

Newsletter

2024

DATA PRIVACY

BDO IT CONSULTING
IT GOVERNANCE & CONSULTING

BDO



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:

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

- ▶ 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.