October 18, 2020

BSA COMMENTS TO THE EUROPEAN DATA PROTECTION BOARD'S GUIDELINES 07/2020 ON THE CONCEPTS OF CONTROLLER AND PROCESSOR IN THE GDPR

BSA | The Software Alliance ("BSA"),[1] the leading advocate for the global software industry, welcomes the opportunity to provide feedback on the European Data Protection Board's Guidelines 07/2020 on the concepts of controller and processor in the GDPR (the "Guidelines"). 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, customer relationship management software, human resource management programs, identity management services, and 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.

As enterprise software companies, BSA members may act as both processors and controllers of personal data under the GDPR. For example, enterprise software companies will generally act as data processors when providing technologies and services used by other businesses and organizations; their business customers will accordingly act as controllers of personal data processed through those services. However, BSA members may sometimes also act as controllers in certain circumstances. For instance, a company that operates principally as a data processor may nonetheless be treated as a controller under the GDPR when it collects data for the purposes of providing services directly to consumers. BSA members therefore commend the EDPB for providing further guidance on the concepts of controllers and processors, which not only helps businesses determine their own roles and responsibilities under the GDPR but ultimately helps to better protect the privacy of personal data.

The EDPB's further guidance on controllers and processors serves at least three important objectives:

- ***Better Protecting Personal Data.*** Distinguishing between controllers and processors is important from a privacy perspective because it allows governments to place different obligations on different types of entities, based on their different roles in handling personal data. It also provides important clarity for individuals about how they can exercise their data

[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.

Avenue des Arts 44
1040 Brussels
Belgium

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

subject rights. As the GDPR reflects, both controllers and processors have strong obligations to safeguard personal data–and those obligations better protect personal data when they are based on the entity's role in handling that data. This approach helps to ensure that the rights and obligations reflected in any privacy or data protection law are carried through an ecosystem in which both controllers and processors may handle personal data.

- ***Clarifying Obligations for Businesses.*** The EDPB Guidelines will serve as an important reference to bring further clarity on the classification and roles of controllers and processors, and their corresponding requirements, especially in the context of complex processing operations. This is particularly important for businesses that may function as processors in some contexts and controllers in others. The controller/processor distinction is also critical to technological developments such as artificial intelligence (AI). AI tools will be used and deployed in a variety of different fields of human activity, including in the business-to-business context. For example, widespread use of AI-enabled manufacturing technology can help create sustainable products in a broad array of industries such as aeronautics and manufacturing. Ensuring that the foundational concepts reflected in the roles of controllers and processors extend to processing conducted in these new technological scenarios is critical to maintaining a high level of data protection.

- ***Promoting Interoperability Among Privacy and Data Protection Laws.*** Privacy and data protection laws worldwide distinguish between controllers and processors, reflecting a global standard that recognizes these different types of entities play important but different roles in handling personal data.[2] The distinction between data processors, which handle a data subject's personal data on behalf of other businesses, and data controllers, which determine the purposes and means of processing a data subject's personal data, is also foundational to leading international privacy standards and voluntary frameworks that promote cross-border data transfers. When laws and frameworks reflect this important distinction, it creates greater interoperability, by enabling processors subject to one law to more readily map those obligations to other laws. For these reasons, BSA has advocated for the concepts of controllers and processors to be adopted in new privacy and data protection laws, including in the United States and India, among many other jurisdictions.[3] The EDPB's Guidelines can promote greater interoperability among global privacy and data protection laws by further emphasizing the importance of these concepts and providing clarity on the lines between processors, controllers and joint controllers.

Recognizing the importance of the EDPB's Guidelines in promoting interoperability, privacy, and clarity, BSA would like to offer specific comments on five aspects of the Guidelines. In doing so, we have sought to highlight the practical application of the Guidelines to the business relationships established between controllers and processors.

---

[2] For example, privacy laws in Hong Kong, Malaysia, and Argentina distinguish between "data users" that control the collection or use of data and companies that only process data on behalf of others. In Mexico, the Philippines, and Switzerland, privacy laws adopt the "controller" and "processor" terminology. Likewise, the APEC Cross Border Privacy Rules, which the US Department of Commerce has strongly supported and promoted, apply only to controllers and are complemented by the APEC Privacy Recognition for Processors, which help companies that process data demonstrate adherence to privacy obligations and help controllers identify qualified and accountable processors. In addition, last year the International Standards Organization published its first data protection standard, ISO 27701, which recognizes the distinct roles of controllers and processors in handling personal data.

[3] Full testimony before US Senate available here: https://www.bsa.org/policy-filings/bsa-testimony-before-senate-committee-on-commerce-science-and-transportation-on-policy-principles-for-a-federal-data-privacy-framework-in-the-united-states; https://www.bsa.org/news-events/news/bsa-statement-on-comments-filed-to-the-joint-parliamentary-committee-on-the-personal-data-protection-bill-2019

1. ***Determining Who Is a Controller.*** At the outset, it is critical that companies can determine, in practice, whether they are acting as a data processor or a data controller for a particular service. We commend the Guidelines for recognizing this is a fact-specific inquiry, which will depend on the "actual activities" of an entity and reflects a "factual rather than a formal analysis."[4] As a result, we agree with the Guidelines that an important question is "where to draw the line between decisions that are reserved to the controller and decisions that can be left to the discretion of the processor."[5]

   Because controllers and processors will continue to adopt a range of new technologies, products, and services, it is important that the EDPB's guidance be sufficiently adaptable to address a range of new scenarios. In this respect, the approach reflected in Part I, Section 2.1.4 is helpful in providing an illustrative list of questions that companies should consider in deciding what are "essential means" and what are "non-essential means," along with a set of examples that companies can draw on in making this determination.

   As the Guidelines recognize, in many circumstances a controller may determine the "essential means of processing" by actively choosing to engage a processor that offers a service that the processor has preliminarily defined in a specific way, and which the controller has determined fits its requirements. In such cases, the Guidelines recognize that a controller "must make the final decision to actively approve the way processing is carried out" – by choosing to use the defined service.[6] At the same time, portions of the Guidelines suggest a controller retains the ability to request changes to defined services – which in practice may not be possible for global services designed to be offered in the same manner to businesses worldwide. In those circumstances, then, the controller's role should be choosing to either use the defined service in processing personal data (if the service meets the controller's requirements) or to not use the defined service (if it does not). Paragraph 82 reflects this approach, by recognizing a controller is either to "actively approve the way processing is carried out" – by deciding to use the defined service – "and/or" be able to request changes if necessary. We suggest revising the third sentence of Paragraph 28 to also incorporate this important "and/or" language:

   > "Even if the processor offers a service that is preliminarily defined in a specific way, the controller has to be presented with a detailed description of the service and must make the final decision to actively approve the way the processing is carried out and/or to be able to request changes if necessary."

2. ***Role of Processors.*** We welcome the Guidelines' recognition that processors have important obligations to handle personal data responsibly. Under the GDPR, these obligations include ensuring that persons authorized to process personal data are committed to confidentiality, implementing appropriate technical and organizational measures, and designating a data protection officer under certain conditions.[7] We suggest clarifying three aspects of the Guidelines to better reflect a processor's role in: (1) documenting instructions from a controller, (2) assisting a controller in complying with data subject requests, and (3) updating a controller about security changes.

[4] Guidelines, ¶¶ 12, 20.
[5] Guidelines ¶ 37.
[6] Guidelines ¶ 28.
[7] Guidelines ¶ 91.

Documented instructions. A processor's obligation to process personal data on documented instructions from a controller is foundational to its role in protecting personal data. As a practical matter, however, 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 processers via the service itself. We accordingly suggest that language in the Guidelines recommending use of a template to document instructions be revised to recognize this approach may be appropriate only for certain services. This could be addressed by revising Paragraph 115 to state:

> "Because such instructions must be documented, certain services may choose to ~~it is recommended to~~ include a procedure and a template for giving further instructions in an annex to the contract or other legal act. Alternatively, the~~y~~ instructions can be provided in any written form (e.g. email), as long as it is possible to keep records of such instructions. In any event, to avoid any difficulties in demonstrating that the controller's instructions have been duly documented, the EDPB recommends keeping such instructions together with the contract or other legal act, when possible."

Assisting a controller with data subject requests. The Guidelines recognize that controllers, rather than processors, are obligated to respond to consumer rights requests.[8] At the same time, under the GDPR a processor is obligated, insofar as possible, to assist a controller in responding to such requests.[9] The nature of a processor's assistance will vary greatly between services, based on the nature of the service and the relationship among the processor, controller, and data subject. We recommend recognizing that in many cases, a processor may assist a controller by providing the controller with the technical measures or tools needed to fulfil a data subject request. We accordingly suggest revising Paragraph 128 to state:

> "While the assistance may simply consist of promptly forwarding any request received, in some circumstances the processor will be given more specific, technical duties, especially when it is in the position of extracting and managing the personal data. In many cases, however, a processor may take reasonable steps to assist a controller by enabling the controller to extract and manage such personal data in response to data subject requests. For example, a cloud service provider may assist a controller by providing the controller, where technically feasible, with the tools needed to access, correct, and delete personal data stored on the cloud service."

Notice regarding security changes. The Guidelines also emphasize the importance of securing personal data held by both controllers and processors.[10] In doing so, the Guidelines recognize that the level of instructions to be provided by a controller to a processor regarding security measures will depend on the specific service.[11] For example, in some cases, a controller may describe minimum security objectives and ask the processor to propose specific measures to achieve them. That practical approach may be inadvertently undercut by other language that could be read to suggest a controller must approve *any* change affecting security measures. We

[8] Guidelines ¶ 129.
[9] Guidelines ¶ 127.
[10] Guidelines ¶¶ 122-124.
[11] Guidelines ¶¶ 124.

recommend clarifying that a controller only needs to consent to changes that are material or adverse, rather than all changes. This can be achieved by revising Paragraph 123 to state:

> "As indicated earlier, the processing contract should not merely restate the provisions of the GDPR. The contract needs to include or reference information as to the security measures to be adopted**, an obligation on the processor to obtain the controller's approval before making material or adverse changes**, and a regular review of the security measures so as to ensure their appropriateness with regard to risks, which may evolve over time. The degree of detail of the information as to the security measures to be included in the contract must be such as to enable the controller to assess the appropriateness of the measures pursuant to Article 32(1) GDPR. . ."

Temporary employees. Finally, we commend the Guidelines for recognizing that interim staff who are authorized to process personal data should be viewed as "under the direct authority of the controller or processor" and not as third parties.[12]

3. ***Recognizing that Processors May Use Data Without Becoming Joint Controllers***. Despite the Guidelines' clarity in defining controllers and processors, the discussion of joint controllers risks conflating these distinct roles. In particular, the portion of the Guidelines addressing joint controllers should be refined to clarify their distinct role and to avoid inadvertently limiting the ability of data processors to maintain and improve the services they provide to controllers. We suggest three potential ways to address these concerns.

   First, the examples in Part I, Section 3.2.2 could be modified to recognize that several of the contemplated scenarios involve two or more joint controllers that together hire a data processor. By revising these examples to identify the data processor in each scenario, the examples can better reflect the full set of entities handling personal data. This approach would also complement the processor examples provided on Page 23. We suggest two revisions:

   - *Travel agency example*. In this example on Page 20, a travel agency, hotel chain, and airline act as joint controllers of a traveler's information. All three entities work together to set up an internet-based common platform. The draft example suggests that the platform carries out processing at the direction of and on behalf of all three joint controllers. If that is the case, the platform should be recognized as a processor of personal data on that platform, acting on behalf of the joint controllers.

   - *Marketing example.* In this example on Page 21, companies A and B launch a co-branded product and share data from their respective client databases to decide on a list of invitees to the event. While both companies are joint controllers for the purposes of processing data relating to the promotional event, the draft example could be modified to recognize that any companies hired by A and B to send out invitations would act as processors that handle data on behalf of the two joint controllers.

   Second, the Guidelines should expressly recognize that data processors do not become joint controllers when they use personal data to improve services provided to a controller. As a

[12] Guidelines ¶ 86.

practical matter, data processors are often asked or required to improve services offered to controllers, such as by developing bug fixes or upgrades, implementing security measures, or to improve the underlying technology utilized by the services, so that those services are as accurate and reliable as possible throughout the course of their business relationship. The controller seeks to benefit from services and underlying technologies that have ongoing improvement. In some scenarios, maintaining and improving a service will require processing personal data handled in connection with that service. For example, an email provider may offer a service that includes filtering out junk mail for its business customers. To improve the accuracy of its junk mail filter, the provider may use personal data processed via the service, such as emails that the business customer identified as potential junk mail.

An overly broad reading of certain statements within the discussion of joint controllership could inadvertently limit processors' from using data to create more reliable and accurate services, by conflating these actions by a processor with the decisions made by joint controllers. To the extent the Guidelines were read so broadly as to treat an email provider like the one described above as a joint controller, it could severely limit processors' ability to offer the accurate and reliable services demanded by their business customers and to uphold data subjects rights. That result should not occur, however, because the processor is improving the service at the direction of a controller, and on its behalf. Similarly, in the context of cybersecurity, a processor may process personal data transiting its systems to better protect the services offered to controllers, including through threat detection, security reporting, and analyzing security trends and data patterns, without transforming the processor into either a joint controller or an independent controller. We suggest clarifying this result by revising two aspects of the Guidelines:

- *Modifying headhunter example.* In this example on Page 22, Company X has compiled a database of jobseekers in connection with providing a headhunting service. It helps Company Y recruit new staff, both by reviewing candidates in its existing database and candidates that directly contacted Company Y. The draft Guidelines treat Company X as a joint controller, because the use of its own database "enhances the matching between job offers and job seekers, thus increasing its revenues." To the extent that reasoning is extended to other scenarios, it could misconstrue the role of data processors that use existing databases to provide services on behalf of controllers. For example, a processor may maintain a database that includes information on known security vulnerabilities and combine information from that database with information provided by a controller, to better secure the relevant service it provides to a controller. When a processor undertakes these actions on behalf of a controller and in line with its direction, it should remain a processor. The example could recognize as much by adding a sentence that states:

  > <u>"A different result may be reached when a processor accesses an existing dataset to provide a requested service to a controller, without using the personal data for unrelated purposes."</u>

- *Expressly recognize the ability of processors to improve services.* The Guidelines should also recognize that when a processor processes personal data provided by a controller to improve services, including to improve cybersecurity, it remains a processor so long

as its acts on behalf of and at the direction of the controller customer.[13] That result logically flows from several statements in the Guidelines, including recognizing that when an "entity involve[d] in the processing does not pursue any purpose(s) of its own in relation to the processing activity, but is merely being paid for services rendered, it is acting as a processor rather than as a joint controller." We suggest adding an additional sentence to Paragraph 60 stating that:

> "For example, a processor may, in accordance with instructions from a controller, process personal data on behalf of a controller to improve the services provided to the controller, without giving rise to joint controllership."

Third, clarify language addressing a controller's use of systems and tools developed by other entities. In discussing joint controllers, the Guidelines acknowledge that using a common data processing system or infrastructure "will not in all cases lead to qualify the parties involved as joint controllers, particularly when . . . the provider is a processor in the absence of any purpose of its own."[14] Yet other unintentionally broad statements could confuse the clear recognition that controllers may engage processors, consistent with their respective roles, without either becoming a joint controller. For example, Paragraph 65 suggests an entity's choice "to use for its own purposes a tool or other system *developed by another entity*, allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities." This broad language should be revised to avoid suggesting that a controller cannot hire a processor to use tools developed by that processor. We suggest two changes:

> First, Paragraph 65 could be revised to state: "Furthermore, the choice made by an entity to use for its own purposes a tool or other system developed by another ~~entity~~ controller, which allows~~ing~~ for both controllers to process ~~the processing of~~ personal data, may ~~will likely~~ amount to a joint decision on the means of that processing by both controllers ~~those entities~~."
>
> Second, in the example of marketing operations on Page 23, the final sentence could reiterate that joint controllers may together engage a processor, by stating: "Under these circumstances, each company is thus a separate controller and the mother company acts as a processor with respect to the personal data processed by each controller."

4. ***Ensuring Practical Application of Subprocessor Requirements.*** The Guidelines helpfully recognize the important role of subprocessors, which can be critical in providing the technology products and services needed by today's businesses, in particular in a multi-layer cloud computing environment. Just as important, the Guidelines emphasize the need for companies to address the practical issues relating to the engagement of subprocessors in the contract governing a processor's activity. These include providing for either specific or general authorization to engage subprocessors, as well as the timeframe for the controller's approval or objection and how the parties intend to communicate regarding this topic.[15]

[13] A company that provides services to other businesses may become a controller if it were to use data for improvement of its systems to benefit itself solely and not its controller customers. However, this situation would not create a joint controllership.
[14] Guidelines ¶ 66.
[15] Guidelines ¶¶ 147 – 157.

At the same time, other statements depart from this practical approach, and suggest that a processor must "actively inform the controller" of any change to a list of its subprocessors.[16] We suggest refining this language to better reflect the approach set out in other portions of the Guidelines and encourage companies to address by contract the frequency and means of updates regarding new subprocessors. By addressing these important issues via contract, companies can help to ensure notices regarding new subprocessors 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 processors 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. We therefore suggest revising the language in Paragraph 125 note 46 to state:

> "In this regard it is, by contrast, e.g. not sufficient for the processor to merely provide the controller with a generalized access to a list of the sub-processors which might be updated from time to time, without pointing to each new sub-processor envisaged. Rather, controllers and processors should address by contract the frequency and means of actively informing the controller of any new subprocessors. ~~In other words, the processor must actively inform the controller of any change to the list (i.e. in particular of each new envisaged sub-processor).~~"

We also commend the Guidelines for recognizing that the GDPR's obligation to subject subprocessors to the "same" obligations imposed on a processor should be construed in a "functional rather than in a formal way."[17] Given the different types of services offered by subprocessors, there will frequently be situations where the "same" obligation imposed on a processor does not exist, given the business model of a particular subprocessor. The following edit to Paragraph 157 would provide additional clarity:

> "Imposing the "same" obligations should be construed in a functional rather than in a formal way: it is not necessary for the contract to include exactly the same words as those used in the contract between the controller and the processor, but it should ensure that the relevant obligations in substance are the same. This also means that if the processor entrusts the sub-processor with a specific part of the processing, to which some of the obligations cannot apply, such obligations should not be included "by default" in the contract with the sub-processor, as this would only generate uncertainty."

5. ***Reducing Security and Privacy Concerns Raised by Audits***. As the Guidelines recognize, the GDPR explicitly incorporates the accountability principle, under which a controller is to verify the guarantees made by a processor. Moreover, processors may demonstrate compliance with their obligations by providing "reports of external audits" to a controller.[18] Processors may also

[16] Guidelines ¶ 125, n. 46.
[17] Guidelines ¶ 157.
[18] Guidelines ¶ 93.

provide other relevant documentation to a controller, such as a privacy policy, terms of service, records of processing activities, records management policy, information security policy, and internationally-recognized certifications such as those in the ISO 27000 series.[19]

At the same time, several statements in the Guidelines reference the use of on-site audits, which have the potential to increase security and privacy concerns, rather than reduce them. 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 will require 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. We accordingly suggest the Guidelines emphasize that reports of external audits and audit questionnaires may provide the controller with the appropriate information to assess a processor's guarantees.[20] By the same token, parties should minimize the circumstances in which on-site audits are contemplated, particularly when on-site audits may create privacy and security risks. We therefore suggest revising the language in Paragraph 141 to state:

> "Further details shall also be set out in the contract regarding the ability to carry out and the duty to contribute to inspections and audits by the controller or another auditor mandated by the controller. The parties should cooperate in good faith and assess whether and when there is a need to perform audits on the processor's premises. In doing so, the parties should limit the use of on-site audits that may raise privacy and security concerns, such as when a processor's facility is used to process personal data held on behalf of multiple controllers. Alternatively, processors should be able to comply with audit requirements by offering to make compliance certifications/third party audit reports available to the customer or offer to provide necessary information through other means. Likewise, specific procedures should be established regarding the processor's and the controller's inspection of subprocessors (see section 1.6 below)."

BSA and its members appreciate the opportunity to comment on these guidelines and stand ready to further assist the Board as it finalizes its guidance.

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

[19] Guidelines ¶ 93.

[20] See Irish Data Protection Commission, Guidance for Organisations Engaging Cloud Service Providers (Oct. 2019), available at https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20for%20Engaging%20Cloud%20Service%20Providers_Nov19.pdf ("As noted above, an audit questionnaire may be sufficient in some cases to meet cloud providers obligations under Article 28(3)(h) GDPR . . . Note that, as cloud providers will typically provide services to multiple data controllers and have security and confidentiality obligations with each, the extent and detail of what is made available in that audit may be restricted.").