VERBAND DER INTERNETWIRTSCHAFT E.V.

Comments on the ePrivacy Regulation

Brussels/Berlin, 30 May 2017

The European Union's proposal for an ePrivacy Regulation[1] was presented on 10 January 2017. In a very tight timeframe, the Commission plans on the proposal being passed in the European Parliament within the year. eco has already commented on the proposal in detail[2] and warns against the Regulation being passed too quickly. eco recommends that central aspects are re-examined and it should be ensured that substantial changes are made in the proposed regulation.

The following aspects, in particular, should be re-examined:

- **A regulation for the processing, storing, and erasure of electronic communication data, in particular metadata**

The ePrivacy Regulation requires that electronic communications content is to be deleted or anonymised by the provider once the recipient has received it (Art. 7 lit. 1). This also applies to the metadata that accompanies such communication. Both aspects are problematic. The unclear definitions provided in Article 4 of the ePrivacy Regulation (especially Art. 4 lit. 3 a-h) give rise to the question of which data is to be categorised and how it is to be dealt with. Not only is this aspect of the Regulation unclear, but it is also too restrictive. The deletion or anonymisation of communication content is a very strict and far-reaching rule, which is complicated by the ambiguous definition of the term anonymisation.

Article 6 restricts the further processing of metadata (Art. 6 lit. 2) to a narrowly-defined area. This article should be revisited, particularly in regards to how metadata is dealt with. A restriction of the use of metadata just for invoicing purposes and for the fulfilment of legal requirements impacts heavily on the testing of and research into new procedures. The European General Data Protection Regulation (GDPR) has a broader legal scope for such usage. Particularly in a field which is characterised by high pressure to innovate, it allows the further processing of data without previous consent – with limitations. This can then be used for statistical purposes, for research purposes, and for other reasons (as laid out in Article 5, GDPR).

[1] Proposal of the European Commission for a Regulation of the European Parliament and Council Concerning the Respect of Private Life and the Protection of Personal Data in Electronic Communication and Repealing Directive 2002/58/EG (COM (2017) 10 final)

[2] The detailed commentary can be found here: https://www.eco.de/wp-content/blogs.dir/20170228_eco_pos_eprivacyreg_en-final.pdf

This flexibility is vital for companies that are headquartered in Europe, and therefore depend on European customers, to compete with global players. The debate that the draft ePrivacy Regulation has sparked over the legality of heat maps to track network usage or malfunctions illustrates how essential the use of metadata is, and how poorly conceived the current proposal from the Commission is.

The regulations foreseen in Articles 6 and 7 of the ePrivacy Regulation are too broad, not specific enough, and not suited to developing a European data economy. They actually pose the risk of undermining current practices which are already in place in inventory management (e.g. e-invoicing, enterprise resource planning (ERP), industry 4.0) or which could be useful for the roll-out of broadband, or perhaps later for traffic planning (e.g. smart cities, connected cars). In regard to the storage and processing of electronic communication data, the articles should be oriented on Articles 5 to 11 of the GDPR. eco sees the further processing of metadata, in particular, to be vital to developing better services in general.

In order to achieve this, the definitions in Article 4 of the ePrivacy Regulation should be checked, and Articles 5 and 6 should be fundamentally reworked. This is connected to the requirement to store metadata for further processing foreseen in Article 7. Automated communication and, in particular, machine to machine (M2M) communication must stay possible in a business (B2B) context.

- **The distinction between data collected independently and contracted data processing must be harmonised with the GDPR**

The current requirements of Article 8 lit. 1 d of the ePrivacy Regulation restrict the use of website metrics solely to the provider of the service. This is a requirement which ignores the reality of the division of labour in the digital economy and is likely to strongly disadvantage smaller providers and even force them off the market. To what extent this use of special high-quality analytical tools represents a problem for electronic communication is not addressed by the proposal.

It goes substantially beyond the framework of the GDPR, which sees the processing by other parties as both possible and legal (see Article 28 GDPR). Such contracted data processing should be possible – and not undermined by over-regulation – in a digital economy which is increasingly specialised and characterised by a clear division of labour.

The distinction between the direct collection of information by the service provider or by a third party does not represent a plausible distinction between them in terms of their respect for confidentiality and for data protection. It is often the case that appropriate, high quality, secure, and legally conform data protection is to be provided more likely from a specialized service provider.

The existing regulation also does not help in overcoming the “consent fatigue” created by the current ePrivacy Regulation (Directive 2002/58/EC), which is seen as a central problem when using website metrics like cookies.

Article 8 lit. 1 d of the ePrivacy Regulation should therefore urgently be amended, using the GDPR as a basis.

- **No European blanket data retention or back door for services**

A guideline for a standardised process for the development of “internal procedures” to answer requests from public authorities is formulated in Article 11 lit. 2 ePrivacy Regulation. The formulation is very imprecise and gives rise to the suspicion that a “universal back door” is being created, which can then be used by investigative authorities. Such back doors, however, are then not only open to investigative authorities, but also to other attackers. There is also the risk that such “internal procedures” include the obligation to collect and store certain user data (real names, postal addresses, etc.).

eco strongly rejects such measures. Given the unclear requirements foreseen in Article 11, eco advises against including it at all in the ePrivacy Regulation and recommends that Article 11 is to be left out completely.

About eco

eco – Association of the Internet Industry represents the interests and fosters all companies that create economic value with or in the Internet. The association currently represents more than 1,000 member companies.

These include, among others, ISPs (Internet Service Providers), carriers, hardware and software suppliers, content and service providers, and telecommunication companies. eco is the largest national Internet Service Provider association in Europe.