Brussels, July 2018

BSA | The Software Alliance's position paper on the EU Regulation on European Production and Preservation Orders for electronic evidence in criminal matters

BSA | The Software Alliance ("BSA")[1], the leading advocate for the global software industry, welcomes the opportunity to provide its views to the European Commission's proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters ("e-Evidence Regulation"). Our members support the efforts of the European Commission to address the challenges facing cross-border law enforcement requests for e-Evidence. We share the desire to achieve greater harmonisation and legal certainty for national authorities, service providers and citizens.

The European Commission's proposal represents an improvement on the current EU regime, under which law enforcement authorities seek e-Evidence either through formal cooperation channels between the relevant authorities of two countries, e.g., through Mutual Legal Assistance Treaties ("MLATs"), or via the exercise of unilateral national powers. The proposal is also an improvement over the possibility of different, potentially conflicting individual Member State laws. Consistent with the Digital Single Market objectives, it is important that the draft Regulation clearly be the exclusive mechanism for law enforcement in Member States to request e-Evidence from service providers across national borders.

In addition, while crafted as an intra-EU law, the draft Regulation is also an important step towards the creation of international agreements with many of the EU's main trading partners to further facilitate cross-border law enforcement access to data and to promote stronger safeguards for individuals and enterprises. BSA fully supports the efforts of the European Commission to achieve this long-term objective.

To ensure that the proposed e-Evidence Regulation creates a harmonised set of rules that are necessary, proportionate, and in full respect of European fundamental rights, we encourage the co-legislators to consider the following issues when reviewing the proposed draft Regulation:

1. **Recipient of European Production Orders ("EPOs")** – The co-legislators should endorse the principle that where an EPO targets the data of an enterprise, the data should be sought in the first instance from that enterprise itself (i.e. the data controller). An EPO should only be directed to a service provider (i.e. the data processor) when seeking data directly from the enterprise would jeopardise a criminal investigation.

[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 offices in Brussels, 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, ANSYS, Apple, Autodesk, Bentley Systems, Box, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Intuit, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, 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

2. **Stored Data vs. Real-Time Interception** – The scope of the future legal framework should be strictly limited to stored data. The co-legislators should not expand the scope of the instrument to cover real-time interception, direct access or data stored at a future point in time.

3. **Timeline for Responding to an EPO** – The timeline for service providers to respond to EPOs should be extended to allow service providers to properly review each EPO Certificate ("EPOC") to ensure that it is valid and respects all relevant safeguards set forth in the draft Regulation. The clarity of the EPOC and time to review is needed to protect European fundamental rights.

4. **Comity Procedure Timeline** – The co-legislators should extend the time period for consultation with third-country central authorities in cases where a suspected conflict of law exists. Member State courts should require compliance with an EPO only where third-country authorities affirmatively confirm there is no conflict. The lack of a timely response from a third-country does not mean that no conflict of law exists.

5. **Grounds for Challenging an EPO** – Law enforcement authorities should be required to disclose additional information in each EPOC in order to ensure that service providers have the necessary information to determine whether an EPO violates the European Charter of Fundamental Rights. The draft Regulation should also recognise that the U.S. Electronic Communications Privacy Act falls within the meaning of Article 15.

6. **Encrypted Data** – The co-legislators should seek to strengthen the principle regarding encrypted data found in Recital 19 and transcribe these obligations into the operative provisions of the text. Service providers should be under no obligation to decrypt data, if they do not have the encryption key, before disclosing it in response to an EPO, regardless of national law.

7. **Dual Criminality** – The draft Regulation should ensure that EPOCs can only be issued where the matter under investigation is a crime in both the Member State of the issuing authority and the Member State of the legal representative of the service provider.

8. **Good Faith Compliance** – In accordance with international best practices, the co-legislators should include a "safe harbour" provision that would protect service providers from any liability under both Union and Member State law for any actions taken in good faith to respond to or comply with an EPO under the draft Regulation.

Avenue des Arts 44
1040 Brussels
Belgium

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

Issues and BSA Positions

1. Recipient of EPOs

BSA Views: BSA **welcomes both Article 5(6) and Recital 34** of the draft e-Evidence Regulation. These provisions direct law enforcement authorities seeking data stored or processed as part of a cloud infrastructure to seek the data from the cloud provider's enterprise customer, rather than demanding disclosure from the service provider directly. The draft legislation includes an important exception for instances where this would be inappropriate, in particular where serving an order on the customer might jeopardise the investigation (e.g., where the customer is the target of the investigation).

Numerous organisations across the EU rely on service providers to store or process data on their behalf, due to the many benefits these services offer, including increased efficiency, cost reduction, and computing power. However, organisations will only use services that they trust. The "proximity principle" set out in the draft Regulation helps to advance that trust by ensuring organisations have maximum control over their data. This principle also better aligns the EU with practice in the United States, where the U.S. Department of Justice has instructed federal prosecutors to seek data from enterprise customers of service providers unless doing so would jeopardise their investigation.

Moreover, BSA **welcomes the references to *force majeure* in Articles 9(4), 10(5), 14(4)(c), and 14(5)(b)** as instances where a service provider is unable to comply with an EPOC or EPOC-PR due to "impossibility." This principle is central to ensuring that service providers are not required to disclose data that is not readily accessible. However, BSA believes that to strengthen this principle, further clarification as to what would fall under *force majeure* should be clarified in a Recital. Beyond instances where the data sought is not held by the service provider, we encourage the Recital to consider technical limitations such as access restrictions and Infrastructure as a Service ("IaaS"). For example, entities providing IaaS often do not have access to the data stored in the IaaS server. Such access would only be possible if the service provider were to physically access the server. In such instances, the investigate measure should instead be issued to the IaaS customer directly.

Recommendation: BSA calls on the co-legislators to **preserve the proposed text of Article 5(6) and Recital 34** to avoid unnecessarily placing service providers in-between Member State law enforcement authorities and their customers (i.e. data controllers), as the latter is the most appropriate party to provide access to data in the enterprise context. The preservation of this principle will ensure that Europe's cloud computing industry is not unduly harmed by the draft Regulation.

Furthermore, the co-legislators should introduce a **requirement for Member State law enforcement authorities to explain to a service provider why the issuing of an EPO directly to an enterprise customer would jeopardise an investigation**. Service providers should be

allowed to challenge the assertion of law enforcement authorities if they believe the EPO could be served directly on the data controller.

Additionally, BSA encourages the co-legislators to **further clarify in a Recital the instances whereby *force majeure* would apply**. The Recital the should reference not only instances where the data sought is not held by the service provider, but also technical limitations such as access restrictions and IaaS products.

2. Stored Data vs. Real-Time Interception

BSA Views: BSA welcomes the scope of the draft e-Evidence Regulation, which does not enable law enforcement authorities in one Member State to impose real-time interception or other "forward-looking" data collection obligations on service providers in other Member States. Such interception obligations are significantly more intrusive on the privacy of individuals and enterprises than stored data disclosure obligations.

In addition, imposing EU cross-border interception obligations would require service providers to take additional costly technical steps including the creation of interception infrastructure and the design of systems to enable interception. This could raise further legal issues such as the need for a regime to compensate providers for building and maintaining interception infrastructure and additional complexities arising from differing Member State obligations on the design of such infrastructures.

The creation of a future legal framework focused on stored-data that is balanced and creates the much-needed harmonisation of Member State law is too important to risk the further delay that would come with any attempts to expand the scope of the draft Regulation to cover real-time interception. As a consequence, the issue of real-time intercept should be **dealt with in separate legislation** that is carefully considered and crafted, rather than addressed as a last minute "add-on" to the draft Regulation.

Recommendation: BSA calls on the co-legislators to **avoid expanding the scope** of the future legislative framework and **reject all attempts to introduce real-time interception or other "forward-looking" data collection obligations** into the draft Regulation.

3. Timeline for Responding to an EPO

BSA Views: BSA is concerned that the timeline set out in Article 9(1) of the draft Regulation, which requires addressees who receive an EPOC to disclose requested data "within 10 days" of receipt, will be **unworkable for the majority of service providers.** While we recognise that some EPOs will relate to emergencies and that these should be executed rapidly (as provided for in Article 9(2)), most EPOs will not involve such urgent cases. For all "non-emergency" EPOs, it is unreasonable to expect service providers to respond within 10 days particularly as some service providers may receive hundreds of EPOCs within that time period. This requirement could also jeopardise the ability of some service providers to respond immediately in emergencies.

Service providers will need time to properly scrutinise each EPOC in order to ensure that it is valid and respects all relevant safeguards set forth in the draft Regulation (e.g., checking to ensure the EPOC does not violate the European Charter of Human Rights) and to direct requests to appropriate systems and teams. More time may also be needed where the provider determines that it has a basis – or potentially an obligation – to object to the EPO. In addition, given that most service providers acting as data processors are unlikely to be familiar with the content and structure of their customers' data, sufficient time will not only be needed to determine which data is necessary to comply with an EPO, but also to ensure that the disclosure of any data does not go beyond the scope of the EPO. Any additional data disclosures risk being classified as a data breach under the General Data Protection Regulation.

Moreover, given that Article 9(2) requires more rapid disclosure in emergency situations, we see no reason to provide Member States in Article 9(1) with discretion to deviate from the general rule. If cases are urgent, then Article 9(2) will govern the disclosure timeline. If cases are not urgent, then **Member States should not be allowed to mandate faster response times**, particularly since this might prevent service providers from raising valid objections to enforcement of an EPO. The opportunity for law enforcement authorities to deviate from the standard timeline for disclosure will undermine harmonisation across the Single Market, while increasing administrative burdens on service providers that operate in multiple EU Member States.

In addition, the requirement to respond to emergency requests, as set out in Article 9(2), "without undue delay, at the latest within six hours upon receipt of the EPOC" is **not a workable timeline for most organisations**. BSA members understand that there are emergency situations whereby data needs to be produced quickly. However, the timeline of within six hours upon receipt of an EPOC does not reflect the challenges of data collection by service providers in complex, multinational entities. The emergency response timeline should be amended to **seventy-two hours**, which will allow for the quick disclosure of data, while also providing software companies of all sizes with sufficient time for collection and proper verification.

Recommendation: BSA calls on the co-legislators to amend Article 9(1) and **delete the 10-day time limit together with the provision conferring discretion to require even quicker disclosure**. Instead, Article 9(1) should instead require service providers to disclose data "without undue delay, and, where feasible, within **thirty days**." We also call for Article 9(2) to be amended so that emergency requests must be responded to within **seventy-two hours upon receipt of an EPOC rather than six hours.**

4. Comity Procedure Timeline

BSA Views: Article 15 of the draft Regulation sets out important safeguards that apply when a service provider considers that an EPO could potentially conflict with third-country laws protecting fundamental rights of individuals or fundamental national security and defence interests. While we welcome this mechanism, we believe **further work is needed to improve the provision**.

Under Article 15, if a service provider considers that compliance with an EPO would conflict with a third-country law, it informs the issuing law enforcement authority. If the law enforcement authority decides to uphold the EPO, it must refer the matter to a domestic court. If the court establishes that a relevant conflict exists, it moves forward to contact the central authority of the relevant third country and provides them with 15 days to respond (with a possible extension to 30 days) with an opinion as to whether a conflict of law exists. If that central authority objects to the EPO, the court must strike down the EPO. In contrast, if that authority does not object or respond within the deadline, the court automatically upholds the EPO.

BSA stresses that this **envisaged framework is an important safeguard**. Without it, EPOs could put service providers in a position where they may either face sanctions for refusing to comply with an EPO, or breach laws protecting fundamental rights in, or the fundamental interests of, third countries. This mechanism also promotes respect for third-country laws and in doing so, encourages those countries to act reciprocally.

However, two aspects of this envisaged mechanism require further consideration:

1. **Timeline** – The 15-day (and 30-day extension) time period for third-country central authorities to respond to notifications from Member State courts is too short. This period should be extended significantly in order to provide such authorities an opportunity to thoroughly examine each EPO on its merits and respond accordingly.

2. **EPO validity** – Article 15 should be revised to require Member State courts to deny enforcement of an EPO unless third-country authorities explicitly indicate that no conflict exists. As drafted, Article 15 directs Member State courts to consult foreign authorities only where they have already "established" that a conflict exists. Accordingly, Member State courts should respect that determination unless informed otherwise, and service providers should not be required to comply with an EPO, notwithstanding such a conflict, simply because the third-country central authority has failed to respond.

Recommendation: BSA calls on the co-legislators to **amend Article 15 to extend the time period for consultation with third-country central authorities**. In addition, **Article 15 should be revised to provide that Member State courts may require compliance with an EPO only where third-country authorities affirmatively assert there is no conflict**. Where third-country authorities are silent, the Member State court should lift the EPO in order to uphold fundamental rights protected by third-country laws and to avoid putting service providers into conflict of law situations.

5. Grounds for Challenging an EPO

BSA Views: While BSA recognises that EPOs will significantly aid the work of European law enforcement, we believe there is a risk that they could be misused in ways that pose a potential threat to EU fundamental rights. Consequently, **we welcome the inclusion of safeguards in**

Articles 14 and 15, which we believe will help protect these rights. However, further work is required to ensure that these provisions will be effective.

With regard to Article 14, service providers are authorised to oppose enforcement of an EPO where, among other circumstances, compliance would "manifestly violate" the European Charter of Human Rights, or where an EPO is "manifestly abusive." While this is not the only safeguard to ensure that EPOs are not abused – for instance, EPOs must be approved by a Member State court or similar authority, and issuing law enforcement authorities may only issue EPOs where similar domestic cases would merit the same investigative measures – it remains a central safeguard. However, the information set out on in an EPOC is quite limited (categories are set out in Article 6(3)). As a result, in many cases it may be **difficult for service providers to evaluate whether compliance with an EPO would violate the European Charter of Fundamental Rights or be manifestly abusive**. To address this concern, issuing law enforcement authorities should be required to disclose more information about the case in the EPOC, and service providers should be offered guidance as to when abuses could be deemed "manifest" on the basis of that information.

As previously mentioned, Article 15 would apply when third-country laws protecting fundamental rights or fundamental interests prohibit disclosure of data sought by an EPO. While many third countries protect these rights robustly, BSA is concerned that they may not use the same terminology as that used in Europe. **Article 15 should remove any doubt that laws protecting privacy and similar civil rights – such as the Electronic Communications Privacy Act in the United States – fall within scope of this Article, even if those laws do not refer specifically to "fundamental rights."**

Recommendation: BSA calls on the co-legislators to **revise Article 6(3) to require issuing law enforcement authorities to furnish more information in EPOCs or produce clear guidance prior to the draft Regulation taking effect**, in order to ensure that service providers have the information necessary to determine whether an EPO violates the European Charter of Fundamental Rights or is otherwise "manifestly abusive." Furthermore, **Article 15 and relevant Recitals should also be amended to expressly recognise that the U.S. Electronic Communications Privacy Act and similar laws qualify as third-country laws that protect "fundamental rights" within the meaning of Article 15.**

6. Encrypted Data

BSA Views: The draft Regulation should not require providers to disclose encrypted data in de-encrypted form, if not in the service providers ability. As such, we welcome Recital 19 which provides that data should be disclosed in response to an EPO "regardless of whether it is encrypted or not." This approach is essential to protect user privacy, and to ensure that service providers can offer cloud encryption key recovery services. **To ensure that this principle is fully respected, we believe it should be incorporated into the operative provisions of the draft Regulation. It should be made clear that this principle prevails in cases of conflict with national law.**

Recommendation: BSA calls on the co-legislators to amend the operative provisions of the draft Regulation to include a provision stating that service providers are under **no obligation to decrypt data, if not the service provider's ability, before disclosing it in response to an EPO** (regardless of national law).

7. Dual Criminality

BSA Views: While the draft Regulation sets out conditions that must be satisfied before an EPO is issued (Article 5), it does not require that the matter under investigation constitutes a crime in both the Member State of the issuing authority and the enforcing Member State where the legal representative of the service provider is located. As a result, service providers may be required by EPOs to disclose data to respond to investigations of matters that are not crimes in the Member State of their legal representative – a potentially concerning outcome that could undermine trust in the EPO system and in service providers over time.

Recommendation: BSA calls on the co-legislators to amend Article 5 to require that EPOCs can only be issued where (i) the **matter under investigation is a crime in both the Member State of the issuing authority and the Member State of the legal representative** of the service provider, and (ii) the issuing law enforcement authority attests that the matter under investigation actually meets the elements of that crime in both Member States.

8. Good Faith Compliance

BSA Views: Although BSA members broadly welcome the draft Regulation, service providers remain concerned that if they comply with an EPO, they run the **risk of potentially breaching existing Union or Member State law** (e.g., rules that require confidentiality, such as patient-doctor confidentiality, or, to take another example, rules on copyright or trade secrets). For example, due to the limited information provided by an EPOC regarding an on-going criminal investigation, a service provider may unknowingly disclosure more data than needed when complying with an EPOC. Complying with an EPOC could force a service provider to disclose data of individuals who are not targets of an investigation but are linked in some manner to the criminal suspect. In such an instance, a service provider should not be held liable for unknowingly disclosing more data than necessary to a Member State law enforcement when complying in good faith with an EPOC.

Recommendation: BSA calls on the co-legislators to **introduce a "safe harbour" provision to the draft Regulation that would protect service providers**, and their officers, employees, agents and advisors, from any liability under both Union and Member State law, for any actions taken in good faith to respond to or comply with an EPO under the draft Regulation.

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