Ladies and gentlemen,

The purpose of this short address is to brief you on some of the core provisions of the Regulation 2016/679, the general Data Protection Regulation or GDPR, which entered into force in May 2016 and shall be applied as of the 25th of May 2018 and to examine how these provisions apply to cyber resilience. In addition, I will attempt to explain why the GDPR is an important economic tool and how it can help boosting EU economy and social integration with a positive impact on EU enterprises.

Firstly, I must explain why we need a new set of data protection rules. The GDPR repeals Directive 95/46/EC, the main EU data protection legislation, which has served us well for more than 20 years. While the data protection principles stipulated in this Directive remain strong, its fragmentation into 28 different national legislations, globalization, technological advancements and the increasing cross – border flow of personal data, called for the need for a new legislation. The provisions of this Directive have been transposed into the Cyprus legal order by the Processing of Personal Data (Protection of Individuals) Law of 2001.

Secondly, I should explain what the GDPR aims to achieve. The GDPR has a dual purpose. It aims to protect natural persons from the processing of their personal data but, at the same time, it aims to ensure the free movement of these data. In this aspect, the GDPR is a legislative tool that regulates when personal data can move freely and when they cannot. In some cases however, the question for the free movement of data is not always clear to answer. In these cases, there should be a balance between the rights of individuals and the legitimate interests of others.

In the past decades, EU digital economy has not been competitive. One of the reasons is attributed to the lack of consumer's trust. Only 15% of EU citizens feel they have full control of the information they provide online. A

lack of trust in the old and fragmented data protection rules, held back digital economy and adversely affected EU enterprises. The GDPR provides one uniform set of rules, for all companies in the EU, which aim to keep costs down and help business grow. It will also help to boost consumer confidence and consequently businesses, taking into account the needs of Small and Medium Size Enterprises' (SMEs).

EU needs to invest in e-commerce and digital economy. To do that, companies must be encouraged to develop a culture for cyber resilience. There is no official EU definition of the term "cyber resilience", but it is commonly accepted to refer to an organization's ability to keep delivering intended services, despite adverse cyber events, such as security breaches or system breakdowns. In the US, cyber resilience is defined as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Cyber resilience relates to, but is not limited to cyber security, because it applies both to technical measures of security but also to organizational or procedural measures. Examples of cyber resilience include having power generators to stay on line during electricity blackouts, keeping backups, having disaster recovery mechanisms in place but also, calling in emergency staff, in cases of crisis, for not disrupting everyday business.

The GDPR is a technologically neutral legal instrument but several articles impose implementing appropriate technical and organizational measures of security, taking into account state of the art technology, the implementation costs, the nature and the scope of processing and the risk of varying likelihood and severity for the rights and freedoms of natural persons. In addition, the Principle of Accountability obliges businesses to be able to demonstrate their compliance with the GDPR. In simple terms, if the core activities of a company pose some cyber or other risks, the company should be cyber resilient but, also, it should demonstrate its resilience to such risks.

The GDPR follows a risk- based approach. In other words, businesses have obligations proportional to the risks associated with their core activities. Lower risk means fewer obligations to a business and higher risk means more statutory obligations. Such risks should always be eliminated or mitigated. Article 30 obliges companies to keep a record of all processing activities and to make this record available to the Data Protection Commissioner, on request. This obligation does not apply to SMEs, i.e.,

companies with less than 250 employees, unless their core activities pose privacy and data protection risks.

According to Article 35, when a type of processing is risky, in particular when using new technologies, the company should carry out a data protection impact assessment, prior to the processing and, if necessary, it should consult with the Commissioner, in line with Article 36. This is a 4 +1 steps procedure. Step 1: describe the envisaged activity. Step 2: check that it has a legal basis and that it abides the principles of necessity and data minimization. Step 3: identify possible risks associated to this activity. Step 4: implement measures for mitigating these risks. If you cannot think of any mitigating measures or if you are not 100% sure that the foreseen measures mitigate the risks effectively, then you must consult with the Commissioner.
At this point, I should elaborate a bit more on some of the core provisions of the GDPR.

The GDPR strengthens existing rights and obligations and introduces new, it promotes the principles of accountability and transparency, it strengthens the cooperation of Data Protection Authorities (the DPAs) in cross-border cases, where a number of persons is affected across several Member States and it establishes the one stop shop which stipulates that every company based in the EU and every person residing in the EU has the right to deal with and bring their case before one DPA.

I understand that many members of CIBA have offices and activities or are part of a group of undertakings that operate in several Member States or in third countries outside the EU. Those members should designate the Member State of their main establishment. In the case of cross border breaches a DPA may act as lead, competent or concerned authority and decisions on such cases will be reached in the frame of a consistency mechanism. When required, the DPAs can carry out joint investigations. DPAs have quite stringent enforcement powers. In certain cases, administrative fines may be up to 20 million euro or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Every data processing should have a legal basis. If the processing relies on consumers' consent, companies should ensure that this is given freely. There are specific conditions for consent when offering information society services directly to children. Article 8 provides that when an information

society service offered to a child is based on consent, the processing shall be lawful, if the child is at least 16 years old. For children below the age of 16, consent should be given by the person holding parental responsibility. Member States may provide, by virtue of national law, for a lower age but not lower than 13 years. Guidelines for implementing the modalities of Article 8 shall be issued in due course.

When processing relies on a contract, including the provision of a service, companies should ensure and demonstrate that the processing is necessary for the performance of that contract. Particular attention should be given to employment relationships. Special categories of personal data, that may lead to discriminations, afford a higher level of protection. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, should be based on one of the conditions of Article 9.

Companies should have mechanisms in place for the exercise of the data subjects' rights provided for, by the GDPR. These include the right to receive information, the right of access and rectification and erasure. These rights are provided by the current legislation but the GDPR strengthens them. For example, the right to erasure is elevated to the right to be forgotten, which is aligned with the 2014 milestone ruling of the Court of Justice of the European Union (the CJEU), in the famous Google Spain case, that forces search engines to remove from the list of results links to published information that infringes the right to privacy.

Particular attention should also be given to novel rights such as data portability, the data subject's right not to be subject to a decision based solely on automated processing, including profiling and data breach notification. Article 23, provides that Member States may restrict, by virtue of national laws, the exercise of the above mentioned rights and obligations. We have included some restrictions into a draft bill for the better and effective implementation of the GDPR, which shall be published soon for consultation.

Chapter IV, of the GDPR, is devoted to the obligations of controllers and processors. Particular attention should be given to data protection by default and by design, set out in Article 25, which obliges companies to

implement appropriate technical and organizational measures, such as pseudonymization, and data minimization, when determining the means for processing and at the time of the processing itself. In addition, if companies assign or outsource some processing activities to external contractors (the processors), particular attention should be devoted to Article 28 which governs the relation between companies and contractors, in their respective capacity as controller and processors.

Articles 34 and 35 of the GDPR oblige companies to inform the DPA and data subjects of data breaches, under certain conditions. Many companies fear that this obligation will have adverse effects. In the recent years we had some examples of serious breaches, by apple, yahoo and others and experience has shown that informing the affected customers did not affect their loyalty. It should also be noted that these companies did not have a statutory obligation to notify their customers, but did so in the frame of their corporate responsibility.

If the core activities of a company consist of processing operations which, by virtue of their nature, scope and/ or purpose, require regular and systematic monitoring of its customers on a large scale, according to Article 37, this company is obliged to designate a Data Protection Officer (the DPO). The position and tasks of the DPO are regulated by Articles 38 and 39, respectively. It should be noted that the role of the DPO is advisory and he acts as a liaison with data subjects and the supervisory authority. It should also be noted that all the legal responsibilities derived from the GDPR, burden the controller and the processor, but not the appointed DPO.

The European Data Protection authorities have issued a number of guidelines for the implementation of the GDPR and concerned companies are advised to study them. All the guidelines will be reviewed soon after the establishment of the European Data Protection Board, which shall replace the Article 29 Working Party, the body consisting of the heads of the 28 DPAS, that advises the Commission on data protection and privacy issues.

There are several tools for demonstrating compliance with the GDPR. Articles 40 and 41 regulate the codes of conduct and their monitoring. Codes of conduct are voluntary, but they can be used for demonstrating GDPR compliance and, also, as appropriate safeguards for the transfer of personal data from the EU to controllers or processors established in third countries who commit, via contractual or other legally binding instruments, to apply those appropriate safeguards and to respect the rights of data

subjects. The same mechanism applies to certifications, data protection seals and marks.

Transfers to third countries can be carried out on the basis of an adequacy decision where the Commission has decided that a country, a territory or a sector therein ensures an adequate level of protection. Such transfers do not require a prior authorization. In the absence of an adequacy decision, transfers can be carried out on the basis of appropriate safeguards such as standard contractual clauses adopted by the Commission or standard contractual clauses adopted by the DPA and approved by the Commission, or by binding corporate rules, approved codes of conduct or approved certification mechanisms with enforceable commitments. Where the transfer affects citizens in several Member States, it may also rely on contractual clauses authorized by a DPA in the frame of the consistency mechanism. In specific situations, transfers may be carried out on the basis of the derogations set out in Article 49 of the GDPR that may rely, inter alia, on consent, performance or conclusion of a contract and the exercise of legal claims.

The GDPR allows Member States, a degree of flexibility, on how to apply certain Articles. My Office, undertook the task of preparing a draft bill for the better and effective implementation of certain provisions of the GDPR, which, as I mentioned before, will be published soon for consultation.

In my closing remarks, I would like to repeat that the GDPR was adopted to promote social integration but also economic growth in the EU. Consumers do not trust the current EU digital economy and this situation has to be remedied. Some businesses already have a culture for cyber resilience; others need to develop such culture. If your company wishes to remain competitive, it should demonstrate its compliance with the GDPR. The GDPR should not be considered as a threat but as a tool for earning your place in constantly demanding and highly competitive markets.

I hope that with this short briefing, I have managed to give you an insight to what lies ahead with regard to the new data protection legal regime.

Thank you for your attention.

Irene Loizidou Nicolaidou
Commissioner for Personal Data Protection