Data Protection Office

DATA PROTECTION IN THE FINANCIAL SECTOR

NOV 2023

Table of Contents

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 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 in the financial sector. It is also aimed at providing guidance on the processing of personal data performed by financial institutions in order to ensure compliance with data protection principles under the Data Protection Act of Mauritius.

2.0 Governing legislations and regulations 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 of:

a) Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT)

Mauritius has demonstrated its unflinching commitment to combat money laundering and the financing of terrorism and proliferation. To this effect, Mauritius has ratified and acceded to numerous international conventions, protocols, and treaties to express its commitment towards the international community to combat this scourge.

Furthermore, AML/CFT compliance is a permanent concern for regulators such as the Financial Services Commission (FSC), the Bank of Mauritius (BoM) and relevant authorities such as the Financial Intelligence Unit (FIU) and the Independent Commission Against Corruption (ICAC) that are mandated to fight corruption through investigation, prevention and education to demonstrate that Mauritius IFC is part of the international network in combating ML/TF.

AML/CFT compliance remains one amongst the top priorities of financial institutions.

The various legislations enacted include the following:

- The Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA)
- The Prevention of Corruption Act 2002
- The Prevention of Terrorism Act (POTA) 2002
- Anti-Money Laundering and Countering the Financing of Terrorism Handbook (AML/CFT Handbook)
- Convention For The Suppression Of The Financing Of Terrorism Act 2003
- Mutual Assistance In Criminal And Related Matters Act 2003.

b) A panoply of acts governing the financial sector such as:

Bank of Mauritius Act 2004, Banking Act 2004, Companies Act 2001 (Corporate and Business Registration Department), Financial Intelligence and Anti-Money Laundering Act (FIAMLA) 2002, Financial Reporting Act 2004, Financial Services Act 2007, Prevention of Corruption Act 2002, The Mauritius Revenue Authority Act 2004, The Good Governance and Integrity Reporting Act 2015, Competition Act 2007, Virtual Asset and Initial Token Offering Services (VAITOS) Act, Asset Recovery Act 2011, United Nations (Financial Prohibitions, Arms Embargo And Travel Ban) Sanctions Act 2019.

c) Various regulations issued under:

Banking Regulations, FIAMLA Regulations, Financial Services Regulations, Insurance Regulations, POTA Regulations, Protected Cell Companies Regulations, Securities Regulations, Stock Exchange Regulations.

Further information on the above is available on the websites of the Mauritius International Financial Centre, FSC, FIU and BoM on the following links:
https://mauritiusifc.mu/regulatory-environment
https://www.fscmauritius.org/en/legal-framework/our-enabling-laws
https://www.bom.mu/about-the-bank/legislation
https://www.fiumauritius.org/fiu/?page_id=2296

3.0 Some examples of supervisory and oversight bodies in the financial sector

a. Ministry of Financial Services and Good Governance

The Ministry of Financial Services and Good Governance 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.[1]

b. Bank of Mauritius (BoM)

The BoM is the central bank of the Republic of Mauritius and is committed to promoting and maintaining monetary and financial stability.[2]

c. Financial Services Commission (FSC)

The FSC is the integrated regulator in Mauritius for the financial services sector (other than banking) and global business.[3]

d. Stock Exchange of Mauritius (SEM)

The principal activities of the SEM, as defined by its Constitution, are[4]:

i. to operate and maintain a securities exchange in accordance with law;
ii. to provide facilities for the buying and selling and otherwise dealing in securities on a securities exchange;
iii. to provide and maintain, to the satisfaction of the FSC adequate and properly equipped premises for the conduct of its business; and
iv. to have operating rules for the markets it operates pursuant to law.

The principal activities of its Subsidiary Company, the Central Depository and Settlement Co. Ltd (CDS), as defined by the Securities (Central Depository, Clearing and Settlement) Act 1996, are to provide depository, clearing and settlement services in order to facilitate dealings in securities on the Exchange.

e. Financial Intelligence Unit (FIU)

[1] https://financialservices.govmu.org/Pages/TheMinistry.aspx
[2] https://www.bom.mu/
[3] https://www.fscmauritius.org/en/licensing/licensed-activities/securities
[4] https://www.stockexchangeofmauritius.com/media/8318/22090090-sem-annual-report-2022-lr-26102022.pdf

Established under Section 9 of the Financial Intelligence and Anti Money Laundering Act 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.[5]

The FIU is also the Enforcement Authority under the Asset Recovery Act and the AML/CFT 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.

f. 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.[6]

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.

g. Mauritius Financial Reporting Council (FRC)

The FRC is a body corporate set up under the Financial Reporting Act 2004. It is an organisation under the aegis of the Ministry of Financial Services, Good Governance and Institutional Reforms. The FRC is mainly responsible for promoting confidence in corporate reporting and good corporate governance.[7]

The Council main objects as defined in the FRAct are:

[5] https://www.fiumauritius.org/fiu/
[6] https://www.mra.mu/index.php/about-us1/mandate-vision
[7] https://frc.govmu.org/frc/?page_id=1517

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.

h. Independent Commission Against Corruption (ICAC)

While not exclusively focused on the financial sector, the ICAC investigates and combats corruption in various sectors, including finance.

Some of the functions of the ICAC are to:

i. educate the public against corruption[8];
ii. enlist and foster public support in combating corruption;
iii. detect or investigate any act of corruption;
iv. detect and investigate any matter that may involve the laundering of money or suspicious transaction that is referred to it by the FIU;
v. take such measures as may be necessary to counteract money laundering in consultation with the FIU;
vi. co-operate and collaborate with the FIU in fulfilling common objectives.

4.0 Mauritius Data Protection Act

a. 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 namely the Data Protection Act 2017 (DPA) which came into force on 15 January 2018.

The rationale of the DPA is to provide for new legislation to strengthen the control and personal autonomy of data subjects over their personal data, in

[8] https://www.icac.mu/about-the-icac/

line with current relevant international standards, and for matters related thereto. 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

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.

b. Data Protection (Fees) Regulations 2020

The Data Protection (Fees) Regulations 2020 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

5.0 Data Protection Office

The Data Protection Office is an independent public office, established by the Data Protection Act, and 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

6.0 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, 31 and 46 of the DPA and are as follows:

i. Investigation of complaints

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.

ii. Power to require information

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 81 of the Prevention of Corruption Act.

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

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

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

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

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 81 of the Prevention of Corruption Act, 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

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.

viii. Prior security check

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

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

7.0 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

8.0 Registration obligation and Mandatory 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/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
- DPO Portal User Guide
- Guide on registration and renewal

9.0 Principles relating to processing of personal data

Financial institutions, similar to all controllers and processors, 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 of 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 about details of the 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.

9.1 Duties of controller

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

The measures mentioned above must include the following:

- Implementing appropriate data security and organisational measures

Financial institutions often comply with the following 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.

Upon the development of policies and procedures, financial institutions are required to put in place appropriate training and/or awareness mechanisms for employees to ensure that the employees understand the relevance of policies and procedures to their 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

- Designating an officer responsible for data protection (Data Protection Officer).

  In accordance with section 22(e) of the DPA, financial institutions must designate a data protection officer responsible for data protection compliance. The roles and responsibilities of data protection officers are further explained in the Data Protection Office guide available on https://dataprotection.govmu.org/Documents/Roles%20and%20Responsibilities%20of%20Data%20Protection%20Officer%20V3.pdf

Financial institutions must also implement mechanisms to verify the effectiveness of the technical and organisational measures implemented.

9.2 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 provide a list of information through relevant notifications as elaborated in section 23(2) of the DPA when collecting personal data. The notifications provided must be clear and effective to individuals to promote transparency and compliance with data protection principles. For instance, data protection information notifications are useful

tools to communicate with data subjects, explaining the organisation's data processing practices, legal basis for processing, data retention policies, data subject rights, and other relevant information. Financial institutions must be clear in application forms, 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 or voluntary.

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

Data protection information notifications should also be provided at appropriate times such as during an account creation. 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 notifications and data protection policies. Financial institutions should ensure that customer-facing staff are knowledgeable about data protection and can address customer inquiries.

If a financial organisation 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 notifications of these third parties.

A financial institution may sometimes record 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. It is important to note that the data subject must be informed about the recording in accordance with section 23 of the DPA under

such circumstances either when stipulating the relevant contract or at the onset of the first phone call.

9.3 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. It is recommended to request consent separately for each distinct purpose of processing. 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.

Moreover, when the lawful ground of processing is based on consent, then 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.

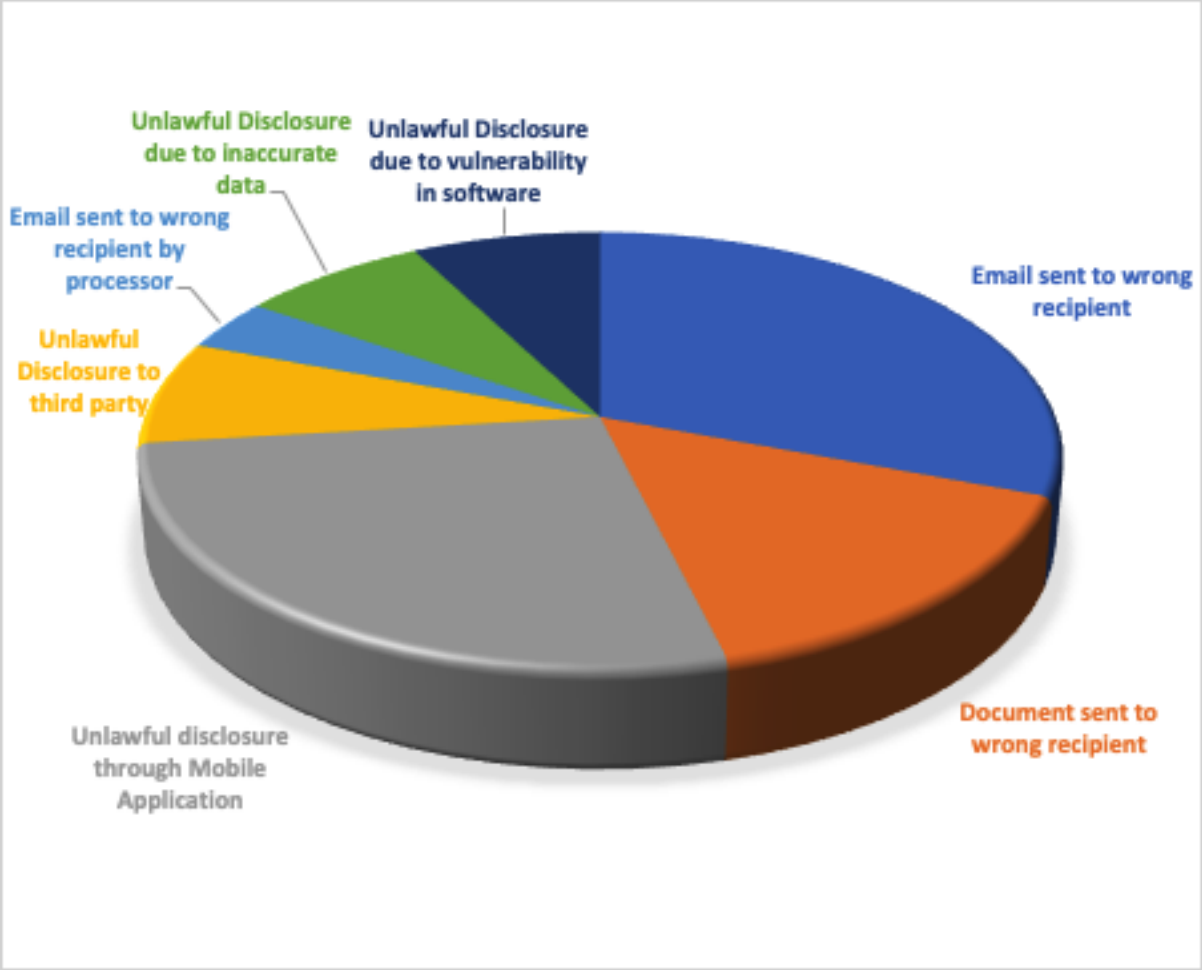
9.4 Notification of personal data breach and Communication to the data subject

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.

From January to September 2023, the DPO received personal data breaches from financial institutions on 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.

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.

9.5 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 anonymised.

9.6 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) as provided below:

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;

ii. for compliance with any legal obligation to which the controller is subject;

iii. in order to protect the vital interests of the data subject or another person;

iv. for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

v. the performance of any task carried out by a public authority;

vi. the exercise, by any person in the public interest, of any other functions of a public nature;

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. for the purpose of historical, statistical or scientific research.

Examples:

- *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 the Financial Intelligence and Anti-Money Laundering Act (FIAMLA) and the Prevention of Terrorism Act (POTA) to identify and report certain transactions to the FIU as part of their anti-money laundering (AML) and counter-terrorism financing (CTF) compliance efforts. 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 are not required for this type of processing.

Any person who contravenes subsection 28(1) 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 organisations should ensure that their processing operations are lawful.

9.7 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 –

(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;

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

(d) the processing is necessary for –

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

(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);

(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.

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

9.8 Personal data of child

According to section 30 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.

9.9 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 organisations are not exempt from these security obligations. Financial organisations should take reasonable steps to store personal data securely such that it is not stolen, lost or used deliberately or accidentally.

Financial organisations 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 (eg smartphones, laptops or tablets). If employees are allowed to use their own mobile devices, refer to our Bring Your Own Devices (BYOD) guidance.

- 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. This may be a particular issue for journalists who spend a lot of time out of the office gathering information or filing reports on location.

- 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 beach management plan.

- staff training and supervision. Organisations should vet new staff to a level appropriate to their position to confirm their identity, reliability and provide training (including regular refresher training) on key security risks, procedures and responsibilities.

Section 31 also states at subsection 4 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 –

(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 organisation is using the service of a cloud provider for its prosessing activities, section 31 (4) will apply.

Financial Institutions must perform regular testing, assessing and evaluating the effectiveness of technical and organisational measures.

9.10 Record of processing operations

Since the rule is the same for all controllers, financial organisations will have to maintain a record of all processing operations under their responsibility according to section 33 of the DPA. How you will record the processing operations will depend on you, however, the Data Protection Office has designed a template to assist organisations which is available on our official website at the following URL: http://dataprotection.govmu.org/English//DOCUMENTS/TEMPLATE%20FOR%20RECORD%20OF%20PROCESSING%20OPERATIONS.XLS.

9.11 Data Protection Impact Assessment (DPIA)

As per section 34, 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:

A form and a list of criteria to evaluate high risk processing are available on the website of this office.

9.12 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 this 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.

9.13 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) 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;

(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;

(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;

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

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

(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."

(2) A transfer pursuant to subsection (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.

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

(4) 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."

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 following link:
https://dataprotection.govmu.org/Pages/eDPO.aspx.

Should the controller relies on any one of the other exceptions, no authorisation from the Data Protection Commissioner is required.

9.14 Rights of individuals

Part VII of the DPA elaborates on the rights of individuals.

9.14.1 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 organisations should record the reasons for this decision and communicate them to the person concerned.

9.14.2 Right of 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.

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.

9.14.3 Right to object

Likewise, an individual has the right to object in writing at any time 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.

10.0 Cloud Computing

Cloud computing has become ubiquitous especially with financial institutions. As per section 36 (1) of the Data Protection Act (DPA) 2017, 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 9.1.3.

It is required to have a written contract between the financial institution and the cloud provider that covers 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, 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, security of processing, and the choice of cloud provider should also be carefully chosen so as to protect the personal data at risk because the primary responsibility of 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 in order to 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.

11.0 Direct Marketing

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

Prior consent of 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 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 in a position to identify itself. It has to provide contact details for an individual to contact them, particularly if they want to opt-out/unsubscribe of 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:

http://dataprotection.govmu.org/English/Documents/2019/Disclaimer/Template%20on%20CCTV%20Policy.docx

12.0 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 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.

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

There are various offences and criminal penalties under this Act 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

Offences	**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 years.
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.

14.0 Processing of personal data for anti-money laundering/ countering financing of terrorism purposes [9]

Data processing in the AML/CFT context shall be based on a clear and detailed legal basis and shall be necessary and proportionate to the legitimate aim pursued.

The question of a “freely” given consent should be carefully considered and it should be ensured that the data subject has a choice. If this is not the case, the data processing has to be based on an alternative legal basis.
AML/CFT framework which often involves specific investigations into suspicions of or actual ML/TF 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 (OE), the provision of personal data in response to requests for information by FIUs and LEAs and the application of monitoring orders by the OE. In those cases, because prior information of the customer would contravene to AML/CFT 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 and are entrusted with specific tasks in this area. Checks and balances as well as oversight need to be implemented. The same does not extend necessarily to private sector institutions which are obliged entities have a different legal status and mandate.

Processing of personal data by OEs in the AML/CFT context should be based on legal obligations 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. 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

[9] Guidelines from Council of Europe

should be accessible in a timely manner by a competent authority through either a register of beneficial ownership or an alternative mechanism. [In determining the beneficial owners, countries are required to ensure that companies co-operate with competent authorities to the fullest extent possible by (i) requiring that one or more natural persons resident in the country is authorised by the country and accountable to competent authorities to provide all available beneficial ownership information, (ii) requiring that a designated non-financial businesses and professions (DNFBP) in the country is authorised by the company and accountable to competent authorities for providing all available BO information or taking other comparable measures.] At the same time, when providing access to BO information, competent authorities should duly take into account the right to the respect for privacy of the persons concerned, taking account of and impact such an access can make on her or his rights and freedoms.

The existence of iInformation 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 (e.g. legislative amendments may be needed to ensure a proper legal basis and allow partners to achieve their objectives).

15.0 Financial Technology (Fintech)

Fintech refers to firms using new technology to compete with traditional financial methods in the delivery of financial services[10]. The financial sector market is evolving at an exponentially fast rate powered by Fintech solutions enabling massive meta data processing capabilities.

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

- Artificial Intelligence

[10] https://en.wikipedia.org/wiki/Fintech

- Blockchain
- Big data
- Cloud computing

Data protection compliance in Fintech is crucial 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.

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.

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.

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) has 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.

16.0 Recommendations

Data processing in the context of AML/CFT should be carried out on the basis of a clear and detailed legal basis respecting the principles of necessity and proportionality and with appropriate safeguards.

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 obligations should be properly substantiated and carefully scrutinised.

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.

Controllers should analyse threats and trends in the area of cybercrime and information security on both a periodical and ad-hoc basis (unexpected trigger events) in order to enhance data security and organisational measures to minimise the risk of breach.

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. Conducting risk-based audit programs to ensure effectiveness of data security policies and procedures.
d. Implementation of information security awareness and training programmes for providing employees with the information and tools needed to protect the organization's information assets.
e. Implementation of access controls to ensure that user access rights reflect defined and documented business needs and job requirements.
f. 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.
g. 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.
h. Logging and monitoring of activities to assess policy compliance, identify intrusions and breaches.
i. Development of formal change management procedures covering both normal and emergency changes to systems processing sensitive information.
j. Evaluation of all transfers of physical media containing sensitive information.
k. Encryption of data in transmission and storage.
l. Implementation of an e-mail acceptable use policy and to clearly describe applicable restrictions on the transmission of sensitive information via e-mail.
m. Encourage the use of privacy enhancement technologies to protect data.
n. Use of a variety of technical safeguards for data security, including firewalls, intrusion detection systems, and vulnerability scanning.
o. Implementation of policies and processes governing the conditions under which remote access is granted and terminated.

p. Ensuring all remote communications are done through a virtual private network that can provide a secure communication channel.
q. Configuration of all servers and workstations with antivirus software that is automatically updated daily with new virus definitions.
r. Passwords adherence to complexity and ageing requirements.
s. Periodic assessments and reviews of entitlement privileges and permissions to systems and data.
t. Scheduled backups of data within a secured storage environment.
u. Implementation of firewalls, intrusion detection system and penetration testing and vulnerability scanning.
v. Strengthen controls of developers' access to controlled information systems and sensitive data.
w. 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.
x. Implementation of appropriate disposal practices and media sanitisation to prevent unauthorised access or use of the information.