Newsletter

DATA PRIVACY

2024

BDO IT CONSULTING

IT GOVERNANCE & CONSULTING

Contents

Navigating the intersection of AI and Data Protection

In the ever-evolving landscape of technology, artificial intelligence (AI) stands out as a transformative force, promising efficiency gains, innovation, and improved decision-making across industries. As we embrace the advantages of AI, it becomes imperative to carefully navigate its intersection with data protection, ensuring that the benefits don't compromise individual privacy. This article explores the relationship between AI and data protection, shedding light on both the benefits and challenges that arise.

Benefits of using AI

The use of AI offers numerous advantages, ranging from automating repetitive tasks to providing essential insights that inform critical decisions. AI technology has demonstrated its value across different sectors, including healthcare, finance, and manufacturing, with significant progress being made as detailed below. This progress shows that AI has the potential to create a positive impact on society.

Healthcare	Transportation	E-Commerce
Real Estate	Travel	Banking

Challenges and Considerations

As we embrace the integration of AI technology, we must recognise the challenges that come with it, particularly in the realm of data protection. Significant concerns include biased algorithms, unauthorised access to sensitive information, and the potential erosion of personal privacy. Striking a balance between innovation and safeguarding individual data is crucial to ensure responsible deployment of AI technologies. In addition, the following three fundamental privacy principles of data accuracy, protection, and control are challenged:

1 **Lawfulness, fairness, and transparency**

AI algorithms lack transparency, making it difficult or impossible for businesses to understand how they make decisions.

2 **Purpose limitation**

The collection of personal data may evolve with the development of self-learning AI, as such the purpose initially defined may change over time.

3 **Data minimisation**

Organisations should only collect the minimum amount of data required for their day-to-day operations to comply with the MDPA. However, AI algorithms typically require as much data as possible for learning. Businesses should always make sure that preventive measures are taken against the risk of data leakage when handling such enormous volumes of data.

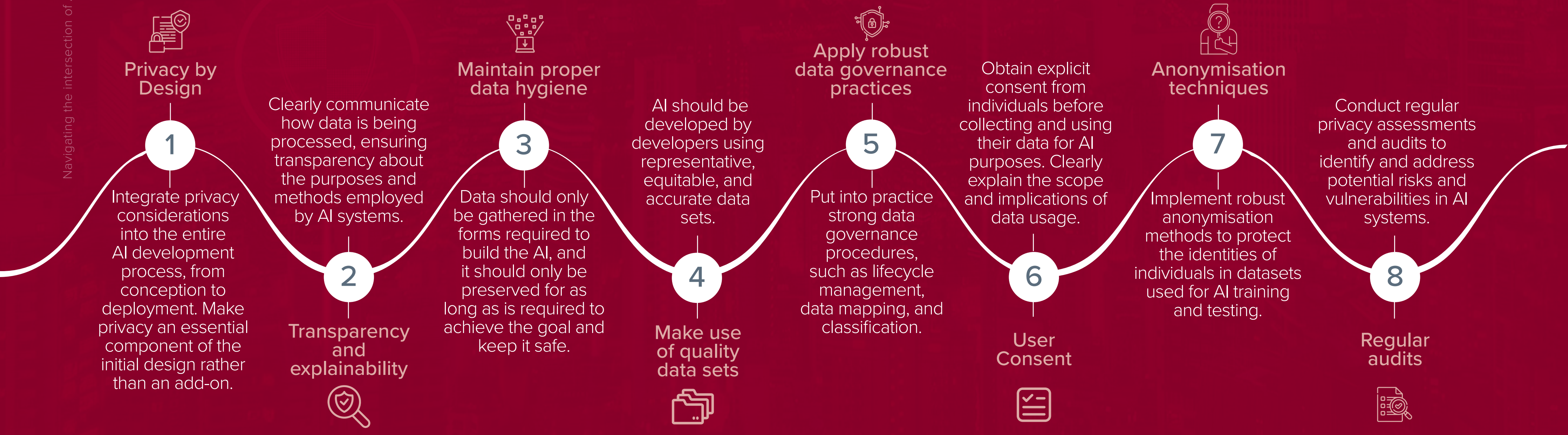
Regulatory Landscape

In response to the challenges posed by AI, countries around the world are diligently drafting regulatory frameworks to ensure the safety, security, and trustworthiness of AI systems. Key players, including leading technology firms, governments, and policymakers, are advocating for a standardised global framework to guide the responsible development of advanced AI systems. The European Union (EU) stands at the forefront, finalising regulations set to be enforced by 2025, adopting a centralised, broad, and prescriptive risk-based approach. In contrast, the U.K embraces a decentralised model, relying on existing regulators for sector-specific regulations to avoid confusion. The U.S. takes a similar approach, with various federal agencies developing sector-specific principles. A December 2023 presidential directive detailing artificial intelligence (AI) safeguards was signed by US President Joe Biden.

As the EU emerges as a global standard-bearer for AI regulation, firms' readiness to comply, backed by a well-defined AI workbench, becomes pivotal. The industry awaits collaborative efforts among policymakers, technology firms, and stakeholders to establish standardised global AI regulations, a call echoed by G7 leaders for responsible technology use.

Practical Data Protection Tips for AI Development

Developers and organisations engaged in AI projects should prioritise data protection as both a legal requirement and a moral imperative. Here are practical tips, including the crucial concept of Privacy by Design:



1 **Privacy by Design**
Integrate privacy considerations into the entire AI development process, from conception to deployment. Make privacy an essential component of the initial design rather than an add-on.

2 **Transparency and explainability**
Clearly communicate how data is being processed, ensuring transparency about the purposes and methods employed by AI systems.

3 **Maintain proper data hygiene**
Data should only be gathered in the forms required to build the AI, and it should only be preserved for as long as is required to achieve the goal and keep it safe.

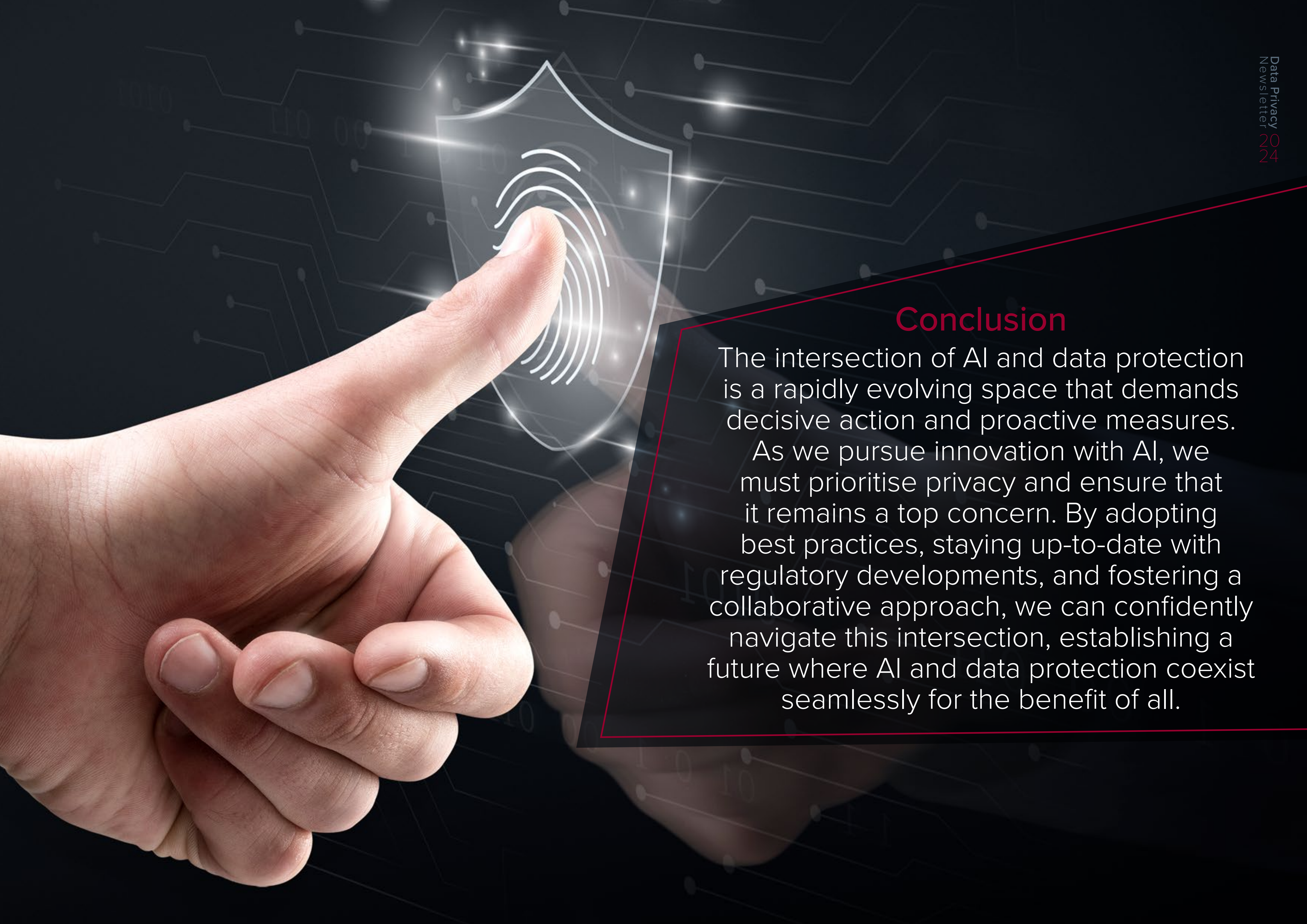
4 **Make use of quality data sets**
AI should be developed by developers using representative, equitable, and accurate data sets.

5 **Apply robust data governance practices**
Put into practice strong data governance procedures, such as lifecycle management, data mapping, and classification.

6 **User Consent**
Obtain explicit consent from individuals before collecting and using their data for AI purposes. Clearly explain the scope and implications of data usage.

7 **Anonymisation techniques**
Implement robust anonymisation methods to protect the identities of individuals in datasets used for AI training and testing.

8 **Regular audits**
Conduct regular privacy assessments and audits to identify and address potential risks and vulnerabilities in AI systems.



Conclusion

The intersection of AI and data protection is a rapidly evolving space that demands decisive action and proactive measures. As we pursue innovation with AI, we must prioritise privacy and ensure that it remains a top concern. By adopting best practices, staying up-to-date with regulatory developments, and fostering a collaborative approach, we can confidently navigate this intersection, establishing a future where AI and data protection coexist seamlessly for the benefit of all.

In conversation with

Drudeisha Madhub

Data Protection Commissioner at
Data Protection Office Mauritius

Question 1

Describe how the Data Protection Office (DPO) drove operational change by educating organizations in Mauritius about data protection laws. What are the initiatives undertaken by the DPO to influence the understanding and implementation of a Data Protection Framework?

Mauritius data privacy framework has been recognized by UN as a leading example in the region. The Privacy Symposium of Africa hosted by this office in November 2023 showcased the success of the data privacy framework Mauritius has implemented so far.

Master Classes at the PSA were delivered to participants with a deeper understanding of the latest developments and best practices in the field of privacy and data protection. They were led by experienced privacy professionals and experts, and provided participants with hands-on training and practical knowledge on a range of privacy-related topics. The Privacy Scorecard Report provided an overview of the privacy and data protection regimes in Uganda, Kenya, and Mauritius. The panel discussions were an important part of the event, as they provided a platform for participants to engage in thoughtful and insightful discussions on the latest developments and challenges in the field of privacy and data protection.

The office undertakes a panoply of compliance and enforcement activities to ensure an effective application of the DPA as can be demonstrated by some statistics below:

Registration of controllers	Registration of processors	Registration revenue (2022)	Complaints	Investigation findings delivered	Appeals against decisions of Data Protection Commissioner
19,071	**1013**	**Rs 2,736,500**	**450**	**73**	**7 (5 upheld)**
Cases won at the Supreme Court of Mauritius	Authorisations for data transfer	Notifications for personal data breaches	Data Impact Assessment analysed	Request for data protection certificate	Certification Awarded
2	**345**	**150**	**19**	**6**	**1 private company**

- Regular interventions are made by the Data Protection Commissioner (DPC) in press interviews, conferences, seminars and international online meetings
- The office participates in numerous international privacy networks such as Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP), Réseau Africain des Autorités de Protection des Données Personnelles (RAPDP), Global Privacy Enforcement Network (GPEN), Common Thread Network (CTN), Global Privacy Assembly (GPA), Council of Europe and the United Nations, amongst others
- The Data Protection Office has implemented a new system, e-DPO, which is an Integrated System that enables Controllers and Processors to do their registration online on the website of the Data Protection Office. The e-service is available 24/7 and provides for:
  - Online registration and renewal of controllers and processors with e-payment facility,
  - Online search of registered controllers and processors
  - Online lodging of complaints and submission of forms (personal data breach notification form, data protection impact assessment form, transfer of data form, certification form and compliance audit form).
- A self-learning training toolkit has been produced and is available on our website. The toolkit explains the basics of the Data Protection Act 2017.
- The office has trained around 250 data protection officers through in-house training.
- This office has published 19 guides on data protection which are available on our website.
- Around 400 requests for legal advice are addressed each year to assist controllers and processors in the implementation of the DPA.
- The Data Protection Commissioner has launched a networking forum of data protection officers to promote knowledge sharing, collaboration and cooperation, learning opportunities and professional development.

In conversation with (Contin'd)

Drudeisha Madhub

Data Protection Commissioner at
Data Protection Office Mauritius

Question 2

What are your views on the emerging challenges and inclusion of Artificial Intelligence in different industries? How robust is the Data Protection framework in Mauritius, in respect of the surging trends on Artificial Intelligence?

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

However, AI presents significant challenges and concerns in the realm of privacy and data protection.

AI is not just about technology but delves into fundamental and interdisciplinary human rights and freedoms. Not only does AI force us to better understand its impact on human rights and fundamental freedoms, but it also entails in-depth reflection on who is responsible for its harmful consequences.

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

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

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

The rapid development of AI has transformed the current business landscape. Businesses leverage AI solutions for a variety of purposes, including automating customer service, improving business intelligence, and facilitating strategic decision-making. While AI has the potential to drive innovation by automating many digital tasks, it is also seen as a potential threat that requires regulation.

The European Union introduced a groundbreaking initiative by the formulation of the EU AI Act and paved the way for comprehensive AI regulation. It is the first legislation of its kind in the world, which regulates the use of AI in Europe, respects the values and rules, and harnesses the potential of AI for industry. The gist of the AI Act is a classification system that determines the level of risk an AI technology could pose to the health and safety or fundamental rights of a person. The framework incorporates four risk tiers: unacceptable, high, limited and minimal.

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

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

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

Compliance Alerts

(Regulatory landscape)

Introduction

The importance of privacy laws has increased significantly in today's globalized world, where data flows across borders. With more than 120 jurisdictions having data privacy laws and continuous evolution in data protection legislation worldwide, businesses that operate online and internationally must anticipate significant changes in the requirements they need to comply with.

In 2023, there were major changes to data privacy laws and regulations around the world. We highlight some of these changes in the diagram below. If your business operates on a global scale, it is essential to stay informed about potential changes and adjust your practices accordingly to avoid penalties.

Country	Year	Major Changes
Jamaica Data Protection Act (DPA) 🇯🇲	November 30, 2023	The Data Protection Act (DPA) in Jamaica, introduced in December 2021, mandates organisations to obtain consent from individuals, ensure data access, implement security measures, report data breaches, and conduct Data Protection Impact Assessments before processing sensitive or high-risk data.
Switzerland Federal Act on Data Protection (FADP) 🇨🇭	September 1, 2023	The FADP is a stringent data protection law based on GDPR, requiring organisations to obtain consent, provide access to personal data, and report breaches within 72 hours. It also mandates the appointment of a Data Protection Officer for high-risk data processing or large amounts of sensitive data.

Country	Year	Major Changes
United States The Virginia Consumer Data Protection Act (VCDPA)	January 1, 2023	By the end of 2023, America has passed new data compliance laws, including the Virginia Consumer Data Protection Act, Colorado Privacy Act, and Utah Consumer Privacy Act. These laws provide individuals with new rights over their personal data, including access, correction, deletion, and opt-out of targeted advertising.
The Colorado Privacy Act (CPA)	July 1, 2023	
The Utah Consumer Privacy Act (UCPA)	December 31, 2023	
Singapore Personal Data Protection Act	July 18, 2023	Singapore's Personal Data Protection Commission (PDPC) has issued advisory guidelines for AI use, focusing on transparency, fairness, and accountability. These guidelines aim to ensure organisations remain compliant with PDPA when using AI/ML technologies, while not being legally binding.
India The Digital Personal Data Protection Act (DPDP)	November 30, 2023	India's data protection law mandates consent from individuals before processing sensitive personal data and establishes a Data Protection Authority to enforce the law, imposing penalties on violators.
South Korea The South Korean Personal Information Protection Act (PIPA)	September 15, 2023	The law passed in 2022, underwent amendments in March 2023, requiring explicit consent for processing sensitive personal data, providing portable data copies, notifying individuals of automated decision-making, and reporting data breaches to the Personal Information Protection Commission (PIPC) within 72 hours.
Australia Privacy Amendment Act	November 30, 2023	The Australian Privacy Act of 1998 has been updated to include expanded scope for offshore entities collecting or disclosing personal information, increased penalties for serious breaches, updated consent obligations, reasonable steps for de-identified information, and DPIAs for high-risk data processing activities.

Country	Year	Major Changes
EU-U.S. Data Privacy Framework	July 11, 2023	The EU and US have agreed on the EU-U.S. Data Privacy Framework, ensuring data protection in international data transfers. The framework consists of seven core principles: notice, choice, accountability, security, data integrity, access, and recourse mechanisms. It requires data subjects to have access to their data and consent for processing.
California Age-Appropriate Design Code Act (CAADCA)	September 15, 2022, to take effect July 1, 2024	The California Age-Appropriate Design Code Act, passed in 2022, applies to products and services geared towards children, those accessed by a significant number, those with common children's interests, and those with similar features.
Indonesia Indonesian Personal Data Protection Law (PDPL)	October 17, 2022	The Indonesian Personal Data Protection Law (PDPL) was passed in 2022 and will take effect in 2024. Similar to the EU GDPR, it sets data processing standards, grants data subjects' rights, and imposes penalties on non-compliant entities. Key requirements include obtaining consent, providing privacy notices, responding to data subject requests, conducting data protection assessments, notifying authorities, complying with overseas data transfer standards, and appointing a Data Protection Officer.

Industry News

Introduction

This section examines some of the significant occurrences and news events that have moulded the data protection landscape and impacted the course of procedures and policies.

5 years of the GDPR

The General Data Protection Regulation (GDPR) celebrated its fifth anniversary on May 25, 2023. It is one of the world's strictest privacy laws, establishing a uniform framework for data flow across the EU's digital single market. The Federal Data Protection Act (BDSG) in Germany and the Organic Law on Data Protection (LOPD) in Spain have also been updated to align with GDPR. Many of the recently enacted laws in Switzerland and South Korea are similar to those in the GDPR.

The AI Safety Summit

The AI Safety Summit in Bletchley Park, UK, resulted in the Bletchley Declaration, a first-of-its-kind agreement between 28 countries, including the US, China, and EU, addressing AI risks, bias, and privacy. However, opponents argue for a lack of specifics and practical suggestions for a strong regulatory framework.

Facebook fined a record €1.2 billion

Meta Ireland was fined the highest GDPR fine ever by the Irish Data Protection Commission on May 22, 2023. The penalties, the fourth of the year, prompted tech giants to comply with data protection laws. Meta plans to appeal and has not yet paid the fine. They were mandated to stop using Standard Contractual Clauses by October 12, 2023. On September 7, 2023, Meta released an update announcing that they will be using the new EU-US DPF for data transfers.

The UK-US 'data-bridge'

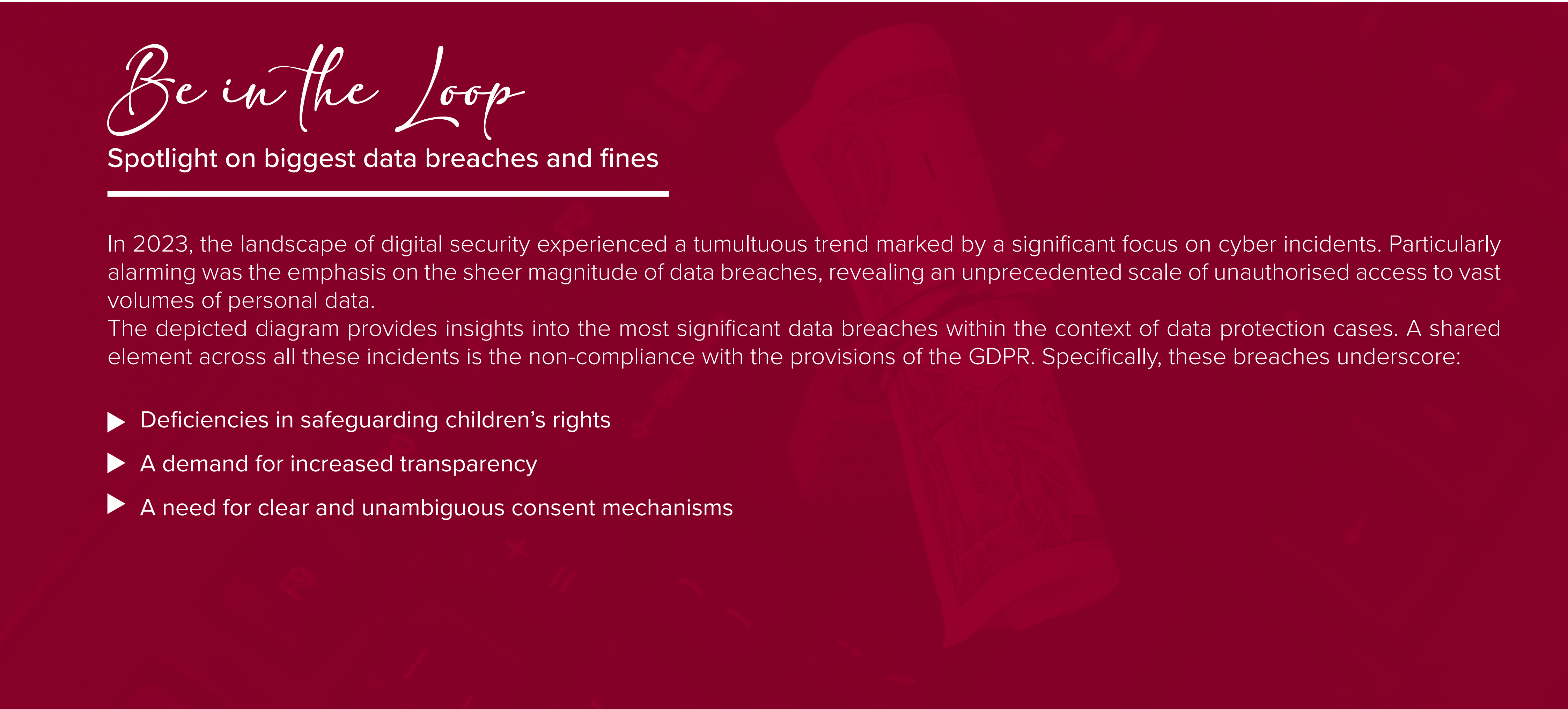
The UK-US "data-bridge" was approved on September 21, 2023, allowing UK-based companies to send personal data to US organisations without additional security measures. However, it has been criticised for privacy erosion and increased US surveillance.

DSIT published AI Skills for Business Competency Framework

The Department of Science, Innovation, and Technology's (DSIT) Office for Artificial Intelligence released the AI Skills for Business Competency Framework in November 2023, aiming to guide workers in understanding AI upskilling needs and creating relevant training programs for businesses.

3rd party cookies in Chrome to be disabled

Starting in the first quarter of 2024, Google intends to gradually remove third-party cookies from its Chrome browser. This is a component of the larger Privacy Sandbox project, which aims to limit cross-site tracking while maintaining the ability to maintain open access to online content and services.

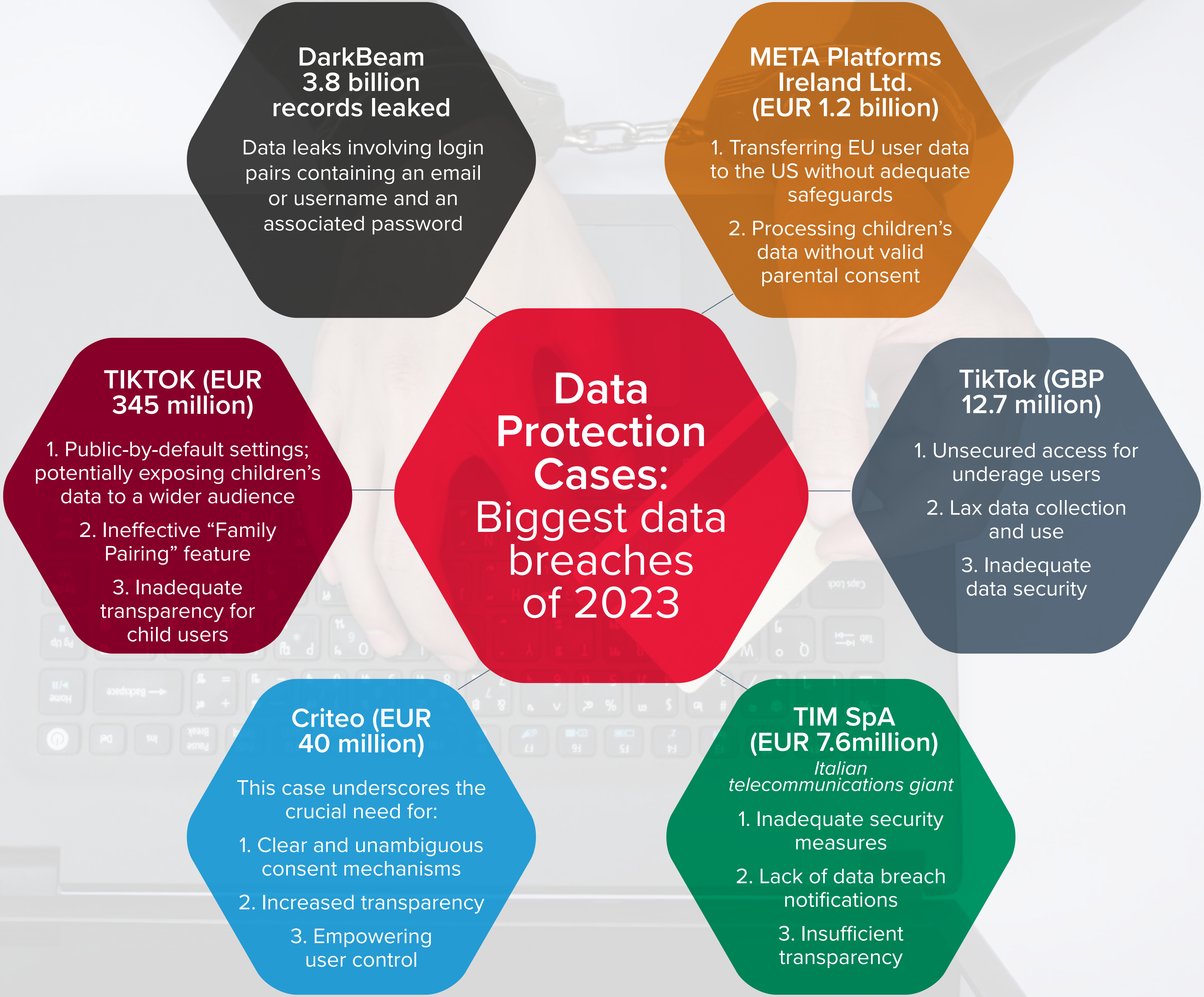


Be in the Loop

Spotlight on biggest data breaches and fines

In 2023, the landscape of digital security experienced a tumultuous trend marked by a significant focus on cyber incidents. Particularly alarming was the emphasis on the sheer magnitude of data breaches, revealing an unprecedented scale of unauthorised access to vast volumes of personal data.
The depicted diagram provides insights into the most significant data breaches within the context of data protection cases. A shared element across all these incidents is the non-compliance with the provisions of the GDPR. Specifically, these breaches underscore:

- Deficiencies in safeguarding children's rights
- A demand for increased transparency
- A need for clear and unambiguous consent mechanisms



Data Protection Cases: Biggest data breaches of 2023

DarkBeam 3.8 billion records leaked

Data leaks involving login pairs containing an email or username and an associated password

META Platforms Ireland Ltd. (EUR 1.2 billion)

1. Transferring EU user data to the US without adequate safeguards
2. Processing children's data without valid parental consent

TIKTOK (EUR 345 million)

1. Public-by-default settings; potentially exposing children's data to a wider audience
2. Ineffective "Family Pairing" feature
3. Inadequate transparency for child users

TikTok (GBP 12.7 million)

1. Unsecured access for underage users
2. Lax data collection and use
3. Inadequate data security

Criteo (EUR 40 million)

This case underscores the crucial need for:

1. Clear and unambiguous consent mechanisms
2. Increased transparency
3. Empowering user control

TIM SpA (EUR 7.6million)

Italian telecommunications giant

1. Inadequate security measures
2. Lack of data breach notifications
3. Insufficient transparency

Events and Webinars

BDO IT Consulting Ltd organised two successful compliance days covering topics on AML and Data Protection, along with a well-received breakfast session on Data Protection. These events provided valuable learning opportunities for professionals, fostering a platform for networking and knowledge exchange.

Business Breakfast at Le Suffren Hotel

15 March 2023

Compliance Conference at The Ravenala Attitude Hotel

31 May 2023

BDO IT Consulting Ltd | IT Governance & Consulting
#Technology. Value Driven.

BDO IT Consulting Ltd | IT Governance & Consulting
#Technology. Value Driven.
BDO

Automation and AI Horizons: Unveiling Future Business Success in Mauritius at The Ravenala Attitude Hotel

31 October 2023

Upcoming Workshop

Click here to register

The Half-Day Workshop on Navigating Privacy in the Era of AI, which will be hosted by BDO IT Consulting Ltd on March 1, 2024, aims to delve into the complexities of privacy in the era of artificial intelligence (AI). Attendees will have the opportunity to gain valuable insights into the challenges and opportunities presented by AI and its impact on privacy, including discussions on privacy by design and data protection audits. By learning from leading professionals in the field, participants can stay ahead in the ever-evolving landscape of technology and privacy.

Navigating PRIVACY in the Era of AI

Data Protection Workshop

BDO IT CONSULTING
IT GOVERNANCE & CONSULTING

Friday, 1st March 2024 9am - 3pm
Hennessy Park Hotel, Ebene

Rs 9,000/p

For more information:
Essar Building, 10 Frère Felix De Valois St, Port Louis ☎ 260 58 35/47
bdoitc_training@bdo.mu

BDO IT CONSULTING ★★★ TRAINING CENTRE ★★★ MQA APPROVED

BDO

For more information, contact us:

Sylvie Greco
Partner
T: +230 260 5889
M: +230 5497 9578
E: sylvie.greco@bdo.mu

Deepshi Hujoory
Manager
T: +230 260 5839
M: +230 5964 0469
E: deepshi.hujoory@bdo.mu

Get in touch with us!

Essar Building, 10 Frère Felix
De Valois St, Port Louis

☎ +230 260 78 00

✉ bdo.it.consulting@bdo.mu

in BDO IT Consulting

BDO