The Software Alliance

BSA

December 10, 2020

BSA comments on the Commission implementing decision on standard contractual clauses for matters referred to in Article 28(3) and (4) of Regulation (EU) 2016/679 (“Article 28 SCCs”)

BSA | The Software Alliance (“BSA”),[1] the leading advocate for the global software industry, welcomes the opportunity to provide feedback on the European Commission’s draft new standard contractual clauses (“Article 28 SCCs”) on the matters referred to in Article 28(3) and (4) of Regulation (EU) 2016/679.

BSA members are enterprise software companies that create the technology products and services that other businesses use. For example, BSA members provide business-to-business tools including cloud storage services, cloud content management, customer relationship management software, human resource management programs, identity management services, and workplace collaboration software. Businesses entrust some of their most sensitive information—including personal data—with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members’ operations.

The GDPR has brought valuable harmonization of applicable rules and increased transparency of data handlers’ responsibilities within EU and EEA countries.[2] The GDPR’s risk-based and technology neutral approach to data protection requirements allows organizations to ensure compliance while adapting their practices and safeguards to the most-suited approach given their business model, activity and risk profile. We appreciate the Commission’s efforts to further support companies’ compliance with the GDPR by developing Article 28 SCCs.

We agree with the Commission that the concepts of controller and processor “play a crucial role” in the application of the GDPR, including through Article 28.[3] We accordingly welcome the new Article 28 SCCs, which are intended to provide a new tool for companies seeking to comply with Article 28’s requirements. While the draft Article 28 SCCs are voluntary – and organizations remain free to implement Article 28’s requirements through customized contract arrangements that reflect the specific products and services at issue – we appreciate the Commission’s efforts to develop Article 28 SCCs that reflect the realities of the digital environment.

We respectfully submit the comments below in response to the Commission’s consultation on the Article 28 SCCs to further achieve this objective and to make the application of these provisions as practical as possible, in particular in a cloud computing environment.

[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, DocuSign, Dropbox, 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] References to EU in the submission are to be read to also mean EEA countries.

[3] See Commission Implementing Decision at (1).

1. The Article 28 SCCs Provide Important Choices for Controllers and Processors Implementing the GDPR's Requirements

The Article 28 SCCs provide an important new option for controllers and processors entering into agreements subject to the GDPR. We welcome the Commission's recognition that controllers and processors may implement the GDPR's requirements in several ways – including through the new Article 28 SCCs. In particular, we appreciate the Commission's acknowledgement that the Article 28 SCCs will be available for use by companies that wish to adopt them on a standalone basis, but that companies may also "choose ... to negotiate an individual contract" containing the requirements of Article 28(3) and 28(4).[4] In addition, companies also retain the option to include the new Article 28 SCCs in a "wider contract" that incorporates additional clauses or safeguards.[5]

This approach reflects the practical reality that contracts between controllers and processors govern a range of different products and services, and ensures that companies can tailor the contracts for those products and services in a manner that best incorporates the GDPR's requirements. It also reflects the GDPR's recognition that a contract between a controller and a processor may be based on standard contractual clauses issued by the Commission, "[w]ithout prejudice to an individual contract between the controller and processor."[6] We accordingly welcome the Article 28 SCCs as an important additional option for controllers and processors to implement the GDPR's requirements.

2. Several Modifications Can Help the Article 28 SCCs Better Reflect Today's Digital Environment

We believe that the Article 28 SCCs are most useful in helping companies achieve compliance with the GDPR when they reflect the realities of today's digital environment. By providing practical and specific ways for companies to implement the GDPR's requirements, the Article 28 SCCs can better assist companies in carrying out obligations under Article 28. We suggest six ways the Article 28 SCCs can be strengthened in this regard.

a. Engagement of Subprocessors

The Article 28 SCCs address the circumstances in which processors may engage subprocessors, which can be critical in providing the technology products and services needed by today's businesses. Under the GDPR, a processor is required to obtain the prior specific or general written authorization of a controller to engage a subprocessor. We recommend revising the approach to general authorization set out in Clause 7.6(a). As described below, this provision should be revised to better reflect how controllers may provide more meaningful general authorization in today's digital environment. The current approach creates two sets of concerns:

Listing of Subprocessors. Clause 7.6(a) option 2 currently contemplates that, with respect to general authorization to engage subprocessors, a processor will provide a list of specific subprocessors it intends to engage and shall inform the controller in advance before replacing any of those subprocessors. This concept of listing may have made sense in an environment of cloud services delivered on premise, which may have been the focus of regulators when the Commission adopted the current SCCs governing data transfers. Now, however, the multi-layer environment in which B2B cloud companies tend to operate makes it operationally challenging to keep such a list updated, which in practice is also no longer a cause of rejection by customers. We encourage the Article 28 SCCs to recognize other methods by which companies may meet the GDPR's requirements.

[4] See Commission Implementing Decision at (5).
[5] See Commission Implementing Decision at (6).
[6] GDPR Art. 28(2).

Specifically, we suggest revising Clause 7.6(a) to encourage companies to address by contract the frequency and means of updates regarding new subprocessors. This ensures that companies can craft notices about new subprocessors that are as meaningful as possible. For example, in a complex service that relies on a large network of subprocessors, a processor may engage a range of new subprocessors each week. By delivering notice about those subprocessors together in a format that is meaningful to the controller, the notice will be better suited to achieving its objective. In some cases, a processor may also determine that a subprocessor is no longer trustworthy – and will need to quickly switch to another subprocessor to protect the personal data on their service. Ensuring that controllers and processors are able to contractually address such scenarios helps to better protect personal data.

Ability to Object. Clause 7.6(a) also contemplates that a processor will provide written notice to a controller of any change to the list of subcontractors provided and specify a time period during which the controller may object to a new subprocessor.

This approach can inadvertently limit the ability of processors to quickly engage new subprocessors in circumstances where the controller may wish for them to do so. For example, in some cases a processor may need to urgently engage a new subprocessor if an existing subprocessor has suffered a data breach or is unable to carry out its contractual requirements.

Instead, Clause 7.6(a) should be revised to enable controllers to provide processors with broader authorization to engage subprocessors, such as by providing general authorization to engage certain categories of subprocessors, without the need to inform the controller in advance of each specific subprocessor. This is particularly important for processors that may depend on a network of subprocessors to provide services to a controller, such as software applications that are operated as services from a cloud-based architecture (Software-as-a-Service or SaaS). These services may use the same cloud-based architecture – which depends on the use of subprocessors – to serve tens, hundreds, or even tens of thousands of controllers. In that scenario, requiring each controller the opportunity to object to each specific new subprocessor – even in the context of a general authorization – can become a significant hurdle for both controllers and processors, given the high volume of subprocessors and the thousands of customers' that may be afforded an opportunity to object to each one.

We recommend revising Clause 7.6(a) to encourage companies to address by contract the frequency and means of updates regarding new subprocessors, which may allow them to better tailor obligations based on the scope and type of data affected.

In addition, companies should be encouraged to provide general authorization focused on <u>categories</u> of subprocessors, rather than individual subprocessors.

b. Audit Rights

The GDPR recognizes that processors are to "allow for and contribute to audits including inspections, conducted by the controller or another auditor mandated by the controller."[7] The current Article 28 SCCs go beyond this language, suggesting in Clause 7.4(c) that audits "may also include inspections at the premises of the data processor and shall be carried out with reasonable notice."

[7] Article 28(3)(h).

The Article 28 SCCs therefore appear to contemplate on-site audits, without recognizing the many privacy and security concerns that on-site audits may create, in addition to the potentially significant costs of audits. For many processors, it may be impossible to accommodate on-site audits given the number of customers they serve from the same premises. Beyond limitations of physical space, on-site audits create significant concerns about ensuring the privacy and security of data that may be available on a processor's premises – particularly for processors that serve tens or thousands of controllers. Indeed, in some situations accessing data within a system in the presence of one controller could contravene confidentiality agreements between the processor and other controllers. For example, in the context of enterprise software companies, a software company may act as processor for a range of controllers, potentially including controllers that compete against each other in the same industry. Allowing on-site access to auditing teams from each of these controllers requires addressing a range of security and privacy issues arising from the controller's presence at a physical location where personal data of multiple controllers is stored. Similarly, a processor may engage a range of subprocessors; parties should have the ability to set out in a contract how the exercise of audit rights may apply in situations involving subprocessors.

Furthermore, the Article 28 SCCs, unlike the new draft standard contractual clauses for transferring personal data to non-EU countries (pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council), do not refer to the possibility of considering *'relevant certifications held by the data processor'* in place of audits.

Rather than provide for such on-site audits, we recommend the Article 28 SCCs be revised to recognize that parties should minimize the circumstances in which on-site audits are contemplated, particularly when on-site audits may create privacy and security risks. We also recommend that it be clarified that compliance with the SCC audit right requirement could be achieved through commitments to make compliance certifications/third party audit reports available to the customer or offer to provide necessary information through other virtual means. We also recommend that the parties be allowed to define by contract the "notice" to be given by the data controller to the data processors, including the specific time period, as well as the means to provide such notice.

c. Documented Instructions/Annex

A processor's obligation to process personal data on documented instructions from a controller is foundational to its role in protecting personal data. Clause 7(a) reflects this important limitation. At the same time, Clause 7(a) suggests that those documented instructions are to be set out in an Annex to the SCCs – an approach that does not reflect the many methods of instruction that controllers and processors can agree to recognize in connection with a product or service.

As a practical matter, the manner in which a controller's instructions are documented can vary greatly based on the type of service at issue. While some services may be suited to documenting instructions via a template, more complicated processing arrangements may envision multiple methods for a controller to provide documented instructions within a single service. Indeed, some services may be designed to permit controllers to instruct processors via the service itself. More generally, the applicable agreement between processor and customer should be recognized as the customer's instructions for the processing of customer personal data, that processing initiated by users of the SaaS service will be deemed customer instructions, and that additional or alternate instructions may be separately documented and agreed upon in writing.

We recommend revising Clause 7(a) to delete the reference to an Annex containing documented instructions.

Alternatively, Clause 7(a) could be revised to state that the Annex should specify the methods or format by which the controller will provide documented instructions, that may include the elements listed above – rather than the instructions themselves.

d. Data Subject Rights

The Article 28 SCCs address a data processor's obligation to assist a controller in fulfilling the controllers' obligations to respond to data subject rights requests only at a high level. We agree that Clause 8(a) is important in recognizing that data processors shall not respond to data subject requests directly, absent authorization from the controller. But we encourage Clause 8 be revised more broadly to set out potential ways that a processor may assist the controller in fulfilling its obligations to respond to data subject rights requests.

In particular, we recommend revising Clause 8 to include language allowing the companies to identify whether the processor will:

- *Provide the controller with the technical and organizational measures that allow the controller to directly access personal data held by the processor, in order for the controller to respond to data subject rights requests itself, or*

- *Respond to individual data subject rights request submitted to the processor by the controller, under a procedure the companies are to set out in an annex.*

This type of language could better assist companies in implementing the GDPR's requirements. It would also benefit individuals, since it can help companies to reach agreements in advance about how they will address data subject rights requests and thus reduce the potential volume of disputes about how requests are to be handled after they are received.

Furthermore, Clause 8(a) goes beyond article 28 GDPR as it requires the data processor to "promptly" notify the data controller about any request. We recommend revising Clause 8 to ensure that parties may determine the specific time period applicable in this respect and any associated costs arising from the data processor's provision of data subjects rights assistance.

e. Special Categories of Data

Clause 7.5 provides additional obligations regarding the processing of special categories of personal data. However, in many cases a processor may not know whether the data processed in connection with a service contains special categories of personal data. For example, a cloud storage provider may be contractually prohibited (or operationally prevented from an architecture perspective) from viewing data stored on its service, unless expressly authorized to do so by a controller – and thus may be unaware of whether that data contains personal data revealing racial or ethnic origin, health data, or other special categories of sensitive data. Such arrangements ultimately benefit individual data subjects, as they are in line with the 'data minimization' Principle relating to the processing of personal data in Article 5 of the GDPR.

We recommend deleting this requirement, for the reasons set out above. To the extent it is retained, it should be revised to require a controller to notify a processor when special categories of data are to be processed.

f. Erasure/Return

Clause 7.2 requires a processor to either delete or return data to a controller “upon termination” of services. While this is an important safeguard, the provision should help companies establish more details around the process for deletion or return of data. For example, companies may not wish for data to be returned or deleted immediately, which could hinder their ability to transfer that data to another company or renew services with the existing processor.

We recommend Clause 7.2 be revised to provide a method for companies to specify the timeframe after termination of services after which data will be deleted or returned. Alternatively, companies could be invited to specify a process for the deletion or return of data in an annex.

g. Data Breaches Notification

According to Clause 7.3.(a) of the SCCs, the data processor ‘*shall notify the data controller without undue delay and at the latest within 48 hours after having become aware of the breach.*’ This requirement goes beyond what is provided under the GDPR and therefore imposes a more onerous burden on the data processor. Specifically, Article 33(2) of the GDPR does not set out a timeframe during which the processor shall notify the controller. Rather, Article 33(2) GDPR indicates that “*the processor shall notify the controller without undue delay after becoming aware of a personal data breach.*” We recommend that the parties are given flexibility to determine the timelines as appropriate for their specific business relationship, as some parties may wish to increase the timelines, set no timelines, or even reduce the timelines to less than 48 hours. Making this language more flexible – rather than including a strict timeline – would better help companies more practically implement the “without undue delay” requirement under GDPR.

Furthermore, the Article 28 SCCs cover data breach notification in different clauses which is likely to lead to inconsistencies in practice (Clause 7.3; Clause 8). Unlike Clause 7.3, Clause 8 does not provide information as to the time period to be respected, but instead relies on the “without undue delay” standard found in Article 33(2) GDPR. In addition, both clauses do not provide the same information to be communicated by the data processor to the data controller.

We therefore *recommend regrouping provisions relating to data breaches so that they are all contained under clause 9. In addition, we recommend deleting the 48 hours notification requirement contained in Clause 7.3(a) as it is not required by the GDPR. Any time period to be respected by the processor in relation to data breach notifications should be solely addressed between the parties by contract and allow them to implement the GDPR’s “without undue delay” standard.*

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