informed markets for securities in Mauritius;
b) monitor and regulate the operations of securities exchanges and the activities of persons providing clearing and settlement services and trading systems for securities;
c) suppress and prevent financial crimes and illegal practices;
d) regulate the disclosure of information by persons issuing securities and by reporting issuers to securities holders and to the public;
e) cooperate and collaborate with domestic and international organisations, law enforcement, supervisory and regulatory bodies;and
f) reinforce the protection of investors in Mauritius from unfair, improper and fraudulent practices.

The FSC fosters a conducive regulatory and business environment that encourages fintech innovation while ensuring an appropriate level of compliance and consumer protection. In particular, the FSC aims to improve the competitiveness of the Mauritius International Financial Centre through the diversification of its product offerings and by supporting industry-led initiatives to develop technology-powered and innovation-driven financial products and services. Some of the key ways in which the FSC supports innovation are:

- establishment and administration of the Regulatory Sandbox Authorisation;
- establishment and administration of the fintech innovation hub;
- proactively engaging with the market participants, stakeholders and the broader community;
- collaborating with local and international counterparts; and
- continuously aligning the legal and regulatory framework to accommodate new or evolving business models and their risks.

The FSC is empowered under section 14C of the Financial Services Act to inter-alia establish a fintech innovation hub. More information regarding the fintech landscape is availale at the link:
https://www.fscmauritius.org/en/fintech-and-innovation

17.4 Securities Exchanges[28]

There are three licensed Securities Exchanges in Mauritius - the Stock Exchange of Mauritius Ltd (SEM), AFRINEX (afrinexexchange.com) and MINDEX Limited.

17.4.1 Stock Exchange of Mauritius Ltd

The Stock Exchange of Mauritius is a full member of the World Federation of Exchanges and has a multi-currency capital-raising, listing, trading and settlement platform and can list and trade products in USD, EURO, GBP and ZAR.

28 https://www.fscmauritius.org/en/licensing/licensed-activities/securities

17.4.2 AFRINEX Limited

AFRINEX is an International Stock Exchange having PanAfrica focus providing state of the art electronic platforms for multi-asset multi-currency listing, trading & settlement and has an exclusive platform to raise capital through private placements of debt/equity.

17.4.3 MINDEX Limited

MINDEX Limited is a digital exchange open to Development Finance Institutions, Institutional investors as well as African retail investors providing a complete financial infrastructure to issue, trade, swap, store and manage any type of real or Virtual Asset.

17.5 Financial Intelligence Unit

Established under Section 9 of FIAMLA in August 2002, the FIU is the central Mauritian agency for the request, receipt, analysis and dissemination of financial information regarding suspected proceeds of crime and alleged money laundering offences as well as the financing of any activities or transactions related to terrorism to relevant authorities[29].

Under Section 13 of FIAMLA, where there are grounds to suspect money laundering, predicate offences or terrorism financing, the Director shall disseminate information and the results of the analysis of the FIU to the relevant investigatory authority, supervisory authority, overseas financial intelligence unit, the Counterterrorism Unit, Registrars or comparable body for appropriate action.

The FIU is also the AML/CFT/CPF regulator for Attorneys, Barristers, Notaries, Law firms, Foreign Law firms, Joint Law Ventures, Foreign Lawyers under the Law Practitioners Act, Dealers in Jewellery, Precious Stones or Precious Metals and Real Estate Agents, including Land Promoters and Property Developers.

17.6 Mauritius Revenue Authority (MRA)

The MRA is a body corporate, set up to manage an effective and efficient revenue-raising system. It administers and collects taxes due in Mauritius within an integrated organisational structure[30].

The MRA is an agent of State and, as such, the Ministry of Finance and Economic Development continues to have overall responsibility for the organisation and monitors its performance.

The MRA is responsible for collecting approximately 90% of all tax revenues and for enforcing tax laws in Mauritius.

29 https://www.fiumauritius.org/fiu/

30 https://www.mra.mu/index.php/about-us1/mandate-vision

17.7 Mauritius Financial Reporting Council (FRC)

The FRC is a body corporate set up under the Financial Reporting (FR) Act 2004. It is an organisation under the aegis of the Ministry of Financial Services and Economic Planning. The FRC is mainly responsible for promoting confidence in corporate reporting and good corporate governance[31].

The Council main objects as defined in the FR Act are:

i. to promote the provision of high quality reporting of financial and non-financial information by public interest entities.
ii. to promote the highest standards among licensed auditors
iii. to enhance the credibility of financial reporting and
iv. to improve the quality of accountancy and audit services.

17.8 The Financial Crimes Commission

The Financial Crimes Commission Act (FCCA) provides for the setting up of the FCC which shall serve as the apex body in Mauritius to detect, investigate and prosecute financial crimes and any other related ancillary offence.

The different categories of financial crimes which fall under the purview of the Act, include corruption offences, money laundering offences, fraud offences and financing drug dealing offences.

The Director of the Investigation Division of the FCC will be entitled to use special investigative techniques for the purpose of gathering intelligence or evidence including: intrusive surveillance, covert intelligence human source and equipment interception. However, it must be just, proportionate and in the public interest to do so as per section 66 of FCCA below: -

" 66. Special investigative techniques

(1) For the purpose of preventing, detecting an offence under this Act or the Declaration of Assets Act, the Director of the Investigation Division shall, with the approval of the Director-General, use the following investigative techniques as may be required for the purpose of gathering intelligence or evidence –

(a) controlled remittance; and
(b) surveillance.

(2)Notwithstanding any other enactment, where the Director of Investigation has reasonable grounds to suspect that an offence under this Act or the Declaration of Assets Act has been, is being or is likely to be committed by any person, the Director of Investigation may, with the approval of the Director-General, apply to a Judge for an Order to use the following investigative techniques as may be required for the purpose of gathering intelligence or evidence –

(a) intrusive surveillance;
(b) the conduct and use of covert intelligence human source; and
(c) equipment interception.

31 https://frc.govmu.org/frc/?page_id=1517

(3) The Director-General shall give his approval under subsection (1) or (2) after being satisfied that it is just, proportionate and in the public interest to do so.

(4) Where, on an application made under subsection (2), a Judge is satisfied that an offence under this Act or the Declaration of Assets Act has been, is being or is likely to be committed, a Judge may grant the Order.

(5) Any evidence gathered using the investigative techniques under subsections (1) and (2) shall be admissible in Court.

(6) The Director of Investigation Division may delegate his powers under subsections (1) and (2) to any officer.

(7) There shall be a Covert Intelligence Human Source Data Controller who shall keep all records and information pertaining to operations where the use of the Covert Intelligence Human Source technique has been used.

(8) In this section –

"conduct and use of covert intelligence human source" means inducing, asking or assisting a person to engage in the conduct of covert human intelligence source as undercover agent to obtain information by means of the conduct of such a source;

"conduct of covert human intelligence source" means a person who –

(a) provides intelligence gathered by interpersonal contact to assist in investigations;
(b) establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating surveillance or intrusive surveillance;
(c) covertly uses such a relationship to obtain information or to provide access to any information to another person; or
(d) covertly discloses information obtained by the use of a relationship, or as a consequence of the existence of such a relationship;

"controlled remittance" means an operation which allows for the performance of an act by one person that would qualify as a financial crime, for the purpose of identifying any person involved in the commission of the financial crime;

"equipment interception" means either remotely or physically interfering with computers or computer-like devices such as, inter alia, tablets, smart phones, cables, wires and static storage devices, for the purpose of obtaining communications, equipment data or other information;

"intrusive surveillance" –

(a) means an act of monitoring, observing or listening to a person, his movements, conversations or other activities; and
(b) communications, from within a place other than a public place; and
(c) includes –
  (i) surveillance from any residential premises or in any private vehicle or private property; and
  (ii) the use of any kind of surveillance device, drones or other electronic device to enter a place other than a public place;

"surveillance" means the continual act of monitoring, observing or listening to a person, his movements, conversations or other activities and communications, from a public place, with the likely result of obtaining private information about that person or another person."

The processing operations as prescribed under the FCCA are in accordance with section 44(1) of the DPA.

Potential consequences of non-adherence to rules and regulations

Criminal liability	In light of the definition of 'financial crime' under the Financial Crimes Commission Act, where any crime has been committed under the law of any financial or competent authority, Financial Crimes Commission may decide after consultation with that authority to investigate into that matter or any ancillary offence whilst taking into consideration its financial implications, complexity, scope, nature or in the public interest.
Section 52(1) of FCCA Obligations of legal persons	The Bank shall ensure that it has adequate procedures in place, which are reasonably necessary, to prevent it or any person acting on its behalf from committing an offence under Part III of the Financial Crimes Commissions Act, failing which it shall commit an offence and shall, on conviction, be liable to a fine not exceeding 20 million rupees.

17.9 Ombudsperson for Financial Services (OFS)

The Office of Ombudsperson for Financial Services shall, in particular:

i. Inform and educate the general public on investments in financial services offered by financial institutions;
ii. Assist the Ombudsperson in dealing with complaints made by consumers of financial services against regulated financial institutions; and
iii. Act without fear or favour and shall not be subject to the directions or control of any other person or authority in the exercise of its functions.

OFS may perform the following activities: -

(a) Investigation
(b) Mediation
(c) Hearing
(d) Make an Award and issue directives
(e) Enter premises
(f) Request for information
(g) Issue instructions and guidelines or impose such other requirements
(h) Share information and, where appropriate, enter into a Memorandum of Understanding, with any relevant supervisory or regulatory authority or law enforcement agency

18.0 MOU with Bank of Mauritius

Cabinet, at its meeting of 25 July 2025, agreed to the signing of a Memorandum of Understanding (MoU) between the Data Protection Office and the Bank of Mauritius. The MoU was subsequently signed on 4 September 2025, thereby formalising a strengthened institutional partnership between the two bodies. It establishes a structured framework for strategic collaboration, with particular emphasis on information sharing, capacity building and mutual assistance in the effective discharge of their respective statutory mandates.

The MoU aims to:

- Strengthen cooperation between financial supervision and data protection oversight;
- Facilitate the exchange of relevant expertise and information; and
- Provide greater clarity to regulated entities, thereby promoting consistent and efficient compliance.

19.0 The Mauritius National Data Strategy and Data Governance

The Mauritius National Data Strategy (NDS)[32] establishes a comprehensive framework to harness the power of data to drive innovation, enhance public service delivery and support economic growth. As a key component of the Digital Transformation Blueprint 2025–2029[33], the NDS serves as the primary guiding document for the financial sector. It provides the strategic roadmap required to balance digital innovation with the stringent requirements of the Data Protection Act 2017, ensuring that data protection aligns with financial stability through responsible handling.

The NDS aims to transform Mauritius into a data-driven hub and a resilient International Financial Center (IFC) by fostering trust and treating data as a high-value national asset.

The following strategic objectives are of critical relevance to financial institutions:

- Improving Data Quality and Sharing: Streamlining inter-departmental and inter-agency data flows.
- Promoting Ethical and Secure Use: Ensuring transparency in the processing of client and institutional data.
- Strengthening Privacy Safeguards: Aligning organizational data management with the DPA.
- Ethical Adoption of AI: Preparing for the safe, trustworthy and ethical adoption of Artificial Intelligence in financial services.

Practical Tools for Implementation: The Four Annexes

To support the operationalization of the NDS, the Data Protection Office has developed four practical annexes. These documents provide the guiding frameworks necessary for financial controllers to manage the data lifecycle effectively.

I. Model Data Governance Framework

This framework mandates a disciplined approach to data collection and empowers organizations to identify opportunities and make informed decisions. It is built upon five essential pillars:

32 SliderReadMore

33 Blueprint – Ministry of Information Technology, Communication and Innovation

- Processes, Policies, Standards and Procedures: Defining the rules of engagement.
- Organizational Structure, Roles and Responsibilities: Establishing clear accountability.
- Technology and Tool Capabilities: Deploying the necessary technical infrastructure.
- Metadata Content (or Data Catalog): Managing accessibility and reliability.
- Compliance and Risk Management: Ensuring ongoing regulatory alignment.

II. Data Sharing Policy Template

This policy serves as the high-level internal directive for financial entities. It establishes the principles under which data can be shared, emphasizing "Data Sharing by Design" and ensuring that any disclosure is done for a lawful purpose connected with the functions of the controller.

III. Data Sharing Protocol Template

The Protocol provides the technical and legal safeguards for specific data transfers. It ensures that the intended recipients are identified and that security and organisational measures are implemented to prevent unauthorized access, alteration or accidental loss during the transfer process.

IV. Data Retention Policy Template

In line with the principle of "Preservation of Information," this annex provides the guidance for retention of personal data. It outlines mandatory protocols for secure disposal including overwriting, degaussing or physical destruction to ensure data is irrecoverable once its retention period expires.
The development of the NDS and its annexes involved significant research and insights from international partners, including the World Bank and the European Union. It is the primary duty of the Data Protection Officer and the controller within the financial organization to internalize these frameworks. By utilizing the Data Management Functions Checklist, institutions ensure the ongoing confidentiality, integrity and resilience of their processing systems, maintaining the trust of the global financial community.

20.0 General Recommendations

This comprehensive guide consolidates the insights on data protection in the financial sector and present a set of recommendations to fortify an organization's data protection framework. These recommendations are designed to address the evolving landscape of cybersecurity threats and regulatory requirements, ensuring that a financial institution remains resilient in safeguarding personal data.

1. Establish a Robust Data Governance Framework

Develop and implement a comprehensive data governance policy that defines roles, responsibilities, and accountability for data protection across the organization.
Regularly update and enforce data classification policies to ensure that sensitive financial data is appropriately identified, handled, encrypted and protected. Some non-exhaustive safeguards to promote the security of personal data is at Annex 1.

2. Accountability

Controllers should adopt accountability measures for the processing of personal data, including data protection impact assessments, privacy by design and by default measures, and the appointment of a Data Protection Officer.

3. Invest in Employee Training and Awareness Programs

Provide ongoing training to employees on data protection best practices, security protocols, and the latest cybersecurity threats.
Foster a culture of security awareness, encouraging employees to report any suspicious activities or potential security incidents promptly.

4. Implement Multi-Layered Authentication and Authorization Systems

Enforce strong authentication mechanisms, including multi-factor authentication (MFA), to prevent unauthorized access to financial data.
Implement a robust authorization system that ensures individuals only have access to the data necessary for their specific roles and responsibilities.

5. Encrypt Sensitive Financial Data

Employ encryption technologies and techniques to protect sensitive financial data both in transit and at rest. Regularly update encryption protocols to align with industry best practices and emerging standards.

6. Advanced Digital Operational Resilience Testing: Threat-Led Penetration Testing (TLPT) and Critical Function Assurance

To significantly bolster digital operational resilience, financial institutions are strongly encouraged to implement Threat-Led Penetration Testing (TLPT). This advanced form of testing moves beyond traditional vulnerability assessments by simulating realistic attacks orchestrated by sophisticated threat actors known to target the financial sector. The objective of TLPT is not merely to identify technical weaknesses but to comprehensively evaluate the resilience of an organization's people, processes and technology against plausible and high-impact cyber scenarios. By mirroring the tactics, techniques and procedures (TTPs) of actual adversaries, TLPT provides unparalleled insights into how an institution would withstand and recover from a genuine cyberattack. Complementing this, rigorous testing of ICT tools and systems supporting critical functions is essential to ensure the continuous availability and integrity of vital services and operations. This dual approach ensures that an organization's entire digital infrastructure, particularly its most crucial components, is robustly protected against the evolving threat landscape leading to more informed security investments and enhanced incident response capabilities.

7. Contractual Agreements with Critical ICT Third-Party Providers

Given the increasing reliance on external ICT services, particularly those deemed critical, financial institutions must ensure their contractual agreements with third-party providers are robust and comprehensive. These agreements should extend beyond general data protection clauses to encompass broader operational resilience and effective oversight. Explicitly, contracts should detail Service Level Agreements (SLAs), specifying

performance targets, availability and quality metrics essential for uninterrupted service. Crucially, they must clearly define the location of data processing and storage, along with any sub-contracting arrangements, ensuring full transparency throughout the service chain. Financial entities and relevant competent authorities must be granted unrestricted access, audit and inspection rights to the provider's premises, data and systems pertinent to the outsourced services. Furthermore, agreements should stipulate comprehensive security measures, robust exit strategies including data portability and migration assistance and require prior written consent for sub-contracting of critical functions, with equivalent obligations flowing down to sub-contractors. Clear protocols for incident reporting, explicit data protection and confidentiality clauses, defined governing law and jurisdiction and provisions for liability and remedial actions are also paramount to safeguard operational continuity and facilitate effective supervision.

8. Comprehensive ICT Risk Management

To safeguard against the evolving digital landscape and ensure continuous operational resilience, financial institutions must implement a comprehensive framework for managing Information and Communication Technology (ICT) risks. This framework encompasses all ICT systems, processes, and assets that underpin critical business functions, aiming to prevent, detect, respond to and recover from disruptions and threats. It requires proactive efforts to identify potential ICT risks across the entire operational environment, including vulnerabilities stemming from internal systems, data flows and external dependencies. Following identification, robust measures must be in place to protect these critical assets through advanced security controls and organizational safeguards. The framework must also emphasize capabilities to quickly detect anomalous activities and ICT-related incidents, enabling timely and effective response and recovery actions to minimize impact and restore services in line with business continuity protocols.This strategic approach ensures that institutions can maintain the integrity and availability of their financial services, adapting to new threats and fostering sustained stability in the digital economy.

9. Stay Compliant with Data Protection Principles

Regularly monitor and update your data protection policies and practices to align with evolving regulatory requirements particularly in compliance with the Data Protection Act, the Cybersecurity and Cybercrime Act 2021 and any other applicable laws and governing frameworks .
Establish a dedicated compliance team to ensure ongoing adherence to regional and international data protection laws where applicable.

Artificial Intelligence

The financial industry has swiftly adopted Artificial Intelligence (AI) technology throughout its operations to obtain multiple advantages despite facing specific dangers namely applying AI systems across multiple areas through automated trading systems and enhanced credit decision tools while using chatbots to boost customer service and supporting investment management and risk management functions including fraud detection and liquidity risk assessment. The AI applications deliver increased operational effectiveness while decreasing expenses and enabling improved personalized services for customers and various stakeholders. The analysis of alternative data through AI helps increase financial inclusion because it provides creditworthiness assessment for individuals who lack traditional credit records. AI systems boost cybersecurity through superior threat detection capabilities for cyber threats and illicit activities and lead to

enhanced profitability through optimized processes and assist users with more efficiency and less manual work requirements.

However, the implementation of Artificial Intelligence (AI) in the finance encounters multiple difficulties and challenges during its adoption process. The implementation of AI in financial operations faces three primary challenges notably: (i) biased lending decisions, (ii) privacy risks from data collection and analysis and (iii) operational interruptions caused by technology problems or security threats. Financial organizations face model risk due to defective and unreliable data along with their inability to handle and adapt to new situations which produces incorrect outputs that result in monetary losses. The intricate nature of AI models especially generative AI creates difficulties in explainability which hinders organizations from following rules that need detailed decision-making explanations. The concentration risk from using limited third-party AI service providers together with market herding behaviours represent major concerns for the financial industry.

The National Institute of Standards and Technology (NIST) offers a complete AI Risk Management Framework for trustworthy AI implementation in finance that directs and guides organizations through all phases of AI development. Financial institutions may also consider the NIST Cybersecurity Framework (CSF) 2.0 alongside the AI Risk Management Framework to strengthen the management of cybersecurity-specific threats and operational risks associated with AI systems.The following recommendations align with NIST functions Govern, Map, Measure and Manage by focusing on:

- Financial institutions need to develop an AI risk management culture with defined accountability systems and complete transparency for AI model operations. Financial institutions need to both understand the capabilities of their models and create documentation systems while establishing independent review procedures for model audits.

- AI systems require organizations to understand their operational context before they can identify related risks during the Mapping stage. Organizations must conduct assessments to detect biases within both AI data sources and generated results and study the potential effects of AI integration on current financial operations.

- Risk assessment and analysis of identified risks should be completed systematically according to the Measure phase. AI models require strict testing and validation procedures because their dynamic nature and ability to learn from live/big data require special attention. Institutions need to evaluate the quality of AI inputs and outputs by verifying that data sources are reliable, accurate and show adequate representation.

- Organizations should establish risk mitigation plans and frameworks through the Management phase based on impact assessments of identified risks. The development of strategies must address hallucinations and bias in generative AI and strictly ensure consumer protection, safety and market conduct law compliance. The financial sector requires effective third-party risk management due to its heavy reliance on external AI service providers.

- Financial institutions must develop AI systems which enable understandable decision-making processes with explainability on how the AI model(s) came up with the output(s), especially when adverse action notifications in credit decisions need specific reasons.

- Organizations need strict data and AI governance to prevent flawed or biased data from affecting AI outputs. Protecting personally identifiable and sensitive information from unauthorized access stands as the highest priority.

- AI systems need to incorporate cybersecurity features which prevent or reduce cyber threats and operational recovery procedures must exist for managing adverse events.

In addition to the NIST AI Risk Management Framework, financial institutions may also consider adopting principles and best practices from other internationally recognised AI governance frameworks and standards, such as International Organization for Standardization/IEC 42001 Artificial Intelligence Management Systems (AIMS), the European Union AI Act and the Organisation for Economic Co-operation and Development AI Principles, to further strengthen responsible, transparent and trustworthy AI governance within the Mauritian financial ecosystem.

Financial institutions can develop a trustworthy, transparent and responsible AI ecosystem that maximizes benefits and Return of Investments (ROIs) by following NIST-recommended practices for risk management and involving human intervention in the final decision for any outcome.

21.0 Specific Recommendations for the Banking Sector

The recommendations contained in this chapter are issued by the Data Protection Office to support banking institutions in implementing appropriate technical and organisational measures required to demonstrate compliance with their obligations and duties under section 22 of the Data Protection Act. Banking institutions are expected to implement the recommendations progressively within a reasonable timeframe of not less than twelve (12) months from the date of issuance of this guide taking into consideration the sensitivity, criticality and financial risk exposure associated with banking and financial data processing activities.

The recommendations constitute baseline measures and controls expected to be implemented by banking institutions. Additional controls and safeguards should also be implemented, where necessary, based on the bank's internal risk assessments, operational environment and business requirements.

1. Data Classification and Financial Data Segmentation Framework

Banks are recommended to adopt a risk-based approach to data classification. Classification and related safeguards may take into consideration:

- the sensitivity and criticality of the data and
- the nature of the information processed including:
  - core banking and financial transaction data;
  - customer account and payment information;
  - know Your Customer (KYC) records;
  - Anti-Money Laundering (AML)/Counter Financing of Terrorism (CFT) information/ Criticality, Privacy and Financial Impact data
  - behavioral / analytics data (profiling[34], scoring)

34 "profiling" under the DPA means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Each data classification would have:

- distinct access controls, encryption standards and monitoring thresholds
- segregation between production, analytics and testing environments.

2. Financial Data Flow Mapping & Traceability

Banks are encouraged to maintain appropriate end-to-end data flow mapping mechanisms to enhance visibility, governance and traceability of data across systems and processes. This may cover, where applicable:

- internal systems (core banking, mobile apps, CRM)
- third-party integrations (fintech APIs, payment gateways)
- cross-border transfers

For enhanced accountability and oversight, banks are advised to consider:

- maintaining traceability of customer data across systems and applications;
- identifying data replication points, backup environments and shadow databases; and
- aligning data flow records with the organisation's Record of Processing Operations and governance framework.

This introduces system-level traceability which is critical for breach investigations and audits.

3. Forensic Readiness Capability

Banks are recommended to implement forensic readiness mechanisms to support:

- regulatory investigations
- internal audits
- cyber incident response
- timely notification and reporting to the relevant regulator(s) under applicable supervisory directives.

Such measures may include:

- log integrity and chain-of-custody procedures
- time-synchronised logging across systems
- data preservation protocols

4. Advanced Monitoring of High-Risk Financial Activities

Banks are advised to deploy behavioural and anomaly detection mechanisms to help identify:

- unusual transaction patterns
- rapid data access / extraction events

These mechanisms are recommended to:

- integrate with SIEM platforms
- trigger real-time escalation workflows
- feed into fraud and AML/CFT/CPF monitoring

5. AI and Automated Decision-Making Governance in Banking

Where banks use AI for purposes such as:

- credit scoring
- fraud detection
- customer profiling,

they are recommended to:

- implement model explainability and auditability mechanisms
- ensure decisions are not solely automated where legal/financial impact exists
- document bias testing and fairness controls
- implement AI model trainings to enhance model performance while also adapting to new data and evolving contexts

6. Strengthened Customer Transparency in Digital Banking

Banks are recommended to adopt enhanced transparency mechanisms. This may include:

- real-time notifications for high-risk transactions
- dashboards allowing customers to manage consent preferences
- banking institutions must ensure that the processing of special categories of personal data complies with section 29 of the DPA and provide alternative authentication methods for customers who choose not to share their biometric data.

7. Vendor Ecosystem Risk Governance (Fintech Integration)

Banks are advised to implement continuous vendor risk monitoring, not limited to onboarding:

- real-time monitoring of API access
- periodic reassessment of fintech partners and third-party providers
- contractual clauses for:
  - audit rights
  - data localisation (where applicable)
  - breach escalation timelines
- other parties such as subcontractors engaged by vendors

This strengthens third-party obligations by introducing ongoing supervision, not just due diligence.

8. Secure Digital Communication Framework

Banks are recommended to implement controlled communication channels. This may include:

- secure customer messaging platforms (instead of email)
- encryption controls for all outbound financial data

9. Customer Risk Awareness and Shared Responsibility Model

Banks are encouraged to integrate customer awareness into risk frameworks. This may include:

- fraud awareness prompts
- real-time risk alerts during transaction processing
- education on phishing and OTP misuse
- literacy about cyberisks and proper use of personal/sensitive data

10. Data Protection Metrics & Board-Level Reporting

Banks are advised to establish data protection KPIs and report to senior management on:

- number of data breaches
- response times
- access violations
- third-party incidents.

11. Dual-Verification for Outbound Communications

Banks are recommended to implement a two-step verification process before sending any customer data externally which may include:

- Mandatory second-person check for emails with attachments
- Automated prompts requiring confirmation of recipient identity
- System-enforced delay (e.g. 30–60 seconds) before sending high-risk emails and conduct a callback verification with the client.

12. Secure Document Handling and Physical Verification Protocol

Banks are advised to introduce procedures for physical document handling such as statements and letters. Such measures may include:

- Identity verification before handing over documents
- “Read-back” confirmation of customer name/account
- Segregated counters for document collection

13. Access Control Validation and Periodic Reconciliation

Banks are recommended to implement:

- Access rights validation checks and account linkage (e.g. for internet banking)
- Periodic reconciliation of user access vs. role
- Immediate alerts for unusual privilege assignments

14. Configuration and Change Management Controls

Banks are adivised to strengthen system governance by:

- Formal change approval workflows
- Pre-deployment testing for bulk updates (e.g. batch files, software conversions)
- Rollback mechanisms for system errors

15. Strict Control on Use of Personal Devices (BYOD Policy)

Banks are recommended to:

- Prohibit use of personal devices for official work involving sensitive data
- Block forwarding of official emails to personal accounts
- Enforce device compliance checks before accessing systems

16. Data Minimisation in Communications

Banks are advised to:

- Limit attachments to only strictly necessary data
- Avoid sending full statements where summaries suffice
- Use masked or partial data where possible
- Encrypt statements with passwords

17. Structured Training on Real Incident Scenarios

Banks are advised to move beyond generic training by:

- Using actual breach scenarios
- Conducting simulation exercises (e.g. phishing, mis-sending drills)
- Targeting high-risk roles (customer service, operations)

18. Segregation of Shared Folders and Template Management

Banks are recommended to:

- Separate blank templates from completed client documents
- Restrict download/upload permissions
- Implement version control and naming conventions
- Ensure there is proper auditing of file access
- To implement a Data Loss Prevention Solution

19. Controlled Email Thread Management

Banks are recommended to:

- Disable automatic inclusion of previous attachments in email threads
- Require review of entire thread before sending
- Encourage "clean send" options where applicable (new message vs reply)

Non-Exhaustive safeguards to promote the security of Personal Data (Annex 1)

Some non-exhaustive safeguards to promote the security of personal data

a. Implementation of physical safeguards to limit physical access to sensitive information, systems, related facilities, and equipment from unauthorized access as well as natural and environmental hazards.
b. Implementation of technical and organisational measures (e.g. privacy policy, information security policy, amongst others) to protect data.
c. Implementation of access controls to ensure that user access rights reflect defined and documented business needs and job requirements.
d. Development of practices that will help to reduce the risk of insider attacks such as segregation and rotation of duties, least privilege, log monitoring and administrative account control.
e. Regular testing of key controls, systems and procedures to obtain assurance and confidence that the security implemented controls are operational and effective in their application.
f. Organization should ensure that all leavers have no access to the entity's information/ client information, organization application or any related software. A leavers checklist is appropriate to set up and proper testing should be conducted for its effectiveness.
g. Logging and monitoring of activities to assess policy compliance, identify intrusions and breaches.
h. Development of formal change management procedures covering both normal and emergency changes to systems processing sensitive information.
i. Evaluation of all transfers of physical media containing sensitive information.
j. Implementation of an e-mail acceptable use policy and to clearly describe applicable restrictions on the transmission of sensitive information via e-mail.
k. Use of a variety of technical safeguards for data security, including firewalls, intrusion detection systems, penetration testing and vulnerability scanning.
l. Implementation of policies and processes governing the conditions under which remote access is granted and terminated.
m. Ensuring all remote communications are done through a virtual private network that can provide a secure communication channel.
n. Configuration of all servers and workstations with antivirus software that is automatically updated daily with new virus definitions.
o. Passwords adherence to complexity and ageing requirements.
p. Periodic assessments and reviews of entitlement privileges and permissions to systems and data.
q. Scheduled backups of data within a secured storage environment.
r. Strengthen controls of developers' access to controlled information systems and sensitive data.
s. Implementation of effective disaster recovery/business continuity planning (DR/BCP) to establish the basis for the organisation to maintain and recover business processes when operations have been disrupted unexpectedly.
t. Implementation of appropriate disposal practices and media sanitisation to prevent unauthorised access or use of the information.

Designed and Printed by The Government Printing-2026