JOINT STATEMENT on GDPR

16 October 2013

Europe's e-communications industry is convinced that the GDPR is an important piece of legislation which will contribute to boosting economic and social growth in Europe. To achieve this will require the right balance between protecting the fundamental right to data protection and privacy and ensuring that business and innovation can flourish within a truly uniform single market. We believe it is possible to achieve a framework that is both future-proof and flexible enough to allow the development of new services in Europe, while maintaining Europe's high standards in the protection of personal data and privacy.

Data drives the new digital economy and is fundamental to a knowledge-based modern society. Care should be taken to ensure that economic growth and development are not impeded by disproportionate and unnecessary regulation and our members remain committed to responsible business practices and accountability in respect of European citizens' rights to data protection and privacy.

With a view to the upcoming LIBE Committee vote, the Associations noted above would like to highlight the following issues which we hope will serve as constructive input to the discussions and the ambitious political timeline:

CONSISTENCY IN LAW: THE NEED TO ACHIEVE A LEVEL PLAYING FIELD FOR CONSUMERS AND BUSINESS

Our Associations call on the EP to ensure the GDPR facilitates a level playing field between all actors of the ICT value chain in order to guarantee a consistent experience of data protection and privacy for all consumers. We believe that EU citizens' personal data should be granted the same level of protection, regardless of the geographical location or the economic sector of the service provider ("same services, same rules"). Therefore, our Associations strongly support the suggested territorial scope of the GDPR applying the same rules to the processing of EU citizens' personal data irrespective of the location of the service provider.

However, the current proposals and discussions do not address the inconsistencies between the GDPR and the ePrivacy Directive (ePD) and their impact on the internal market and consumer experiences and protections. In order to achieve a comprehensive technology neutral framework, it is of utmost importance to treat functionally equivalent services and data equally in terms of legislation. Our Associations would like to stress that the latter element has not yet been achieved by the Commission proposal and as such, needs to be addressed by the Council and the European Parliament by eliminating the inconsistencies between the new Regulation and the ePrivacy Directive. It is vital that a dual regulatory regime for the e-communications industry is avoided.

FUTURE PROOFING: A RISK BASED APPROACH

The principle of a risk-based approach should underpin the Regulation (eg: formalities of consent, definition of personal data). The GDPR should recognise more the importance of the context in which data are captured and used and risks emerge, and support measures to address any such

risks. We believe risks can be mitigated by adopting key GDPR articles on privacy by design, impact assessments, and by the use of anonymisation and pseudonymisation and other accountability measures that also consider the user experience and that facilitate understanding and choice.

A risk-based approach is useful in addressing areas such as consent and profiling for example:

An **explicit consent** model is not appropriate for all online contexts and should be reserved for those contexts and categories of data that present the highest risks. Data is often collected and shared across borders in real-time, simultaneously between multiple parties. An over reliance on an explicit consent regime may burden users and lead to notice and choice fatigue, numbing people to the importance of making privacy decisions when it matters. An excessive consent regime may lead to less, not more privacy.

A risk based approach would focus efforts on ensuring those data and contexts presenting a risk of real harm for individuals are to be subject to a higher degree of protection, and risk mitigation designed into products, services and business processes.

Profiling happens every day across a number of industries and services to the benefit of European society. Profiling per se is not negative. Issues such as location-based customer care or customized offers tailored to an individual's needs simplify the day-to-day life of European customers and citizens. The economic opportunities inherent to data analytics do not require that individuals' privacy be sacrificed and vice-versa. Therefore, any legislative effort should be focused on the potential adverse legal effects of the decisions taken on the basis of profiling. If the profiling activity has no adverse impact on an individual, it does not cause any harm. On the contrary, it will most likely streamline the efficiency of a number of services provided to the society.

Privacy assurance mechanisms allowing the processor to demonstrate its compliance with the Regulation is an element of the risk-based approach considered in the Council which is supported by our Associations as it could significantly reduce red tape.

INTERNATIONAL TRANSFER OF DATA

European and global companies have a substantial economic need for cross-border data flows between countries and regions with sometimes very different privacy regimes. Facilitating responsible and privacy protective international data transfers is therefore key. Steps to further simplify international data transfers are important in order to reduce administrative burdens of EU/EEA businesses, to strengthen international trade and the international competiveness of EU businesses, while at the same time ensuring that citizens' personal data will benefit from the same level of protection as if they were in the EU/EEA.

Closely connected to this topic is the urgent need for the European Commission to conduct a transparent review of the current Safe Harbor Agreement, due since 2008, to include a review of the oversight and enforcement mechanisms.