Ladies and gentlemen,

The purpose of this panel 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 2016. In addition, I will attempt to explain how this legislation will help to boost EU economy and social integration and have 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.

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).

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. In addition, the GDPR provides that the Commission shall further regulate certain Articles by implementing or delegates Acts. Therefore, it should be noted, that we have a long way to go before this legislation is finalized. Nonetheless, this should not prevent businesses from taking all necessary steps to be fully prepared to implement the GDPR from day one.

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.

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. According to the principle of accountability, EU companies should be in a position to demonstrate their compliance to the GDPR. The one stop shop 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.

In cross border cases there may be competent and interested DPAs but one DPA may act as a lead authority, in the frame of the one stop shop. In cases where the involved DPAs cannot reach a consensus on how to deal with a particular cross border case, the consistency mechanism provided for in Chapter VII of the GDPR, shall be activated to ensure consistent enforcement actions. The GDPR arms DPAs with quite stringent enforcement powers. In certain cases, imposed 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.

Companies, operating in several Member States, should decide in which one they shall have their main establishment. This will determine the DPA they will have to deal with. Each company should review all its processing activities and ensure compliance with the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation integrity and confidentiality and accountability. Article 30 of the GDPR, obliges companies to maintain a record of all processing activities and update it when necessary. The same exercise, is carried out under the current legislation, with the notification obligation. The GDPR does not provide an obligation to notify the Commissioner, but forces companies to make these records available to the Commissioner, on request. Companies, should also review their privacy policies and adjust them, if necessary, in simple terms, comprehensible to children.

Every 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, which 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 the draft bill for the better and effective implementation of the GDPR, but we wish to discuss them with the Commission before we consult with interested stakeholders, both in the public and the private sector.

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 organisational measures, such as pseudonymisation, and data minimisation, both at the time of the determination of the means for processing and at the time of the processing itself, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons. If 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.

Other Articles of Chapter IV of the GDPR, oblige companies to keep the records of processing activities, already mentioned, to cooperate with the supervisory authority, to inform the DPA and data subjects of data breaches, under certain conditions, to carry out data protection impact assessments, in particular when considering new technologies and to consult the Commissioner when an impact assessment indicates that the processing would result in a high risk in the absence of measures taken to mitigate the risks for the data subjects. DPAs, shall adopt and publish a list of processing operations that require an impact assessment and may adopt and publish a list of operations that do not require one.

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 guidelines for data portability, data protection impact assessments, data protection officers and lead authorities and soon will issue additional guidelines for consent, profiling, data breach notifications and profiling. You are strongly advised to thoroughly study these guidelines and to regularly check my Office’s website for updates. 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.

Articles 40 and 41 regulate the codes of conduct and their monitoring. Codes of conduct, which are voluntary, can be applied 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 respect the rights of data subjects. The same mechanism applies to certifications, data protection seals and marks. Despite such certifications seals and marks being voluntary, they can be applied as a toolkit for demonstrating compliance with the GDPR or for the transfer of data to third countries, in line with GDPR Article 46(2)(f).

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.

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 are more privacy friendly than others. If your company wishes to remain competitive, it should demonstrate its compliance with the GDPR. The GDPR should not been 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

25/09/2017