WORKSHOP ON MAURITIUS DATA PROTECTION ACCREDITATION WITH THE EUROPEAN UNION

Thursday 24 November 2011
at
La Petite Canelle – Domaine Les Pailles

Speech of Hon. Yatin Varma, Attorney General

Honourable Minister of ICT, Mr Tassarajen Pillay Chedumbrum

Head of EU Delegation, Mr Alessandro Mariani

Mrs Tira Greene, EU Consultant,

Mrs Drudeisha Madhub, Data Protection Commissioner,

Heads of departments, parastatals, ministries and private organisations,

Distinguished Guests

Ladies and Gentlemen,

I am pleased to be present at this workshop organised by the Data Protection Office in collaboration with the EU delegation to discuss the reform of data protection rules in Mauritius. It is comforting to see that the Data Protection Commissioner has adopted a proactive approach to the reform by seeking technical assistance from the EU, in order to maximise the chances of securing the accreditation of Mauritius as an adequate third country in data protection with the European Union.

Mauritius has always been at the forefront in the adoption of a comprehensive package of ICT Laws namely the Computer Misuse and Cybercrime Act, the Information and Communication Technologies Act, the Electronic Transactions Act, amongst many others, which demonstrates the willingness to materialise the dream of all Mauritians, the one of making Mauritius a cyber island a reality. The ICT sector has through the constant efforts of the government now achieved the place of the third pillar of the Mauritian economy.

Ladies & Gentlemen,

The government has also placed as one of its top priorities the protection of the human rights of all its citizens- data protection being one of them. The Law Reform Commission in its last report concluded that there is a need to review the constitutional right to privacy found in our constitution in order to include data protection as one of the essential components of the right to privacy.

The UN Declaration of Human Rights provides that everyone has the right to the protection of personal data. This right is particularly important in today's world – a world in which rapid technological changes allow people to share personal information publicly and globally on an unprecedented scale.

While social networking sites and photo sharing services have brought dramatic changes to how we live, new technologies have also prompted new challenges. It is now more difficult to detect when our personal data is being collected. Sophisticated tools allow the automatic collection of data. This data is then used by companies to better target individuals. Public authorities are also using more and more personal data for a wide variety of purposes, including the prevention and fight against terrorism and serious crime.

Ladies & Gentlemen,

I am a firm believer in the necessity of enhancing individuals' control over their own data.

The security and wellbeing of our citizens is the critical concern of any government. If we want to be successful in protecting the safety of our peoples against very sophisticated enemies, then we need to show caution whilst using personal information and use the right technology and expertise to detect, disrupt and prosecute those who would do us harm.

Harm can be caused to the citizen when information is shared carelessly, so our regime has to protect the use of personal data, but must also enable the use and sharing of the personal data for legitimate purposes. There is a right balance to be struck.

Being successful in the fight against cybercrime does not require continuous and systematic

surveillance of users on the internet. Systematic tracking and tracing of users is itself in clear breach of fundamental legal principles and should therefore not be accepted. However, we must also avoid a situation where such surveillance is left to Internet Service Providers and other service providers. In other words: we should only provide for targeted measures, where required and proportionate, with all appropriate safeguards.

Ladies & Gentlemen,

Data Protection Rights should be built on three pillars:

The first is the “right of the individual to be forgotten”: a comprehensive set of new rules have to be adopted to better cope with privacy risks online. When modernising the legislation, care should be taken to allow people to have the **right** and not only the **"possibility"**to withdraw their consent to data processing. The burden of proof should be on data controllers – those who process your personal data. They must prove that they need to keep the data rather than individuals having to prove that collecting their data is not necessary.

The second pillar is "transparency". It is a fundamental condition for exercising control over personal data and for building trust in the Internet. Individuals must be informed about which data is collected and for what purposes. They need to know how it might be used by third parties. They must know their rights and which authority to address if those rights are violated. They must be told about the risks related to the processing of their personal data so that they don't lose control over their data or that their data is not misused. This is particularly important for young people in the online world.

Greater clarity is required when signing up to social networking sites. Unfavourable conditions such as restricting control of users over their private data or making data irretrievably public – are often not clearly mentioned. In particular, children should be fully aware of the possible consequences when they first sign up to social networks. All

information on the protection of personal data must be given in a clear and intelligible way – easy to understand and easy to find.

Ladies & Gentlemen,

The third pillar is "privacy by default". Privacy settings on websites often require considerable operational effort in order to be put in place. Such settings are not a reliable indication of consumers' consent. This has to be changed.

The "privacy by default" rule will also be helpful in cases of unfair, unexpected or unreasonable processing of data – such as when data is used for purposes other than for what an individual had initially given his or her consent or permission or when the data being collected is irrelevant. "Privacy by default" rules would prevent the collection of such data through, for example, software applications. The use of personal data for any other purposes than those specified should only be allowed with the explicit consent of the user or if another reason for lawful processing exists.

Our data protection reform will be vital for understanding the dangers in the all-encompassing digital world in which we live.

I thank you for your kind attention.