PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

GDPR-oriented privacy laws in South Africa and Mauritius

Webinar - 22 April 2021

Audience Questions on Mauritius

Answered by Drudeisha Madhub, Data Protection Commissioner, Mauritius

"Mauritius can be proud for having done so much since 2004." [A webinar participant]

Scope of the law

1. Does the same registration requirement apply to sub-processors based in Mauritius (if the processor is not based in Mauritius)?

   As per section 14 of the DPA, no person shall act as controller or processor unless he or it is registered with the Commissioner.

   The same registration will apply to a sub processor based in Mauritius.

   If a sub processor is not based in Mauritius, then it will have to abide by the data protection law in that country plus the contractual requirements with the controller wherever the latter's establishment is.

2. A US-based social media company (i) with no presence in Mauritius, and (ii) who doesn't use equipment in Mauritius processes the personal data of people based in Mauritius. Will the company have to comply with the Mauritius data protection law?

   Unlike GDPR which has an extra- territorial effect, the Mauritian DPA applies as provided in section 3 (5) of the Act
   a) to a controller or processor who –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), every controller or processor referred to in subsection (5)(b) shall nominate a representative established in Mauritius and as per section 3 (7), for the purpose of subsection (5)(a), any person who –
   a) is ordinarily resident in Mauritius; or
   b) carries out data processing operations through an office, branch or agency in Mauritius, shall be treated as being established in Mauritius.

   The DPA's application is thus territorial in scope. The absence of extra territorial effect does affect us in certain ways as we cannot prosecute companies established outside MU and which are processing Mauritian Citizens personal data. However, we are somehow reassured when the companies are from the EU where GDPR is in force, heavy penalties for non-compliance with GDPR will be applicable in case of any breach.

   Regarding the point of "uses equipment in Mauritius " by any social media, the fact has to be well established through enquiry conducted by this office and the country where the servers are processing the personal data have to be clearly identified.If the servers are processing the personal data are outside Mauritius, then the data protection law of that country will apply to the US-based social media company.

   If you are using Mauritian data and a complaint is lodged at this Office, we will enquire as to how cooperation can be established with the supervisory authority where your headquaters are based.

3. Is there a difference in the way that the law covers personal data on a server in the country compared with a computer accessing cloud data?

   When the personal data is processed on a server located in Mauritius, the DPA will apply.

   When a computer is accessing cloud data outside Mauritius but the controller/processor is in Mauritius, the DPA will apply irrespective of whether the cloud server is outside Mauritius.

4. I understand data subjects are living individuals. How is the right to erasure and rectification exercised with respect to deceased individuals?

   The DPA applies to living individuals only.

The role of the Data Protection Officer

5. Is there a threshold to the requirement of having a Data Protection Officer (DPO)? For example. are very small companies required to have a DPO?

   The threshold will vary from organisation to organisation. A small company may designate someone that can fulfil this role of DPO despite shouldering other functions in the company. However, there should be no conflicts of interest between the different functions.

6. You advised that it is mandatory to have a DPO. Does this have to be a full time independent role or can it be combined with an existing role like an Information Security or Legal Officer?

   The role of DPO can be fulfilled by either an full time person or part-time person depending on the organisation. It can be combined with existing role like an Information Security or Legal Officer as long as it meets the requirements of this role as per our guide:

   - Roles and Responsibilities of Data Protection Officer

   We also offer training courses to DPOs.

International transfers

7. How is transnational flow of data managed in Mauritius for transnational businesses?

   Cross-border data flows have become a prerequisite for sound business strategies worldwide. To ignore the potential benefits of data sharing to a global data economy is a serious issue we have to avoid at all cost. A robust domestic policy drawing the fine balance between the benefits and risks of data flows is a must for both emerging market economies and highly developed market economies alike.

   Mauritius is the first African country to have signed and ratified the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in September 2020 and to have incorporated principles of the EU GDPR in its domestic law.

   The importance of harmonising domestic laws with international privacy laws or instruments facilitates data flows and trade between countries whilst ensuring an adequate level of protection to individuals. In this increasingly digital world, cross-border data flows are the lifeblood of international trade especially during the COVID-19 pandemic with the sharing of health data across the globe.

   Our rule for international transfers is based on section 36 of the DPA which are summarised as follows:

Transfer to another country may be made where any one of the below conditions are met-

- Proof of appropriate safeguards provided to the Commissioner or
- The data subject has provided his explicit consent or
- For the performance of contract or pre-contractual measures taken with the data subject or
- For the conclusion or performance of a contract concluded in the interest of the data subject or
- For reasons of public interest as provided by law or
- For legal claims or
- For the vital interest of the data subjects;
- For compelling legitimate interests of the controller or processor
- For public register containing information which is required to be transferred.

Since the sector of Business Process Outsourcing plays an important part in the economy of Mauritius, aligning our data protection principles with that of the European Union will instill confidence in the data protection framework in Mauritius for European Companies to outsource activities to Mauritius.

Organisations may also use Binding Corporate Rules (BCRs) and Standard Contractual Clauses(SCCs) for transfers incorporating data protection safeguards.

8. I heard the term "Data in Transit". What is “data in transit” compared with data not in transit?

Data in transit, or data in motion, is data that is actively moving from one location to another such as across the internet or through a private network. Wherever data is moving, effective data protection measures for in-transit data are critical as data is often considered less secure while in motion.

Data at rest (data not in transit) is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way. Security measures must also be in place to protect the data at rest.

The risk profile for data in transit or data at rest depends on the security measures that are in place to secure data in either state.

The DPA (section 3(5)) does not apply to data which is transitting only through Mauritius.

9. Are we allowed to have a bulk application through the Record of Processing Activities (ROPA) to seek the Data Protection Commissioner's approval regarding activities related to cross-border data transfers?

As per section 35 (1) of the DPA, every controller or processor must obtain authorisation from the Office prior to processing personal data in order to ensure compliance of the intended processing with the DPA and in particular to mitigate the risks involved for the data subjects where a controller or processor cannot provide for the appropriate safeguards referred to in section 36 in relation to the transfer of personal data to another country.

Besides, under section 35 (2), the controller or processor must consult the Office prior to processing personal data in order to ensure compliance of the intended processing with the Act and in particular to mitigate the risks involved for the data subjects where –

a) a data protection impact assessment as provided for in section 34 indicates that processing operations are by virtue of their nature, scope or purposes, likely to present a high risk; or
b) the Office considers it necessary to carry out a prior consultation on processing operations that are likely to present a high risk to the rights and freedoms of data subjects by virtue of their nature, scope or purposes.

Bulk applications are possible if they relate only to one organisation. You have to fill in the transfer of personal data form which is different from the record of processing template.

Please refer to question 7 above as well.

Special categories of personal data

10. Regarding the Mauritius example on biometrics in identification systems, as an emerging offshore financial centre, how are you and financial services regulators approaching privacy enhancing technologies in relation to authentication techniques (e.g. Strong Customer Authentication under PSD2 in an EU/UK context)?

    First of all, our financial service regulators are registered as controllers with the Data Protection Office and are required to abide by the overall provisions of the DPA. In so doing, they are implementing the necessary procedures at their end to demonstrate compliance and to also comply with their respective laws.

    The privacy by design approach promotes privacy and data protection compliance from the start of the project and then throughout its lifecycle and is catered in section 31 of the DPA. That is the controller or processor must ensure that appropriate security and organisational measures are in place at the time of the determination of the means for processing and at the time of the processing to provide a level of security appropriate to the harm that might result from the unauthorised access to, alteration of, disclosure of, destruction of the data and its accidental loss.

    The controllers are advised to carry out a Data Protection Impact Assessment (DPIA) as per section 34 of the Data Protection Act 2017 (DPA) given where the processing will result of high risk to the individuals. This will also help the controller to identify and minimise any data protection risks of the project.

    The controllers must download the DPIA form and submit it to office.

    In case, they encounter difficulties regarding the questions, they can refer to the guides on (1) High Risk Processing Operations and (2) how to complete the DPIA form.

11. Is consent compulsory for the processing of special categories of personal data under the DPA 2017?

    Special categories of personal data are considered sensitive and are subject to special protection.

    Consent is not the only lawful basis for processing personal data and/or special categories of personal data. The controller will need to satisfy a condition under section 28 and a condition under section 29 of DPA for processing special categories of personal data.

    Section 28 – Lawful processing

    (1) No person shall process personal data unless –

    - *a) the data subject consents to the processing for one or more specified purposes;*
    - *b) the processing is necessary –*
        - *i. for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;*
        - *ii. for compliance with any legal obligation to which the controller is subject;*
        - *iii. in order to protect the vital interests of the data subject or another person;*
        - *iv. for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
        - *v. the performance of any task carried out by a public authority;*
        - *vi. the exercise, by any person in the public interest, of any other functions of a public nature;*
        - *vii. for the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or*
        - *viii. for the purpose of historical, statistical or scientific research.*

Section 29 – Special Categories of personal data

(1) Special categories of personal data shall not be processed unless –

- *a) section 28 applies to the processing; and*
- *b) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;*
- *c) the processing relates to personal data which are manifestly made public by the data subject; or*
- *d) the processing is necessary for –*
  - *i. the establishment, exercise or defence of a legal claim;*
  - *ii. the purpose of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to a contract with a health professional and subject to the conditions and safeguards referred to in subsection (2);*
  - *iii. the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; or*
  - *iv. protecting the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.*

(2) The personal data referred to in subsection (1) may be processed for the purposes referred to in subsection (1)(d)(ii) where the data are processed by or under the responsibility of a professional or other person subject to the obligation of professional secrecy under any enactment.

The Data Protection Commissioner as a Supervisory Authority

12. Some EU Supervisory Authorities are criticised for not exercising their punitive powers (in particular, fines) as heavily as others. For example, the UK and Irish regulators are viewed by some as being more conservative then their French and German counterparts in this regard. What is your view on the exercise of such powers and how leniently or heavily would you say that your Authority exercises these powers?

    The DPA provides for criminal penalties which are serious in nature as prosecution is involved and appeals on decisions of the DPC are a current feature in Mauritius.

    Under section 43 (1), any person who commits an offence under this Act for which no specific penalty is provided or who otherwise contravenes this Act shall, on conviction, be liable to a fine not exceeding 200, 000 rupees and to imprisonment for a term not exceeding 5 years.

    As per section 53 (3) of the DPA, no prosecution shall be instituted under this Act except by, or with the consent of, the Director of Public Prosecutions (DPP).

    Thus, when there is an offence, the office will request the advice of DPP for prosecution and it will be the Intermediate Court which will try an offence under the DPA or any regulations made under it and decide on the fine and imprisonment.

13. How is the Data Protection Commissioner funded in Mauritius? I know in the UK and South Africa this office is funded by Government which has its drawbacks as opposed to being funded by fines. Information regulators funded by fines appear to be proactive as opposed to being reactive.

    The Mauritian Data Protection Office is operating under the aegis of the Ministry of Information Technology, Communication and Innovation (MITCI).

    Under section 4(2) of the DPA, in the discharge of its functions under this Act, the Office acts with complete independence and impartiality and is not subject to the control or direction of any other person or authority.

Our budget is funded by the Government and managed by our parent Ministry (MITCI). Being under the auspices of a larger ministry or governmental body has both its boon and bane. Where the office is out of budget, then the parent Ministry funds the outstanding amount. The disadvantages are that the budget of the office might be cut at the time of a financial crisis or during a pandemic and for each item that the office will need, approval of the parent ministry will then need to be sought.

Each system has its own pros and cons but financial independence is guaranteed as our budget is wholly used by our office.

EU adequacy

14. An EU adequacy decision is important for the offshore sector in Mauritius especially for those doing business with Europe and thus processing personal data of EU citizens. Regarding the application process submitted by the Mauritius government (or DP Commissioner?), by when can Mauritius aspire to receive a positive adequacy decision from the EU Commission?

    We have an ambitious reputation to earn Mauritius as a country that provides adequate safeguards on data protection. My Office has already started discussions with the European Union. Our parent Ministry has invited 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.

    EU adequacy is a lengthy process.

    The COVID-19 pandemic is undoubtedly having a great impact on how we are operating nowadays. Mauritius has been in its second lockdown since 10th March 2021 and we are now in the second phase of deconfinement.

    We are currently awaiting the finalisation of the consultancy nominations. At this point, it is very difficult to provide a timeline by when Mauritius can achieve EU Adequacy. However, the prospective timeframe could be next year.

Questions edited by Stewart Dresner,
Founder and Chief Executive,
Privacy Laws & Business stewart.dresner@privacylaws.com