Brussels, January 2019

BSA | The Software Alliance's Response to the EDPB Public Consultation on the Proposed Guidelines on the Territorial Scope of the GDPR

On 16 November 2018, the European Data Protection Board ("EDPB") published draft guidelines on the territorial scope of the General Data Protection Regulation ("GDPR") for public consultation. BSA | The Software Alliance ("BSA")[1], the leading advocate for the global software industry, welcomes the publication of the EDPB's draft guidance and appreciates the opportunity to provide comments to help inform the EDPB's final version of these important guidelines.

In particular, we welcome the clarity the EDPB's draft guidelines will bring to many issues related to the territorial scope of the GDPR. However, there are a number of areas where the draft guidelines would benefit from greater clarity, in order to help the software sector and its millions of customers to operationalise the GDPR in day-to-day compliance and business activities. We detail below where we would recommend amending the draft guidance.

Issues and BSA Recommendations

1. The "Establishment Criteria" - Application of the GDPR to processing based on activities of an establishment of a controller or processor in the Union (Article 3(1))

The EDPB's draft guidelines provide helpful clarity on the meaning of Article 3(1) and the scope of the establishment criterion. The draft guidance will be useful for many companies headquartered or operating primarily outside the EU as they seek to understand whether and when they must comply with the GDPR.

Many of our members offer data processing services. We therefore welcome the draft guidance clarifying the applicability of the GDPR, including that Article 3(1) should not be read to suggest that non-EU controllers will become subject to the GDPR merely by virtue of using the services of an EU-established processor. This clarification is particularly important to the **success of cloud services providers** who offer processing services from establishments in the Union.

However, some aspects of the draft guidelines on Article 3(1) remain unclear:

[1] *BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the internationals 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, Siemens PLM Software, 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

- **Where a non-EU data controller uses a data processor in the EU**: The draft guidelines state that non-EU data controllers will not become subject to the GDPR merely by virtue of their use of a data processor in the Union. The draft guidelines also make clear that data processors based in the Union will be subject to GDPR data processor obligations.

BSA comments: As noted above, we welcome the EDPB's draft guidance on this issue. Nonetheless, scenarios where non-EU data controllers (not subject to the GDPR) use EU-established data processors (subject to the GDPR) raise further questions that the draft guidelines do not address. For example, the draft guidelines identify obligations that would apply to EU-established data processors in this context. Several of these obligations relate to the use of sub-processors. However, it is unclear whether and how these obligations would vary where those sub-processors are also – like the data controller – outside the EU and not otherwise subject to the GDPR.

Furthermore, EU-established data processors will be bound by the instructions and requirements set forth contractually by their respective non-EU data controllers. There remains a possibility that non-EU data controllers, who are not subject to the GDPR, will be reluctant to follow GDPR requirements placing EU-established data processors at risk of non-compliance. We would welcome clarity in the final guidance that EU-established data processors should not require cooperation from their respective non-EU data controllers for issues that do not require their cooperation (e.g. signing a data protection impact assessment or standard contractual clause ("SCC")).

In addition, while the draft guidelines note that the Chapter V provisions on data transfers will apply to the EU-established data processor, it is unclear what grounds under that Chapter would actually be available in practice to enable transfers to non-EU data controllers. This point is particularly challenging given that the European Commission has not yet recognised SCCs for data flows from a data processor located in the Union to a non-EU data controller.

- **Where a data controller subject to the GDPR uses a non-EU data processor**: The draft guidelines state that where a data controller subject to the GDPR uses a non-EU data processor, data controllers "*may need to consider imposing, by way of contract, the obligations placed by the GDPR on processors subject to it*" (p. 10).

BSA comments: The above scenario is relatively common practice. Yet the draft guidelines remain unclear. The draft guidelines appear to be suggesting either that (1) in this scenario data controllers need to impose all data processor obligations set out in the GDPR, or (2) data controllers only need to impose requirements referred to in Article 28(3). We recommend revising this section of the draft guidelines to be more specific by deleting the phrase "may need to consider" and by clarifying that Article 28(3) alone applies.

- **"Inextricable linkage" between activities of the establishment of the data controller or data processor in the Union and the relevant data processing:** The draft guidelines state that even if the EU-located establishment is not actually processing data

itself, if the activities of that establishment are "inextricably linked" to the relevant processing by the non-EU-located data controller or data processor, the GDPR will apply.

BSA comments: The question of how to determine if data processing is "inextricably linked" to the activities of an establishment in the EU is **central to determining when Article 3(1) of the GDPR applies to processing that takes place outside the EU**. However, the draft guidelines could more clearly indicate that, when an inextricable link is established between the relevant data processing by the non-EU-located data controller or data processor and the activities of the EU-located establishment, the GDPR applies only to the data processing that is inextricably linked to the establishment's activities.

For example, in the second example given in the guidelines (p. 7), the draft guidelines consider a Chinese e-commerce company that has established a European office in Berlin in order to lead and implement marketing towards EU markets. The draft guidelines conclude that "*[t]he processing of personal data by the Chinese company*" is inextricably linked to the marketing activities of the European office. However, the draft guidelines should also **specify the territorial limits in that case**, to make clear that not all processing by the Chinese company is subject to the GDPR. Statements in the guidelines (e.g., "*If such a[n inextricable] link is identified, the nature of this link will be key in determining whether the GDPR applies to the processing in question, and must be assessed against the elements listed above*." (p. 7)) indicate that the EDPB's intent was not to suggest that all processing operations of a data controller or data processor are automatically within scope of the GDPR whenever such an inextricable link is identified. Nevertheless, BSA would recommend a more definitive statement on this point.

- **When the EU cannot be used as a "data haven" for processing that raises "inadmissible ethical issues":** The draft guidelines are clear that the territory of the EU cannot be used as a "data haven" for unethical processing that breaches EU fundamental rights or other national laws relating to public order.

BSA comments: While BSA members fully respect EU fundamental rights, the draft guidance lacks detail (and the Article 29 Working Party guidance on "controllers" and "processors" cited by the EDPB guidelines on this point in footnote 19 does not further elaborate). As a result, software companies will struggle to develop and implement "red flags" in order to identify and prevent processing that could otherwise potentially breach this prohibition. We recommend that the final guidelines remain more closely focused on the territorial scope of Article 3, and that this section be **removed**.

2. The "Targeting Criteria" - Application of the GDPR to processing based on offering goods or services to, or monitoring the behaviour of, data subjects in the Union (Article 3(2))

We welcome the EDPB's draft guidance on when Article 3(2) applies. For many non-EU data controllers, clarifying that Article 3(2) is not necessarily triggered when a data subject is merely temporarily present in the EU (i.e., Example 9)) is particularly helpful. In addition, BSA welcomes

the clarification (as illustrated in Example 10) that Article 3(2) does not apply when processing data of EU nationals, residents and citizens who are outside the Union.

However, similar to the "establishment criteria", elements of the draft guidelines on Article 3(2) remain unclear:

- **Offering of goods or services to legal persons in the Union, where natural persons (data subjects) are mere points of contact:** The draft guidance does not address scenarios where goods or services are offered to legal persons – such as companies – through contacts to individuals

BSA comments: The draft guidelines provide helpful clarity on many issues relating to interpretation of Article 3(2)(a). However, the draft guidelines do not address scenarios where goods or services are offered to EU legal persons, such as companies or other organizations established inside the EU, through communications to individuals (such as procurement officers or other corporate employees) who are natural persons, and thus data subjects. The draft guidance should clarify that in these situations, although natural persons are points of contact, Article 3(2)(a) would not apply, as the goods and services in question are not "offered" to "data subjects in the Union," but rather are offered to legal persons who, under the GDPR definition of "personal data" in Article 4(1), cannot be data subjects.

- **When monitoring of EU data subject behaviour will fall under Article 3(2)(b):** The draft guidelines take the position that the question of whether Article 3(2)(b) applies to particular monitoring should be assessed without reference to any "intention to target" EU-located data subjects on the part of the data controller or data processor. The draft guidelines also set out that "monitoring" under Article 3(2)(b) can include scenarios where the data controller has a "specific purpose in mind", such as behavioural analysis or profiling. This can include activities such as "*[o]nline tracking through the use of cookies…*"

BSA comments: The draft guidelines state that there is no need to show an "intention to target" EU-located data subjects when determining the application of the GDPR to processing under Article 3(2)(b). In addition, the EDPB also takes the view that online tracking through the use of cookies can be a form of targeting under Article 3(2)(b). As cookies are an industry-standard technology used on nearly every website on the Internet, taken together these positions would mean that **huge numbers of websites that have nothing to do with the EU are subject to the GDPR** if even a single EU data subject seeks them out and visits them. Such and outcome would be unworkable and is surely broader than what the EDPB intended. We recognize that the guidelines do nuance this point to a degree ("*The EDPB does not consider that any online collection or analysis of personal data of individuals in the EU would automatically count as "monitoring". It will be necessary to consider the controller's purpose for processing the data*" (p. 18)). However, as the draft guidance emphasises that any use of data for the purposes of "behavioural analysis" or profiling would be sufficient to trigger Article 3(2)(b) (p. 18) and does not further detail how any intention to target EU data subjects could be relevant, this **issue is**

not sufficiently resolved. We recommend clarifying that while there is no explicit need to show an "intention to target" under the GDPR, nevertheless such a showing should be part of the Article 3(2)(b) analysis in practice.

Other examples given in this section (e.g., behavioural advertising) are similarly unhelpfully broad. To help ensure that factors triggering application of the GDPR under Article 3(2)(b) are recognized in practice, we would recommend providing m**ore granular replacement examples**.

3. Representatives of controllers or processors not established in the Union (Article 27)

The appointment of an EU representative is an important step for many non-EU companies seeking to comply with the GDPR. For that reason, BSA welcomes the EDPB's detailed draft guidance on this requirement. However, in certain respects the EDPB's draft guidelines on appointing an EU representative risk creating practical difficulties in day-to-day compliance (particularly for SMEs wholly established outside the EU).

We believe the draft guidelines would benefit from further surrounding Article 27:

- **Characteristics and capabilities of the representative:** The draft guidelines recommend that even when a company takes on the legal representative role, a "single individual" should be assigned as lead and that the representative should be specified in a service contract (p. 20). The draft guidelines also take the position that the representative should be able to efficiently communicate in the "*language or languages used by the supervisory authority and the data subjects concerned*" (p. 23).

BSA comments: Many of the recommendations in the draft guidelines provide helpful clarity for companies seeking to appoint and operationalize relationships with legal representatives. However, the final guidance should be clear that these are recommendations only and are not "one-size-fits-all" requirements that must be followed in every case.

In particular, the requirement that the representative be able to communicate to all data subjects and supervisory authorities in their own languages – with "help of a team if necessary" (p. 23) – should be clearly identified as a recommendation rather than a requirement. A requirement of this kind will prove **prohibitively costly and difficult to implement**, in particular for smaller companies offering goods or services into the whole of the EU, which is not an uncommon scenario given the way online start-ups seek to scale up their services. A start-up offering services to all EU Member States would need to hire a representative fluent in (or teams supporting representatives fluent in) 24 separate languages. This requirement is far out of proportion to what the GDPR requires. Article 27(4) of the GDPR requires the representative to be able to "address" supervisory authorities and data subjects in place of the data controller or processor, without specifying other operational or language requirements for the representative. The use of external translator services, on a case-by-case basis and only where needed, should also be endorsed.

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