December 21, 2020

BSA COMMENTS TO THE EUROPEAN DATA PROTECTION BOARD'S RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA

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 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the "Recommendations"). 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 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.

As enterprise software companies, BSA members help companies worldwide use digital tools to provide products and services to their customers. Those customers – and the companies that serve them – rely on the ability to send data across international borders, subject to appropriate privacy projections. Cross-border transfers are needed for a range of consumer-facing services such as e-commerce (which depend on moving data across borders to track and fulfil orders), and business-to-business services across industries ranging from automotive to agriculture, finance, healthcare, manufacturing, human resources, and many others. Indeed, companies that operate globally must send data across international borders to perform daily business transactions like processing payroll, sending emails, or storing documents on cloud-hosted servers. This work has taken on increased importance amid the COVID-19 pandemic, which has spurred companies in all industries to increasingly rely on remote workplace tools and cloud-based technologies and has enabled medical researchers and hospitals worldwide to coordinate their research and treatment efforts: in fact, COVID-19 vaccines are being developed at an unprecedented pace partly thanks to researchers and developers' ability to access electronic health data and use supercomputers to rapidly search for medicines that can be repurposed as effective COVID treatments.

[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.

Avenue des Arts 44
1040 Brussels
Belgium

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

BSA members have long recognized the importance of responsible international data transfers. In 2016, BSA was granted permission to participate as an amicus in *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ("*Schrems II*"), and we participated before both the Irish High Court and the Court of Justice of the European Union ("CJEU").[2] In those proceedings, we emphasized the importance of the Standard Contractual Clauses ("SCCs"), which provide a vital privacy-protective mechanism that is used by millions of companies—based in countries worldwide—that transfer data in and out of Europe. Nearly 90 percent of companies transferring data out of the EU rely on SCCs.[3]

We commend the EDPB for publishing the Recommendations to help companies conduct a case-by-case assessment of their data transfers after the *Schrems II* decision. Our comments on the Recommendations underscore the importance of this case-by-case assessment, which is set forth in the CJEU's decision (but also the GDPR) and is built out in the six-step process envisioned by the Recommendations. However, we are concerned that several of the illustrative use cases set out in Annex 2 to the Recommendations are in conflict with this case-by-case approach. Indeed, several of these use cases may not reflect the full set of circumstances the CJEU directed companies to consider when assessing transfers after *Schrems II*. We accordingly urge the EDPB to more fully realize the case-by-case assessment in the Recommendations and to ensure the use cases included in Annex 2 reflect the full range of circumstances relevant to data transfers, in line with the CJEU's decision.

I. *Data Transfers Must Be Assessed on a Case-By-Case Basis*

The CJEU's *Schrems II* decision recognized the continued validity of data transfers conducted pursuant to SCCs, which underpin transfers of personal data from the EU not only to the US, but to over 180 countries—including Australia, Singapore, South Korea, Brazil, India, and Mexico, among many others. At the same time, the CJEU emphasized that companies that transfer data from the EU to a third country pursuant to SCCs must conduct a "case-by-case" assessment of those transfers.[4] This assessment ensures that companies comply with the GDPR's requirement that personal data be transferred to a third country only if it is subject to appropriate safeguards.[5] This approach further aligns the principle contained in GDPR Article 24 together with Recitals 74, 75 and 76 of the GDPR; namely that such risk should be evaluated on the basis of an "objective assessment" that examines whether data processing operations "involve a risk or a high risk". In particular the CJEU recognized that in some cases controllers and processors may need to adopt "supplementary measures" in addition to the SCCs to "ensure compliance with [the required] level of protection."[6]

The EDPB's Recommendations set out how companies are to conduct a case-by-case assessment of their data transfers. Under the six-step process put forward in the Recommendations, companies are to:

1) Know their transfers
2) Identify the transfer tools on which they rely
3) Assess whether the Article 46 transfer tool relied upon is effective "in light of all the circumstances of the transfer"

---

[2] *See* https://www.bsa.org/news-events/news/bsa-welcomes-irish-high-courts-decision-to-grant-bsa-amicus-status.

[3] IAPP-EY Annual Governance Report 2019 (Nov. 6, 2019), available at: https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/ (stating approximately 88% of companies transferring data out of the EU rely on SCCs).

[4] *Schrems II*, Para. 134.

[5] GDPR Art. 46.1.

[6] *Schrems II*, Para. 133. In October, BSA published seven high-level principles that companies can use in developing legal, technical, and organization measures suitable for their own particular services, in light of the *Schrems II* decision. See BSA Principles: Additional Safeguards for SCC Transfers, available at https://www.bsa.org/files/policy-filings/10222020bsascctransfers.pdf

4) If not, adopt supplementary measures
5) Implement certain procedural steps for effective supplementary measures, and
6) Re-evaluate the assessment at appropriate intervals

As a general remark, we would recommend that the published guidance should not be understood as exhaustive or binding. Companies must work to devise further effective measures that implement the CJEU's requirements. The EDPB should clarify and emphasize that measures and use cases envisioned are not exhaustive and other measures not contemplated may prove sufficient.

Although we recognize this six-step process is important in guiding companies in conducting a case-by-case assessment of their data transfers, we urge two changes to more closely align the process with the requirements set out by the CJEU.

- ***First, the Recommendations should more clearly reflect "all the circumstances" of a data transfer.*** In describing the validity of transfers conducted pursuant to SCCs, the CJEU emphasized at least five times that a supervisory authority evaluating the validity of a transfer must take into consideration "*all the circumstances* of the transfer."[7] Indeed, the CJEU focused several times on the question posed to it by the referring court – asking it to "specify *which factors* need to be taken into consideration" in assessing a data transfer.[8] In response, the CJEU explained that a supervisory authority determining whether to suspend or prohibit a data transfer must assess "in the light of *all the circumstances* of that transfer" whether the SCCs "are not or cannot be complied with" and whether the protection of the data "cannot be ensured by other means."[9] As set out below, the current Recommendations focus on a narrow set of relevant circumstances; these should be broadened to more fully reflect the entire set of particular circumstances relevant to transfers and should expressly recognize the relevance of considering the 'likelihood' of government requests for the specific data to be transferred.

  Step Three of the Recommendations risks undermining the CJEU's broad requirement to consider "all" circumstances of a transfer, by reading the relevant circumstances narrowly. While the heading of Step Three directs companies to assess whether a transfer tool is effective "in light of all of the circumstances of the transfer," the substance of Step Three puts forward a narrow view of "all" such circumstances. For example, Paragraph 33 highlights several applicable circumstances, including the purpose for which data is transferred, the types of entities involved in the transfer, the sector in which the transfer occurs, the categories of data transferred, whether the data will be transferred or instead stored in the EU but accessed remotely from a third country, the format of the data to be transferred, and the possibility of onward transfers. But this list should be much broader, reflecting other foundational aspects of a data transfer including the type of personal data, the nature and type of service for which the data is transferred (e.g., consumer-facing or business-to-business), the volume of personal data transferred, and the extent to which a customer makes decisions about where the data is transferred and stored, among others.

  More fundamentally, Step Three should be updated to expressly recognize that "all the circumstances" to be considered include whether a company has been subject to a particular type of

[7] *Schrems II*, Paras. 112, 113, 121, 146, 203.3 (emphasis added).
[8] *Schrems II*, Para. 90. *See also Schrems II* Para. 102 ("The referring court also seeks to ascertain *what factors* should be taken into consideration for the purposes of determining the adequacy of the level of protection where personal data is transferred to a third country pursuant to standard data protection clauses") (emphasis added).
[9] *Schrems II*, Para. 146 (emphasis added).

government access request and if so, the amount, nature, and frequency of such requests. Read broadly, language in Step Three could discourage companies from considering this objective and relevant information in their assessment. For example, Paragraph 42 urges companies to consider publicly-available legislation, and when such information is unavailable, urges them not to "rely on subjective [factors] such as the likelihood of public authorities' access to your data." This approach fails to recognize that important objective indicators exist about how often government authorities actually execute requests in practice for the particular type of data to be transferred. For example, a company will know if it has ever been subject to a particular type of government request and, if so, how many – an objective fact that is highly relevant to its assessment of a particular transfer. We would specifically recommend clarifying in Paragraph 42 that, while the likelihood of public authorities' access in the specific case of a transfer scenario cannot be used as the sole criteria to determine the risk, it *needs to be factored* in the assessment as the corresponding safeguards will in turn have to be developed based on such risks.[10]. Indeed, the realistic risk of being subject to such a request varies significantly based on the business model (data transfers for business purposes vs consumer-facing services) or the category of data (business data vs private information). It is not proportionate to request companies that receive no or few government requests to introduce new measures to the same extent as those companies who regularly are the subject of these requests. This also fails to include a risk-based approach, despite the fact that the GDPR refers on several occasions to the necessity of applying a risk-based approach to various processing activities.

The EDPB recommendations should therefore specify that companies assessing a transfer take into account the likelihood that the transferred data will actually be subject to a government access demand.

The actual practices of government authorities are a key consideration in the CJEU's reasoning that must be taken into account under the *Schrems II* decision. The CJEU repeatedly emphasized that companies "must" take into account the "relevant aspects" of a country's legal system when assessing data transfers, including those aspects set out in the non-exhaustive list in GDPR Article 45(2).[11] That list includes not only the existence of "relevant legislation," but also the "*implementation* of such legislation."[12] The CJEU's decision accordingly stressed this need to consider how government authorities function in practice – not just in theory. For example, the CJEU emphasized that its examination of the SCCs focused on whether those clauses "make it possible, *in practice*" to provide the required level of protection and whether they "*in practice*, ensure" the protection of personal data.[13] Similarly, the CJEU emphasized that the validity of a particular SCC transfer turns on whether it "incorporates effective mechanisms that make it possible, *in practice*, to ensure compliance with the level of protection required by EU law."[14] As a result, the CJEU recognized there are situations where, "depending on the law *and practices* in force in the third country concerned, the recipient of [] a transfer is in a position to guarantee the necessary protection" of data through SCCs alone –

[10] For example, these may include binding contractual commitments by the data recipient to challenge government access requests in certain circumstances.
[11] *Schrems II*, Paras. 203.2, 104, 105,
[12] GDPR, Art. 45(2) (emphasis added) ; *see also Schrems II* Para. 87 (citing GDPR, Art. 45(2)). .
[13] *Schrems II,* Paras. 137, 148 (emphases added). Indeed, the CJEU recognized that Mr. Schrems' complaint focused on actual practices, alleging "that the law *and practice*" in force in the United States did not ensure adequate protection of personal data. *Schrems II,* Para. 52 (emphasis added).
[14] *Schrems II*, Para. 137. *See also Schrems II* Para. 141 (emphasizing that it is "*compliance* with an obligation" to provide access to government authorities third party law that is to be treated as a breach of the SCCs).

whereas in other situations the SCCs "might not constitute a sufficient means of ensuring, *in practice*, the effective protection of personal data."[15]

Under the CJEU's decision in *Schrems II*, companies must evaluate the risks that may arise from transfers in light of all current and relevant legislation, guidance, and implementing measures which may give rise to meaningful limitations and means of redress which bear on the level protection in the sense of the GDPR Article 45(2). Given the importance of a full and current understanding of these relevant aspects, we encourage the EDPB to consider further emphasizing the relevance of sources of information in the jurisdiction of the data importer (not just the data exporter), such as independent and competent administrative and judicial authorities, NGOs, associations, and academic institutions.

In evaluating all circumstances of a transfer, companies should also assess the actual practices of government authorities to identify scenarios that may be low risk and those that may be higher risk. Identifying such risks – and tailoring additional safeguards accordingly – is consistent with the GDPR's overarching risk-based approach to data protection and its emphasis on proportionality. As the Article 29 Working Party recognized in supporting a risk-based approach to data protection frameworks, although the "[f]undamental principles" applicable to companies handling personal data should remain the same, a company's implementation of accountability tools and measures "can and should be varied according to the type of processing and the privacy risks for data subjects."[16] Furthermore the provisions of GDPR Article 24 on assessing risk, notes that "appropriate … measures should "tak[e] into account the nature, scope, context and purposes of processing as well as the risks …[to] the rights and freedoms of natural persons".

We accordingly urge Step Three be clarified to expressly recognize that companies should consider the actual practices of government authorities in assessing "all the circumstances" of that transfer, in line with the CJEU's decision. If companies do not take into account this important and objective information, it may convert their assessments into theoretical exercises, which do not reflect the actual practices and circumstances relevant to a transfer. That narrow reading is contrary to the CJEU's direction that all "relevant aspects" of a third country's legal system be considered.[17]

- ***Second, the Recommendations should clarify that additional safeguards may be effective whether they are technical, contractual, or organizational***. As written, many aspects of the Recommendations focus on technical safeguards, which appear to be given more emphasis than the contractual and organizational safeguards discussed in the Recommendations. That emphasis is inconsistent with the CJEU's decision, which does not suggest that one type of safeguard should be given more consideration than another type. The GDPR is intended to be a "technology neutral" legislation that avoids dictating technical requirements in order to allow companies sufficient flexibility to consider

[15] *Schrems II*, Para. 126 (emphases added). Despite the Recommendations' approach to discounting actual practices in this portion of Step Three, other aspects of the Recommendations reinforce the importance of looking to how authorities function in practice. *See, e.g.*, Recommendations Para. 44 (observing that a transfer tool may be ineffective "owing to the third country's legislation *and/or practices applicable to the transfer*") (emphasis added); Recommendations Para. 110 (observing that a "warrant canary" safeguard may be appropriate for certain data importers that are theoretically subject to government access requests but not have received such requests). Recommendations Para. 112 (focusing on review of "any order to disclose data"); Recommendations Paras. 114, 118 (similarly focusing on specific "orders" actually received by a data importer); Recommendations Paras. 124, 127, and 129 (describing organizational measures that address "requests" actually received by a data importer).

[16] *See* Article 29 Working Party, Statement on the Role of a Risk-Based Approach in Data Protection Frameworks, May 30, 2014, at p.3, *available at* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

[17] *Schrems II*, Para. 203.2 (requiring that "the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses . . . and, as regards any access by the public authorities of that third country to the personal data transferred, the *relevant aspects* of the legal system of that third country") (emphasis added).

"[what is] state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons… to ensure a level of security appropriate to the risk".[18] Indeed, the GDPR elevates contractual commitments – not technical ones – and emphasizes that controllers and processors "should be encouraged to provide additional safeguards *via contractual commitments* that supplement standard protection clauses."[19] Moreover, the ability to provide safeguards via contract is foundational to the principle of accountability, which the Recommendations seek to embody.

We urge you to modify the Recommendations to reflect the importance of contractual and organizational safeguards, which companies must also consider after conducting a case-by-case analysis of their own data transfers. For example, in Step Four, the Recommendations suggest that "contractual and organizational measures alone will generally not overcome access to personal data by public authorities of the third country."[20] But that statement is inconsistent with the CJEU's decision, which directs companies to implement *appropriate* safeguards – without requiring those safeguards to be technical in nature. As the CJEU stated, in the absence of an adequacy decision, "the controller or, where relevant, the processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards" that "should ensure compliance with data protection requirements."[21] The CJEU's decision does not mention the term "technical" safeguards – and the Recommendations' heavy reliance on such safeguards, to the potential exclusion of contractual and organizational safeguards, is accordingly misplaced. Additional statutory protections can be required through contractual measures which make it more challenging, if not impossible to access a certain category of data. In addition, enhanced redress mechanisms are in place in third countries for certain categories of protected recipients (e.g. in healthcare). We also seek to point out that civil causes of action and compensation constitute redress and effective legal remedies in some countries (e.g. the US) – the EDPB guidance should take into account the full range of redress mechanisms. Contractual measures such as the obligation to challenge incoming requests, to disclose as much as legally allowed to the data subject/data exporter, to notify if legally allowed, and to fully notify of and provide legal assistance to exercise redress, are powerful contractual safeguards.

The guidance should therefore reflect that such technical, contractual, or organizational safeguards should be proportionate to the type and amount of processing occurring.

[18] GDPR, Article 32.
[19] GDPR, Recital 109.
[20] *Schrems II,* Para. 48.
[21] *Schrems II*, Para. 131.

II. *Several Illustrative Use Cases Risk Undermining the Case-By-Case Approach Set out in the Recommendations and Should Be Revised*

The Recommendations' case-by-case approach to assessing data transfers is critical to helping companies identify and implement appropriate safeguards. At the same time, several of the use cases in Annex 2 of the Recommendations risk undermining this careful assessment, by taking into account only a narrow range of circumstances.

We accordingly urge clarification of the use cases in Annex 2 to: (1) broaden the range of "all circumstances" that companies must consider in assessing data transfers, and (2) emphasize the importance of organizational and contractual safeguards, in addition to technical safeguards. Two use cases illustrate these concerns:

- ***Use Case Six: Transfers to cloud services providers or other processors which require access to data in the clear.*** Use Case Six focuses on transfers to cloud service providers or other processors that require access to unencrypted data. This use case introduces a global concern as to the functioning of any company which relies on transfers to provide services to customers for which accessing the data in clear is crucial and which, as a consequence, cannot render data unreadable without impeding the provision of their services. The finding that EDPB "cannot envision technical measures that would prevent access" has the potential to have a global impact on nearly every company, including multinational corporations that are critical to economies and research being performed around COVID-19. Such a broad statement is inconsistent with the way business is performed today and raises serious concerns about the continued data flows between the EU and its major trading partners. This use case only considers three circumstances relevant to the envisioned transfer, however, and not the broad range of circumstances the CJEU directed be taken into account in assessing data transfers. For example, the third factor is focused on the "power" granted to public authorities in the recipient country to access the transferred data. As noted above, however, the *practice* of public authorities in exercising those powers is among "all the circumstances" relevant to any transfer. Indeed, in countries that may lack clear written rules regarding public authorities' powers to access data, such practices may be among the most meaningful objective information for companies in assessing the circumstances relevant to a data transfer.

  Additionally, Use Case Six might call into question the ability for all companies to ensure the security of their digital services. For example, global cloud service providers offer cutting-edge security services, currently protecting sensitive data from attacks from malicious actors. Strict prohibitions on decryption at any point in the processing undermines IT security as the so-called packet inspection is necessary to hinder the transfer of malicious traffic and to absorb DDoS attacks. If decryption is prohibited, many businesses would struggle to maintain a high level of IT security, and IT network and critical infrastructure would be impacted as a whole. The European Agency for Cybersecurity (ENISA) recently highlighted the increasing number of phishing campaigns and ransomware attacks on healthcare systems since the beginning of the COVID-19 crisis[22]. The reality of today's cyber threat landscape means that Europe cannot afford to lower cyber security standards or compromise the resilience of its critical infrastructure by hampering access to security solutions and measures.

[22] https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic

On the basis of the three narrow circumstances discussed in Use Case Six, the EDPB posits that it is incapable of envisioning an effective *technical* measure to prevent access from infringing on data subject rights.[23] This statement may inadvertently narrow the scope of measures that may be considered. While indicative examples may be helpful to provide a sense of the limits of responsive measures, it should not create a perception that the measures and use cases described are prescriptive or exhaustive. While the EDPB may not envision further sufficient measures, this should not prejudice transferring entities and member state DPAs from considering further measures which may, upon scrutiny, prove sufficient in light of current or future contractual, organizational or technological capabilities. For example, the CJEU judgment allows for the consideration that additional limitations and means of redress in third countries' law and practice, combined with the implementation of contractual and supplementary measures, which the EDPB already identifies (such as enhanced transparency, notification, challenging of requests, and empowering data subjects to exercise redress mechanisms) provides sufficient protection.

Additionally, the Use Case should clarify that appropriate safeguards need not be solely technical in nature. Under the CJEU's decision, companies are to consider "appropriate safeguards" – and the CJEU does not require that those safeguards be technical to be appropriate. Nor does the GDPR require technical safeguards in this circumstance. Rather, as noted above, the GDPR recognizes the importance and effectiveness of contractual safeguards.[24] For example, , an important contractual safeguard might be provided through a provision requiring the data importer to notify the data exporter of a request by a government authority where the importer is not prohibited from doing so by law or a contractual commitment to provide only the minimum information necessary to the government where the data importer cannot redirect the request to the data exporter. Indeed, after assessing all of the circumstances of a particular transfer, controllers and processors may be capable of identifying a combination of organizational and contractual measures that can provide appropriate safeguards. We accordingly urge Use Case Six be revised to more fully reflect these circumstances. Failure to do so could effectively mandate the use of encryption technology where the data exporter holds the cryptographic keys for companies who need to transfer data outside the EEA and access it in the clear. As noted above, this type of mandate could harm the security of those services. Additionally, in practical terms, such a mandate could be incompatible with products demanded by today's businesses and consumers, which often require cloud providers have access to data in the clear in order to provide services. Indeed, companies rely on a range of products and services that do more than simply store data, but also require access to that data to run tasks such as search, or to analyze traffic and usage information needed to maintain the service..

- ***Use Case Seven: Remote access to data for business purposes.*** Use Case Seven similarly contemplates only a narrow set of circumstances relevant to a data transfer.

  As an initial matter, Use Case Seven suffers from the same flaws discussed above with the prior use case: (1) it considers only a narrow range of circumstances, including the "power" given to public authorities and does not expressly address how public authorities use such powers in practice, and (2) it only addresses potential technical measures, without recognizing that contractual or organizational measures (or a combination of contractual and organizational measures) may provide appropriate safeguards consistent with the CJEU's decision and the GDPR.

[23] Recommendations, Para. 88.
[24] GDPR Recital 109.

The concerns raised by this narrow approach are compounded by the broad scenario addressed by Use Case Seven, which encompasses any multinational company making data remotely available in a third country. To the extent the Use Case is read broadly, to suggest that no technical safeguards may be available to support such transfers in at least some countries, it may have a sweeping economic effect that is not required by the CJEU's decision. For example, broadly read, Use Case Seven could call into question a range of services demanded by consumers and the businesses that serve them, including business functions and communications for global companies or providing 24/7 customer support through a "follow-the-sun" model under which on-call engineering teams worldwide can be used to constantly monitor cybersecurity issues (which form an fundamental basis to guaranteeing the effective functioning of the security of processing as per GDPR Article 32, 33 and 34) and respond to customer support inquiries at all hours. The provision of such services is intended to allow both companies to comply with their obligation to ensure the security of personal data as required under Article 32 of the GDPR, whether they act as controllers or processors. These services are demanded not only by all multi-national companies, which rely on the ability to make such transfers across wide range of industry sectors, but also by consumers, since many popular apps are built on a global cloud infrastructure and require data transfers for the provision of their service. As noted above, the CJEU's decision does not prevent companies from offering these services – but rather requires them to assess a broad range of "all circumstances" in connection with those transfers and to consider a broad range of safeguards that may be appropriate and proportional for them.

Use Case Seven impacts any multinational company relying on intra-group transfers to properly function and provide services to customers for which accessing the data in clear is crucial. Broadly read, Use Case Seven could make it impossible to transfer personal data in this context without encryption, thereby offering companies only the possibility to rely on a technical measure to allow the transfer, in conflict with the CJEU's decision and the GDPR.

We accordingly urge Use Case Seven be revised to more fully reflect the broad set of circumstances that companies should consider in assessing their transfers, as well as the broad range of safeguards that may accompany such transfers, including not only technical measures but also contractual and organizational ones. Failure to do so will have an economic impact that cannot be overlooked, and which would be a collateral consequence that could not be foreseen from the CJEU's decision. It would also contradict the key premise that the right to data protection is not absolute: it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality[25].

[25] GDPR, Recital 4

III. *Companies must be able to effectively implement risk assessments in order to ensure compliance with and enforcement of the ruling*

We appreciate the pragmatic effort of the EDPB to clearly outline the process to be undertaken, illustrated with examples, but some aspects of the Recommendations remain disconnected from the reality of the industry and are extremely burdensome, especially for small and medium enterprises. For examples, in paragraphs 10, 31 and 33, the EDPB refers to the necessity to consider "all actors participating in the transfer". This means that exporter, assisted by importer, would be required to list the full chain of sub-processors potentially in an infinite way, which in practice, in complex supply chains is close to unfeasible. We suggest rephrasing paragraph 31 to clarify that the actors participating in the transfer are the (i) controller; (ii) processor; and (iii) processor's direct sub-processors processing data in the third country. In addition, the Recommendations should expressly recognize that although a risk assessment needs to be performed before transfers take place, it should be possible to perform a risk assessment for a given set of foreseen transfers, and not prior to each transfer, especially in the context of the risk analysis prior to commercializing or using a service that transfers the same types of data for the same purposes at scale

***

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

For further information, please contact:
Thomas Boué, Director General, Policy – EMEA
BSA | The Software Alliance
thomasb@bsa.org or +32 (0)2 274 13 15