November 2011

A new Regulatory Framework for Data Protection.

Our organisations (CableEurope, ECTA, ETNO and GSMA Europe) represent the full spectrum of industry players involved in the European electronic communications industry, incorporating fixed and mobile telecoms operators, Internet services providers and cable companies. Our industries provide access, hosting and content services to European consumers, helping to create a platform for strong economic growth via eCommerce and innovative eServices. Our members are both national and pan-European players and can therefore provide a unique insight into the impact of Europe's data protection legislative framework from both a business and consumer perspective.

As an industry coalition and throughout the data protection review process, we have brought to the attention of various EU policy makers some of our main concerns and proposals. We believe that the key outcome of the legislative review should be to establish a user-centric privacy framework that empowers users and supports business innovation.

At this juncture, we wish to outline some priority considerations on the future of data protection in the European Union, which are as follows:

1. Harmonisation and enforcement
2. Innovation and the role of self-regulation
3. Consistent privacy experience for individuals and businesses: equivalent services, same rules
4. Accountability and privacy by design
5. International data transfers

1. Harmonisation and Enforcement

The overriding objective of the Data Protection Directive review should be to provide data subjects with a uniform privacy experience irrespective of where the data subject and the data controller are located within the European Union. It is thus imperative to have a data protection framework that is harmonised to the greatest extent possible across Member States. While EU/EEA-wide coordinated and uniform enforcement has an essential role to play in the application of the data protection

framework, it is critical from the outset that we do not have a legal instrument that can be interpreted in different ways by Member States when being transposed into national law.

A non-consistent application of privacy rules across Member States is burdensome for businesses that are providing equivalent services across different Member States since they are required to maintain different compliance regimes which results in increased costs. Therefore, the new legal framework must not leave any room for ambiguity.

In order to improve privacy levels and support a consistent privacy experience for data subjects while reducing administrative burdens and cross-border restrictions, a preferable legal instrument would be a Regulation rather than a Directive. A harmonised approach will facilitate the free movement of data and will also foster the necessary consumer confidence and trust to strengthen economic growth.

2. Innovation and the role of self-regulation

Consumer trust, both in the ICT industry's business conduct and security standards, as well as in the ability of governments to enforce consumer protection standards effectively, has a major impact on the growth of the digital economy. A consistent and high level of data protection is in everyone's interest, given the ICT industry's contribution to such growth. It is therefore both a business objective and an overarching public policy objective to ensure that the right privacy framework is in place and to ensure that the consumer is adequately protected.

Having said that, it is of equal importance that measures for the promotion of data protection are designed in such a way so as to not slow down or impede consumers' online experience and so as not to prevent businesses from executing against the vision and objectives of the Digital Agenda at a time when its achievement is crucial for Europe. Innovation requires the inclusion, not exclusion, of the consumer. All efforts should focus on maintaining a healthy environment that encourages innovation and prevents excessive and burdensome regulation that could stifle innovation, development and the uptake of new technologies.

In this context, the important role of self-regulatory initiatives should be encouraged and prioritised. Self-regulation that includes the principle of accountability can work well to recognize the dynamic nature of privacy and ensure the protection of individuals. Self-regulation is able to respond in a timely and effective manner to changes in technology and business models than ex-ante regulation or ex-post measures by data protection authorities.

The current code of conduct regime stated in Art 27 of the 95/46/EC Directive does not provide the flexibility and encouragement needed to secure privacy in the development of new technologies. We propose a new, modernised and more compliant provision in the new privacy framework, which defines the possiblity of self-regulation and also clearly stipulates the pre-requisties. A lower level of supervision by data protection authorities could be granted to those companies that adopt self-regulatory regimes.

3. Consistent privacy experience for individuals and businesses: equivalent services, same rules

Individuals located in the EU/EEA should be granted the same level of protection for personal data, regardless of the geographical location, technology used or the economic sector of the service provider ("equivalent service -same rules"). Data protection rules should be flexible, technologically neutral and should horizontally apply to all economic sectors and actors targeting and processing personal data of individuals located in the EU/EEA. Therefore, sector specific regulation for parts of the ICT value chain is inappropriate and inadequate, also in light of the constant development of new services which are difficult to categorize within the current definitions used in the ePrivacy Directive.

Data protection rules should apply to processing activities following a risk-based approach. They should be triggered by the harm or potential harm caused by the processing to data subjects, irrespective of the geographical location within the EU/EEA or in third countries or economic sector in which the data controller is active. Uniform rules and their application are of utmost importance to individuals located in the EU/EEA, in order to build the same level of protection and therefore confidence in using more ICT-developed services. Such an approach will not only benefit consumers but will improve the competitiveness of EU/EEA-based companies.

4. Accountability and privacy by design

The reviewed data protection framework should move towards principles that build on increased accountability for all actors involved in data processing. Adopting principles building on accountability for actors across the value chain means that private and public organisations are responsible for the handling of data, beyond simple compliance. For instance, the development of Binding Corporate Rules, the appointment of Data Protection Officers and the adoption of voluntary Privacy Impact Assessments are all instruments reflecting the concept of accountability. In this context, Privacy by Design should be understood as a concept aimed at encouraging organisations to incorporate the concept of privacy into devices and processes and it should not be confused with the concept of Privacy by Default, which seems to entail yet another layer of ex-ante obligations.

A move from an ex-ante regime based on compliance to a more flexible and future-proof ex-post legal system underpinned by the accountability rule requires enhanced transparency, proportionality and enforcement mechanisms. As private organisations should be accountable for their handling of data vis-à-vis individuals, public authorities should ensure increased transparency, accountability, proportionality and judicial control in respect of all demands made to ISPs and other intermediaries for data related to their customers.

5. International data transfers

International data transfers are a key issue for the competitiveness of European companies. However, the current rigid EU rules applying to the transfer of data to third countries no longer seems appropriate. Considering the new economic reality, personal information flowing across borders has become the norm. In complex situations with multiple data controllers, processors and jurisdictions (e.g. cloud computing,) the current provisions of the Directive may severely impede the

free flow of personal data and, thus, the development of economic activities outside the EU by EU-based companies. Information flowing across borders is becoming the norm and the routes are less defined by point-to-point communications but rather by a number of different actors with varying different roles and responsibilities. Therefore, generally, international data rules need to be modernized and simplified between companies and within a 'group of companies'

In order to address these shortcomings, we believe that the future EU legal framework should recognize the concept of "group of companies" as referred to in the Madrid Resolution of data protection authorities. Internal privacy policies of multinational groups would then include the guarantees that the transferred personal data will benefit from the same level of protection as if they were processed within the EU borders. Such an approach would imply that instead of considering single data transfers as adequate or not based on the country of destination, the assessment of adequacy would be based on the accountability of the data controller. Irrespective of whether the data transfer is within the same EU Member State, within the EU/EEA or outside the EEA, the data controller would be held liable for the protection of personal data. This approach also seems compatible with the principle of 'accountability'.

In addition, Binding Corporate Rules currently only apply to data controllers. In an increasingly complex on-line environment, the revision of the directive should also include the possibility of an internal governance model to cover the processing of personal data by pan-European and multi-national players (eg. Binding Safe Processor Rules).

Conclusion

The review of the Directive 95/46 is an opportunity to modernize and adapt the existing data protection provisions to reflect important technological and societal developments that have occurred in recent years as a result of becoming a globally connected society. The new framework should be forward-looking and capable of supporting future generations and technology trends. Europe has an opportunity to provide thought-leadership in this area and to create an innovative and flexible approach that allows businesses to grow and provides consumers with the confidence they need to embrace all that the ICT sector can offer. Our coalition is ready to work with the European Institutions and other stakeholders to address these issues, in order to help achieve an efficient, effective and competitive Digital Single Market.