BSA RECOMMENDATIONS ON THE EPRIVACY NEGOTIATIONS

March 2021

EXECUTIVE SUMMARY

BSA | The Software Alliance ("BSA")[1] is the leading advocate for the global software industry before governments and in the international marketplace. Our members[2] are enterprise software companies that create the technology products that power other businesses, offering tools such as cloud storage services, customer relationship management software, human resource management programs, identify management services, and collaboration software. Businesses entrust some of their most sensitive information with BSA members, and our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations, including the confidentiality of communications.

BSA is committed to advancing policies that enhance trust in digital services. The proposed ePrivacy Regulation ("ePR") seeks to make important updates to the 2002 ePrivacy Directive; however, we believe further discussion is needed to fully consider the potential impacts of the ePR on EU consumers, businesses, and suppliers. We encourage the co-legislators to carefully evaluate the proposal and not rush to finalize the text, particularly as the ePR is likely

[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.

[2] BSA's members include: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, Box, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, 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

to directly overlap and – in its current form – conflict with other existing or proposed EU legislation and strategies.

BSA has sought to act as a constructive partner throughout the ePR legislative discussions, and we set out below some of the reasons why we believe the draft remains in need of further refinement. We have prepared ten recommendations to improve on the current European Parliament Report and Council General Approach, and we offer a detailed analysis of the legislative instruments that may create competing obligations or requirements for service providers.

BSA's recommendations for EU policymakers focus on:

- ***Adopting a technologically neutral and innovation-friendly ePrivacy Regulation***

    1. Ensure that the scope of the ePrivacy Regulation maintains a distinction between data at rest and data in transmission.
    2. Allow for additional flexibility for grounds for processing in Business-to-Business relations.
    3. Provide the necessary exemptions for cybersecurity activities.
    4. Design enforcement mechanisms consistent with GDPR.

- ***Ensuring a cohesive body of laws with the EU Acquis***

    5. Clarify the possible overlap between GDPR and the ePrivacy Regulation.
    6. Ensure that the Digital Services Act and ePR do not create competing obligations.
    7. Clarify the consent requirements for data-sharing under the Data Governance Act.
    8. Unlock the potential of data-sharing by designing an ePR that supports the EU Data Strategy.
    9. Ensure that the EU can continue to adhere to the highest Cybersecurity standards.
    10. Foster the uptake of Artificial Intelligence in Europe and design an ePrivacy that supports Machine-to-Machine communications and Internet of Things technologies.

ADOPTING A TECHNOLOGICALLY NEUTRAL AND INNOVATION-FRIENDLY EPRIVACY REGULATION

As the proposed ePR would seek to update the ePrivacy Directive of 2002, it is of paramount importance to ensure that new legislation supports innovation and responsible business practices and that it functions alongside equally significant EU legislative instruments and strategies, including the GDPR.

1. Ensure that the scope of the ePrivacy Regulation maintains a distinction between data at rest and data in transmission

The draft ePR was meant to be a *lex specialis* to the GDPR "[aiming to] particularise and complement it as regards electronic communications data that qualify as personal data."[3] After four years of negotiations in the Council and the Parliament, the scope of the proposal is not closer to ensuring the necessary legal certainty as to the boundaries between the supposed *lex specialis* and GDPR.

BSA considers the distinction between data at rest and data in transmission the founding principle for the ePrivacy Regulation, along 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, which would both apply to the same datasets, therefore creating a competing compliance structure whereby service providers – and end-users – would not necessarily know which rule would apply.

The Council version of the text includes some language attempting to clarify that the draft ePR would only apply to so-called "data in transmission", while the processing of data received by end-users would happen under GDPR. This would create a bright-line rule regarding when the ePR obligations end and the GDPR obligations begin. The European Parliament's proposal, in contrast, expressly extends the ePR obligations to electronic communications data regardless of whether that data is in transit or stored (Art. 5(1)). Under this proposal, the ePR, in effect, would replace the GDPR as the primary law governing processing by providers of electronic communications services —creating substantial compliance challenges for the many providers whose services include electronic communications service functionality, but

[3] Explanatory Memorandum to the Proposal for a Regulation on Privacy and Electronic Communications, COM(2017) 10 final.

are not solely electronic communications services, and/or involve processing of electronic communications data, but not only electronic communications data.

A former version of the draft discussed under the Finnish Presidency had suggested amendments[4] to the text in Art. 2(2)(e), including the helpful Recital 8 which would provide further clarification for third-party service providers. BSA strongly recommends re-including these amendments, which would ensure that the boundaries between GDPR and the draft ePR are sufficiently clear.

2. Allow for additional flexibility for grounds for processing in Business-to-Business relations

The original draft ePR proposal allows exclusively consent as the grounds for processing of communications data – while the Council General Approach has included limited exceptions which would broaden the grounds for processing in certain instances. With the objective of ensuring confidentiality of communications, the proposal does not take into consideration how different services, and even different sectors, may adapt or settle how communications data should be processed. This is particularly important in the context of Business-to-Business (B2B) relations and in the employment context.

In B2B relations, businesses rely heavily on contractual agreement to ensure that they can benefit from tailored services, especially in the digital sphere. Moreover, digital services are often comprised of several different layers, which may be provided by different separate entities. In such cases, all these entities rely on contractual agreements to settle their responsibilities and obligations. This is particularly important, as it allows the necessary flexibility to choose which services best address the need of a company, and at the same time ensures that service providers have the sufficient legal certainty to determine their obligations. It is fundamental to underline how all businesses value greatly the confidentiality of their communications, which constitutes a key aspect of their ability to protect their intellectual property rights, trade secrets and business operations. Businesses in the EU greatly benefit from the ability to enter into contractual agreement regulating the digital services they receive, and this remains true for all services related to electronic communications services and more broadly to data processing. **BSA strongly recommends including language to allow for more flexibility in B2B relations, distinguishing between Electronic Communications Services (ECS) provided to consumers and to businesses.**

The ePR does not account for such subtlety, nor does it include mention of using contractual means as grounds for processing in a B2B setting. Moreover, the European Commission's

[4] Council text of 15 November 2019, Document number 14054/19

Impact Assessment for the ePR proposal does not raise any concerns regarding the necessity for an exclusively consent-based system in the B2B space.

The Council General Approach has included limited flexibility for the processing of metadata, under the so-called "further compatible processing", which is not included in the original Commission proposal and the European Parliament Report. The addition of such flexibility does provide some additional coverage for several B2B activities but does not clarify a number of significant issues.

The draft ePR does not provide any legal certainty for those services that do not have a direct interface with an end-user and may therefore not be able to obtain their consent, or may not be notified if the end-user has rescinded their consent. This is particularly important in the context of B2B relations, where ECS are often provided by a company that relies on software designed by a separate entity which have no practical nexus to the end user – yet would still qualify as an ECS provider under the draft ePR. BSA recommends including language in the final ePR that would ensure that service providers that do not have the possibility to obtain consent from end-users are still able to provide their services.

Software updates are a fundamental aspect of the functioning of an enterprise. They ensure that an organization can adopt and maintain state-of-the-art cybersecurity practices that are tailored to their specific risk profile and constantly provide the most recent and efficient functionalities. Both the Council General Approach and the European Parliament Report provide for very limited grounds to update software on terminal equipment without the consent of the end-user, limited only for cybersecurity purposes. Even where software updates are not specifically "necessary" for security, software that is not routinely updated can lead to security vulnerabilities being uncovered, and exploited, and can also impair other important aspects of the system, such as its usability, accessibility, and other functionalities. **Limiting the exception 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). Accordingly, multi-purpose software updates that include updates with a security purpose should be permitted without consent. BSA recommends extending the exception to all software updates, while including language to protect the end-user's rights such as a clause that would not allow for updates "if that would result in the end-user having a lower privacy standard".

The issue of software updates is particularly important in the context of employment and the use of terminal equipment, as neither the Commission's draft ePR proposal nor

the Council General Approach provide clarifications as to which entity should consent to the processing of communications data, the employer, or the employee. Companies may, quite reasonably, wish to collect electronic communication data for business analytics, and should, at the enterprise level, be able to opt all their employees into such data collection, subject to their own compliance with GDPR and other legal obligations. The European Parliament Report introduced very narrow language to allow the processing of communications data on terminal equipment when it is used "strictly technically necessary for the execution of an employee's task" (Art. 8(1)(db)). While the European Parliament's approach is a step in the right direction, BSA believes that further clarification is necessary to ensure that in the context of employment, the employee, or the company, on behalf of the employee, can consent to the processing of information on terminal equipment used for business reasons. This is particularly important with regards to software updates, which need to be up-to-date and state-of-the-art throughout a company. 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. And if providers cannot maintain the security and reliability of their enterprise customers' IT systems through software updates, they could find themselves in breach of their contractual obligations to their enterprise customers. This is true both for cybersecurity updates, and for functionality updates. BSA strongly recommends broadening the language – stating that an employer can give consent for modifications to terminal equipment used in the context of employment – of the European Parliament Report Art. 8(1)(db), to ensure that businesses are able to control the proper functioning of their processes.

3. Provide the necessary exemptions for cybersecurity activities

The original draft ePR proposal did not include clear exemptions for processing of communications data for the purposes of cybersecurity. Given today's ever-evolving cybersecurity threats, which are often deployed through ECS, it is of paramount importance to ensure that a final ePR allows for fundamental cybersecurity activities, and at the same time does not conflict with existing cybersecurity obligations and requirements mandated by EU law, and more broadly by commonly established global best practices.

The Council General Approach retained some useful language inserted in the proposal, with the objective to provide more flexibility in processing data – also on terminal equipment – for the purposes of cybersecurity. BSA welcomes the efforts of the General Approach in Recital 8aa, 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. To fully meet the highest cybersecurity standards, 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

Moreover, with the objective of adding further legal certainty as to the confines of ePR and corresponding cybersecurity activities, BSA strongly recommends re-introducing language from the Finnish Presidency proposal, which would provide for an Art. 2(2)(f), stating:

> *"2. This Regulation does not apply to:*
>
> *[…]*
>
> *(f) electronic communications processed upon receipt 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."*[5]

BSA recommends re-introducing the above language as it would unequivocally exempt fundamental and legitimate cybersecurity activities of the scope of the Regulation.

4. Design enforcement mechanisms consistent with GDPR

The Commission and Parliament proposals both envisaged that the supervisory authorities responsible for monitoring compliance with the GDPR should also be responsible for enforcing the ePR (Art. 18), and that the GDPR's cooperation and consistency mechanisms should apply (Art. 20). BSA strongly supports this approach and encourages further improvement of its implementation under both the GDPR and the future ePR. Harmonization of enforcement mechanisms between the ePR and GDPR would ensure the ePR is applied consistently and seamlessly, across Member States and in relation to the GDPR.

For the sake of efficiency, it is particularly important that companies operating in several EU Member States have the possibility to designate one lead regulator which then coordinates and cooperates with its counterparts in other Member States. Putting competence in national regulators, absent a robust cooperation mechanism, effectively means situation where providers could be subject to oversight by several supervisory authorities for the same activities across the EU - a system that creates unnecessary burdens for companies and supervisory authorities alike.

---

[5] *Ibid.* Council text of 15 November 2019, Document number 14054/19

BSA therefore urges the EU institutions to adopt Articles 18 and 20 of the Commission and Parliament proposals to ensure that regulators enforce the ePR through the same cooperation and consistency mechanism as the GDPR, including the one-stop-shop.

ENSURING A COHESIVE BODY OF LAW

The draft ePR aims at updating the ePrivacy Directive of 2002 and ensuring that the updated European Electronic Communications Code definitions are matched with legally certain obligations and responsibilities. Nevertheless, the proposal in its current form is likely to severely impact current and pending EU legislation and strategies. While some of the objectives of the ePR were indeed to update current legislation, several proposed Commission instruments would be significantly limited by an ePR that does not include language to ensure that it does not overlap with other legislation, and especially that it does not impose competing responsibilities and obligations. **Complying with one EU instrument should not create conflicts with another**.

5. Clarify the possible overlap between GDPR and the ePrivacy Regulation

Chiefly, and as illustrated above, **the current proposed ePR would significantly overlap with GDPR**. Without legally certain obligations, grounds for processing and data protection requirements, this overlap would significantly weaken both GDPR and ePR. BSA strongly recommends ensuring that the confines between ePR and GDPR are clear, and especially that the distinction between so-called data at rest – where GDPR would apply – and data in transmission – where ePR would apply – is maintained in a final version of the draft proposal.

6. Ensure that the Digital Services Act and ePR do not create competing obligations

The proposed **Digital Services Act** ("DSA") explicitly excludes Electronic Communications Services from its scope, *prima facie*, this would ensure that no overlap between the requirements and obligations of DSA and ePR would surface. However, a potential conflict of public policy objectives may occur depending on the outcome of the ePrivacy trilogues. The European Parliament Report suggests that ancillary communication features in other applications are not covered by the ePR regulation and would make them fully subject to the DSA, whilst the Council General Approach mandates that "minor ancillary services" to Electronic Communication Services would be included in the scope of the ePrivacy Regulation (Recital 11a). In this case, DSA obligations would overlap with ePR requirements, and it would likely be impossible to carry out the mandated content moderation obligations under DSA, without being in breach of the draft ePR. This is particularly true for services that combine

many different features into a single offering, where some features would fall within the scope of the DSA, and others of the ePR. Consider, for example, a service such as business communication platform, whose primary functions suggest it is an interpersonal communications service and therefore ancillary communication features should certainly fall within the scope of ePrivacy. These platforms often offer a storage functionality to their users, plus livestream broadcasts which have the capability of being public through a link that is shared. DSA may apply to those individual features within the service. To ensure that digital service providers do not find themselves needing to breach one EU law to comply with another, **BSA strongly recommends to fully exclude minor ancillary services from the ePR, to ensure that digital services providers can comply with the requirements of the DSA without risking breach of ePR.**

7. Clarify the consent requirements for data-sharing under the Data Governance Act

The proposed **Data Governance Act** ("DGA") establishes further rules on the sharing of public data, with the meritorious objective of incentivizing the sharing and re-use of publicly held data, including personal data. While the DGA does not include mandates to share data, it certainly aims to foster such practice. **The proposed ePR would significantly limit the ability of public bodies to share data, in particular as it does not provide clarity on how consent would be provided in the context of employment. In most cases, any data to be shared under the DGA could be considered communications data, and therefore subject to ePR.** This would entail that the sharing would be subject to the consent of all end-users involved in the management of the data to be shared at any given time. Moreover, this would create likely unsurmountable obligations for the public sector body willing to share the data, and for the data sharing service providers, which would often not have the possibility to obtain consent – and manage any changes thereof – from all end-users.

8. Unlock the potential of data-sharing by designing an ePR that supports the EU Data Strategy

The **EU Data Strategy** sets out the ambitious aim to "create a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint. It should be a space where EU law can be enforced effectively, and where all data-driven products and services comply with the relevant norms of the EU's single market. To this end, the EU should combine fit-for-purpose legislation and governance to ensure availability of data, with investments in standards, tools, and infrastructures as well as competences for handling

data."[6] While the Strategy does not provide additional information on the possibility of mandatory schemes for industrial data sharing, it is certainly clear that the main objective would be to incentivize the sharing of such datasets. **Under the proposed ePR rules, such data sharing would be subject to consent-based requirements – as it would unlikely fall under so-called further compatible processing – especially as the consent-model for B2B relations and for employment relations would mandate that each individual end-user consents to the sharing of data produced in an industrial setting.** This would essentially disincentivize any voluntary or contractually based data sharing agreement, as its functioning would hinge on the ability of the parties to constantly suspend, amend, or radically change the data sharing structure depending on the consent of each individual end-user. Moreover, lacking a clear distinction between data at rest and data in transmission, it would also not be clear when and whether at all such data could be shared. Additionally, the consent-based model would mandate that each entity processing the data would need to comply with ePR, which would make compliance near to impossible for all those entities which do not have a direct relation with each end-user involved.

9. Ensure that the EU can continue to adhere to the highest Cybersecurity standards

The proposed ePR would significantly conflict with existing and proposed cybersecurity legislation and best practices. In particular, the ability to process communications data in transmission without consent from all end-users is an intuitive necessity for cybersecurity purposes. The Council General Approach has inserted some important clarifications in this space, but lacks a clear exception for cybersecurity activities, similarly to the Commission original proposal and European Parliament Report. Moreover, **the approach taken by all proposals with regards to software updates would run counter to the universally acknowledged cybersecurity best practices to ensure that software is always up to date throughout a network**.[7] A key aspect of cybersecurity is the ability to detect and analyse threats and vulnerabilities, and often to share information with governmental and private entities in order to prevent, mitigate, and respond. The anonymization and deletion of communications data requirements provided by the ePR proposal would significantly hamper the ability of cybersecurity service providers, public or private, to carry out this important function. Additionally, both the proposed NIS 2.0 Directive (Art. 26) and Digital Operational Resilience for the Financial Sector Regulation (Art. 13) seek to institute coordination mechanisms for sharing information on incidents, threats, and

[6] A European Strategy for Data, COM(2020) 66

[7] "Software patching is one of the most critical activities in IT governance and central to cybersecurity." , European Union Agency for Network and Information Security, *Effective Patch Management*, at https://www.enisa.europa.eu/publications/info-notes/effective-patch-management

vulnerabilities, which in some case may be mandatory, and which would similarly run counter to the proposed ePR.

10. Foster the uptake of Artificial Intelligence in Europe and design an ePrivacy that supports Machine-to-Machine communications and Internet of Things technologies

The European Union has also set an ambitious agenda for the uptake of **Artificial Intelligence in Europe**. While an important aspect of that agenda is the abovementioned Data Strategy, it is important to also mention fundamental processes such as Machine-to-Machine (M2M) and Internet of Things (IoT) communications. Such communications would be in the scope of the draft ePR, though this would present considerable challenges in a consent-only based model. This is particularly true in the industrial setting, where M2M/IoT communications constitute an important aspect of industrial processes – often across different facilities. In such cases it would not always be possible for the service provider to obtain the consent of all end-users – especially considering the abovementioned issue of consent in the employment context – and it would be counterintuitive to derogate from contractual agreements between companies, which would instead regulate the processing of M2M/IoT communications in B2B settings. In particular, while some M2M/IoT 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/IoT 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.

For further information, please contact:

Matteo Quattrocchi,
Senior Manager, Policy – EMEA
matteoq@bsa.org