Dear Chair person,

Distinguished guests,

The issue of safer internet is one of the biggest challenges of our era. The debate for making internet safer, has been addressed by the industry, practitioners, academics and regulators for many years and it shall continue to puzzle them for years to come.

In my view, there is NO correct answer to the question HOW DO WE MAKE INTERNET SAFE. In my view, the correct way of stipulating the question should be, HOW DO WE MAKE INTERNET SAFE **TODAY**.

This is due to two reasons. Firstly, not everyone agrees on what we perceive as safe internet. It is a matter of different perspectives or, to say the least, of tackling the same problem from different angles. Secondly, what we consider as safe TODAY may not be safe by TOMORROW. At a time where the line between our activities in the natural and the digital world is thinning to a blur, I believe it is important to ask three very important key questions:

What do we understand by safe(r) internet?

What is the role of the legislator in the emerging digital era?

How do these questions relate to core data protection issues?

<u>Safer Internet</u>

The concept of safe internet is understood differently by various stakeholders.
For social networks, it means building a safe environment where users can socially mingle as they would in the real world.
For advertisers, it means pursuing legitimate goals like monitoring on line and off line behaviors with aim to provide more targeted advertising.
For commercial stakeholders, safer internet means expanding the markets through e-commerce.

And from the parents' point of view, safe internet means protecting the rights of their children.
As regards data protection Authorities, safe internet is about ensuring the privacy of the users and consumers. After all, as it has been said repeatedly, personal data are the hard currency of the 21st century.

All these views can be summed up in two words: **building trust**. On a number of occasions, Justice Commissioner Ms. Jurova and her predecessor Ms. Reading have recalled that, one of the primary aims of the General Data Protection Regulation (the GDPR), which is expected to be adopted in the coming months, is to build on EU citizens' trust. Providing a robust legislation, among other things, will promote e-commerce and boost EU economy, will enhance citizens' rights in relation to their privacy and the processing of their personal data and it will give enterprises a uniform legal frame to carry out their activities, both across the Member States but also outside the Union. To that effect, the Commission, pursuant to the revocation of the Safe Harbor Agreement, has been working towards the new Privacy Shield Adequacy Decision, which I will attempt to outline in a while.

The role of the legislator

Due to rapid technological developments, it is literarily impossible, for any legislation, to foresee and prevent the challenges/ threats laying ahead. Therefore, the role of the legislator, when regulating safe internet, is to put the horse in front of the cart. This means that, instead of acting retrospectively, the legislator should provide the legal frame for technology to develop in the coming years. Technology, should be developed in line with the legislation. Legislations adopted in reaction to technology are bound to fail. While the GDPR remains technologically neutral, it aims to provide the legal frame within which technology should develop in the coming decades.

The GDPR does not have all the answers. Take for example the controllers' obligations with regard to the processing of children's personal data. Article 8 sets out the conditions applicable to children's consent in relation to information society services. It provides that, when *the offering of information society services*

directly to a child is based on consent*, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.* Furthermore, it provides that *the controller shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology.*

Article 8 of the GDPR is one of the cases where the horse has been put in front of the cart, in a technologically neutral legal instrument. While it creates a clearly defined binding obligation to obtain the consent of the holder of parental responsibility over the child, it does not regulate the modalities for the implementation of this obligation. It simply states that available technology should been taken into consideration.

The role of the DPAs

The GDPR strengthens the role of the Data Protection Authorities. The Article 29 Working Party, is an independent institution composed of the 28 Data Protection Commissioners and the European Data Protection Supervisor. It was established under Article 29 of Directive 95/46 and has only a consulting role. The European Data Protection Body (EDPB), which will substitute the Article 29 Working Party, will still have a consulting role but it will also be empowered to issue binding decisions, in certain conditions provided for by the GDPR. The Article 29WP has adopted an Action Plan for road-mapping things that have to be done before 2018, when the GDPR will be put into effect. For example, in the case of Article 8, the EDPB will issue guidelines to controllers for the modalities for obtaining the consent of parental responsibility holders.

The Article 29WP worked extensively on the draft Privacy Shield Adequacy Decision. The Privacy Shield was negotiated between the EU and the US, pursuant to the annulment of the Safe Harbor Decision by the Court of Justice of the European Union, in the case of Maximillian Schrems vs Irish Commissioner. But, I believe it is best if I leave it to Mr Schrems to explain the particularities of this

milestone ruling. I should add however that, last week, the Art.29WP issued an Opinion, summarizing the collective concerns of the DPAs in relation to the Privacy Shield. While it welcomes the first draft as a significant improvement in relation to the invalided Safe Harbor. The Art.29WP urges the Commission to resolve these concerns, identify appropriate solutions and provide the requested clarifications in order to improve the draft adequacy decision and ensure that the protection offered by the Privacy Shield is, indeed, essentially equivalent to that of the EU.

Conclusions

To conclude, as far as Data Protection Authorities is concerned, safe Internet means ensuring the rights to privacy and personal data protection, both online but also offline. Legislating safe internet requires putting the horse in front of the cart. The role of the Data Protection Authorities is to supervise and ensure the application of the legislation but also, to give guidance for the implementation of the rulings of the European Courts.

Thank you for your patience.