Brussels, 4 July 2019

The present document is an informal submission on behalf of BSA | The Software Alliance,[1] answering the questions posed by the Finnish Presidency as preparatory work for the discussions in the Working Party on Telecommunications and Information Society on the ePrivacy Regulation.

1) The main objective of the proposed regulation is to protect the fundamental right of private life and confidentiality of the communications. To this end, which parts of the proposed regulation could be considered as the most essential?

BSA continues to emphasize the importance of maintaining a clear distinction between the scope of the proposed ePrivacy Regulation and GDPR, and particularly the corresponding obligations they would establish. The current Council draft text maintains such a distinction between *Data at Rest* and *Data in Transmission* as per Art. 2(2)(e;f). We would urge the Presidency to maintain this language, and in possible Trilogue negotiations ensure that this distinction is included in a final version of an ePrivacy Regulation. BSA strongly supports a well-functioning ePrivacy Regulation which ensures legal certainty and clear protections, without overlapping with the GDPR.

2) On which parts of the text more discussion is still needed? As the text stands now we would like to especially have your views on:

- **Which parts are the most problematic and how can those problems be concretely solved?**

- BSA continues to emphasize the importance of ensuring the confidentiality of communications, the protection of personal data and a clear distinction between personal and non-personal data. To that end, we suggest aligning the proposed ePrivacy Regulation with the GDPR grounds for processing personal data, whilst maintaining clear protections for the confidentiality of communications. The grounds for processing under the ePrivacy Regulation – built exclusively on a consent of the end-user – remain too limited given its scope, and would have a significantly negative impact on AI and Machine-to-Machine communications.

- A further clarification of the definition of end-user in an employment setting is fundamental. The current language in Recital 19b, paired with Art. 8, would all but impede the functioning

[1] *BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.*
BSA's members include: Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

of most industrial and business processes in all sectors. It is fundamental to adjust this language to B2B services. If each individual employee would have to be required to consent to any processing or software updates of the terminal equipment they use for their employment, business and industrial processes would be entirely dependent on the discretion of each individual employee for their functioning. Ensuring that terminal equipment software is up-to-date and in line with all the safety and security standards is a fundamental premise of any company, regardless of size. BSA suggests changing the language in Recital 19b and Art. 8 to make it so that consent for processing must be given by the legal entity (e.g. the representative who is legally entitled to act on behalf of the company or employer) and not by an employee on an individual basis.

- The current language of Art. 8 on Software Updates is a welcome step in the right direction, but still fails to include usability, accessibility and other functionality-related updates which do not impact the privacy settings of terminal equipment. We are particularly concerned that the exception to the consent requirement remains focused only on those software updates that contain a security component. Even where software updates are not "necessary" for security, software that is not routinely updated may create security vulnerabilities, and may impair other important aspects, such as its usability, accessibility, and other functionalities. Limiting the exception in Article 8(1)(e) to software updates that are "necessary for security reasons" only would not allow service providers to fully address the challenges caused by outdated software, as this cannot be done by security updates alone. Outdated software requires updates to address 'bugs' along with performance, design and functionality issues. Security updates are not meant to solve such issues and consequently, updates are often bundled to address a variety of issues, including compliance with legal obligations (e.g. introduction of more granular cookie controls).

    - **Are there some parts of the text you consider unnecessary and which should be deleted?**

BSA continues to support the deletion of Art. 10. While web browsers can successfully block cookies, they do not know how to distinguish between the purpose of each specific cookie. Only publishers who deploy cookies are in a position to know the purpose of each cookie and their relationship to data processing. BSA remains highly sceptical as to how any version of Article 10 will work in practice across not just web browsers, but software more broadly. BSA strongly supports the principle of effective users' control over their data, complemented with the accountability principle, both of which the General Data Protection Regulation already addresses. Consequently, we encourage the Presidency to preserve the deletion of Article 10.

3) Some delegations have indicated that further alignment with the General Data Protection Regulation and ePrivacy rules would be needed. In this regard, what kind of specific changes to the text would be needed?

- The grounds for processing under the ePrivacy Regulation, provided by Art. 6, should be aligned with Art. 6 of the GDPR, ensuring better alignment between the two Regulations and a more comprehensive approach to data processing.

- The introduction of recent language on data retention also warrants further discussion given the potential overlaps with GDPR deletion requirements.

4) What should be the next steps to be taken to continue the negotiations in the Council?

- BSA suggests a thorough analysis of the scope of the ePrivacy Regulation and its possible overlap with GDPR, in particular taking into account the assessment of the implementation of GDPR carried out by the Commission.
- Similarly, BSA continues to be concerned about the possible negative effects of the ePrivacy Regulation on AI, Machine-to-Machine communications and machine-learning. We strongly suggest carrying out a further impact assessment of the relevant ePrivacy language, and considering the possibility of narrowing its scope or providing for additional grounds for processing. This is particularly important in light of the recent High-Level Expert Group work on AI and the development of a vibrant AI ecosystem in the EU.

We remain at your disposal for any question or comments.

Yours faithfully,

Thomas Boué

Director General, Policy – EMEA
BSA | The Software Alliance