Ladies and Gentlemen,

Firstly I would like to thank you for the invitation to brief you on how the new General Data Protection Regulation (GDPR) will strengthen the fundamental rights of the individuals in a technologically driven environment.

The right to the protection of an individual's private sphere against intrusion from others was laid down in an international legal instrument for the first time in Article 12 of the United Nations Universal Declaration of Human Rights (UDHR) of 1948 in respect for private and family life. The UDHR influenced the development of other human rights instruments in Europe.

The Council of Europe was formed in the aftermath of the Second World War, to bring together the states of Europe to promote the rule of law, democracy, human rights and social development. For this purpose, the European Convention on Human Rights (ECHR) which was adopted in 1950, was entered into force in 1953.

Under Article 8 of the ECHR, a right to the protection against the collection and use of personal data forms part of the fundamental right to respect for private and family life, home and correspondence, was established.

The Convention 108 of the Council of Europe was the first international legally binding instrument dealing explicitly with data protection.

The European Court of Human Rights has examined many situations in which the issue of data protection arose, concerning interception of communication, various forms of surveillance and protection of the rights of individuals, in respect of their personal data.

It has clarified that Article 8 of the ECHR obliges states to comply with Convention 108 and ensure that the right for private and family life is fully respected.

Under EU law, data protection was regulated for the first time by the Directive 95/46/EC on the protection of individuals regarding the processing of personal data and the free movement of such data. The territorial application of the Data Protection Directive, extends beyond the 28 EU Member States, including also the non-EU Member States that are part of the European Economic Area, that is Iceland, Liechtenstein and Norway.

The Charter of Fundamental Rights of the European Union became legally binding with the Lisbon Treaty, which came into force on 1 December 2009. The Charter not only guarantees respect for private and family life (Article 7) but it also establishes the right to data protection (Article 8), as a fundamental right in EU law.

In January 2012, the Commission proposed a data protection reform package in order to adapt to the new technological advancements, globalisation and the increasing cross-border flow of personal data, leading to stronger data protection rights. The package includes the General Data Protection Regulation (GDPR), which replaces the Data Protection Directive and the General Data Protection

Directive, which provides for data protection in the areas of police and judicial cooperation in criminal matters.

Under the GDPR, the data protection principles set out the main responsibilities for organisations. The principles are similar to those in the current legislative framework, with a new accountability requirement. The GDPR requires the implementation of measures by organisations to promote and safeguard data protection in their processing activities. Organisations should be able at any time to demonstrate compliance with data protection provisions to individuals and to supervisory authorities.

For processing to be lawful under the GDPR, organisations should determine the legal basis for processing personal data. If the processing relies on the person's consent, organisations should ensure that, it is freely given, it can be withdrawn at any time and that the privacy notice is written in an intelligible and easily accessible form, using clear and plain language. Equally important is that, organisations shall be able to demonstrate that individuals have consented to the processing of their personal data.

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.

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.

The GDPR creates **some new fundamental rights for individuals and strengthens some** of the rights that currently exist.

Individuals will also have **to be informed** about the retention period of their personal data, their right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal and their right to lodge a complaint with the supervisory authority.

The GDPR clarifies that the reason individuals **can access** their personal data is to be aware of and verify the lawfulness of processing. The right of access demonstrates that, individuals can obtain from an organisation confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, they can be provided with a copy of their personal data, free of charge. Where they make the request by electronic means, the information shall be provided to them in an electronic format.

In addition, individuals are entitled to **have their personal data rectified** if it's inaccurate or incomplete. If an organisation does not rectify the information, it

must explain the reason to the individuals, informing them of their right to complain to the supervisory authority.

Also known as "**right to erasure", the right to be forgotten** entitles individuals to obtain from an organisation the erasure of personal data concerning them, without undue delay and cease further dissemination of the data. The conditions for erasure, as provided in article 17, include the data no longer being necessary in relation to the purposes for which they were collected, or withdrawal of consent by an individual.

Instead of requesting erasure, an individual can request a **restriction of the processing** of its personal data. Restriction can be requested for example, in case the personal data is inaccurate or unlawful or the individual no longer needs the information but it requires it to establish, exercise or defend a legal claim.

Further, individuals have the **right to object** to processing based on legitimate interests or the performance of a task in the public interest, including profiling, to direct marketing and to processing for scientific or historical research purposes and to statistical purposes. Organisations must inform individuals of their right to object "at the time of first communication" and in their privacy notice.

When personal data is subject to automated processing on the grounds of consent or a contractual agreement, the data subject has the **right to data portability**, which can be seen as an extension of the right of access.

Last but not least, the GDPR provides safeguards for individuals against the risk that a potentially negative decision is taken without human intervention. That is, they have the **right not to be subject to a decision when it is based on automated processing, including profiling**, which produces legal effects concerning them or similarly significantly affects them.

The aim of the GDPR, which replaces the current legislative framework, is to protect all EU citizens from data breaches in a world that is much different from the time in which the 1995 Directive was established.

Organisations will be obliged to take every possible organisational and technical measure to fulfill the rights of the individuals as they are facing strict administrative fines up to 20 million Euros, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is the higher.

This new legal framework for the protection of personal data is a robust change towards data transparency and empowerment of individuals.

Thank you very much for your attention.

Irene Loizidou Nicolaidou November 14, 2017

Commissioner for Personal Data Protection