An Online Event with the Mauritius Data Protection Commissioner and Members of South Africa's Information Regulator

By Drudeisha Madhub
Data Protection Commissioner, Mauritius
Website: https://dataprotection.govmu.org/

Privacy Laws & Business
www.privacylaws.com
22nd April 2021

Mauritius

- Located off the southeast coast of Africa, Mauritius is an island state of about 1.3 million people.
- It has a reputation for stability and racial harmony among its mixed population.
- The country's economy is diversified and also relies on its offshore financial activity, textile industry and production of sugarcane. Medical tourism, outsourcing, new technologies and the luxury industries are among developing sectors.

Capital: Port - Louis

Mauritius Data Protection Act (DPA)

2017

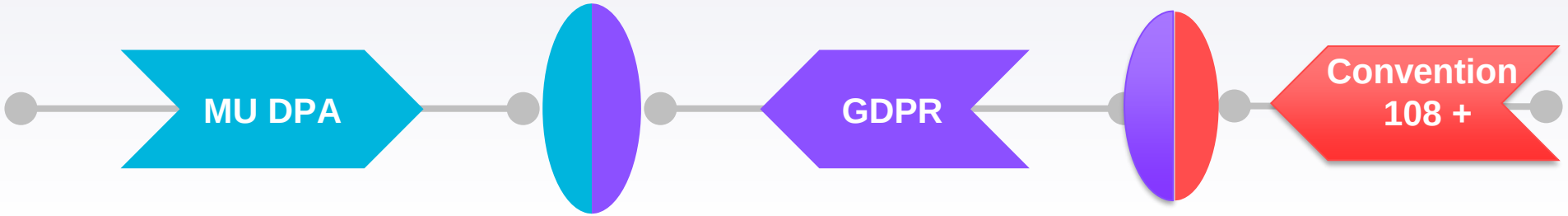
- Amended in 2017 to become a new and improved legislation namely, the Data Protection Act 2017 which came into force on 15 January 2018.

2004

- First Enacted in 2004.

- Regulates the processing of personal data.
- Makes provisions about the functions, powers of the office, enforcement and application of the legislation.
- Seek to bring Mauritius data protection framework in line with international standards, namely the EU General Data Protection Regulation (GDPR) and convention 108+.

Differences between MU DPA and EU GDPR



Requires controllers and processors to register with the Data Protection Commissioner before processing personal data

Criminal law that can entail to imprisonment upon conviction.

Max fine is Rs 200,000

Does not require registration with Supervisory authorities

Monetary penalties i.e., administrative fines.

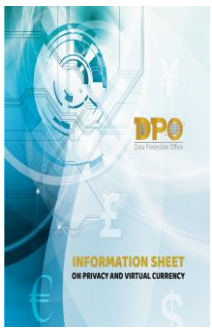
Less severe breach- Max. fine is €10 million or 2% of a company's annual revenue, whichever is greater.

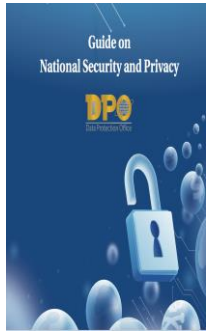
for more severe breaches – Max. fine is €20 million or 4 % of a company's annual revenue, whichever is greater

Talks about judicial and non-judicial sanctions in Art 12 which are considered effective remedies.

How the DP Commissioner educates the business community in Mauritius

- Mass sensitization - By conducting workshops, issuing press communiqué amongst others.
- Training - Inhouse training on the DPA is provided to members of the private and public sector.
- Publication of guidelines
  - Available: https://dataprotection.govmu.org/Pages/Downloads/Guidelines-Data-Protection-Act-2017.aspx
  - Newly issued:
  - Information Sheet on Privacy and Virtual Currency
  - Guide on National Security and Privacy
- Data Protection Training Toolkit
  - *Self-learning training toolkit.*
  - *Explains the concepts of the DPA in a very simplified language with numerous practical examples*





Typical complaints regarding multinational companies

The office receives complaints against multinational companies. Issues that we have received so far are mainly with regard to data subjects access requests and disclosure of personal data which has occurred accidentally.

Investigation on complaints made by individuals

Complaints by Individuals

- Individuals have the rights to file complaints under the DPA where their privacy is being infringed and the DPA has full powers under the act to investigate and provide remedies or prosecution whichever is applicable. The powers are defined under part II of the DPA.

- **The steps of investigation are as follows:**
  - *The individuals fill in the official complaint and declaration forms and submit them to this office.*
  - *An enquiry is then initiated with all parties concerned.*
  - *At the end of the enquiry, the Commissioner provides her decision.*
  - *Any person aggrieved by the decision of the Commissioner, may within 21 days from the date when the decision is made known to him, appeal to the ICT Appeal Tribunal (Section 51).*

- **The outcome of the investigation may be:**
  - *An amicable resolution by the parties concerned or*
  - *A prosecution can be instituted under this Act except by, or with the consent of, the Director of Public Prosecutions.*

- **Any fines or sentence under this Act is issued by the Intermediate Court after any hearing of parties.**

Enforcing the law on multinational companies

Multinational Companies

- Concerning multinational companies, as per section 3 (5) of the DPA, the Act applies to a controller or processor who –
  - (a) is established in Mauritius and processes personal data in the context of that establishment; and
  - (b) is not established in Mauritius but uses equipment in Mauritius for processing personal data, other than for the purpose of transit through Mauritius.

- As per section 3(6) of the DPA, every controller or processor referred to in section 3 (5)(b) shall nominate a representative established in Mauritius.

- There are multinational companies that have branches in Mauritius and are incorporated under the laws of Mauritius. The DPA will thus apply the same way as for any domestic companies and they will need to comply with the provisions laid down in the DPA.

- For those not incorporated in Mauritius but uses equipment in Mauritius, the DPA will still apply to them and any communication or will be done through its representative established in MU.

Examples of cases that have required an appeal to a judicial proceeding

Use of Fingerprint for attendances purposes

- A complaint was lodged in 2013 at this office under section 11 of the Data Protection Act 2004(DPA) against Respondent with regard to her dismissal as she refused to provide her fingerprint for the recording of attendance.
- The office opened an enquiry. After the investigation, the DPC provided her decision in "… *Complainant was justified in not providing her consent to Respondent…*"
- The company appeal to the Information and Communication Technologies (ICT) Appeal Tribunal. The Tribunal upheld the decision of the DPC and being dissatisfied with the determination of the ICT appeal tribunal, the Company made an appeal to the Supreme Court of Mauritius.
- The Supreme Court also upheld the decision of the ICT Appeal Tribunal and that of the DPC.

Camera in Lorry

- The Office received a complaint in November 2016 from Complainant (Union of Employees) against Respondent (a logistic company) regarding the installation of CCTV cameras in its lorries further to the request made by the Companies which Respondent was servicing. The complainant informed this office that the driver and helper that worked in such lorries were feeling unsecured in the performance of their duties whereby every personal gesture was being monitored.
- An enquiry was opened by this office and the DPC found the cameras in the lorry was privacy intrusive and demanded the company to remove the cameras.
- Respondent appealed to ICT Appeal Tribunal against the decision of the Commissioner. The office is currently awaiting the decision of ICT Appeal Tribunal for this case.

Madhewoo VS State of Mauritius – Supreme Court

- Adult citizens of Mauritius are required by law to carry identity cards which bear their names and signatures.
- The National Identity Card (Miscellaneous Provisions) Act 2013 was amended to introduce a new smart identity card, which incorporates on a chip the citizen's fingerprints and other biometric information relating to his or her external characteristics.
- Mr Madhewoo did not apply for a biometric identity card. He challenged the constitutionality of the 2013 Act at the Supreme Court.
- The Supreme Court held that the storage and retention of the fingerprints were not reasonably justifiable in a democratic society. Following the Supreme Court judgement in the case Madhewoo M. v the State of Mauritius and Anor and Jugnauth Pravind Kumar (Hon) v the State of Mauritius & Anor [2015] SCJ 178 , the Act was subsequently amended to delete fingerprint data after the card had been issued to the cardholder.

Madhewoo VS State of Mauritius – Privy Council

- On 24 November 2015, Mr Madhewoo was granted leave by the Supreme Court to appeal before the Board of the Judicial Committee of the Privy Council ('the Board'). He challenged the Supreme Court's evaluation on the constitutionality of the legal obligation imposed by the State to provide fingerprints and other biometric information under Section 4 of the Act and the storage of the identity card data on a database amongst others.
- In the Board's view, the requirement to provide fingerprints for an identity card does not give rise to any inference of criminality as it is a requirement imposed on all adult citizens
- The Board confirms the decision of the Supreme Court that the compulsory taking of fingerprints and the extraction of minutiae involve an interference with the Appellant's right under Section 9(1) of the Constitution not to be subjected to bodily harm except with his consent. It is to be noted that this right is not absolute. A limitation to the right not to be subjected to bodily search is permissible, under Section 9(2) of the Constitution, if provided by law in the interests of, inter alia, public order.
- As regards the storage and retention of fingerprints and other biometric data, the Board held that a law which provides for the storage and retention of such information regarding the identity of a person in principle constitutes a permissible derogation, in the interests of public order, under Section 9(2) of the Constitution.

Madhewoo (Author) VS State of Mauritius – Human Rights Committee

- The author has on 15 December 2017 communicated to the Human Rights Committee that the State of Mauritius has violated his rights under article 17 of the International Covenant on Civil and Political Rights. The Optional Protocol entered into force for the State of Mauritius on 23 March 1976.
- The Committee noted that:
  - the State party did not explain how the storage and retention of fingerprints on identity cards can prevent identity theft – the lawful purpose for processing this data.
  - the facts before it disclose a violation by the State party of the author's rights under the article17 of the Covenant.
  - the State party is under an obligation to provide the applicant with an effective remedy. Consequently, it is required to provide sufficient guarantees against the risk of arbitrary and misuse of the author's fingerprints which could result from the issuance of an identity card, and to re-examine the merits of the decision to store and retain fingerprints on identity cards in light of these findings.

Implementation of the DPA by multinational companies

- Multinational companies outsourcing to Mauritius are defined as those which are either establishing a branch in MU or choosing a processor in MU to process data on their behalf. In both ways, the DPA will apply and they will need to abide by all the provisions laid down in the Act.

- If they are choosing a processor in MU, there will need to have a contract between the controller and processor as stipulated under section 31 (4) of the DPA which are equivalent to standard contractual clauses or can include Binding Corporate Rules (BCRs) as well.

- In many respects, 'accountability' is the heart of good governance, as it requires an actual tangible commitment to act or to not act in a certain way. They will be held accountable for compliance with DPA where applicable by this office.

- Article 14 of convention 108+ is on Transborder flows of personal data which aims to facilitate the free flow of information regardless of frontiers while ensuring appropriate protection of individuals with regard to processing of personal data. Article 14 paragraph 1 applies to data flows between Parties to the Convention. *Article 14 also mentions that all Parties, having subscribed to the common core of data protection provisions set out in the Convention, are expected to offer a level of protection that is considered appropriate and therefore in principle allows data to circulate freely.*

The role of the Data Protection Assessment Certificate and the criteria for assessment.

Data Protection Impact Assessment

- Section 34(1) of the DPA stipulates that all controllers and processors must carry out a DPIA prior to the processing of personal data where such processing is likely to present a high risk to the rights and freedoms of the individuals. A DPIA helps to identify privacy risks, foresee problems and bring forward solutions. It serves as an assessment tool to decide whether the security measures in place are adequate compared to the risks to individuals and whether the necessity of an envisaged processing operation does not outweigh the rights and freedoms of individuals.

- The Data Protection Office has provided a list of criteria for assessing high-risk processing operations on its website. The criteria for the assessment is provided below:
  - Evaluation or scoring personal aspects/behaviour of people including profiling;
  - Automated decision-making producing legal or similar significant effects;
  - Systematic monitoring by observing, monitoring or controlling data subjects;
  - Sensitive data (special categories of personal data) or data of a highly personal nature;
  - Data processed on a large scale;
  - Matching or combining data sets;
  - Data on vulnerable persons to whom the data relates (e.g. people with mental illness, asylum seekers or elderly people, patients, children, etc.);
  - Innovative use or application of new technological or organisational solutions;
  - When the processing “prevents data subjects from exercising a right or using a service or a contract”.

- A DPIA form and a guide on how to complete the DPIA are available on the website of the Data Protection Office at the following URL: https://dataprotection.govmu.org/Pages/Home%20-%20Pages/Document%20%26%20Forms/Data-Protection-Impact-Assessment-and-High-Risk-Operations.aspx

Certification

- To enhance transparency and compliance with the Data Protection Act 2017, certification (Section 48) has been introduced to help controllers or processors to demonstrate accountability and compliance with the Act and to allow data subjects to quickly assess the level of data protection of relevant products and services.

Certification body	• Certification will be issued by the Data Protection Office.
Compulsory and Fee?	• Certification is voluntary and free.
Validity	• Certification is valid for three years and is subject to renewal. Controllers or processors may apply for renewal of the certification before the date of its expiry.
Withdrawal	• Certification is subject to withdrawal where the conditions for issuing the certification are no longer met.
Criteria	• A detailed document for certification published is available at the following link:https://dataprotection.govmu.org/Pages/Home%20-%20Pages/Document%20%26%20Forms/Certification.aspx

A progress report on discussions with the European Commission on an adequacy declaration for Mauritius

- Following the proclamation of the Data Protection Act (DPA) 2017 in Mauritius, the next milestone is to achieve EU adequacy so that Mauritius can be recognised as a safe and adequate country in data protection.

- We have already initiated the EU adequacy procedure with the EU. Upon recommendation from the representative of the Delegation of the European Union to the Republic of Mauritius and the Republic of Seychelles, we drafted and submitted the Terms of Reference (ToR) in 2020 to our parent Ministry for inviting proposals through restricted international bidding for the services of an expert consultant to carry out a complete assessment and evaluation of the existing data protection law in Mauritius, its application and provide an opinion on the adequacy of Mauritius with the European Union. We are currently awaiting the finalisation of the consultancy nominations.

Convention 108 and Covention 108+

- Mauritius has been party to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) since 1 October 2016.
- The Government of Mauritius has leapt forward by the ratification of Convention 108+ in September 2020 which is a universal instrument that can be adopted by countries outside the EU and also offers opportunities to the country to be recognised on the global market by the implementation of appropriate safeguards to protect privacy right.
- The ratification of the convention 108+ has triggered organisations in Mauritius to start their journey to implement data protection and respect the rights of data subjects into their respective organisations. This has forced them to be more privacy-friendly in their processing of personal data.
- Remarks: *It would be desirable that there are free transfers of personal data among those countries that have ratified the convention 108+.*

Ratifying Convention 108 in June 2016

Links between the Data Protection Commissioner and other regulator authorities in Mauritius

- Other regulatory authorities often seek the advice of the office when necessary and the office collaborates with them whenever required.

Links between the Data Protection Commissioner and other Data Protection Regulatory Authorities in Africa and in other regions of the world

- My office forms part of different international privacy networks such as GPA, CTN, GPEN, AFAPDP, RAPDP, UN amongst others which englobe different countries. Such participation enables the office to establish a dialogue with enforcement authorities, exchange information, undertake or support specific activities and sharing of enforcement knowledge as well as expertise along with best practices.

THANKS!