KPMG

MIoD Mauritius Institute of Directors
Promoting Corporate Governance across the board

Audit Committee Forum

Position Paper 12

Ethical considerations around data management



October 2025

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 in Mauritius have set up the Audit Committee Forum (the Forum) in order to help Audit Committees in Mauritius, from 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 capacity 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 12 deals with Ethical considerations around data management.

Previous Position Papers

- 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 a whistleblowing system (September 2018)
- Paper 7: Audit Committee's Guidelines for the Evaluation of Retirement Obligations (August 2019)
- Paper 8: Guidelines for the Audit Committee on Data Protection (October 2020)
- Paper 9: Guidelines for the Audit Committee on Business Continuity (October 2021)
- Paper 10: Management of Cyber security risks in the new normal (October 2022)
- Special Edition on 10th Anniversary of ACF: 100 Best practices for Audit Committees (October 2023)
- Paper 11: Effective Audit Committee conversations (October 2024)

Previous Position Papers may be consulted/downloaded from: KPMG Southern Africa and http://www.miod.mu/publications

KPMG

© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Contents

1.	**Introduction**	**5**
2.	**Data protection**	**6**
	Personal data	6
	Organisational data	6
	Legal and ethical considerations	7
3.	**Data management challenges and trends**	**8**
	Data – a critical asset	8
	Data management trends and challenges	8
	Key risks and ethical considerations	9
	Responding to key challenges	9
	Strategies for navigating ethical challenges	11
4.	**Ethics around data management**	**12**
	Data-driven decision making	13
	Artificial Intelligence (AI)	14
	Implementing data ethics	14
	Implications for non-adherence to laws and regulations	15
5.	**Guidance for Audit Committees**	**16**
6.	**Conclusion**	**17**

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.

Ujoodha Sheila – Chairperson	Langlois Stephane
Ah-Hen Clairette	Leung Shing Georges
Chung John	Molaye Sanjay
Gooroochurn Bharatee	Mooroogen Sumita
Kee Mew Mervyn	Ong Su Lin
King Antoine	Puddoo Shashi
Kistnamah Nagesh	Ramdhonee Kalindee
Koenig Fabrice	Sibartie Oumila
Secretary: Bishundat Varsha	MIoD Coordinator: Mulung Nafeeza

We sincerely thank Mrs Drudeisha Madhub, the Data Protection Commissioner for her contributions to this paper.

KPMG

© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.



© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.



Introduction

In today's digital era, data represents both an asset and a liability, necessitating an evolution of the role of the Audit Committee. The sheer volume, variety, and velocity of data now generated far surpass the capacity of traditional governance frameworks. At the same time, the increased reliance on data-driven systems, such as artificial intelligence (AI) and predictive analytics, coupled with escalating cyber threats, present both significant opportunities and complex ethical dilemmas.

Ethical considerations in data management are far from abstracts; they intersect with regulatory requirements, societal expectations, and organisational integrity. Risks such as unauthorised surveillance, algorithmic bias, data breaches, and opaque governance underscore the consequences of mismanaged data. Conversely, robust ethical frameworks can promote transparency, inclusivity, and respect for individual rights, ensuring that data-driven innovation reflects societal values.

As key governance bodies, Audit Committees are tasked with overseeing internal controls and ensuring regulatory compliance. Yet, in a rapidly evolving digital economy, there is a growing expectation that they uphold the ethical stewardship of data. This entails overseeing the entire data lifecycle: collection, storage, access, usage, and sharing—both within and beyond the organisation. Ethical data management is not merely a technical or legal obligation; it is a core governance imperative.

This position paper aims to provide a comprehensive examination of the ethical considerations surrounding data management, with a particular emphasis on the implications for Audit Committees. It explores not only the compliance dimensions but also the evolving challenges in cybersecurity, the ethical tensions between privacy and security, and practical guidance to foster a culture of ethical data use.

KPMG

© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Data protection

The Audit Committee Forum (ACF) Position Paper 8, Guidelines for the Audit Committee on Data Protection, provides key information on the six principles for collecting, processing, and managing personal data on data subjects. In this position paper, the focus is more on ethics in data management, which complements the requirements of the Mauritius Data Protection Act 2017 (DPA 2017).



Personal data

Personal data encompasses any information that can identify an individual, directly or indirectly—such as names, addresses, biometric data, IP addresses, financial records, and behavioural data. Ethical management of personal data is grounded in principles of consent, transparency, fairness, and purpose limitation. Collecting more data than necessary, failing to inform individuals about how their data will be used, or using data beyond its original purpose are breaches not only of law but also of public trust.

One of the most significant ethical issues is the concept of informed consent. In practice, many privacy policies are complex, lengthy, and challenging to interpret. This undermines the principle of autonomy and transparency. Ethical data management requires simplifying these interactions to empower individuals with genuine control over their data.

Organisational data

Organisational data refers to internal documents, strategic plans, intellectual property, and other proprietary information. Unlike personal data, organisational data is typically protected for reasons of confidentiality, competitive advantage, and operational security. However, ethical management remains crucial—especially when data crosses departmental or geographic boundaries, or when third-party vendors are involved.

KPMG

© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Legal and ethical considerations

Audit Committees in Mauritius must consider local legal frameworks, institutional practices, and cultural sensitivities when overseeing ethical data management. The DPA 2017, modelled on the EU General Data Protection Regulation (GDPR), sets out the primary obligations regarding personal data protection.

Data Protection Act 2017 (Mauritius)

The DPA 2017 mandates that personal data be processed lawfully, fairly, and transparently. Organisations must have a clear legal basis for data processing, such as consent or legal obligation. Audit Committees should ensure their organisations respect key data subject rights, including the right to access, correction, erasure, and objection.

Cross-border data transfers must only be made to jurisdictions with adequate data protection standards. Technical and organisational safeguards must be implemented to protect personal data against unauthorised access or alteration.

Role of the Data Protection Commissioner (DPC)

The DPC is responsible for enforcing the DPA 2017. Audit Committees must verify that the organisation:

- Has registered with the Data Protection Office, if applicable.
- Employs a qualified and independent Data Protection Officer (DPO).
- Maintains an internal breach notification system aligned with the DPC's 72-hour reporting requirement.

Sector-specific considerations

Organisations regulated by the Financial Services Commission (FSC) or Bank of Mauritius (BoM) face additional scrutiny. FSC emphasises customer data protection, ethical AI, and secure outsourcing. The BoM requires encryption, cybersecurity audits, and the ethical use of credit data.

Cybersecurity and Cybercrime Act 2021 (CCA)

The CCA criminalises data breaches and unauthorised access. It also addresses offences such as Phishing, Identity Theft, and Illegal Interception of Data. Ransomware attacks, if settled through payment, may violate the provisions of this Act. The Board must ensure alignment of incident response policies with national law and timely notification to the Computer Emergency Response Team of Mauritius (CERT-MU) when required.

Cultural and Public Sector ethics

Data ethics in Mauritius must reflect the country's multicultural values, traditions of inclusiveness, and public expectations of privacy. In such a diverse society, sensitivity in the collection, processing, and use of personal data is essential to avoid discrimination or unequal treatment. Public trust is strengthened when organisations demonstrate respect for cultural values alongside compliance with legal requirements.

Surveillance, biometric tracking, and public data systems (e.g., Smart Cities initiatives, National Identification Systems, e-Government) must undergo both ethical and legal review before implementation.

Mauritius DPA 2017, which aligns closely with the EU's GDPR, provides the legal framework to ensure transparency and fairness in processing personal data. Audit Committees should encourage the systematic use of Data Protection Impact Assessments (DPIAs), particularly for high-value projects involving personal data, as well as continuous stakeholder engagement to balance innovation with individual risks.

By integrating these jurisdiction-specific practices, Audit Committees in Mauritius can ensure legal compliance, reinforce ethical standards, and foster public trust in the responsible stewardship of data. This proactive approach not only mitigates regulatory and reputational risks but also positions organisations as leaders in ethical digital transformation within a multicultural society.

KPMG

© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Data management challenges and trends

Data – a critical asset

Data is a critical asset in today's world, driving informed decision making, enhancing operational efficiency, and enabling innovation across various sectors. Below is a closer look at how data delivers on such key areas:

Informed decision making

Data provides the foundation for making informed decisions and allows leaders to analyse trends, understand customer behaviour, and evaluate the effectiveness of strategies. High-quality data leads to better insights, which can significantly impact an organisation's success.

Problem solving and efficiency

Organisations can use data to identify inefficiencies and areas for improvement. By monitoring key performance indicators and analysing operational data, organisations can proactively address challenges before they escalate into larger issues.

Understanding customers

Data helps organisations gain insights into customer preferences and behaviours. This understanding enables businesses to tailor their products and services to meet customer needs, ultimately enhancing customer satisfaction and loyalty.

Innovation and competitive advantage

In the digital age, data is essential for driving innovation. Companies that effectively leverage data can develop new products, optimise existing services, and create personalised experiences for their customers. This capability provides a competitive edge in the marketplace.

Quality and reliability

The quality of data is paramount. Poor-quality data can lead to misguided decisions and the wastage of resources. Organisations must prioritise data governance to ensure accuracy, consistency, and completeness, which are crucial for reliable analytics and decision making.

Predictive capabilities

Advanced analytics allow organisations to anticipate future trends and behaviours. For example, data can help forecast market demands, identify potential risks, and optimise resource allocation.

However, while there are tremendous benefits to be derived from the appropriate data management, there are risks which also need to be addressed and managed.

Data management trends and challenges

Without any doubt, data has become the lifeblood of any organisation. If organisations are serious about increasing competitive edge and improving decision making, they must ensure that their data are accurate, of high quality, and up to date. With organisations accumulating vast amounts of data from various sources, data management has become increasingly complex.

Common obstacles faced by organisations include:

- **High data volume**: Makes storage and analysis complex.
- **Poor data quality**: Leads to errors and misinformed decisions.
- **Lack of systems/processes**: Causes inconsistency and inefficiencies.
- **Integration difficulties**: Hard to unify scattered, siloed data.
- **Limited automation**: Manual handling slows down analysis.
- **Data analysis complexity**: Tools require skilled handling.
- **Skill shortage**: Few experts available; training is costly.
- **Security risks**: Sensitive data must be protected from breaches.
- **Weak governance**: Lack of policies leads to compliance and quality issues.

KPMG

© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Key risks and ethical considerations

With these challenges, some of the key risks and ethical considerations which need to be addressed by the Boards are:

Cybersecurity threats



- Data misuse, breaches, and fraud are rising.
- Organisations must manage operational, legal, and reputational risks.

Artificial intelligence



- Automation enhances service but raises concerns over transparency, bias, and explainability.

Data leaks



- Often caused by human error, poor infrastructure, or third-party failures.
- Prevention includes employee training, proper system configuration, and vendor audits.

Sophisticated hackers and ransomware



- Why some pay ransom: To reduce downtime or due to a lack of backups.
- Why not to pay ransom: Encourages more attacks, no guarantee of data return, legal and insurance issues.

Lack of preparedness



- Organisations should invest in cybersecurity, implement incident response plans, and ensure transparent communication.
- Organisations should use backups and collaborate with law enforcement.

Responding to key challenges

The real damage extends beyond the technical fallout; the risks can have far-reaching consequences, directly affecting brand perception, customer trust, reputation, and even financial stability. How to address these challenges need to be set from the top with leadership or directors setting clear policies and processes thereon.

Below are some of the most common challenges faced by organisations today:

Data management – storage / back-up / use of cloud

Cloud storage has become a widely accepted and common medium of data management. Cloud storage enables the remote storage and retrieval of data over the internet, providing flexibility, security, and scalability for both personal and organisational needs.

Cloud risk assessment is necessary to ensure that systems and data migrated to the cloud do not introduce any new or unidentified risks to the organisation.

Boards need to be clear about their responsibilities when selecting a Cloud Service Provider (CSP), a third party that the organisation relies on to support core operations and to process sensitive or personal information, potentially exposing the business to risk. The focus should be on ensuring the confidentiality, integrity, availability, and privacy of information processing, while keeping risks below the accepted internal risk threshold.

The agreement for cloud storage falls under a shared responsibility model, with the CSP managing the security and compliance of the cloud environment, and the client remaining accountable for managing and configuring security and compliance within the cloud in accordance with their needs and risk tolerance.

Regulators, such as the BoM, have issued guidelines on controls that are applicable across organisations, including strategies, assessments and reporting, security testing, and third-party service provider due diligence. The responsibilities for data protection, security, and control and third-party reliance go well beyond the Chief Information Security Officer's (CISO's) role and include responsibilities of both senior management and the Board. Boards and Senior Management must therefore exercise caution to make the right choices about who they work with.

Use of personal communication equipment and social media

In this digital era, the lines between personal and professional lives are increasingly blurred, leading some employees to use their personal email accounts and/or social media apps for business communication. Though this practice might stem from convenience, it overlooks several significant risks.

It is important that Boards understand these risks to protect the organisation's sensitive information against cybercriminals or unintended information leaks. These risks are:

- Security vulnerabilities – lack of encryption, two-factor authentication and other security measures increase risk of email being intercepted or exposed and unauthorised access to confidential business information which may put the entire organisation at risk.
- Compliance and legal issues – Data protection legislation mandates strict controls over how personal and sensitive information is handled. Failing to comply may result in hefty fines, legal penalties, and potential personal liability for employees.

KPMG

© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

- Lack of oversight and control - companies lose visibility and control over business correspondence. This complicates data management and retrieval for audits and legal investigations, posing a significant risk to operational integrity and compliance.
- Professionalism and brand image - business communications sent from personal email accounts can dilute the organisation's brand image. Consistent, branded email addresses reinforce the organisation's identity and help maintain trust and credibility with clients and partners.

While organisations have a responsibility towards society to protect data, they need to balance this requirement with maintaining functionality. Boards are responsible for setting up a holistic approach to information security based on thorough risk management.

Audit Committees should consider:

- the establishment of a clear, enforceable policy that strictly prohibits the use of unapproved personal devices or accounts for corporate communications.
- continuous user education and cybersecurity awareness training to explain the risks to employees, thereby transforming a simple rule into a cultural norm that safeguards sensitive information and maintains professional integrity.

Responding to ransomware attacks

In the event of a ransomware attack, experts advise the following steps:

Immediate response steps	Containment and recovery	Communication and prevention
• Isolate infected systems – Disconnect devices to stop the spread. • Notify IT security – Activate the incident response plan. • Document the attack – Record evidence (e.g., ransom notes).	• Don't pay the ransom – No guarantee of data recovery. • Assess the damage and restore from clean backups. • Ensure systems are secure before reconnecting them.	• Be transparent with stakeholders. • Improve security via updates, employee training, and offline backups.

Most ransomware attacks target sensitive organisations where downtime has severe impacts. To quickly resume normal operations, organisations may be tempted to pay a ransom, but this may have serious long-term consequences.

Faced with the ethical dilemma of whether to pay the ransom or not, Directors must remember that in some jurisdictions, the law explicitly prohibits ransom payments to cybercriminals, and law enforcement agencies may view paying ransom as a sign of complicity or obstruction of justice, leading to future legal action.

Artificial intelligence (AI): navigating the cybersecurity and privacy tightrope

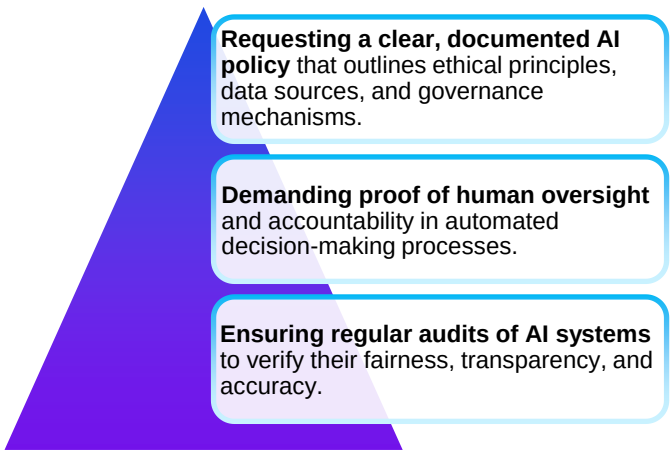
Companies are increasingly turning to AI as a powerful tool to protect digital assets and sensitive data. AI promises to revolutionise cybersecurity by identifying vulnerabilities, automating security operations, and preventing cyberattacks in real-time. However, as AI systems advance, the potential for misuse also increases.

AI relies on vast amounts of personal data, raising concerns about surveillance, data collection, and automated decision making.

AI designed to detect unusual patterns of activity could potentially monitor an individual's online presence without their consent, raising concerns about the erosion of privacy.

This creates a situation where the line between legitimate security measures and invasive surveillance becomes blurred. Therefore, directors, as stewards of their organisation, must ensure that AI is deployed responsibly, avoiding infringing upon civil liberties, bias, and data manipulation.

Boards of directors cannot ignore the ethical implications of AI on cybersecurity. They must advocate for responsible AI and support the creation of an ethical framework for the future.



© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Strategies for navigating ethical challenges

To effectively navigate the ethical challenges, in particular regarding ransom payments, organisations should adopt a comprehensive approach:

Preparation and prevention: Invest in robust cybersecurity measures, including employee training, advanced threat detection, and regular data backups. Preparedness reduces the likelihood and impact of ransomware attacks.

Incident response planning: Develop and regularly update an incident response plan. This plan should include decision-making protocols, legal considerations, and communication strategies.

Stakeholder engagement: Involve key stakeholders, including legal, compliance, and public relations teams, in the decision-making process. Consider the perspectives of customers, employees, and regulators.

Expert consultation: Seek guidance from cybersecurity experts, law enforcement, and legal advisors. They can provide valuable insights and support during an attack.

Evaluate alternatives: Explore alternatives to paying the ransom, such as independent data recovery or negotiating with attackers. Assess the feasibility and risks of these options.

Guidance from and requirements under the Mauritius Data Protection Act 2017 (DPA 2017)

While ensuring compliance with DPA 2017, Audit Committees can also avail themselves to guidance and explanatory notes/templates issued by the Data Protection Commissioner (DPC) to ensure compliance with the DPA and formulate their policies and processes.

1. **Data Protection Officer (DPO) -** appointment of a dedicated DPO with sufficient resources and reporting directly to the Audit Committee. The DPO is crucial for monitoring compliance, advising on DPIAs, and training staff.
2. **Data Protection Impact Assessment (DPIA)** - ensuring that a robust DPIA process is in place, especially for new technologies and projects involving large-scale processing of personal data. This would provide a more concrete action item for organisations to demonstrate their commitment to privacy.
3. **Cross-border data transfers** - scrutiny of cross-border data transfer policies and contracts to ensure they comply with the legal requirements, such as the specific conditions for such transfers, the need for adequate safeguards or explicit consent from the data subject, and necessary authorisation from the DPC where required.
4. **Public awareness and data subject rights** - ensuring that privacy notices are clear and accessible and that mechanisms for data subjects to exercise their rights (e.g., access, rectification, objection) are simple and effective, as well as educating the customers and employees about their data rights.
5. **Enforcement and audit** - stay informed about potential audits and ensure their organisation is prepared to demonstrate compliance, which is more than a reactive measure to a data breach.

KPMG

© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Ethics around data management

Ethics in business refers to a system of moral principles, policies, and values that guide how an organisation operates and interacts with its employees, customers, suppliers, and other stakeholders. As per Principle 1 on Governance Structure of The National Code of Corporate Governance for Mauritius (2016), an organisation should have a Code of Ethics, which states that *"The Code should lay out clear corporate values and standards of behaviour in the organisation's dealings. When adopting a Code of ethics, the organisation should address primarily the issues relating to ethical practices of relevance to the particular circumstances of its business environment, including the practical application of its corporate values and the concepts of honesty and integrity."*

Since the implementation of the GDPR in 2018, focusing on data protection and privacy for individuals within the European Union, and the DPA 2017, ethics in data management especially regarding data privacy has become increasingly important and critical for any organisation dealing with personal data.

Ethics in data management involves the responsible handling of data throughout its lifecycle while taking into consideration the moral principles that guide decisions about data. The data lifecycle refers to the sequence of stages that data undergoes, such as creation/collection, storage, processing, analysis, usage, archiving, retention, and deletion. Thus, organisations collecting personal data must ensure that such data is protected throughout the data lifecycle and that it is used in a way that respects the individuals' rights and promotes equitable outcomes.

It is essential for business professionals and anyone working with data to apply the following ethical guidelines regarding:

Consent and control	Ensure that each individual gives explicit consent to the collection of personal data while retaining control over how the organisation is using such data.
Transparency	Ensure that the organisation is open to individuals about how data is collected, stored, used, and shared internally or externally.
Fairness	Ensure that the data collected is used to create outcomes that are fair, non-discriminatory, and that do not cause inadvertent harm to people.
Accountability	Ensure that whoever handles data throughout its life cycle is responsible for data integrity and any ethical implications related to such data.
Privacy and security	Ensure that there is adequate protection of personal and/or sensitive information from unauthorised access, use, or disclosure.

The intention behind the collection of data also matters. Collecting personal data when it is unnecessary or is misrepresenting the methods or intentions of data collection are considered unfair and unethical, even if they have consented to provide such data.

The challenge for those in charge of governance within organisations on data ethics is more than just a simple "tick the box" exercise of reviewing the above ethical guidelines. It goes much further, requiring an understanding on why and what data is being collected, and ensuring its integrity is preserved throughout its life cycle and without causing inadvertent harm when used for decision making.

KPMG

© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Data ethics go hand in hand with data integrity. It focuses on the ethical handling of data throughout its lifecycle. Data integrity emphasises the accuracy, quality, completeness, consistency, reliability, and validity of an organisation's data as it is maintained over time and across different formats. Data integrity is a critical component of data ethics as high data integrity is essential for building credibility and trust in data-driven processes and for making decisions based on reliable data.

The BoM has provided procedures regarding data integrity in its *"Guideline on Cyber and Technology Risk Management" (29 May 2025)*, which can be applied by any organisation. Section 57 of the Guideline states that a financial institution shall:

i. store backup information at an alternate site, both online and offline, which should be safeguarded by protective and detective controls;

ii. establish a system and data backup strategy with appropriate frequency of backup which is based on the criticality of the information;

iii. ensure that the restoration of its system and data backups can be carried out with minimum downtime and limited disruption, in line with recovery objectives;

iv. test the restoration of its system and data backups to validate the effectiveness of its backup restoration procedures. The frequency shall be commensurate to the criticality of the information and be at least twice a year for critical information and systems; and

v. ensure that any backup data is protected at rest and in transit to ensure its confidentiality, integrity and availability.

Trust in this digital era also relates to the trustworthiness of data management and ethical use. Organisations need to strive for data integrity and ethical data management throughout its life cycle. Data should be kept up to date and free from errors or inconsistencies to ensure that decisions based on the data are reliable and trustworthy. By addressing these ethical considerations, organisations ensure that they are managing data responsibly and ethically while building trust with data subjects and stakeholders and avoiding potential regulatory, financial, and reputational risks, amongst others. It is of utmost importance to ensure that privacy, security, and ethics are always managed.

Data-driven decision making

Nowadays, with the widespread use of social media and mobile devices, the increasing use of cloud computing, Internet of Things (IoT) devices, and AI, consumer data is being easily collected, rapidly analysed, and shared. Organisations have seized such opportunities to increase data collection and integrate such data into their regular operations. This has led to a growing demand for "Big Data" analytics as well as increasing risks related to data ethics.

"Big Data" analytics, using algorithms, is assisting an organisation in the discovery of seemingly hidden patterns while providing insights that can even predict the behaviour of existing clients and potential new clients with the introduction of new products and services to the market. Organisations are relying on results obtained from data analytics to drive decision making. The process, known as data-driven decision making, uses data to inform the organisation's decision-making process and validate a course of action before committing to it.

Algorithms play a central role in data analytics by enabling systems to extract insights, identify patterns, and generate predictions from datasets. At their core, algorithms are sets of defined instructions used to perform tasks or solve problems—typically executed by computers through programming languages. However, since algorithms are designed and written by humans, they may inherently reflect human bias. Moreover, it is also essential to determine the source of data being used, as data integrity is critical when using data-driven decision making. Errors in datasets can create ripple effects, producing biased results that lead to poor decision making and ultimately impact the organisation. This may also raise concerns regarding the fairness of outcomes from biased algorithms and/or data, as part of the ethical guidelines that the organisation should respect.

Therefore, internal controls must ensure that algorithm developers follow proper standards, taking into consideration data ethics. Additionally, the source data should be accurate and complete, and the basis used for analysing consumer data and behaviour should be validated by Management to prevent misuse of data, bias, and discrimination in data categorisation and analysis. Data security contributes to the data's integrity by ensuring it has not been compromised by threats such as cybersecurity or personal data breaches. Ethical data handling promotes trust and credibility in data-driven processes by avoiding misrepresentation, manipulation, and misuse.

KPMG

© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.



Artificial Intelligence (AI)

As we are rapidly stepping into the AI era, with accessibility to generative AI platforms such as ChatGPT, along with the widespread of other AI-related applications, ethics around data management including data generated from AI applications requires the attention of those in charge of governance in organisations. When investing in AI and machine learning, both the source of data and the integrity of that data are critical. Without proper oversight, there is a risk that data may be sourced without the consent of data subjects and/or that biased or incomplete datasets may be used for machine learning or using AI to analyse such data.

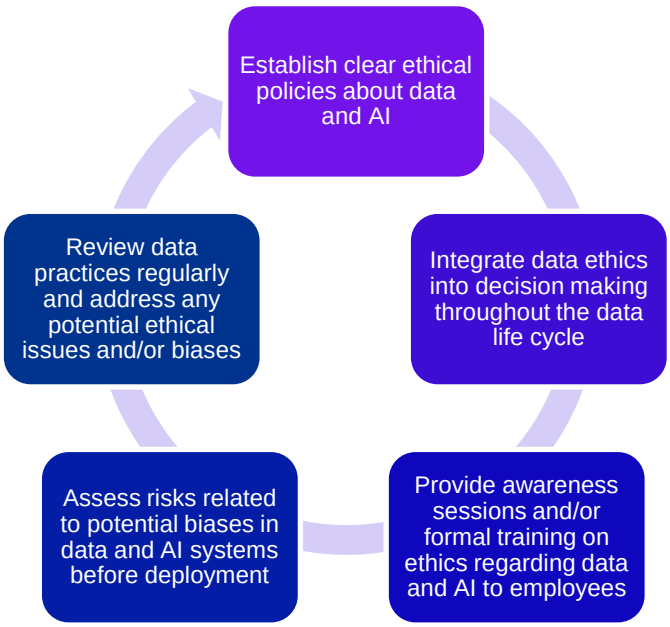
Any person responsible for training or handling machine-learning algorithms needs to be aware of the ethical considerations mentioned above and understand how they could potentially violate any of them to make the most appropriate decisions, after consultation with management and the Board, where necessary. AI is also used today for creating algorithms using prompts, and therefore, it is essential to consider that even AI may be subject to hallucinations. Moreover, an unrepresentative dataset used for training machine-learning algorithms may lead to bias and unfair outcomes. Biased algorithms can intentionally or unintentionally cause harm to people. Therefore, ensuring adequate controls (e.g., human oversight) for reviewing and approving the algorithms before their use is a key requirement.

While AI can surely assist organisations in increasing productivity, depending on its application, it may also bring additional risks, such as hallucinations and misuse, that need to be considered and mitigated. When using AI, the onus is therefore on the person or organisation using the technology and its results. It is important to ascertain the reliability of information obtained from AI, as there may be elements of bias. Therefore, an AI Policy is essential to guide the use of AI and its ethical considerations to ensure that the technology is being used in the best interest of the organisation, all while adhering to a proper set of rules and regulations.

Implementing data ethics

The Board must set the tone regarding ethical guidelines on data and AI, which must be clearly stated in the organisation's Code of Ethics. Everyone in an organisation, regardless of their position, roles, and functions, needs to be aware of data ethics as an integral part of the organisation's culture. Data analysts, data scientists, IT professionals, and anyone closely involved with data (personal or organisational) are required to be more attuned to data ethics.

When implementing data ethics, the following needs to be taken into consideration:



Relevant key process owners can work in collaboration with IT professionals and/or subject matter experts regarding the implementation of data ethics and related internal controls throughout the data life cycle and AI systems. The objective is to ensure that the organisation has adequate documentation on data ethics and that processes are aligned with ethical practices without breaching any rules and regulations and causing inadvertent harm to individuals.

KPMG

© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Implications for non-adherence to laws and regulations

Although the implications of non-adherence to laws and regulations around data management and adopting non-ethical behaviours are known, there are still instances where organisations have been fined for failing to comply with data protection laws and/or for making false and misleading statements about their use of AI:

a) In July 2025, the Polish Data Protection Authority (UODO) issued a GDPR fine of over EUR 3.8 million to McDonald's Poland, along with additional penalties for its processor, 24/7 Communication Sp.

b) In May 2025, the Personal Information Protection Commission (PIPC) of South Korea fined the e-commerce platform Temu KRW 1.369 billion (USD 1,004,896) for transferring personal data abroad without notifying users and failing to appoint a domestic agent as required by law.

c) In December 2024, Italy's data protection agency fined ChatGPT maker OpenAI EUR 15M (USD 15.58M) for processing users' personal data to train ChatGPT without having an adequate legal basis and violating the principle of transparency and the related information obligations towards users.

d) In March 2024, the US Securities and Exchange Commission (SEC) charged two investment advisers, Delphia (USA) Inc. and Global Predictions Inc., with making false and misleading statements about their use of AI. The firms agreed to settle the SEC's charges and pay $400,000 in total civil penalties.

For instance, in the example (d) above, Audit Committee members need to ensure that the organisation is not involved in AI washing, which is a deceptive marketing tactic that consists of promoting a product or a service by overstating the role of AI integration within it.

The risks for organisations with non-ethical behaviours are mostly related to legal, financial and reputational. It is however important to emphasise that the element of trust has become increasingly central in this digital and AI era. Annette Nazareth, former SEC commissioner, aptly stated that *"Compliance is not just about avoiding penalties. It's about building trust."*

Audit Committee members should be mindful that the loss of stakeholder trust can have lasting impacts. As the saying goes, trust takes years to build, seconds to break, and a lifetime to repair.

KPMG

© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

Guidance for Audit Committees

The organisation's Code of Ethics is part of the governance reporting of the Board. However, Audit Committee members need to ask whether ethics in data management and artificial intelligence are already part of the organisation's culture. This is where clear guidance on the management of data throughout its life cycle needs to be formulated from the top and cascaded down to all employees of the organisation. The focus should be on the ethical aspects regarding data privacy and data generated from AI, which are used for decision making. This may require organising awareness sessions for employees on ethical guidelines and practices, with the continuous support from the Board and Management to sustain such change.

A few questions to be considered by Audit Committees members include:

Strategy and governance

- Does the organisation's ethics policy cover data management, data-driven decision making and the use of AI, where applicable?
- Does the organisation have policies and procedures, including internal controls, related to data governance, data management, data-driven decision making, and the use of AI?
- How does the organisation ensure that data ethics have been integrated into decision making throughout the data life cycle?
- Are employees aware of the organisation's code of ethics, including ethics around data management?
- When was the last time the organisation performed an audit of company culture, including ethics?

Privacy and consent

- Do we obtain meaningful, informed consent from individuals before collecting their data?
- Are there effective processes to handle data subject rights (access, correction, deletion)?
- Is personal data anonymised or minimised where possible?
- How does the organisation ensure that privacy, security, and ethics in data are managed at all times?

Transparency and accountability

- Can we clearly explain how data is collected, used, and shared?
- Are there reporting mechanisms for unethical or improper data use?
- Do we disclose our data governance policies to stakeholders?
- How ready is the organisation to address potential personal data breaches internally and vis-à-vis the Data Protection Office and relevant external stakeholders?
- Do contractual agreements with third parties include ethical considerations related to data management and the use of Artificial intelligence, where applicable?

Security and risk management

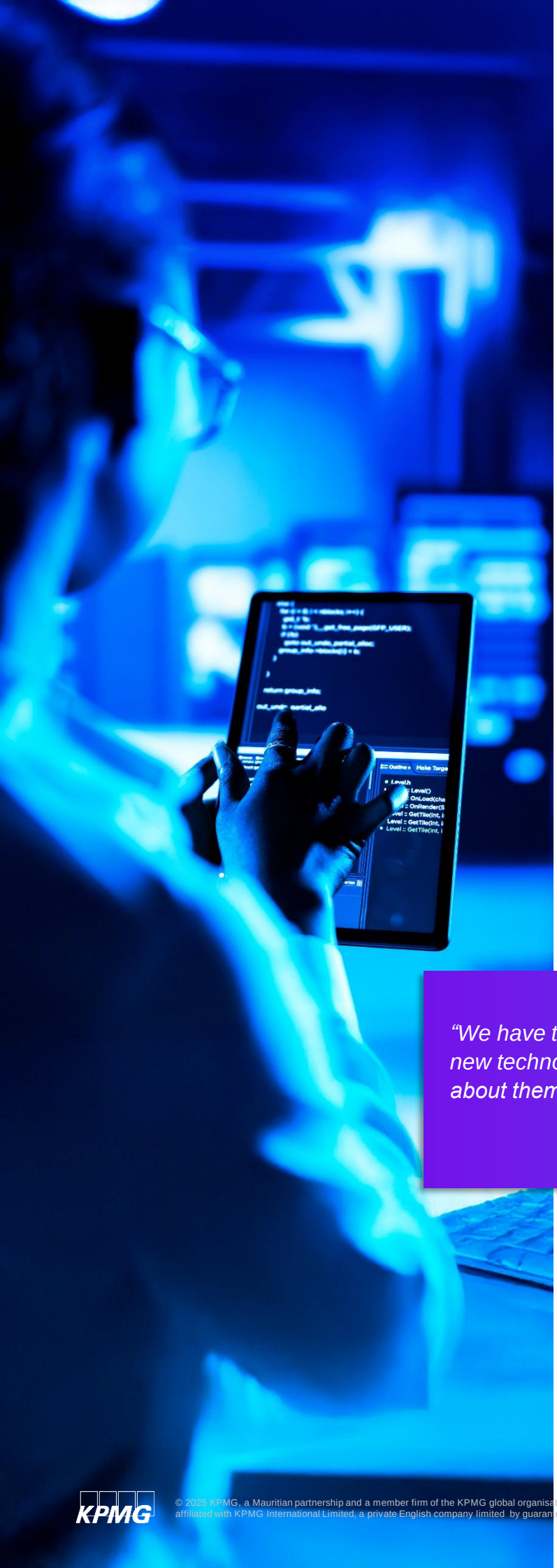
- Are robust data security measures (encryption, access controls, monitoring) in place?
- Do we regularly test, audit, and update our data protection systems?
- Is there a crisis response plan in case of a breach or misuse incident?
- Does the organisation have internal resources (including internal auditors) with relevant skills and competencies on ethics related to data and AI to perform risk assessment and controls evaluation?
- What business activities use data-driven decision making and AI, and is there human oversight to ensure alignment with business objectives and its ethical use?
- How does the organisation ensure that it has the required IT systems to detect, protect against, and respond to cyber-attacks, thus safeguarding its data throughout its life cycle?
- How ready is the organisation to deal with the risk of a ransomware attack, and how would it respond if ever such a risk materialised?

Emerging technologies and trends

- How does the organisation assess ethical risks from new technologies (AI, cloud, real-time analytics)?
- Does the organisation monitor evolving global regulations and best practices?
- Is there a roadmap for ethical adoption of advanced data tools?
- Has the organisation considered new job profiles (e.g., Data Scientists, Machine Learning Engineer, AI Ethics Specialist) for recruitment to ensure that they remain competitive and stay relevant in this new digital era?

KPMG

© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.



Conclusion

As data continues to shape the foundation of modern innovation, the ethical challenges surrounding its management cannot be treated as secondary concerns—they are central to building trustworthy and sustainable digital ecosystems. Ethical data management is more than regulatory frameworks; it demands a proactive commitment to values such as privacy, fairness, transparency, and accountability. Organisations that recognise these obligations are better equipped to foster trust among stakeholders, mitigate risks, and contribute positively and continuously to society.

Ultimately, the ethical considerations in data management underscore a crucial reality: data is not merely a technical resource but a reflection of human lives and social structures. Decisions about how it is collected, processed, and shared must be guided by principles that safeguard individual rights and ensure equitable outcomes. Looking ahead, embedding ethical reasoning into data governance will be essential not only for regulatory alignment but also for promoting innovation that is inclusive, responsible, and resilient.

In this way, ethical data management should be seen as a strategic enabler of trust, long-term sustainable value, and societal benefit in a data-driven world.

"We have to take the unintended consequences of any new technology along with all the benefits, and think about them simultaneously." — Satya Nadella

References

- https://digitalpolicyalert.org/event/29996-personal-information-protection-commission-fined-temu-for-alleged-violations-of-data-protection-law
- https://www.reuters.com/technology/italy-fines-openai-15-million-euros-over-privacy-rules-breach-2024-12-20/
- https://www.sec.gov/newsroom/press-releases/2024-36
- https://en.wikipedia.org/wiki/AI_washing#References
- https://vinciworks.com/blog/lessons-from-a-gdpr-fine-mcdonalds-poland-and-the-high-cost-of-processor-oversight-failures/

KPMG

© 2025 KPMG, a Mauritian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Printed in Mauritius.

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
6th Floor, Building A5, Hyvec Business Park
15 Wall Street, Ebene 72201, Mauritius
T: (230) 468 1015 **F:** (230) 468 1017
E: info@miod.mu **W:** miod.mu
Business registration number: C08077130

kpmg.com/socialmedia

Disclaimer:

The information contained in Position Papers disseminated by the Audit Committee Forum is of a general nature, and is not intended to address the circumstances of any particular individual or entity. The views and opinions of the Forum do not necessarily represent the views and opinions of KPMG, the Mauritius Institute of Directors and/or individual members. These guidelines are for discussion purposes only and in considering the issues, the culture of each entity should be taken into account as must the charter for each entity's Audit Committee. Although every endeavour is made to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No reliance should be placed on these guidelines, nor should any action be taken without first obtaining appropriate professional advice. The Audit Committee Forum shall not be liable for any loss or damage, whether direct, indirect, consequential or otherwise which may be suffered, arising from any cause in connection with anything done or not done pursuant to the information presented herein.

This publication does not provide guidance on how to deal with individual situations, nor does it provide a complete description of relevant legislation. Reference may need to be made to the legislation and other pronouncements mentioned in the text and to the organisation's professional advisers for detailed information.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved. Use of this system is governed by KPMG's Intranet Usage Policy

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit https://home.kpmg/xx/en/home/misc/governance.html