Honourable Yatindra Nath Varma, Attorney-General

Honourable Minister of ICT, Mr Tassarajen Chedumbrum Pillay

Head of EU Delegation, Mr Alessandro Mariani

Mrs Tira Greene, EU consultant

Heads of departments, parastatals, ministries and private organisations,

Distinguished Guests

Ladies and Gentlemen,

It is an honour and pleasure to welcome you all this morning to this very important workshop on 'Mauritius Data Protection Accreditation with the European Union' organised by the Data Protection Office in collaboration with the EU Delegation.

As you are aware, we are gathered today to express our concerns and views on the current legal framework for data protection in Mauritius. This is the opportunity to understand correctly what importance data

protection has in our local context and how it is applied internationally with the assistance of Mrs Tira Greene, our EU Consultant.

Information technology and especially the internet with tools like Google, YouTube, and Facebook have revolutionised our lives. They are connecting people across all boundaries of time, distance, culture, and experience. But it has also drastically changed privacy and data protection.

One Journalist of *New York Times*, Mr C.P. Snow once said:-

"Technology is a queer thing. It brings you great gifts with one hand, and it stabs you in the back with the other."

The question we are all asking ourselves today is - Does data protection from a holistic point of view really make a positive difference in our lives?

The fact is that the demarcation line between public life and private life has grown thinner, and if we do not legislate as we should, this thin line will disappear.

The reality is that extensive data banks collect and process personal data, challenging the individual's right to privacy in various ways.

Information and Communication Technologies have developed in such a way that information about us is constantly being recorded, communicated, stored and analysed, often without our knowledge, let alone our consent.

This is why the government has the duty to regulate cyberspace. But how can anything be decided concerning a space nobody owns, but whom everybody around the world is connected to just like an ombilical cord? The answer is data protection because data protection principles cut across borders and this is the reason why Mauritius has sought adequacy with the European Union to be recognised as internationally compliant. Data protection is a field of law bearing its own specificities designed to answer the tricky questions just posed. It is the legal framework to prevent unfair collection and processing of personal data.

We easily overlook the fact that every action involving technology is recorded somewhere. It can be used and it can be abused. George Orwell's famous novel '1984' constantly reminds us that we are under complete surveillance. There is a "Big Brother" watching us almost everywhere we go! Social networking sites, cloud computing, location-based services and smart cards- we leave digital traces with every move we make.

In this 'big data world' we need robust rules. Our knowledge-based economies thrive on free exchange of data. Our aim should be to preserve freedom of information and data flows, to create a level-playing field for businesses when it comes to data protection obligations, and to protect the personal data of individuals.

This reform will greatly simplify the regulatory environment and will substantially reduce the administrative burden. We need to drastically cut red tape, review the notification obligations and requirements that are excessively bureaucratic, unnecessary and ineffective. Instead, we

will focus on those requirements which would really enhance legal certainty.

Frequent incidents of data security breaches undermine consumers' trust in the online economy. Companies should beef up their precautions against identity theft and better protect consumers' personal data. They should also notify breaches of data security and confidentiality to the Data Protection Office.

I intend to recommend **a mandatory requirement to notify data security breaches to be included as a further amendment to the Data Protection Act**. I understand that a mandatory notification requirement may be considered as an additional administrative burden. However, I do believe that an obligation to notify incidents of serious data security breach is entirely proportionate and would enhance consumers' confidence in data security and oversight mechanisms.

It would also create a stronger incentive for business to conduct serious privacy impact assessments to protect personal data and to implement

the appropriate security measures protecting the confidentiality, the integrity and the availability of personal data.

We have to be as creative in our thinking on regulatory design, as those who have created and designed the internet and the cloud. Take the cloud, the story goes that the data in cross-border and cross-continent flows is impossible to regulate. This is not my vision of the future. Or take the "right to be forgotten" or the right to privacy. "Impossible" some may say. Well, I don't agree. I am sure that we can learn from all experiences to build a data protection regime fitted to our new age.

Today, we are starting the public consultation aimed at hearing your concerns, and of all those committed to a cyberspace which opens limitless opportunities, but which should never be at the expense of human rights.

I wish you all a very fruitful workshop.