GLOBAL DATA ALLIANCE 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

December 21, 2020

The Global Data Alliance[1] welcomes the opportunity to provide comments 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").

The Global Data Alliance is a cross-industry coalition of companies, headquartered in different regions of the world, that are committed to high standards of data privacy and security. Global Data Alliance member companies rely on the ability to transfer data responsibly around the world to create jobs and make local industries more competitive. Cross-border data transfers power innovation and growth across the globe and all sectors of the economy — from manufacturing and farming to local start-ups and service providers. Data transfers enable the digital tools and insights that are critical to enabling entrepreneurs and companies of all sizes, in every country, to create new kinds of jobs, boost efficiency, drive quality, and improve output. In fact, the importance of data flows 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.

Members of the Global Data Alliance share a deep and long-standing commitment to protecting data across technologies and business models, as they recognize that today's cross-border economy depends

[1] The Global Data Alliance (globaldataalliance.org) is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. The Alliance supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. Alliance members include BSA members and American Express, Amgen, AT&T, Citi, ITB360, LEGO, Mastercard, Medtronic, Panasonic, Pfizer, Roche, United Airlines, Verizon, Visa, UDS Technology, and WD-40 Company. These companies are headquartered across the globe and are active in the advanced manufacturing, aerospace, automotive, consumer goods, electronics, energy, financial services, health, supply chain, and telecommunications sectors, among others. BSA | The Software Alliance administers the Global Data Alliance.

on the trust of customers and the general public. The Global Data Alliance, therefore, supports policies that protect privacy and personal data while enabling data to move across borders.

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. We are concerned, however, that several of the illustrative use cases set out in Annex 2 to the Recommendations suggest an approach that departs from the considerations set by the Court in the Schrems II decision. Our comments below also underscore the importance of this case-by-case assessment which is set forth in the CJEU's decision and is built out in the six-step process envisioned by the Recommendations.

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.[2] 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.[3] The CJEU recognized that in some cases controllers and processors may need to adopt "supplementary measures" in addition to the standard SCCs to "ensure compliance with [the required] level of protection."[4]

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

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.

[2] *Schrems II*, Para. 134.
[3] GDPR Art. 46.1.
[4] *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

- ***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."[5] 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 taking into consideration" in assessing a data transfer.[6] 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."[7] 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 in line with the GDPR risk-based approach, this list should be much broader, reflecting other foundational aspects of a data transfer including the nature, scope, context 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 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, when such information is unavailable, urges them and 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.

  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

[5] *Schrems II*, Paras. 112, 113, 121, 146, 203.3 (emphasis added).
[6] *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).
[7] *Schrems II*, Para. 146 (emphasis added).

data transfers, including those aspects set out in the non-exhaustive list in GDPR Article 45(2).[8] That list includes not only the existence of "relevant legislation," but also the "*implementation* of such legislation."[9] 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.[10] 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."[11] 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 standard SCCs – but others where the SCCs "might not constitute a sufficient means of ensuring, ***in practice***, the effective protection of personal data."[12]

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. 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."[13]

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

[8] *Schrems II*, Paras. 203.2, 104, 105,
[9] GDPR, Art. 45(2) (emphasis added).
[10] *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).
[11] *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).
[12] *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).
[13] *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.

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 and implementation by government authorities be considered.[14]

- ***Second, the Recommendations should clarify that an organization may use the combination of technical, contractual, or organizational safeguards that correspond to its level of risk***. As drafted, 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. 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."[15] Moreover, the ability to provide safeguards via contract is foundational to the principle of accountability, which the Recommendations seek to embody.

The Recommendations should better reflect the importance of contractual and organizational safeguards. 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."[16] 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."[17] Consistent with the CJEU's decision, different companies may reach different conclusions about which combination of safeguards offer the most effective protections for the personal data that it transfers..

Several Illustrative Use Cases Appear Inconsistent with the Case-By-Case Approach Set out in the Recommendations and Should Be Revised

While the Recommendation helpfully attempts to illustrate some of the case-by-case analyses that the CJEU instructed data exporters to take, several of the use cases in Annex 2 take into account only a narrow range of circumstances. GDA submits that this may cause confusion and uncertainty for data exporters.

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. Specifically, one of the use cases illustrates these concerns (that are also found in other use cases):

[14] *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).
[15] GDPR, Recital 109.
[16] *Schrems II,* Para. 48.
[17] *Schrems II*, Para. 131.

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

  As an initial matter, Use Case Seven solely considers two circumstances relevant to the envisioned transfer, and not the broad range of circumstances the CJEU directed be taken into account in assessing data transfers: (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.

  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 best-practices demanded by consumers and the businesses that serve them, including 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 and respond to customer support inquiries at all hours. 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. 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 for them.

  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.

The Recommendations create uncertainty regarding transfers of personal data that are central to ordinary business functions and pose little risk to data subjects.

One of the most essential transfers of personal data undertaken by multinational companies involves the access or transfer of employee personal data to a centralized human resource hub. Centralizing data regarding employees' salaries, benefits, demographics, and performance is essential to creating fair and consistent employment policies across an enterprise. Company management must also have the capacity to investigate claims of employee misconduct or abuse. Because the GDPR generally does not permit alternative legal bases for these transfers (such as consent for instance), the implication that it may not be permissible to transfer the data of EU employees to company headquarters outside of the European Union is troubling and has the potential to disrupt international commerce in a significant way.

Companies need time to design and perfect the additional safeguards that are suitable for their operations before enforcement actions commence.

While multinational companies have been assessing and implementing additional safeguards since July 2020, this is a constantly evolving landscape. We encourage the EDPB to recognize that companies making a good faith effort to undertake the six-step process outlined above should not face immediate liability if their implementation of safeguards is incomplete.

***

The Global Data Alliance 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