Good morning everyone.

Thank you for inviting me to open this seminar and thank you to BDO IT Consulting for organising it on the New European Union General Data Protection Regulation. It is an honour to be here with you.

Technology, nowadays, is allowing businesses and government to make use of personal information on an unprecedented scale in order to pursue their activities. Data protection is a dynamic field that is constantly challenged and influenced by advances in technology and innovation in business practices. Accordingly, the scale of data collection and sharing has increased considerably. Personal data protection, therefore, plays a central role in our country's digital development.

Individuals both in Mauritius and beyond want to feel confident that their privacy is strongly protected. To this end, they want to know if their personal information is safe and secure and not exposed to unlawful activities. As the global economy shifts further into a connected information space, the relevance of data protection and the need for controlling privacy increase further.

The starting point of an effective system of data protection is that the use of personal data needs to be fair; lawful; accurate; adequate; and the data itself needs to be kept for no longer than is necessary. Moreover, appropriate security and organisational measures must be taken to prevent unlawful disclosure or unauthorised access. The Data Protection Office is seen as an effective regulator trusted with responsibilities to protect the privacy rights of individuals by enforcing the provisions of the Data Protection Act.

Since its creation, my office has deployed considerable efforts to ensure that data controllers comply with their legal obligations. Among its main functions are registration of data controllers, complaints investigation, compliance audits and security checks, sensitisation, and providing advice to organisations.

The present legislation on protection of data, which dates from 2004, no longer fitted our evolving digital context and had to be updated. Thus, the Data Protection Office...
proposed a new data protection legal framework, which is based on the New European Union General Data Protection Regulation 2016/679 (commonly known as the GDPR), to make the existing Data Protection Act coherent with current technological advances thereby seeking to address the concerns of all stakeholders in a balanced manner.

Therefore, it was crucial to align our existing law with relevant international standards namely the GDPR which will come into force in May 2018 in EU Member States, and, the European Convention for Protection of Individuals with regard to Automatic Processing of Personal Data (commonly known as Convention 108), which Mauritius acceded to on 17 June 2016 at Strasbourg, France.

On a side note, Convention 108 is the first and only international legally binding instrument dealing explicitly with data protection and currently has 51 signatories including 47 Council of Europe Member States as well as Uruguay until Mauritius became the 49th State Party and the first African country. The treaty entered into force on 1 October 2016 in Mauritius. One amongst the advantages derived as being a party to the Convention is that Mauritius is considered a country with a safe flow of data to attract foreign investment. This is indeed a prestigious moment for our country.

The European Union enacted the GDPR to address the difficulties and shortcomings arising under the EU Directive 95/46/EC and to "harmonise" data privacy laws across Europe as well as to give greater protection and rights to individuals. Within the GDPR, there are large changes for the public as well as businesses and bodies that handle personal information. Likewise, the GDPR sets a stronger basis than Directive 95/46/EC for a greater level of consistency as the regulation is directly applicable in the Member States. The GDPR is also designed to address technological and societal changes that have taken place over the last 20 years by adopting a technology-neutral approach to regulation.

In view of that, the objective of the Data Protection Bill is to repeal the Data Protection Act and replace it by a new and more appropriate legislation which will strengthen the control and personal autonomy of individuals over their personal data,
thereby contributing to respect for their human rights and fundamental freedoms, in particular their right to privacy, in line with the GDPR on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

The contrast between the existing Act and the bill is that whilst the current Act sets out how an individual’s personal information can be used by companies, government and other organisations, the bill changes how an individual’s personal information can be used or controlled. It is a step change and comprehensive reform of our current data protection standards. The Data Protection Bill has recently been adopted in our Parliament on Friday 8th December 2017 and will soon be proclaimed.

The benefits of aligning the bill with GDPR are mainly to attract foreign investment through the facilitation of businesses working with European countries to transfer data therefrom. With a European market of millions of euros, this new legislation will enhance the ‘ease of doing business’ requirements and build trust between Europe and Mauritius. Moreover, a stronger and more coherent data protection framework, backed by effective enforcement will allow the digital economy to flourish by putting individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities.

Additionally, there are obligations for better data management for businesses and new rights for people to access the information companies hold about them. The Data Protection Office will have effective powers to ensure that the principles of the Act, as well as the rights of the individuals concerned, are upheld in accordance with the wording and the spirit of the bill. On this note, it is, however, important to highlight that the right to protection of personal data is not an absolute right and has to be considered in relation to its function in society. It is also closely linked to respect for private and family life protected by our Civil Code and Constitution.
Besides, an increased accountability of data controllers will make organisations implement controlled business processes resulting in better organisation, greater productivity and efficiency, and higher level of security. Thus, being compliant will also help businesses to gain and strengthen customer trust, confidentiality and loyalty. In a recent survey, carried out by Price Waterhouse Coopers (PwC) in the US, nearly all of the respondents (92%) considered compliance with the GDPR a top priority on their data privacy and security agenda in 2017.

The new data protection framework will significantly improve the digital legal landscape to respond to the new EU requirements for adequacy, thereby attracting foreign investors. The risks of data breaches will be minimised and enhanced data subjects’ rights will give individuals greater control over their personal information. The legal and practical certainty for economic operators and public authorities will be reinforced.

In conclusion, the reform rests on several pillars (key components): coherent rules, simplified procedures, coordinated actions, user involvement, more effective information and stronger enforcement powers. The major changes brought in the new legislation are as follows:

- Modernising the existing data protection principles and key definitions such as consent and personal data;
- Introducing new concepts such as data protection impact assessments, notification by data controllers of personal data breaches to the Data Protection Office and data subjects (the individuals), voluntary certification mechanisms and data protection seals and marks for data controllers and rights to object to automated individual decision-making, including profiling;
- Simplifying the complaints’ mechanism and the procedures related to hearings conducted by the Data Protection Office.

On this note, I wish you a fruitful seminar.

Thank you for your attention.