Comments on recent Council Presidency texts on ePrivacy

This document includes views of the American Chamber of Commerce to the EU (AmCham EU) on the recent text proposals published by the Bulgarian Council Presidency, including the Presidency text from 7 March 2018[1], discussion paper from 22 March 2018[2] and Presidency text from 13 April[3]. These views draw from the 2017 AmCham EU position paper[4].

Key message

1. **We welcome attempts by the Presidency to introduce more flexibility into the Commission proposal**
2. **However, alignment with the General Data Protection Regulation (GDPR) does not go far enough. The regulation continues to focus on regulating processing rather than interference.**
3. **More flexibility is needed on permitted processing of communication content and metadata**
4. **AmCham EU continues to advocate for a technology-neutral approach and calls on legislators to consider the impact of the suggested restrictions beyond cookies and browsers.**

Recommendations

Alignment with the GDPR

We note and welcome the Presidency's attempts to clarify the relation between the ePrivacy proposal with the GDPR as highlighted in **recitals 2a and 2 aa** (Presidency text 7 March 2018). However, this does not address the problem of identifying whether any legislative gaps are left after the entry into force of the GDPR, which should be the actual focus of the ePrivacy Regulation. Furthermore, these recitals do not go far enough as the proposed wording here and in other provisions does not resolve the problem of overlap and divergences between the two set of rules.

The lack of clarity between the GDPR and the proposed ePrivacy Regulation stems from the fact the latter continues to confuse the concept of data protection (regulating the processing of data related to individuals) with confidentiality (protection of communications from unauthorised access by third parties during transmission). These rights are intentionally separated in the EU Charter of Fundamental Rights (Articles 7 and 8) and that same separation should be reflected in both legal instruments. The GDPR should comprehensively provide for data protection, while the ePrivacy Regulation should protect the confidentiality of communications.

[1] Document 6726/18: http://data.consilium.europa.eu/doc/document/ST-6726-2018-INIT/en/pdf
[2] Document 7207: http://data.consilium.europa.eu/doc/document/ST-7207-2018-INIT/en/pdf
[3] Document 7820/18: http://data.consilium.europa.eu/doc/document/ST-7820-2018-INIT/en/pdf
[4] http://www.amchameu.eu/position-papers/position-paper-amcham-eu-position-paper-proposal-regulation-e-privacy

AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

American Chamber of Commerce to the European Union
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
amchameu.eu • European Transparency Register: 5265780509-97

More information:
Name Surname
xxx@amchameu.eu

Data in transmission

In the light of the previous comment (overlap with the GDPR), the concept of 'transmission' should be defined narrowly, according to existing protocols and distinguish real-time communications from asynchronous communications. It should also be noted that including data in transmission in the scope is problematic in the context of machine-to-machine communications (M2M), as noted in the following section.

Clarifications through recitals, while welcome and helpful, are insufficient without the introduction of similar clarity in a corresponding provision of **Article 5**, which currently does not state that the prohibition in 5(1) is limited only to when electronic communications data is in 'transit'. Instead, Article 5(1) suggests that it does apply to stored data as it uses the verb 'processing' which under the GDPR (Art 4(2)) clearly includes actions related to stored data such as 'organisation', 'structuring' and 'storage'.

The proposal attempts to clarify the scope regarding data 'in transmission' (**Recital 2a, recital 15 a** – Presidency text 7 March 2018). However, instead of focusing on trying to define the moment for a specific technology when the transmission phase ends, the wording should be simplified and clarify that the transmission phase ends with the provider of the electronic communication service provider and not the end-user.

Machine-to-machine communication

The Presidency texts remains silent on the applicability of the prohibitions proposed to M2M communications. We would like to reiterate that AmCham EU does not believe such services should be included in the scope.

Inclusion of processing during transmission in the scope reduces the currently available legal bases for such processing from the wider set of legal bases available under GDPR for personal data (e.g. legitimate interest, performance of contract or public interest) and/or unregulated processing of non-personal data. However, computing in the Internet of Things context is increasingly moving closer to the sensor, in phenomena known as 'edge computing' and 'fog computing'. The added value is to decrease bandwidth, overcome unreliable connectivity, increase reliability, reduce latency and improve security and privacy. This processing takes place during transmission and hence would be covered by the Regulation as currently drafted.

This could be particularly problematic in use cases where the M2M service is self-provisioned by an organisation but does not include processing of data of individuals (e.g. smart agriculture sensors). If none of the additional legal bases for processing the data are relevant (which is more than likely as no personal data is involved), it is unclear how consent would be used as there is no obvious end-user in a self-provisioned service.

It could also be problematic in use cases where the entity providing the service does not have a direct contractual relationship with the end-user. One example is smart traffic management – such as smart traffic lights - where road users' data may be processed but there is no user interface providing the possibility to obtain consent. This would not be an issue under GDPR as either public interest or legitimate interest would be valid legal bases to process the data.

Furthermore, the presidency text now insists even more on the applicability to both legal and natural persons (as **Recital 2aa, 2a, Art 1a, Article 5**). As we underlined in the past, legal persons benefit from a range of protection, and should be excluded from the scope – as they are excluded from the GDPR.

Ancillary services

We welcome attempts to clarify that **ancillary services** are only covered if there are interpersonal communications services (**article 11 a**). However, we remain concerned about its broad scope and wonder why there is a need for such a catch-all clause. It does not seem proportionate to the risk of processing such communication data.

Deletion of communication data

As we noted in our previous positions, storage and erasure of data should be context-based to reflect different users' expectations for different types of services and questioned whether a one-size-fits-all approach is in line with user expectations. Instead of the proposed Recital 15a and Article 7, we suggested the following language to achieve this objective:

Article 7 - 'Without prejudice to Article 6, the provider of the electronic communications service shall erase electronic communications content or process such data in accordance with Regulation (EU) 2016/679'.

Security

We welcome the introduction of an exception to permitted processing for ensuring network and information security (**Recital 8** - Presidency text 7 March 2018). However, we see some contradiction in the different texts proposed by the Presidency at this point. On the one hand, the Bulgarian Presidency suggests excluding security related processing from the scope (text from 7 March 2018). On the other, it suggests language for security under Article 8 and its relevant recitals (Presidency text 22 March – Article 8 (2) (e)).

We would also like to underline that any related exception should also consider the need to fight fraud and abusive use of a service (e.g. sharing child abuse images).

Permitted processing

We regret to see that the Presidency text from 7 March 2018 still refers to the consent of 'all' the communication parties (**recital 15**), a concept that does not work for any service that allows for interoperability with another provider (such as email). In general, we would also like to emphasise the need to provide more flexibility and move away from an overreliance on consent, especially given the really broad potential scope of the Regulation.

We also note that the suggested consent requirement for employees in **recital 19b** seems to be at odds with the GDPR, as the latter is sceptical whether consent in this context can be valid. A 'one-off' consent for businesses subscribing to electronic communication services is not mentioned in this recital, as a definition and a legal description of the improvements for legal persons is missing. On the contrary, the recital makes it very clear that companies are now completely dependent of the consent

American Chamber of Commerce to the European Union
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
amchameu.eu • European Transparency Register: 5265780509-97

More information:
Maika Föhrenbach
mfo@amchameu.eu

of their employees, for any electronic communication service or software/app update, in relation to work phones, tablets or connected machines (**Recital 19b**, 2nd sentence).

The Presidency also asks Member States to provide input on the processing of metadata to encompass more purposes or create another legal basis. In this context, AmCham EU reiterates its support to broaden the scope of permitted processing of metadata communication data and to mirror the flexibility existing in the GDPR.

The text from 13 April includes additional exceptions introduced in **Article 6.2.(a)** to allow processing of metadata for purposes of network management and optimisation, and a new basis in **Article 6.2.(f)** for processing for the purpose of statistical counting at the request of a public authority, subject to a number of conditions. However, this does not take into account the risk-based approach as included in the GDPR and does not provide enough flexibility for a future-proof ePrivacy Regulation. The Council text does not refer either to 'legitimate interest' nor the principle of 'compatible further processing'.

Emergency calls, Incoming call blocking, publicly available directories

We continue to believe that provisions in articles 13 and 14 are historic elements that are no longer relevant in today's context. They relate to commercial practices and consumer protection rather than privacy or security. If they remain relevant, they would be better addressed under the telecoms regulatory framework.

In particular, we are concerned that the reference to 'publicly available' has been deleted in article 13 para 1, and article 15 throughout paragraphs 1, 2 and 3.

Terminal equipment data

We welcome the suggested change of the title in Article 8 in the 22 March presidency text. We would like to reiterate our call for a technology-neutral legislation. While we appreciate more flexibility, **Articles 8 and 10** will have a broader impact than just on cookies. This needs to be taken into account when defining the wording.

With that in mind, we suggest additional exceptions in our list of proposed amendments. Limiting exceptions to information society services only is unhelpful, as other services – including communication services – rely on the use of storage and processing capacity of a device. This is why AmCham EU supports the deletion of **recitals 23 and 24** in the Commission proposal, which are technology specific.

The presidency introduced some flexibility on third-party processing for audience measurement on behalf of the provider of the information society service (**article 8 (1) (d)**). In our amendment proposal, we suggested the following solution:

Article 8 (1) (d) - 'It is necessary for audience measurement, including reach measurement of the use of information society service for the purpose of calculating remuneration'.

Accordingly, we also welcome the Presidency proposal in **Recital 21** according to which 'access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose'.

Furthermore, an exception for processing and storage has been introduced for security updates (**article 8 (1) (e)**). As per the above, while we welcome the recognition that processing is necessary for security purposes, this exception should also recognize the legitimate need to fight fraud and abusive uses. Furthermore, it is important to be consistent on the type of security exception across ePrivacy. An overarching – as opposed to article-specific - exemption would provide more legal clarity.

Especially if the terminal equipment is used in a business context, e.g. work phones, tablets, laptops or other terminals which are used by employees to fulfil job-related tasks, the 'end-user' giving consent must be the legal person, for which the terminal equipment is utilised.

Software Privacy Settings

We are significantly concerned about latest iteration of Art 10. The proposed change to article 10 (1) to 'any other parties' exponentially expands the scope to any piece of software, and applications that stores information, regardless of where the information is actually stored (i.e. purely on the device) or the type of information.

We are equally concerned that the latest amendment to Art. 10 (2) would require the user to be navigated through the privacy settings every time an update is pushed. We understand that it may be the case in situation where the updates results in a change in the privacy setup of the software, but question the value when the update is simply to fix a bug, security update or provides new features that does not require any processing of information.

Our general concern is that these provisions and the related recitals have been clearly drafted with a specific use-case in mind. Users will face operational difficulties of granular choices: the provisions do not allow for sufficient flexibility – consent gathering should be adapted to the context and tailored to the consumers' preferences. This is not going to happen with standardized privacy options and will not prevent consumer fatigue. The text should set out future-proof principles to enable companies to engage in an open dialogue with users to inform them on what's at stake and to empower them to choose on a flexible and specific basis.

Direct marketing communications

A new provision **Article 16(2a)** allows Member States to set a time limit for using customers' contact details for direct marketing. We are concerned that this may cause fragmentation of the Digital Single Market and will be contrary to the choice and nature of this Regulation intended to avoid divergent implementation at Member State level and ensure legal certainty across Europe.

AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

American Chamber of Commerce to the European Union
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
amchameu.eu • European Transparency Register: 5265780509-97

More information:
Maika Föhrenbach
mfo@amchameu.eu