

**Speech of Honourable Tassarajen Pillay
Chedumbrum,**

Minister of Information and Communication
Technology,

Data Protection Workshop

Date: Monday 17 December 2012

Time: 9h30

Venue: Maritim Hotel, Balaclava

Mrs Madhub, Data Protection Commissioner,

**Heads of departments, parastatals, ministries
and private organisations,**

Distinguished Guests,

Ladies and Gentlemen,

Good Morning,

I am delighted indeed to be here today, and to be able to demonstrate my personal engagement in the common cause which brings us together that is: **Data Protection.**

Today, we are living in a world where computer speed is growing so fast that security and privacy issues have become the most important concerns of the ICT sector. Technology is being used to transfer huge databases of information electronically within a fraction of a second. The need for protecting personal, sensitive and confidential data has become the primary concern of all organisations to maintain confidentiality, availability and integrity of information. All enterprises are required to take the appropriate measures to ensure data security and protection wherever data is being used and/or stored either across networks, storage or endpoint systems.

Ladies and Gentlemen,

The Data Protection Office has deployed considerable efforts to ensure that all Data Controllers are protecting their data. A Data Controller (ie, governmental body, private company or any organisation) is required to keep only relevant data which must also never be disclosed to any unauthorized party. The Data Protection Office also ensures that each and every Data Controller has a disaster recovery and business continuity plan in order to retake the business within a minimum period after any disaster such as virus attack or any natural calamity which involves personal data.

Most of the time solution providers provide the necessary security facilities or applications such as anti-virus or firewall to prevent malware attacks. These solutions improve data governance by providing an inbuilt security

usage of personal data by enterprises. Many organisations in Mauritius can find the right solution they are searching for and they can well monitor and reduce propagation of confidential data by adopting simple security measures and informing all users to be very alert.

On the other hand, a computer is a perfect witness as it records the suspect's activities, through the user's direct words and actions. This type of evidence also assists the investigators of the Data Protection Office to carry out an investigation. In order to obtain and analyze this information in a rapid, cost-effective manner, investigators require solutions to help them produce reliable evidence for lodging appropriate charges, to identify accomplices and provide leads for other unsolved investigations.

By using many individual tools, investigators spend countless hours sieving through mountains of data, searching for information that may be relevant to their investigation.

This is why forensics tools provide investigators with a powerful platform that collects digital data, performs analysis, reports on findings and preserves them in a court vetted, forensically sound format.

Distinguished Guests,

In this workshop, the audience and the participants will have the opportunity to think about the latest Forensic Tools that:

- can automate laborious processes into a few simple steps.
- have the ability to acquire data from most commonly used operating systems and
- perform disk-level forensics on the acquired data efficiently,
- assist organisations to be able to reach case resolutions faster than ever before.

Ladies and Gentlemen,

Cloud computing is offering instant access to a large number of the world's most sophisticated supercomputers.

It also provides the service of social networking like storage, processing and software as a service to internet users. Cloud computing is often used to send messages, store photographs and upload videos.

Personal information posted online, together with data outlining the user's actions and interactions with other people, can create a rich profile of the person's interests and activities.

Consequently, freely available online information is often used by advertisers to serve targeted advertisements. Also, personal data published on social networking sites are used by any third party for a wide variety of purposes, including commercial purposes, and may pose major risks such as

identity theft, financial loss, loss of business or employment opportunities and physical harm.

Mobile security is becoming increasingly important in mobile computing as it relates to the security of personal information stored on smartphones. Users utilize smartphones as communication tools but also as a means of planning and organising their work and private life. Within companies, these technologies are causing profound changes in the organisation of information systems and therefore have become the source of new risks.

Smartphone collects and compiles an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company. All smartphones are preferred targets of

attacks. These attacks exploit weaknesses related to smartphones that can come from means of communication like SMS, MMS, wifi networks, and GSM. There are also attacks that exploit software vulnerabilities from both the web browser and the operating system. Finally, there are forms of malicious software that rely on the weak knowledge of average users.

Different security counter-measures are being developed and applied to smartphones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable applications.

Ladies and Gentlemen,

The aim of this workshop is thus to sensitize data controllers, data processors and data subjects on the need to safeguard privacy by understanding the impact of latest technologies on their personal data.

Before ending, I would like to commend the initiative of the Data Protection Office for organizing such an important workshop.

Thank you

