



**ANNUAL DATA PROTECTION DAY CONFERENCE**

**Address by**

**Mr DHANESSWURNATH THAKOOR**

**CHIEF EXECUTIVE**

**FINANCIAL SERVICES COMMISSION**

**26 JANUARY 2023**

**Honourable Mahen Kumar SEERUTTUN**, Minister of Financial Services and Good Governance

**Honourable Deepak BALGOBIN**, Minister of Information Technology, Communication and Innovation

**Mrs. Drudeisha MADHUB** – Data Protection Commissioner

**Dr. Kaleem USMANI** – Head of Computer Emergency Response Team.

**Ms. Lakshmi APPADOO** – Acting Chief Executive Officer, Financial Services Institute

Distinguished speakers

Captains of the Industry

Members of the Press

Distinguished Participants

Ladies and Gentlemen

All protocols observed.

A very good morning to you all.

Let me first thank the organisers for inviting me to share a few words on Data Protection in the financial services sector on the occasion of this annual conference commemorating the Data Privacy day. Data, ladies and gentlemen is the new gold therefore must be protected. Allow me, at the very outset, to commend the organizers for such an important theme of today, which is data protection, and iterate the engagement and strong commitment of the Financial Services Commission when it comes to data security for the consumers of the financial services and global business sector. I welcome and support this initiative as there is a need to bring together experts to discuss on how the data protection rules can be implemented effectively and further enhanced.

Ladies and gentleman,

I'll start by bringing back an old discussion which is a classic starter of basic IT classes. We were told that data is what we collect about any subject and information is how you interpret the data to make something meaningful out of it. And its relevance is even more in today's world, the world that we call "Information Age". We are all data subjects and we generate data as we go along. What we wear, what we consume, where we go and even now these days our cars, our printers, our machines are all generating data. And that data has also some connection with us. We are now what is called tightly connected real-time online systems.

Dear Audience

According to Finance-online website statistics, about 42 million messages on WhatsApp are being exchanged per minute and at the same time, 230,000 new malware versions are being created every day. It is estimated that data consumption at the end of year 2024 is expected to reach 149 zettabytes. One zettabyte is equal to one billion terabytes. And to give a scale of comparison, if we take one of those external hard disk that we have, it's about one terabyte. So we are talking about 149 billion of these discs worth of data being needed. This is massive information and a source of concern as well. And that's why everybody, regulators, policymakers, governments are worried about the way the human subject has been transformed into a massive data generating machine and there is a need to protect, to regulate the way the data is used, and to regulate the way the information is being passed on.

And we, as the regulator, we are also data subjects. We do receive data, we collect them, but at the same time, we also generate data. Data protection at the level of industry is not something new and these existed since a long time. If we take patents, copyrights, these

are all forms of data protection or intellectual protection that existed but today we have reached a stage that these massive data generation has to be harnessed in a much better way for the protection of each and every person.

Dear Audience,

At the level of the Commission, we have the duty, as a registered data controller, to ensure that the right to privacy is respected as regards personal data processed on all types of data subjects such as licencees and employees. I can state that we have got basically three ways in which we are actually concerned.

1. who is doing the action?
2. what we do? and
3. with whom we engage?

**Who is doing** is that the staff of the FSC. They are all bound by the confidentiality clause of Section 83 (1) of the Financial Services Act, thereby requiring each and every staff to take an oath of confidentiality, before the Supreme Court. And the noteworthy point in it that this is remains even after the termination of employment of the person or after retirement and it also extends to our service providers to whom we deal with.

The second part is **what we do** and the law also provides us by way of our action, what we do with the data collected, whether on the individuals or whether licencees, on the business plans etc. These are all important pieces of information that are generated on a day by day basis. And we have therefore two very important guiding principles in which we operate. First, is the part pertaining to confidentiality and to what extent we can keep information confidential to us, how do we treat it, we are all bound by confidentiality in line with Section 83 (2) and (4) of the Financial Services Act as well by the oath of confidentiality previously mentioned. The other guiding principle is disclosure requirements. We do not

operate in a vacuum and we are all connected. And therefore the law allows us to share information in specific circumstances, for example when sharing information necessary for the administering our relevant Acts, required as part of an international agreement or information is shared to another law enforcement agency, and these are spelt out in Sections 83(7) and 87 of the Financial Services Act.

Moving from there, with **whom we interact**, is also important. We are part of an international financial center and therefore information exchange is crucial. And information exchange is basically the basis and the foundation of the global business. And here I talk about due diligence that needs to be carried out, how do we verify international investors about their fitness and propriety, how do we check whether someone has been involved in some kind of financial crime in another jurisdiction. These are the interaction that we make with both domestic as well as international counterparts. Further, we voluntarily engage into Memoranda of Understanding for proper and specific type of information to be exchanged which helps to keep our jurisdiction clean. I wish to share that the FSC is signatory of over fifty MoUs with widespread and important local and international counterparts such as Autorité des Marchés Financiers, France, Financial Services Authority, Dubai and Financial Conduct Authority, UK, to name a few. And the most important one in all these is our signatory of the MMoU with the International Organization of Securities Commissions (IOSCO), which allows for technical information exchange.

This illustrates how the Commission is structured and how in today's world, it is able to use and share information in a well-defined regulatory framework that is conducive for good business. Information dissemination from a regulator is crucial in maintaining confidence in a jurisdiction and international jurisdictions with good reputations tend to have a very defined manner in which information is imparted.

Ladies and Gentlemen,

The FSC is required to be in compliance with international standard setting bodies such as the FATF. The FSC, through its legislative framework, is mandated to request, share and process data for AML/CFT purposes, while ensuring the necessary safeguards in terms of data protection and privacy. As a jurisdiction which is compliant and largely compliant with all the 40 FATF Recommendations, it is worth noting that the above is in line with Recommendation 40 which states that competent authorities should maintain appropriate confidentiality for any request for cooperation and the information exchanged, in order to protect the integrity of the investigation or inquiry, consistent with both parties' obligations concerning privacy and data protection. The FATF does emphasize on the importance of AML/CFT and Data Privacy and Protection for public interests and on the importance of information sharing between public and private sector stakeholders through Public-Private Partnerships. At the level of the FSC, we believe in public-private partnership as an essential component to building a robust financial system that guards against illicit activities and support a flourishing economy. We have walked the talk and already put in place several joint committees with our private sector representatives which meet on a regular basis.

Ladies and gentleman,

We cannot ignore the fact that the whole world is fast moving towards digitalization, we are moving more towards connected systems and in the connected systems, digitalization makes that information exchanged between parties is becoming automated, instant as well as computer managed. At the Commission, we are very much innovation focused. But at the same time, we make sure that whenever we participate into any form of data exchange, we have to ensure that we have got the necessary protection, we are within the limits and the parameters of the Act. Let me mention some of these.

We will be embarking in a number of projects going forward. One of them will be the National Insurance Claims Database whereby we will have a central repository of motor insurance related information. And for that purpose, we have ensured right from the beginning that we have all the parties together and that information exchange is made in such a way that all identity information and rights are fully protected. We have engaged our data protection officer into the processes so that we are aligned with all requirements.

The Commission is also recipient of massive data from foreign counterparts. And we plan in the coming years to come up with the concept of Digital Identity. Ladies and gentlemen the more we move in this world, the more we need to realize that the manual way of looking into data protection will not be relevant in the automated world in which we are trying to move. So that's why we are now coming up with our own digital identity and information exchange system where we will rely heavily on tokenisation and the control of these systems to ensure that the data are kept confidential and within the parameters of the law.

At the same time, we have also embarked and shortly it will come live with the recognition and acceptance of digital signatures through public key cryptography technologies and we will be able to accept digitally signed documents and therefore accelerate the pace at which we process and store information. I would also like to mention here that we pay great attention to our store of data. Since a year now we have already moved our data store to a TIER IV data center so as to ensure that we add another layer of protection and in terms of where we are storing data.

But ladies and gentleman, I'm still worried. We are living in a world of contradiction, where on one hand, the authorities are all putting rules, regulations and systems to ensure that data is well protected in the interest of the end consumers but the same time we as individuals, we are exposing ourselves and freely, giving away our own personal data to

lots of third parties. I name here the massive and extensive intrusion of social media in our daily life. People are now shedding away all personal, including biological information about yourself on the net, on social media platforms. And this all in exchange of some free services, in exchange of information that they want to share, in communities they want to partake, they want to be friends etc. But we need to be wary with whom and what we are sharing. The biggest threat that will come in the coming years will be about how it will impact our own existence in a legal framework. It is worth mentioning here that crime related to identity theft is becoming more and more common and they are all through backdoors that we leave open while we are existing as subjects in the new information world. According to a recent report from IBM, the global average total cost of a data breach has reached 4.35 million US Dollars in 2022.

With these words, ladies and gentlemen, I like to conclude that of course, the solution to all these is not a return to the age where we wouldn't have such connected systems. That's not realisable. But what we need to ensure that we people, the business, the regulators, we all together are fully data literate and able to navigate into the new data world.

Thank you.

*Dhanesswurnath Thakoor*

*26 January 2023*