

**Q&A with
South Africa
and
Mauritius
DPAs**



Scope of the law



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

Scope of the law



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?

Scope of the law



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?

Scope of the law



I understand data subjects are living individuals.

How is the right to erasure and rectification exercised with respect to deceased individuals?

The role of the Information Officer



Is the portal to register Information Officers now available?

The role of the Information Officer



In terms of the Information Officers and Deputy Information Officers (under POPIA), does the law state where these individuals should be located? Does the Information Regulator have a recommendation or guidance on this point?

The role of the Information Officer



Does an Information Officer (IO), or Deputy IO, have to be appointed within the company and in the country, or could this person be appointed out of the company and outside the country?

The role of the Information Officer



Assuming they are part of the same holding company, would it be acceptable in terms of the guidance notes regarding registration of a IO and a DIO to have a IO in the UK and the DIO in SA? Or will we need to register the IO based in SA and register the DIO who is based in the UK?

The role of the Information Officer



The position of the Information Officer is similar to that of the DPO under the GDPR. Based on the most recent guidelines published on 1 April on the position of the Information Officer, doesn't the fact that both the IO and the DIO have to be employees of the private body challenge the independence of the person in terms of having their tasks and assessments "conditioned to" [I think the question means "aligned with"] the body which employs them?

The role of the Information Officer



POPIA - PAIA: Can a company nominate more than one Information Officer? For example one for PAIA the other for POPIA.

The role of the Information Officer



The IO is responsible for developing/monitoring compliance against a PAIA manual and compliance framework. Can someone else draft the manual and framework but the IO retains accountability for monitoring and compliance around the manual and framework?

The role of the Information Officer



Sec 30 of the GDPR requires that 'Each controller and, where applicable, the controller's representative, shall maintain a Record of Processing Activities within its responsibility'. I understand the POPIA has a similar requirement concerning a record of processing activities. Could you please comment on what the similarities and differences are concerning a record of processing activities in terms of the POPIA compared to the GDPR?

The role of the Data Protection Officer



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 role of the Data Protection Officer



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?

International transfers



What is the equivalent of Standard Contractual Clauses (under GDPR) in POPIA?

International transfers



What clauses are required in intercompany agreements to allow information processed in South Africa to be transferred outside the Republic to a company based in the UK?

International transfers



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?

International transfers



Does SA's Information Regulator (in light of POPIA) recognize the EU data protection regime as providing an adequate level of protection, (meaning that there is no need for additional transfer mechanisms)?

International transfers



Would EU Binding Corporate Rules be considered adequate for transfers of data out of South Africa?

International transfers



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

International transfers



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

International transfers



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?

Consent



We are doing customer satisfaction surveys for clients. They give us their customer list. Is it allowed to email these data subjects regarding the service that was provided to them? Or do they have to opt in?

Legal persons



How does the Information Regulator expect responsible parties to apply the principles in POPIA to information concerning judicial (rather than natural) persons? Will the IR be publishing guidance on that?

Legal persons



Does South Africa provide an adequate level of protection for the data of legal entities, although GDPR does not cover the data of legal entities?

Special categories of personal data



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)?

Special categories of personal data



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

The Information Regulator as a Supervisory Authority



Will there be a certification process for IO's or service providers assisting entities to get compliant?

The Information Regulator as a Supervisory Authority



In what instances will the Regulator not take action on complaints?

The Information Regulator as a Supervisory Authority



What challenges have been envisaged regarding enforcement of the laws?

The Information Regulator as a Supervisory Authority



Can we expect the Information Regulator to be tough on the public sector? They seem to be very intertwined with the Department of Justice (even their website is 'gov.za'!) Will they be deferential to government?

Data Protection Commissioner as a Supervisory Authority



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 than 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?

Data Protection Commissioner as a Supervisory Authority



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.

EU adequacy



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?

Other issues



The scenario is that a Responsible Party has contracted the performance of background checks, including criminal records, on applicants to job vacancies, to a third party (Operator). Who should submit such a Prior Authorization? The Responsible Party, or the Operator contracted by the Responsible Party?

Other issues



In the case where an Accountant is a Trustee of a Trust and is appointed as the IO of that Trust, how best can they enforce their responsibilities across the beneficiaries and other Trustees?