Brussels, June 2020

BSA Recommendations to the German Presidency for a balanced ePrivacy Regulation

Background

BSA | The Software Alliance ("BSA"),[1] the leading advocate for the global software industry, has shared its concerns with regards to the Draft ePrivacy Regulation ("ePR") in several instances,[2] and has endeavored to act as a trusted partner throughout the legislative discussions. BSA appreciates the efforts made during the Finnish and Croatian Presidencies to improve on the text but continues to consider the most current Council draft text in need of further improvements in order to address the potential impact of the ePR on EU consumers, businesses, and suppliers. As Germany is about to begin its Presidency, BSA would like to provide a set of recommendations on improving the current Council text.

With the objective of supporting the discussion of the file in the Council, BSA has drafted this document to outline the most pressing issues in the Council text, while striving to safeguard the important principles introduced by the Regulation.[3]

An overarching concern with regards to the Regulation pertains to its limited grounds for processing, exclusively built upon consent. While the objectives of the Regulation are certainly meritorious, and respond to very concrete concerns, the text addresses these concerns without regard to different business models, users, and technology. This is particularly impactful on enterprise software ("B2B"), where very diverse operators often rely on contractual agreements to process communications data. BSA continues to have concerns that different sectors and technological solutions would be regulated with a "one-size-fits-all" approach. It is important to align the ePR with the GPDR grounds for processing, especially as the body of law and best practices on GDPR begins to solidify and in view of the upcoming GDPR review.

This document takes into consideration as main reference the Council text from 6 March 2020. When otherwise, the text referred to will be indicated in parenthesis by its document number.

[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 30 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, Atlassian, Autodesk, Bentley Systems, Box, Cadence, Cloudflare, CNC/Mastercam, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] BSA Policy Paper on Outstanding issues to be resolved for a balanced ePrivacy Regulation – February 2019 (link); BSA Answers to ePrivacy Questionnaire – July 2019 (link)

[3] This document references to the Council text of 6 March 2020.
In bold: amendments to the original Commission proposal by Council
~~**In strikethrough bold**~~**:** deletions suggested by BSA
In underlined bold: additions suggested by BSA

Avenue des Arts 44
1040 Brussels
Belgium

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

Material scope: data processed after receipt and "third-party" definition

The current drafting of the material scope in Art. 2(2)(e) deletes the useful clarification that processing after receipt by an "entrusted third party" is outside of the scope of the Regulation, which served to draw a clear distinction between "data at rest" and "data in transmission" for third parties. BSA strongly advises to retain the previous language of Art. 2(2)(e) (Document 14054/19), as such a clarification on the scope of the Regulation is essential for the functioning of the Regulation and of GDPR. While some language to this end was added in the new Recital 8aa, it does not completely clarify that all processing by entrusted third parties is outside of the scope of the Regulation. This wording is important to move towards a clearer distinction between the circumstances in which the proposed ePrivacy Regulation (1) will apply in addition to the GDPR and (2) those in which the GDPR alone will apply.

BSA considers the distinction between data at rest and data in transmission the founding principle for the ePrivacy Regulation, alongside with the possibility for third parties to process communications data on behalf of end-users. Lacking such a distinction, it would not be possible to have legal certainty on the confines between GDPR and ePrivacy.

The definition of a "third party" previously described in recital 19, now the last paragraph of Recital 8aa is also relevant to the scope of the proposed ePrivacy Regulation. Recital 8aa states that electronic communications service ("ECS") providers will be considered third parties when providing other services not part of the electronic communications service. This important clarification should be preserved. It ensures that ECSs that provide a range of services, as many do, will understand clearly when their processing is subject to the ePrivacy Regulation and when it is not.

Recommendations:

- Retain the previous language in Art. 2(2)(e) (Document 14054/19, latest Finnish Presidency text).
- Retain the current draft language of the last paragraph of Recital 8aa.

Material scope: Cybersecurity exceptions

The new language of Art. 2 on the material scope of the regulation pertaining to cybersecurity has been entirely deleted, losing the helpful clarification of 2(f) for processing electronic communications data to ensure the security of the end-user's network and information systems, including their terminal equipment. BSA strongly recommends retaining the previous language of the Article (Document 14054/19), as it unequivocally carved out fundamental and legitimate cybersecurity activities of the scope of the Regulation.

With regards Recital 8aa, we welcome the efforts of the Presidency to streamline the language defining the cases in which processing of data is allowed for ensuring network and information security, both by the end-user concerned as well as by a third-party entrusted by the end-user to perform this function. Nevertheless, removing all references to the possibility to process data before receipt, for the purposes of cybersecurity, would severely hinder the cybersecurity capabilities of both the cybersecurity technology providers and of the end-user they protect. We believe the previous language of Recital 8 provided the necessary legal clarity and would ultimately help achieve the objective of higher security resilience. In order to fully meet this objective, as noted, the entrusted third party must be permitted to process the data **prior to**

receipt by the end user. This is necessary as it allows providers of security technologies and services to detect threats through their threat intelligence tools and to stop these threats before they reach the end user's environment.

Recommendations:

- Retain the previous principle set out in Art. 2(2)(f) that there should be a cybersecurity exception (Document 14054/19, latest Finnish Presidency text).
- Add the wording "even before receipt" in Recital 8aa, to allow for fundamental cybersecurity activities.

Article 2
Material Scope
2. This Regulation does not apply to: […]
(f) electronic communications data processed by the end-users concerned or by a third party entrusted by the end-user in order to ensure the security of the end-user's network and information systems including their terminal equipment.

Recital 8aa, last sentence of the first paragraph:
This could include processing of electronic communications data on the end user's terminal equipment or within or at the edge of the end-user's closed network even before receipt by third parties mandated by the end-user for the purpose of protecting the end-user's terminal equipment or closed network..

Grounds for processing for electronic communications data

BSA welcomes the additional flexibility added by the Croatian Presidency, allowing for the processing of metadata on the grounds of legitimate interest, as per Art. 6b(1)(e). Nevertheless, BSA continues to consider the grounds for processing of the Regulation extremely limited and not in line with technological developments and the ever-developing digital services provided in Europe. In particular, a "one-size fits all" approach to consent with regards to communications data, which does not take into account users and business context, specifically in the B2B sector, is bound to create significant burdens for companies, both providing and receiving services.

BSA would also recommend retaining the previous wording of Article 6(1)(a) "when it is necessary to provide an electronic communication service" (Document 14054/19), as such language guarantees more legal certainty and clarity for all operators. Moreover, to further align the proposal with the GDPR, BSA recommends that the legal grounds for processing communications content and metadata be extended to statistical and scientific research purposes (as per the previous wording of Art. 6b(1)(f)).

Furthermore, the Regulation would greatly benefit from additional clarifications on how consent would be provided by end-users. Once again, in the B2B setting, operators often do not have direct contact with all the end-users, and would therefore find themselves in an uncomfortable grey area whereby the consent is given by some end-users but not all (e.g. a software designed to support customer service communications sold to a retail company, whereby the retail company would consent to using the software and data processing, but the software developer would not have a direct contact or interface to obtain the consent of the clients of the retail company).

Recommendations:

- Retain the previous wording of Art. 6(1)(a) (Document 14054/19, latest Finnish Presidency text).
- Retain the previous wording of Art. 6b(1)(f) and add similar language to Art. 6a.
- Consider whether further changes to the grounds for processing under the ePrivacy Regulation Art. 6 are appropriate. In particular, we recommend that these are aligned with the legal bases for processing under Art. 6 of the GDPR as far as possible, ensuring better alignment between the two Regulations and enabling a more seamless approach to data processing.

Article 6
Providers of electronic communications networks and services shall be permitted to process electronic communications data only if:

(a) **it is necessary to provide an electronic communication service**; or

Article 6a [previous art 6(3)]
Without prejudice to Article 6(1), providers of electronic communications **networks and** services **shall be permitted** to process electronic communications content **only** if:
[…]
(c) it is necessary for statistical purposes, or for scientific research purposes, provided it is in accordance with Union or Member State law and subject to appropriate safeguards, including encryption and pseudonymisation, to protect fundamental rights and the interest of the end-users. Processing of electronic communications metadata under this point shall be done in accordance with paragraph 6 of Article 21 and paragraphs 1, 2 and 4 of Article 89 of Regulation (EU) 2016/679.

Article 6b [previous art 6(2)]
Without prejudice to Article 6(1), providers of electronic communications **networks and** services **shall be permitted** to process electronic communications metadata **only** if:
[…]
(f) it is necessary for statistical purposes, or for scientific research purposes, provided it is in accordance with Union or Member State law and subject to appropriate safeguards, including encryption and pseudonymisation, to protect fundamental rights and the interest of the end-users. Processing of electronic communications metadata under this point shall be done in accordance with paragraph 6 of Article 21 and paragraphs 1, 2 and 4 of Article 89 of Regulation (EU) 2016/679.

Data retention

The current language on data retention requirements is improved, and is more workable and balanced.

Recommendations:

- Retain the current drafting of article 7.1.
- Carefully examine e-privacy data retention language in light of other applicable legislation (GDPR deletion requirements, art.17), CJEU jurisprudence (Tele2 case as well as ongoing litigation Case C-511/18), and potential conflicting policy objectives and

requirements in other draft legislative instruments (e-Evidence Regulation, Terrorist Content Online Regulation).

Protection of end-users' terminal equipment information: Software updates

BSA approves the objective of the Croatian Presidency to streamline Art. 8 for the protection of the end-user's terminal equipment. More legal certainty and clarity in this aspect are certainly welcome. While allowing service providers to rely on legitimate interest under Art. 8(1)(g) is surely an important step in the right direction, this is still heavily limited both on the cybersecurity and – more broadly – functionality side of software updates.

In the context of cybersecurity, the use of concepts such as content data and metadata is not always the correct definition for all cybersecurity activities – which often need to happen throughout the functioning of the terminal equipment and beyond – therefore BSA would strongly recommend reintroducing a specific exception for the protection of terminal equipment related to cybersecurity.

Moreover, the current wording of Recital 21b explicitly excludes the possibility to rely on legitimate interest for software updates for the functionality of the terminal equipment. BSA recommends providing a broader exception. Even where software updates are not specifically "necessary" for security, software that is not routinely updated can create security vulnerabilities, and can also impair other important aspects of the system, such as its usability, accessibility, and other functionalities.

Second, in the employment context, the text of Art. 8(1)(e) should make clear that the end-user who decides on business software updates must be the enterprise user (i.e. the employer, rather than the individual employee). Recital 19b appears to establish a similar approach with respect to the processing of electronic communications data, but this is not clear. If any single employee can choose to reject, postpone, or turn off an update (either functional updates or security updates), this could create wider systemic security vulnerabilities and other risks for the enterprise. As terminal equipment could be leased, or used in a "bring your own device" manner, the legal question of ownership is irrelevant here.

Recommendations:

- Consider whether further alignment with GDPR would be possible, especially in coordination with additional changes to Art. 6, and all the relevant recitals.
- Retain the previous language of Art 8.1 (da) for a clear cybersecurity exception (Document 14054/19, latest Finnish Presidency text).
- Broaden the language in Art. 8 (or alternatively in Recital 21b) so that exceptions are not limited to software updates that are "necessary for security reasons." In particular, consider alternative language to include usability, accessibility and other functionality-related updates which do not impact the privacy settings of terminal equipment.
- Consider revisions to Recital 19b and the inclusion of an additional similar recital (new recital 23a) in relation to Art 8.1 to establish that the employer (*i.e.*, the legal person), rather than the individual employee, is the authority that decides on whether software updates should be installed in the context of employment. We have proposed suggested text for Recital 19b and a new Recital 23a below.

(19b) Providers of electronic communications services may, for example, obtain the consent of the end-user for the processing of electronic communications data, at the time of the conclusion of the contract, and any moment in time thereafter. In some cases, the legal ~~**entity**~~ person having subscribed to the electronic communications service may allow a natural person, such as an employee, to make use of the service in accordance with Regulation 2016/679. **In such case, consent may be obtained from the legal person concerned, and need not be obtained from the individual user**.

(23a) Terminal equipment which is used for business reasons, such as computers, laptops, tablet computers or smart phones, for example to control production facilities and machines or to run business software, has to be automatically updated, maintained and managed to reflect the relevant business needs and to comply with information security requirements. In this context, the end-user is the legal person (employer), for example a company, who may give consent to the use of processing and storage capabilities of terminal equipment and the collection of information from terminal equipment.

Article 8
Protection of end-users' terminal equipment information
1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:
[…]
(d) it is necessary for audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user **or by a third party on behalf of one or more providers of the information society service provided that conditions laid down in Article 28, or where applicable Article 26, of Regulation (EU) 2016/679 are met; or**
(da) it is necessary to maintain or restore the security of information society services or terminal equipment of the end-user, prevent fraud or detect technical faults for the duration necessary for that purpose; or
(e) it is necessary for a software update provided that:
(i) such update is necessary for security usability, accessibility, or other functionality-related reasons and does not in any way change the privacy settings chosen by the end-user
(ii) the end-user is informed in advance each time an update is being installed, and
(iii) the end-user is given the possibility to postpone or turn off the automatic installation of these updates; or

Machine-to-machine and Internet-of-Things language

The draft Regulation would bring M2M communications in scope of the Regulation only when they happen over a "publicly available network" (Recital 12). Further, the most recent draft also establishes that use of processing and storage capabilities without the consent of the end-user in the IoT context would be allowed when necessary for the provision of the service requested (Art 8(1)(c) and Recital 21).

These changes are an improvement. But this construct still presents problematic limitations when transposed to industrial environments (where use of the capabilities may, for instance, be for quality control, machine learning or analytics). Recital 21 should clarify that the term "service" in the M2M context should be construed in the broadest possible context to incorporate all processing permitted by contract.

In particular, while some M2M communications do happen at the application layer, it is not always the case. This is particularly true when software companies are designing the software that allows the devices to function and communicate, which would lead to consider such service providers as Electronic Communications Services, and not as end-users. For this reason, BSA strongly recommends including the compliance with contractual obligations as a valid grounds for data processing in the M2M context. This would be beneficial not only for the broader development of M2M communications and IoT, but especially in the industrial and B2B setting, where contractual agreements are the typical basis for regulating the relations between two companies.

Recommendation:

- Include compliance with contractual obligations as a valid ground for data processing in the M2M context.

Privacy Settings

BSA also welcomes the decision by the Croatian and Finnish Presidencies to confirm the deletion of Article 10. BSA continues to stress that 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 skeptical 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 GDPR already addresses. Consequently, we encourage the Council to preserve the deletion of Article 10.

Recommendation:

- Preserve the deletion of Article 10.

For further information, please contact:
Thomas Boué, Director General, Policy – EMEA
thomasb@bsa.org or +32.2.274.1315