KPMG

MIoD
Mauritius Institute of Directors
Promoting Corporate Governance across the board

Audit Committee Forum

Position Paper 8

Guidelines for the Audit Committee on Data Protection

October 2020

kpmg.com/mu
miod.mu

About the Audit Committee Forum

Recognising the importance of Audit Committees as part of good Corporate Governance, the Mauritius Institute of Directors (MIoD) and KPMG have set up the Audit Committee Forum (the Forum) in order to help Audit Committees in Mauritius, in both the public and the private sectors, improve their effectiveness.

The purpose of the Forum is to help Audit Committee members adapt to their changing role. Historically, Audit Committees have largely been left on their own to keep pace with rapidly changing information related to governance, risk management, audit issues, accounting, financial reporting, current issues, future changes and international developments.

The Forum provides guidance for Audit Committees based on the latest legislative and regulatory requirements. It also highlights best practice guidance to enable Audit Committee members to carry out their responsibilities effectively. To this end, it provides a valuable source of information to Audit Committee members and acts as a resource to which they can turn for information or to share knowledge.

The Forum's primary objective is thus to communicate with Audit Committee members and enhance their awareness and ability to implement effective Audit Committee processes.

Position Paper series

The Position Papers, produced periodically by the Forum, aim to provide Board directors and specifically Audit Committee members with basic best practice guidance notes to assist in the running of an effective Audit Committee.

Position Paper 8 deals with the Guidelines for the Audit Committee on Data Protection.

Previous Position Papers are listed below and may be accessed at http://www.kpmg.com/mu and http://www.miod.mu/.

Paper 1: Best Practice Guidance Notes for Audit Committees (July 2014)

Paper 2: Interaction of Audit Committee with Internal and External Auditors (May 2015)

Paper 3: The Audit Committee's Role in Control and Management of Risk (December 2015)

Paper 4: Guidelines for the Audit Committee's assessment and response to the Risk of Fraud (October 2016)

Paper 5: Guidelines for the Audit Committee's approach to Information Technology Risk (July 2017)

Paper 6: Audit Committee Guidelines for evaluating whistleblowing systems (September 2018)

Paper 7: Audit Committee's Guidelines for the Evaluation of Retirement Obligations (July 2019)

Members of the Forum

Collectively, the Forum is made up of the following members drawn from diverse professional backgrounds with significant experience in both the private and the public sectors.

The drafting of this paper has been done in consultation with the **Data Protection Office** in Mauritius.

Ujoodha Sheila – *Chairperson*	**King** Antoine
Aumeerally Feriel	**Koenig** Fabrice
Chung John	**Leung Shing** Georges
Cundasawmy Robin	**Mamet** Linda
De Marassé Enouf Maurice	**Molaye** Sanjay
Dinan Pierre	**Mooroogen** Sumita
Gooroochurn Bharatee	**Ramdin-Clark** Madhavi
Ibrahim Nesmah	**Reetun** Khemraj
Kee Mew Mervyn	
Secretary:	*MIoD Co-ordinator:*
Bishundat *Varsha*	***Mulung*** *Nafeeza*

Contents

Sources that have been used in writing this Paper:

- *The Data Protection Act 2017 (Republic of Mauritius), http://dataprotection.govmu.org/English/Legislation/Pages/Data-Protection-Act-2017-.aspx*
- *ECIIA and FERMA. 2019. GDPR and Corporate Governance: The Role of Internal Audit and Risk Management One Year After Implementation. Bruxelles, Belgium. https://www.eciia.eu/wp-content/uploads/2019/11/GDPR-and-corporate-governance-ECIIA-FERMA.pdf*
- *Introduction to data protection: some basic concepts. 2020. Information Commissioner's Office. Accessed August 12, 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/*
- *NCCG (National Committee on Corporate Governance). 2016. The National Code of Corporate Governance for Mauritius. 2nd ed. https://nccg.mu/sites/default/files/files/the-national-code-of-corporate-governance-for-mauritius_2016.pdf*
- *GDPR: What? When? Why? 2020. Chartered Institute of Internal Auditors. Accessed August 12, 2020. https://www.iia.org.uk/resources/auditing-business-functions/data-protection/gdpr-what-when-why/*

Introduction

Organisations in all sectors hold growing amounts of personal data on employees, customers and other external stakeholders. **Personal data** can be described as any information which can enable the identification of a person. This does not necessarily mean 'private' information, as even information that is known to the public, such as an individual's professional details, can be considered as personal data. If an individual is identifiable from these details alone or by combining with any other information, it is still viewed as personal data.

Many organisations keep large quantities of personal data not only internally but often also through external storage services. With the massive social and technological changes in recent years, an increasing amount of data, including personal data, is being shared. Processing personal data poses security challenges, hence the need for regulations to protect individuals as well as organisations.

The necessity of laws on data protection is derived from the principle that all individuals have the right to the protection of their private life, personal data being an integral part of it. This fundamental right to privacy is applicable to anyone inside and outside an organisation.

Being in an era of rapid technological change, it is necessary to ensure that privacy rights are properly protected. While this has been a global interest for years, various parts of the world have tried to empower their citizens for their privacy rights.

The Board of Directors' inability to ensure protection of personal data may be considered a failure to exercise reasonable care and diligence, and this could result in action for damages, termination or disqualification. Effective data protection compliance could be good for an organisation's reputation. Potential clients and stakeholders, along with the general public, will respect organisations that make an effort to manage personal data with care.

The terms referred to in writing this Paper and their definitions are included in the Appendix (pages 18 and 19).

Legislation

In Mauritius, Sections 3 and 9 of the Constitution of Mauritius and Article 22 of the Mauritian Civil Code clearly emphasise on the right to privacy. Mauritius enacted the Data Protection Act in 2004, providing protection to individuals on their privacy rights in terms of the techniques used to capture, transmit, handle or store their data. The Act was consequently replaced by *The Data Protection Act 2017* following Mauritius' evolving digital context and international standards, namely the *General Data Protection Regulation* (*GDPR*), aiming at reinforcing the personal autonomy and control of data subjects over their personal data.

The *GDPR* intends to strengthen and unify data protection for all individuals within the European Union (EU) and addresses the export of personal data outside the EU. It provides for harmonisation of the data protection regulations throughout the EU, therefore making it easier for non-EU organisations to comply with these regulations.

The Mauritius Data Protection Office, under the aegis of the Ministry of Information Technology, Communication and Innovation, came into operation in February 2009 and is responsible for ensuring compliance with *The Data Protection Act 2017*. The Mauritius Data Protection Office ensures that the principles of data protection are observed in Mauritius.

Oversight responsibility of the Board of Directors:

If a business holds information on individuals for any purpose and processes these **personal data** in any form, *The Data Protection Act 2017* applies to them. A key aspect for complying with the Act remains the importance of a strong corporate governance culture within an organisation. **Principle 4** of the National Code of Corporate Governance for Mauritius (2016) on Director Duties, Remuneration and Performance clearly states that "*Directors should be aware of their legal duties… The Board is responsible for the governance of the organisation's information, information technology and information security.*"

The Board is required to exercise a level of care, skill and diligence in their duties towards their organisation, leading to **Principle 5** on Risk Governance and Internal Control which states that "*The Board should be responsible for risk governance and should ensure that the organisation develops and executes a comprehensive and robust system of risk management. The Board should ensure the maintenance of a sound internal control system.*"

Audit Committee's role for Data Protection

Audit Committees are responsible for the verification of an organisation's financials and oversight of the internal and external audit processes, and are important recipients of information from management and external sources.

Outside of the financial services industry, where separate risk committees have become an established best practice, Audit Committees have also begun to take on a new role. They are increasingly being asked to monitor new issues such as data privacy and digitalization, exposing them to new compliance risks.

Management is responsible for establishing and maintaining the integrity of the organisation's data protection internal controls, including identifying privacy risks and vulnerabilities and implementing appropriate safeguards. The Audit Committee can assist the Board with respect to its oversight responsibility and could handle this responsibility through a sub-committee such as a "Data Privacy Committee."

Typical functions that can be exercised by the Audit Committee in this context are as follows:

— Assist the Board of Directors in fulfilling its risk oversight responsibilities with respect to the protection of the organisation's assets, including confidential, proprietary and personal information, reputation and goodwill in all forms;
— Oversee and monitor the organisation's material compliance with applicable information security, privacy and data protection laws, industry standards and contractual requirements;
— Promote the integrity, adoption and coordination of data security processes across the organisation to help ensure that data and system security is an organisation-wide business objective and priority; and
— Oversee the data protection performance and the overall implementation of the organisation's data protection strategy.

The Audit Committee shall consult with the Board of Directors, provide guidance and formulate recommendations regarding the organisation's management of data privacy risks.

Key questions from Audit Committees:

1. Has a compliance audit been conducted to understand whether the organisation is compliant with *The Data Protection Act 2017* and where further work is required?
2. Does the organisation have a trail of personal data it holds?
3. Has the organisation issued, as a minimum, these policies?
   - Privacy/Data Protection Policy;
   - Cookie Policy (if the organisation has a website and is using cookies);
   - Information Security Policy.
4. Are personal data assets protected (e.g. encrypted)?
5. Does the organisation process personal data on a large scale and/or is the organisation a public body?
6. Has the organisation designated a data protection officer, as required under Section 22(2)(e) of *The Data Protection Act 2017*?
7. Has a reporting procedure to the Mauritius Data Protection Office been established for use in the event of a personal data breach?
8. Has the organisation established a program to raise awareness and train personnel on the management, security and disclosure of personal data?
9. Have data protection principles been enshrined into contracts with relevant third parties/data processors?
10. Are special categories of personal data (i.e. sensitive data) protected, stored and backed up securely?

11. Has the organisation set a document explaining the organisation's data strategy, outlining any goals around data collection, management and use:
    a) Why is the organisation collecting data?
    b) Is the data-driven business strategy to grow sales and revenue, improve customer experiences, build trust and relationships, differentiate the business or get a competitive edge?
    c) Are there critical data the organisation needs but does not have or risky data the organisation has but no longer needs?
12. Have internal policies been set in relation to:
    a) data collection, retention and access;
    b) maintaining an accurate data inventory;
    c) training on privacy policy and practices;
    d) conducting compliance audits of third parties; and
    e) requiring third parties to comply with privacy policies?
13. Does the organisation have sufficient resources in-house to manage the data privacy, protection and compliance program or does it need to outsource that function?
14. How ready is the organisation to provide evidence of compliance to the Mauritius Data Protection Office or any other data privacy regulators?
15. Has the organisation incurred any costs in the past due to inadequate data privacy protection, and how has the business strategy been changed to address any future risks and exposure?

Compliance with privacy rules

Organisations that collect and use personal data need to pay close attention to local and international privacy laws. Audit Committees and Boards of Directors need to be conversant with laws and regulations around data privacy.

To keep up with privacy compliance standards across the globe, access to a unified database of global privacy and security regulatory requirements, controls and standards can help.

An Audit Committee should ask management what the organisation is doing to comply with data privacy laws. Is management ensuring the organisation stays on schedule to meet any requirements while also staying within budget for its compliance efforts?

Once the organisation meets the requirements, it needs to have a data privacy compliance program to ensure it is continually monitoring compliance.

Audit Committees need to be assured that management has the right processes and controls in place to mitigate any risk to that data and how they are being used.

Audit Committees will want to look beyond compliance with current laws to consider ethical issues that data use presents. Just because an organisation collects data does not mean it can—or should—use it, or allow third parties to access it.

Data ethics or "fair" data use standards are an emerging topic of practice, which means there are not always clear rules or laws outlining how organisations can use personal data.

Many organisations are growing their use of technologies such as artificial intelligence and machine learning as part of their value-creating business models. There are few, if any, regulations around this type of implementation, which can leave organisations open to ethical scrutiny.

Audit Committees will want to discuss with management where to draw these ethical and privacy lines and how the organisation can ensure they are not crossed.

Audit Committees will also want to ask how their organisations evaluate the privacy and ethical impact of new products or third-party partners. Such risk processes should allow organisations to meet regulatory and other market expectations.

Obligations on controllers, processors and data protection officers

The Data Protection Act 2017 requires the registration of controllers and processors under Section 14 with the Mauritius Data Protection Office and, under Section 22 (2)(e), the appointment of a data protection officer (DPO). The Mauritius Data Protection Office, however, does not register or certify a DPO.

As per *The Data Protection Act 2017*, the following three key roles are specified:

1 Controllers
2 Processors
3 Data protection officers

The definitions and legal requirements thereon are included in the Appendix.

Controllers

Some key obligations of controllers are as follows:

— Review and list all the types of personal data being processed;
— Ensure sufficient security and organisational measures are in place to protect personal data, and special categories of personal data;
— Ensure all disclosures of personal data comply with *The Data Protection Act 2017*;
— Designate an officer responsible for data protection issues;
— Ensure data is processed according to the purpose specified;
— Check that transfers for personal data abroad comply with *The Data Protection Act 2017*;
— Verify that registration and renewal obligations of controllers and processors are updated; and
— Ensure that relevant consents are obtained from data subjects related to the collection, storage, processing, rectification, transfer and/or erasure of personal data as per *The Data Protection Act 2017.*

Processors

Some key obligations of processors are as follows:

— Ensure the implementation of appropriate security and organisational measures;
— Act only on instructions received from the controller, under a written contract established to that effect;
— Shall be bound by obligations devolving on the controller under Section 31(1) of *The Data Protection Act 2017*; and
— Ensure that any person employed by the controller or processor is aware of and complies with relevant security measures.

Data protection officers

The Mauritius Data Protection Office encourages controllers and processors to appoint a DPO to inform and advise them, as well as their employees, on their obligations to comply with *The Data Protection Act 2017* and other data protection standards. The DPO will be the contact point with respect to data subjects, the Mauritius Data Protection Office and internally within the organisation (controller). The DPO may be an individual or a team. In the case of a team, all members should understand clearly their roles and responsibilities in respect of the duties of a DPO.

The DPO is expected to have professional experience and knowledge of data protection laws and standards. The DPO should also have a good knowledge of the business sector of the controller, that is how the operations are carried out, as well as the information systems, data security and data protection needs of the controller. Regarding personal qualities of a DPO, he/she, for instance, should be honest with high professional ethics.

The DPO should have adequate professional training on data protection, whether from internal resources, materials provided by the Mauritius Data Protection Office or third-parties. The DPO's main concern should be enabling compliance with *The Data Protection Act 2017*. Thus, the DPO should be chosen judiciously with regard to the data protection issues that may arise within an organisation.

The DPO should work in an independent environment and manner, report to the highest management level and have adequate resources to enable the controller or the processor to meet his/her obligations under *The Data Protection Act 2017*. The following highlights the minimum tasks that a DPO should carry out:

— Inform and advise the controller/processor and its employees about their obligations to comply with *The Data Protection Act 2017* and other data protection laws.
— Monitor compliance with *The Data Protection Act 2017* and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits.
— Be the first point of contact for the Mauritius Data Protection Office and for individuals whose data are processed (employees, customers, amongst others).

However, the controller/processor can add more tasks to meet business requirements.

Note: DPOs should not be dismissed or penalised by the controller or the processor for performing their tasks. For instance, a DPO may consider that a particular processing is likely to result in high risk and advise the controller or the processor to carry out a data protection impact assessment, which the controller or the processor may not agree with. In such a situation, the DPO cannot be dismissed for providing advice.

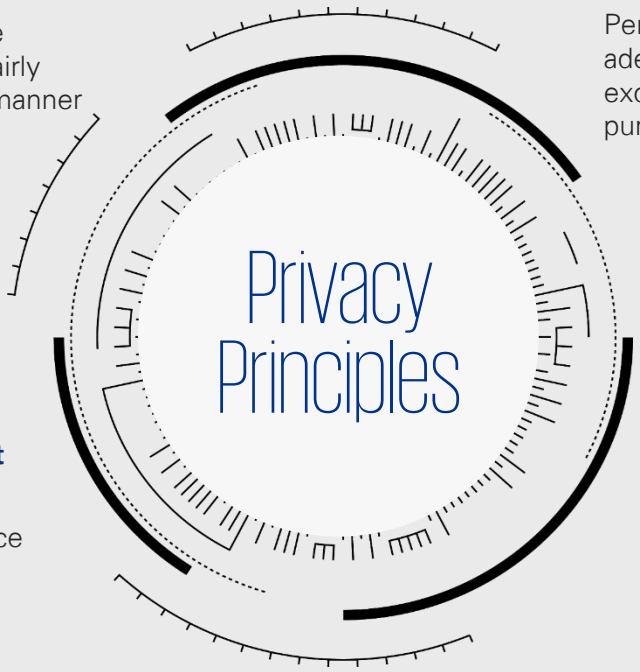
More details on the complete obligations of Controllers, Processors and DPOs can be found in Part IV, V and VI of *The Data Protection Act 2017*.

Further guidance on role of the DPO can be found in the document "Roles and Responsibilities of Data Protection Officer" on the Mauritius Data Protection Office website at https://dataprotection.govmu.org.

Transfer of personal data is further elaborated in Section 36 of *The Data Protection Act 2017*.

Principles of data protection

As per Section 21 of *The Data Protection Act 2017*, the following six privacy principles form the fundamental conditions which controllers must follow when collecting, processing and managing personal information on data subjects:



Lawfulness, Fairness and Transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to any data subject.

Data Minimisation

Personal data shall be adequate, relevant and not excessive in relation to the purpose.

Rights of data subject

Personal data shall be processed in accordance with the rights of data subjects.

Purpose Limitation

Personal data shall be collected for specified, explicit and legitimate purposes.

Storage Limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data was collected.

Accuracy

Personal data shall be accurate and, where necessary, kept up to date.

Practical considerations on the implementation of data protection mechanisms

Practical considerations when embarking on the implementation of data protection and ongoing adherence within an organisation:

— Obtain full support from top management;
— Understand the legal requirements around data protection;
— Include data protection as part of the culture of the organisation;
— Ensure proper data protection related policies and procedures are in place, including risk registers/assessments;
— Educate employees on data protection (e.g. awareness training and regular refresher courses);
— Identify Data Protection Champions across the organisation to guide employees on data protection;
— Ensure there is an internal resource person knowledgeable in information systems;
— Collaborate with compliance and/or internal audit department/officer to perform regular assessments; and
— Consult key resources when in doubt (e.g. legal firms, Mauritius Data Protection Office).

It is important that there is no room for interpretation nor judgment when implementing and/or ensuring compliance with data protection related policies and procedures.

Also, a few challenges that organisations may encounter when implementing clauses of *The Data Protection Act 2017* include:

1. Destruction of electronic data

   – Streamline personal data collection, processing and storage (in hard and/or soft copy) among a few selected staff and departments for better control purposes, especially when determining who has access to personal data and when the need to destroy personal data arises. This will also help to manage risks related to non-adherence to *The Data Protection Act 2017*.

   – Find appropriate methods to erase electronic personal data from relevant information technology (IT) systems within the organisation, especially upon request from the individual, and/or when the period of retention of the individual's personal data by the organisation has lapsed. Also, take into consideration the erasure of personal data on regular data backups performed by the IT department.

   – Set appropriate security and organisational measures for the destruction of personal data, as required under Section 31 of *The Data Protection Act 2017*.

2. Data sharing

   – Many organisations have no clear view with whom they share personal data and, more often than not, lack the appropriate contractual framework. *The Data Protection Act 2017* allows the data sharing with other controllers only if there is a legal basis for data processing.

   – Organisations should create an up-to-date list of their existing service providers as well as other third parties with whom they share personal data and gather all existing agreements. As a first step, the role of the third parties must be assessed and, if need be, the existing contract amended to reflect the mandatory provisions. This can require significant time and efforts, depending on the number of vendors and their willingness to accept the proposed changes to the contract.

– Sections 28, 31 and 36 of *The Data Protection Act 2017* detail the lawful, cross-border processing and sharing of personal data, and associated security implications.

3. Engagement of everyone

– The process of getting compliant with privacy laws such as the EU *GDPR*, the *Modernised Convention 108 (Convention 108+)* and *The Data Protection Act 2017* asks for the design and implementation of new policies, procedures, administrative and legal documentation as well as additional controls and security in the area of information technology [refer to section 1.5 of the Appendix].

– To achieve this objective, several functions across the organisation such as Human Resources, Legal, IT, Marketing, Compliance, Finance and Company Secretarial, amongst others, will need to be solicited and will have to devote time and energy to this project in addition to their normal day-to-day responsibilities and workload.

The above-mentioned list provides only a glimpse of the key challenges that organisations are facing, not to mention creating and updating notices to individuals, consent forms, data protection impact assessments, establishing a personal data breach notification procedure, etc.

Common pitfalls to avoid:

— **Too late:** Starting too late to identify gaps in data protection.

— **High-level overview:** Has an analysis of all data needs and usage been made in the organisation rather than a high-level overview only?

— **Inadequate skills:** Are there sufficient and adequate skills within the organisation to handle data protection, as ensuring compliance requires comprehensive sets of skills ranging from regulatory to information risk management, IT, information security and business process analysis?

— **Dealing with the wrong partner:** Has the organisation considered the right partner for data protection implementations? Has the person or outsourced entity successfully done implementations, not just assessments?

— **One-person exercise:** Is there a dedicated team to handle data protection, as this is not a one-person exercise?

— **Only an IT issue:** Data protection is a business issue, and not solely an IT one.

— **Generic guidance:** Better results are achieved when standards are devised internally rather than relying solely on best practices.

Potential consequences of non-adherence to rules and regulations

Potential consequences of not having the right framework for data protection and/or non-adherence to data protection rules and regulations are:

— Breach of trust between an organisation and its stakeholders;
— Financial loss and/or reputation damage; and
— Penalties and upon conviction, imprisonment [refer to Section 43 of *The Data Protection Act 2017*].

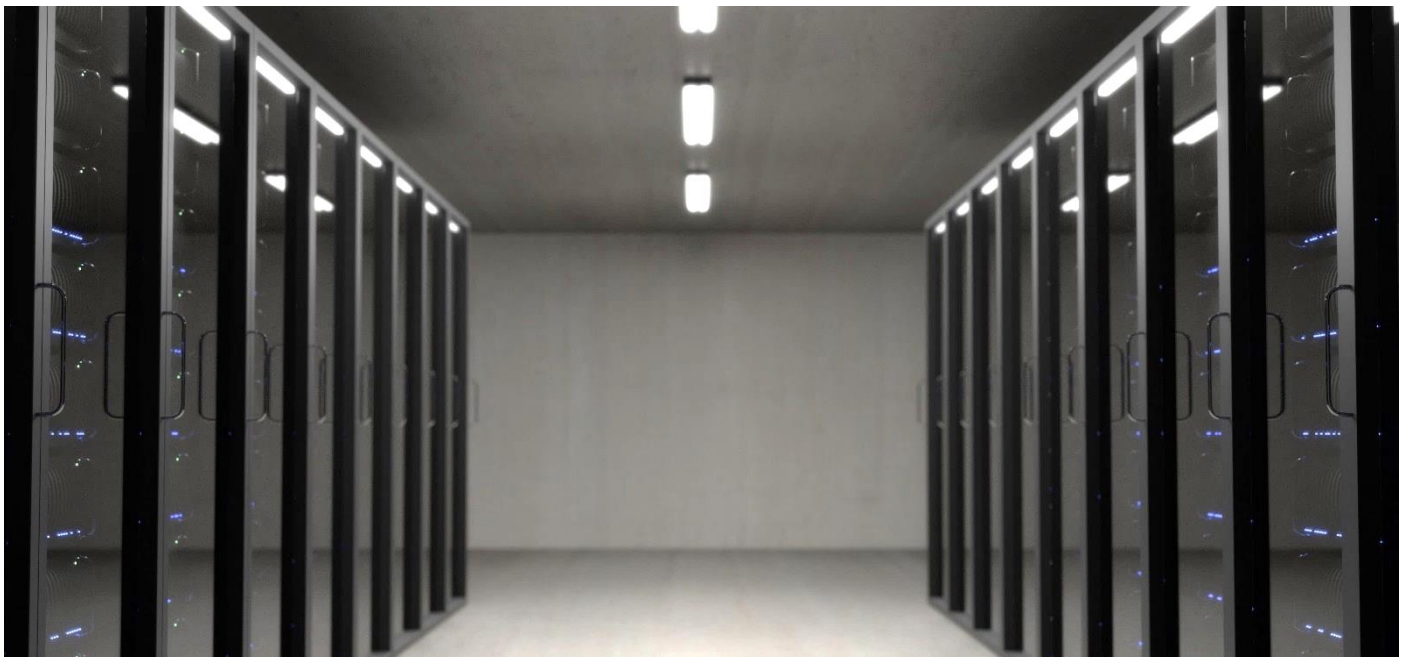
The consequences of non-adherence to *GDPR* are onerous and it is recommended that each organisation in Mauritius performs an assessment of its own exposure to *GDPR*. *GDPR* will require some non-EU businesses that operate in the EU to re-think parts of the activities they carry out in the EU. This makes it much harder to operate certain 'global' services, and will require them to truly put an EU lens on business activities which are undertaken in the EU.

To decide whether a Mauritian controller/processor is bound by the *GDPR*, it is important for each controller to understand the application of Article 3 of the *GDPR*.

The document "Guidelines 3/2018 on the territorial scope of the *GDPR*" published by the European Data Protection Board gives a detailed explanation of how *GDPR* may apply to a controller outside the EU.

Organisations that sell products to EU citizens directly or have activities in the EU must be fully aware of the implications of the *GDPR* and how it applies to Mauritian controllers/processors.

Fines for breach of data protection rules under *GDPR* are included in section 1.4 of the Appendix.



Specific areas

Cloud storage

Data privacy considerations for cloud services:

A. Assess the different jurisdictional privacy laws in force in the country where the data sits.
   - Depending on the cloud deployment and/or service model selected, data is usually stored or processed in various countries.
   - Consequently, DPOs should assess the need to comply with privacy laws in local and other jurisdictions and to whether they offer the same level of safeguards as the EU *GDPR* and *The Data Protection Act 2017*.

B. Review compliance of the cloud service provider to privacy frameworks and standards.
   - As prescribed by privacy laws and regulations, organisations should implement both technical (e.g. encryption) and administrative controls (e.g. Service Level Agreements) to protect their data.
   - DPOs should ensure that the Cloud Service Providers comply with privacy frameworks (e.g. NIST Privacy Framework to improve enterprise privacy) and standards (e.g. ISO 27001, ISO 27002 and ISO 27701).

C. Assess how secure the data is.
   - Encrypted data is unreadable and has neither a market value nor is of interest to third parties.
   - Encryption can be deployed at several layers (i.e. Network, Application, Database, and so on) but emphasis should be laid on the encryption mechanism to be deployed and the encryption key management.

For Cloud Storage, Section 36 of *The Data Protection Act 2017* will apply if the server is found outside of Mauritius. In the event the controller cannot provide proof of appropriate safeguards for the protection of personal data or cannot rely on any of the exceptions provided in Section 36(1) of *The Data Protection Act 2017*, then, according to Section 35 of *The Data Protection Act 2017*, the controller must consult and seek authorisation from the Mauritius Data Protection Office prior to processing personal data and to mitigate the risks involved for data subjects (individuals) where the controller intends to transfer personal information to another country.

Sensitive data

Special categories of personal data (sensitive data) are defined in section 1.1 of the Appendix.

For processing sensitive data, a controller will need to satisfy conditions laid down in Sections 28 and 29 of *The Data Protection Act 2017*.

Sensitive data shall not be processed unless:

a) Section 28 applies to the processing; and

b) The processing is carried out in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, former members, or persons with whom it has regular contact in connection with its purposes;

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 Section 29;
   iii. the purpose of carrying out the obligations and exercising specific rights of the controller or the data subject;
   iv. protecting the vital interests of the data subjects or another person where the data subject is physically or legally incapable of giving consent.

Implementation controls needed when dealing with personal data and/or sensitive data:

1. Maintain an inventory of sensitive information stored, processed, or transmitted by the organisation's technology systems including those located onsite or at a remote service provider. Creating an initial list of where sensitive information is stored can be simple enough. The difficult task comes with maintaining the list and continually hunting for that data.

2. Remove sensitive data or systems not regularly accessed by the organisation from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business units needing to occasionally use the system, else completely virtualise and power off until needed. However, having sensitive information in a powered-off virtual machine still carries risks since the virtual machine file can be stolen. Therefore, ensure that secure virtualisation monitoring tools are in place to both harden and monitor the virtual infrastructure.

3. Monitor and block unauthorised network traffic. Deploy an automated tool on network perimeters that monitors for unauthorised transfer of sensitive information and blocks such transfers while alerting information security professionals. This is data loss prevention in a nutshell.

4. Only allow access to authorised cloud storage or email providers. There is much less visibility into third party cloud/email providers than there is for internally owned assets. Because of this, it is important to at least have a policy to prohibit access to these providers. The next step is to block access to them entirely at the network perimeter.

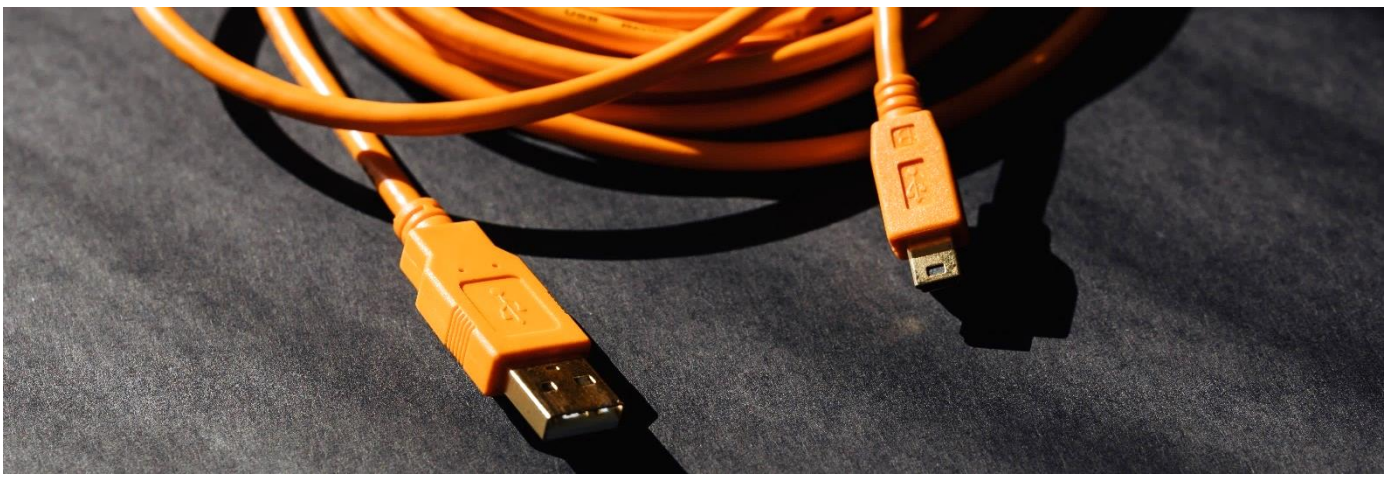
5. Monitor and detect any unauthorised use of encryption. For the same reason that encryption is used for legitimate services, hackers will use encryption to hide what data is being stolen. This helps them evade detection to reach their ultimate goal. It is important not only to look for anomalous encryption on the network, but also for computer generated domain names.

6. Encrypt the hard drive of all mobile devices. In case mobile devices such as laptops or phones are lost, make sure the encryption is configured properly to prevent attacks against stealing decryption keys from memory when the system is in hibernation or sleep mode.

7. Manage USB devices. If USB storage devices are required, enterprise systems should be configured to allow the use of specific devices. An inventory of such devices should be maintained and regularly updated.

8. Configure systems not to write data to external removable media if there is no business need for using such devices. A USB drive is more at risk of being an attack vector than a medium for data exfiltration. However, in some environments, data exfiltration will be a major concern. In that case, blocking USB access completely is the best choice. If there is a business case for USB access, a per user exception can be made.

9. Encrypt data on USB storage devices and provide training to employees so they are aware of the risks of data on USB drives. It is necessary to provide them with the tools to secure the organisation's critical data.



Conclusion

In line with corporate governance requirements, Boards of Directors are responsible and accountable for protecting data and through their Audit and Risk Committees, Board members must ensure that they maintain the trust and privacy of information on a global scale.

These new privacy laws represent a material amount of risk for an organisation. So, anything that tends to be risk and/or compliance focused tends to run through the Audit Committee.

Boards of Directors need to ensure that their organisations have a data privacy program in place, equipped with the right capabilities to sustain compliance. The most effective way to demonstrate an ongoing compliance posture under any of the new data privacy legislations, is to establish a privacy compliance framework and fully support the officer mandated to ensure the security of personal data.

Since a lot of data and therefore personal data are in digital format nowadays, IT and cyber risks become important areas to focus on. Hence, Directors and especially Audit and Risk Committee members need to be cyber-savvy enough to ask the right questions around data protection.

In the process of implementing the requirements of the EU *GDPR* and *The Data Protection Act 2017*, advice should be sought from both legal and IT security perspectives.

In this context, the Mauritius Data Protection Office and the local branch of ISACA can be consulted for guidance in their respective fields of expertise. In addition, several professional institutions have issued Self-Assessment Questionnaires to perform a gap analysis and measure the level of compliance with the law. An action plan can be derived from the results of this type of exercise and a road map designed for implementation, and avoidance of further exposure.

> “Security is, I would say, our top priority because for all the exciting things you will be able to do with computers - organising your lives, staying in touch with people, being creative - if we don't solve these security problems, then people will hold back.”
>
> **Bill Gates**

Appendix

Appendix

Definitions and Legislations

Section 1.1: Some key definitions:

- **Personal data:** any information relating to a data subject.
- **Data subject:** 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.
- **Processing:** 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:** 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:** a person who, or a public body which, processes personal data on behalf of a controller.
- **Consent:** means 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/she signifies his/her agreement to personal data relating to him/her being processed.
- **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 to 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.

Section 1.2: Requirements as per *The Data Protection Act 2017*

Abiding by *The Data Protection Act 2017* and applying these principles can be beneficial to attract foreign investors. It improves the 'ease of doing business' requirements and builds trust between the world and Mauritius. Moreover, a stronger and more coherent data protection framework, backed by effective enforcement will allow the digital economy to flourish by putting individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities. Hence, the risks of data breaches will be minimised.

Controllers: Section 14 of *The Data Protection Act 2017* clearly makes it a legal requirement for controllers to register with the Mauritius Data Protection Office. Non compliance with the registration requirement of *The Data Protection Act 2017* leads to a person liable to fines not exceeding MUR200,000 and to imprisonment for a term not exceeding 5 years.

Processors: Section 14 of *The Data Protection Act 2017* clearly makes it a legal requirement for processors to register with the Mauritius Data Protection Office.

Data protection officer: According to Section 22(2)(e) of *The Data Protection Act 2017*, controllers and processors shall designate an officer responsible for data protection compliance issues.

Section 1.3: Criteria for lawful processing of data

There are 9 criteria for processing personal data lawfully under *The Data Protection Act 2017*.

There must be at least one valid lawful basis in order to process personal data. Which criteria is most appropriate to use will depend on the purpose of processing personal data.

1) **Consent:** clear consent must be given by the data subject for processing his/her personal data for a specific purpose(s).
2) **Contract:** for the performance of a contract with the data subject, or the latter has requested the controller to take specific steps before entering into a contract (most common example being requesting for a quote, which implies gathering certain data).
3) **Legal obligation**: the processing is necessary for complying with the law (not including contractual obligations as stated above).
4) **Vital interests:** the processing is necessary to protect someone's life (e.g. access to medical information).
5) **Public task:** in such case, for the controller to perform a task in the public interest or its official functions, and the task or function has a clear basis in law. The Bank of Mauritius has to process personal data in processing applications from banks for fit and proper persons.
6) **Legitimate interests:** the processing is necessary for legitimate interests of the controller or the legitimate interests of a third party to whom the data is disclosed as per Section 28(1)(b)(vii) of *The Data Protection Act 2017*. There are three elements to the legitimate interests basis:
   a. Purpose test: are you pursuing a legitimate interest?
   b. Necessity test: is the processing necessary for that purpose?
   c. Balancing test: do the individual's interests override the legitimate interest?
7) **Performance of any task by a public authority:** the most common examples in Mauritius being public utilities such as electricity and water, the consumption of which will be dependent upon providing certain personal data.
8) **For the exercise, by any person in the public interest, of any other functions of a public nature:** For the administration of justice.
9) **For the purpose of historical, statistical or scientific research:** the most relevant example would be Statistics Mauritius.

Section 1.4: Administrative fines under *GDPR* rules

There are two tiers of administrative fines:

— Up to EUR10 million, or 2 percent of the worldwide annual revenue of the prior financial year, whichever is higher, shall be issued for infringements of: (Controllers and processors under Articles 8, 11, 25-39, 42, 43, Certification body under Articles 42, 43, Monitoring body under Article 41(4)); and

— Up to EUR20 million, or 4 percent of the worldwide annual revenue of the prior financial year, whichever is higher, shall be issued for infringements of:

- The basic principles for processing, including conditions for consent, under Articles 5, 6, 7, and 9;
- The data subjects' rights under Articles 12-22;
- The transfer of personal data to a recipient in a third country or an international organisation under Articles 44-49;
- Any obligations pursuant to Member State law adopted under Chapter IX; and
- Any non-compliance with an order by a supervisory authority (83.6).

Section 1.5: *Modernised Convention 108 (Convention 108+)*

Details on the ratification of the *Modernised Convention 108 (Convention 108+)* can be accessed on https://dataprotection.govmu.org.

KPMG
KPMG Centre
31 Cybercity, Ebène, Mauritius
T: (230) 406 9999 **F:** (230) 406 9998
E: kpmg@kpmg.mu **W:** KPMG.com/mu
Business registration number: F07000189

Mauritius Institute of Directors
1st Floor, Standard Chartered Tower
19 Cybercity, Ebène, Mauritius
T: (230) 468 1015 **F:** (230) 468 1017
E: info@miod.mu **W:** miod.mu
Business registration number: C08077130