SIIA Accelerating Innovation in Technology, Data & Media

202.289.7442 1090 Vermont Ave NW Sixth Floor
www.siia.net Washington DC 20005-4905

**Software & Information Industry Association Comments**
**Regarding the European Data Protection Board's**
**Draft Recommendations 01/2020**

The Software & Information Industry Association (SIIA) welcomes the opportunity to provide written comments to the European Data Protection Board (EDPB or the Board) in response to the draft "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data." SIIA is the leading organization representing financial information, education technology, specialized content, information and publishing, and health technology companies. Our diverse membership of more than 700 companies and associations provide services that are vital to our economic and social wellbeing; including helping learners of all ages prepare to succeed in their future, managing the global financial markets, developing software that solves today's challenges, providing critical information that informs global businesses large and small, and innovating for better health care and personal wellness outcomes.

Cross-border data flows are essential for enabling economic growth, facilitating the transatlantic trade relationship, supporting business operations, and meeting the needs of digital services. SIIA's members, which include both data exporters and importers, depend on the ability to transfer personal data from the EU to the US for a wide variety of routine and necessary commercial purposes, including performing global HR functions, providing digital services to European consumers and businesses, and combating financial fraud. To carry out these functions, our members rely on standard contractual clauses and other Article 46 mechanisms for the lawful transfer of data, particularly in the wake of the Schrems II decision which invalidated the Privacy Shield Framework as a transfer mechanism. Like businesses around the globe, SIIA's member companies are committed to safeguarding personal data and need leadership from the EDPB to forge a path forward that will enable lawful data flows.

We have significant concerns that the draft Recommendations fail to set us on that path. As proposed, the draft Recommendations propose a prescriptive approach that would not only cause immeasurable damage to the transatlantic and other global trading partnerships, but also restrict and, in many instances, end access to digital goods and services for European consumers and businesses. Moreover, if finalized as proposed, the Recommendations would prohibitively disrupt routine business operations, including those that ensure European employees get paid on time, that malfeasants cannot commit financial crime, and the responsible monitoring for cybersecurity threats. To avoid this, we urge the EDPB to revise the draft Recommendations in the interest of creating a sustainable and scalable approach based on actual risk, the nature of the data, and alignment with the GDPR and the Schrems II decision.

We focus our concerns on several red flag themes in the draft Recommendations, including the:

- foregoing of a reasonable grace period despite setting forth complex, resource-intensive, and layered obligations that cannot be implemented overnight,
- omission of transfers outside the scope of the draft Recommendations,
- lack of clarity regarding the ability of data exporters to make objective assessments regarding the risk of data access by public authorities,
- omission of a risk-based approach,
- apparent foreclosing of an assessment based on the full statutory and public record of U.S. surveillance laws,
- imposition of an unrealistic and overburdensome duty on data exporters to become legal experts in global data privacy, criminal process, and national surveillance standards,
- standards that exceed or misalign with the GDPR, and
- a focus on use cases that do not involve data transfers or presume violations.

Overlying each of these themes is the considerable concern that the impact of the draft Recommendations will be borne both disproportionality and unfairly by SMEs to the detriment of competition, consumers, and European economic innovation.

**A Grace Period is Necessary**

Like the EDPB's earlier FAQs, the draft Recommendations do not confer a grace period nor any abeyance of enforcement actions to give companies time to adopt meaningful compliance measures. Moreover, the draft Recommendations state that they are "applicable immediately following their publication," which puts companies at risk of needing to scale up their compliance obligations multiple times as the EDPB concludes its public consultation and considers changes to the first released draft.

We understand the sensitivity and difficulty of the EDPB's obligation to set forth guidance for a decision by the Court of Justice, which amounts to a constitutional judgment. Nevertheless, the expectations of immediate compliance with the risk of costly enforcement actions are unreasonable and unfair, and can be remedied with "prosecutorial discretion." As proposed, for instance, the draft Recommendations contemplate that data exporters will bear the tremendous burden of conducting in-depth essential equivalency assessments based on the laws of numerous third countries; a burden which is tantamount to requiring in-house expertise or resources for outside counsel specialized in foreign laws relating to data privacy, criminal process, and national surveillance, among others. It is simply infeasible for data exporters to meet this compliance burden immediately. By way of comparison, we note that

it takes the European Commission years to make similar assessments with respect to adequacy decisions.

The same is true for other requirements within the draft Recommendations, including mandates for multiple data transfer assessments and the opening of complex commercial agreements to include new terms relating to supplementary safeguards. Even setting aside the enormous resources this would take, these measures cannot be implemented in a vacuum. Meaningful compliance will require an implementation period during which companies can deploy procedures and systems to meet the strictures of the draft Recommendations, as well as renegotiate complex commercial agreements. We recommend, therefore, that the EDPB revise the draft Recommendations to include a reasonable grace period on enforcement to allow companies adequate time to implement the changes necessary for compliance.

**Identifying Transfers Outside the Scope of the Draft Recommendations**

Although the draft Recommendations discuss the requirement for data exporters to "know their transfers" in depth, it omits any guidance on assessing which transfers should be within the scope of that assessment. At a minimum, the Board should revise the draft Recommendations to expressly exclude the following data transfers:

- those to a data importer that is subject to the GDPR pursuant to Article 3(2) or (3),
- transfers initiated by a data subject that are not attributable to the data exporter, including when data subjects send an email, publish a post, share a document, travel to a third country, or remotely access data, and
- "transfers" initiated by third parties that are not attributable to data exporters, such as the unauthorized access of data by hackers.

**The Need for Clarity and Objective Assessments of Risk of Access by Public Authorities**

SIIA's member companies, along with companies across a broad range of industry sectors, rely on the need for daily transfers of data from the EU to the US. These data transfers underpin the $7.1 trillion transatlantic trading relationship, our investment partnerships, and the digital economy. Unless the legal and policy outcomes relating to transatlantic data transfers forge a pragmatic, evolving, and risk-based process, these critical trade and economic partnerships will be devastated. One way the EDPB's adopted recommendations can mitigate this risk is by expressly clarifying that objective assessments relating to the risk of access by public authorities can remediate the need for supplementary measures. This meets both the letter and the spirit of the Schrems II decision and will harmonize the draft Recommendations with the European Commission's recent draft standard contractual clauses.

The building blocks for this course correction are already in place. Paragraph 33, for instance, logically and appropriately recognizes that the legal context of a third country's laws will depend "on the circumstances of the transfer," and goes on to list exemplary circumstances for the case-by-case assessment. Other paragraphs contemplate that the legal assessment should address both the laws and practice of the third country. *See, e.g.,* Paragraphs 30 and 32.

Nevertheless, other draft provisions ameliorate this budding standard. Paragraph 42 is particularly problematic. There, the draft Recommendations set forth the prioritization of publicly available legislation for the assessment. This fails to give weight to other equally important recitations of law and practice, such as guidance and case law (particularly for common law jurisdictions like the United States). Moreover, Paragraph 42 could be interpreted to permit only using "other relevant and objective" factors for the assessment when there is no legislation. This ignores the complexity of both policymaking and compliance assessments, which often involve an interplay between legislation, rulemaking, guidance, rules of practice, enforcement outcomes, and actual experience receiving and responding to such requests.

Even more problematically, Paragraph 42 can be interpreted as creating a ban on considering the likelihood of a public authorities access to data, which the draft Recommendations appear to treat as a per se "subjective" assessment. In many cases, however, assessments based on these criteria are patently objective and based on the complex interplay between legislation, rulemaking, case law, guidance, other publicly available commitments, and the actual and objective experiences of the data importer. The draft Recommendations should allow for objective assessments relating to the likelihood of access by public authorities.

Indeed, doing so would better align the draft Recommendations with the European Commission's implementing decision for new standard contractual clauses. Section II, Clause 2 of that implementing decision states that parties can consider "the specific circumstances of the transfer, including . . . any relevant practical experiences with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred." This assessment criterion is in addition to considering "the laws of the third country of decision in light of the circumstances of the transfer, including those requiring to disclose data to the authorities or authorising access by such authorities, *as well as applicable limitations and safeguards*." (emphasis added).

**Prioritizing a Risk-Based Approach**

Another practical way forward is to revise the draft Recommendations to adopt a risk-based approach, both to assess if supplementary measures are needed and, when they are, to ascertain which are necessary. This would align with the GDPR, prevailing risk

management/strategy practices, and the European Commission's draft implementing decision on standard contractual clauses.

Undertaking this approach would require some significant revisions. For instance, the draft Recommendations only account for the "nature of the data" in Article 49, which addresses adopting supplementary measures. As a result, under the draft approach, data exporters would not even consider the nature of the data and whether it poses any particular risk, such as in the context of access by public authorities. The EDPB should remedy this both by including the nature of the data as a consideration, as well as expressly acknowledging that it is important to distinguish between categories of data. It is neither practical nor helpful to require data exporters to treat categories of data like service metadata, configuration checks, or logs the same as data relating to gender, medical status, sexual orientation, or political or religious affiliation.

The provenance for our recommended approach is grounded in the GDPR. Articles 24, 25, 32, and 34, for instance, all contemplate risk-based approaches. Articles 24, 25, and 32 set out standards for controller responsibilities, data protection by design, and the security of processing respectively, and expressly balance the obligations against the "risks of varying likelihood and severity for the rights and freedoms of natural persons." Article 34, similarly, contemplates the "likelihood of [a] personal data breach resulting in a high risk," with respect to obligations to notify data subjects. Recitals 75-77 and 90 expand on these risk-based approaches. The draft Recommendations can and should align with these processing and other obligations.

**Foreclosing a Full Accounting of U.S. Law**

We are concerned that, as drafted, the Recommendations make legal conclusions about U.S. law beyond what was within the record of the CJEU at the time of the Schrems II decision. In the box on page 15, for instance, the draft Recommendation categorically states that based on the CJEU's judgment regarding Section 702 of FISA "the level of protection of the programs authorised by 702 FISA is not essentially equivalent to the safeguards under EU law." It goes on to conclude that "if the data importer or further recipient to which the data importer may disclose the data falls under 702 FISA, [standard contractual clauses] or the Article 46 transfers tools may only be relied upon for such transfer if additional supplementary technical measures make access to the data transferred impossible or ineffective."

The problem with this conclusion is that it is based entirely on the record relating to Section 702 of FISA as decided by the CJEU, which irrefutably held that in those circumstances the statute does not meet the essential equivalency standard. The draft Recommendations, however, should not foreclose objective analyses of the full state of play with respect to American surveillance law, both in terms of relevant updates since the record was created for the Schrems II decision or specifics not captured by the record before the

CJEU in Schrems II. To avoid interfering with ongoing negotiations relating to the Privacy Shield and other nuances relating to a full record of U.S. law, the draft Recommendations should avoid opining on it beyond the specifics of what was set forth in the Schrems II decision based on that limited record.

**Misallocated Burden**

As proposed, the draft Recommendations put the entire onus for assessing the adequacy of third country laws on data exporters and importers, many of which are small and/or nascent businesses that lack the resources and internal expertise for such a legal undertaking. This imposition is unrealistically prescriptive and unfair, and it amounts to requiring data exporters, irrespective of their resources, to become legal experts in global data privacy, criminal process, and national surveillance standards. Moreover, the draft Recommendations set forth such a recommendation even though objective experience shows that it takes institutions like the European Commission years to conduct similar assessments to determine adequacy under the GDPR. It is illogical to expect that companies, including small businesses and startups, can scale these legal assessments when mature and well-resourced government institutions are not able to do the same. The proposal to make the Recommendations effective immediately following their publication only compounds this, giving businesses no time to undertake a legal assessment that the European Commission takes years to make. We urge the Board to revise the draft Recommendations to remove this impracticable obligation and instead focus on an achievable, risk-based approach that enables rather than disrupts data flows.

**Misalignment with the GDPR**

The primary goal of the draft Recommendations should be to set forth standards that enable data flows in a manner that aligns with the GDPR's protections. We are concerned, however, that in many respects the draft Recommendations either exceed GDPR standards or extend them to data transfers in a way not contemplated by the regulation. This is both inappropriate and sets forth obligations that are impractical and that unduly disrupt data flows.

For example, the Executive Summary and Paragraph 4 reference the accountability principle in Article 5(2) of the GDPR as a basis for the CJEU's holding in Schrems II that data exporters must identify supplementary measures on a case-by-case basis. The Article 5(2) accountability provision, however, relates expressly and solely to the Article 5(1) principles of processing data and not to data transfers. Indeed, none of the processing principles in Article 5(1) refer nor relate directly or by cross-reference to the articles governing data transfers. At a minimum, the EDPB should revise the draft Recommendations with a clear explanation for why the accountability principle is relevant.

Similarly, in setting out the accountability principle for transfers Paragraph 3 states that "[c]ontrollers and processors must be able to demonstrate [compliance accountability] efforts to data subjects, the general public and data protection supervisory authorities." The GDPR, however, does not create these obligations between the data controllers and processors and the general public. This statement, therefore, exceeds the scope of the GDPR and the EDPB should revise it to align with the GDPR's requirements.

The draft Recommendations also inappropriately extend GDPR requirements by treating data transfers as a processing purpose rather than as an activity tied to a processing purpose. This results in misapplications of the purpose limitation principles in Article 5(1) and the accountability principle in Article 5(2).

With respect to the Article 5(1) principles, we would like to draw attention to the extension of the GDPR's data minimization principle in the Executive Summary and Paragraph 11 for the "know your transfer" standard. There, the draft recommendations state it as a requirement "that the data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred to and processed in the third country."[1] The data minimization principle at Article 5(1)(c) of the GDPR similarly requires that personal data be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed." It is unclear why the draft Recommendations are extending the data minimization principle to a data transfer. Doing so is a misapplication of Article 5(1)(c), which is intended to require data minimization in relation to a processing *purpose*, but not in relation to every *processing activity* done for that purpose.

Data transfers are not a processing purpose, but rather a processing activity necessary to achieve the underlying processing purpose. Provided that the data minimization principle is met with respect to the underlying processing purpose, then the GDPR requirement is met, irrespective of whether the data stays in Europe or is transferred to a third country as an activity to meet the underlying purpose. In other words, if a transfer is part of a processing operation undertaken for a specific purpose, there should not be a separate test for any of the purpose limitation principles in Article 5(1) that focus separately on the transfer from the other processing activities. Indeed, doing so is a de facto amendment of the GDPR and inappropriate in the context of these Recommendations.

**Focus on Use Cases Not Involving Transfers**

Annex 2 sets forth use cases relating to the recommended supplementary measures, but ultimately the restrictive approach taken means these examples either do not involve transfers of personal data or they presume violations of the GDPR. The result is that the draft Recommendations entirely exclude illustrative examples of data transfers that can incorporate supplementary measures for the lawful transfer of data. This underscores the

[1] This same standard is again misapplied in Paragraph 65.

unduly prescriptive approach of the draft Recommendations as written, which if finalized would disrupt rather than facilitate data flows. We encourage the Board to reconsider the use cases and instead include risk-based and practical solutions for supplementary measures that enable the lawful transfer of that data.

For instance, Use Case 2 relates to the transfer of pseudonymized data. The conditions for this include maintaining the additional information to reidentify the data solely within the EEA. As a result, this use case does not involve "information related to an identified or identifiable individual," and does not amount to a transfer of personal data. Logically, therefore, the use case does not trigger any of the GDPR obligations relating to transfer. The resulting "use case" therefore is not a suitable example for how a supplementary measure can enable a lawful transfer of personal data.

Similarly, Use Case 3 sets out conditions so restrictive that it negates the premise that it involves a transfer of personal data. In Use Case 3, the Board contemplates situations in which encrypted data merely transits third countries. The technical supplementary measure includes a condition that the decryption of the data must only be possible outside the country of transit. As with Use Case 1, this example is irrelevant to the question of how businesses can securely and lawfully enable data transfers because it does not involve the transfer of "information related to an identified or identifiable individual."

Use Case 5 suffers from the same defect. There, the illustrative example is intended to cover data transfers involving split or multiparty processing, however it imposes the condition that the data exporter "split the data in such a way that no part an individual processor receives suffices to reconstruct the personal data in whole or in part." The result is that the data exporter is not transferring personal data because it is not "information related to an identified or identifiable individual," making yet another irrelevant use case that does not contemplate a data transfer. The same legal conclusion is true for Use Cases 1 and 4.

When these Use Cases are considered together with Cases 6 and 7, in which the EDPB presumes GDPR violations that cannot be remedied, we are left with a draft Recommendation that fails to address even a single instance in which personal data can be transferred lawfully using supplementary measures. The consequences of this approach are dire, for all of the reasons we have previously stated.

If the draft Recommendations are finalized with these technically infeasible standards, the unintended consequences will be rife, particularly arising from Use Cases 6 and 7. These include:

- the cessation of routine business operations facilitated by SaaS providers, including sending emails and other messages, using online collaboration tools, videoconferencing, and processing payments,

- increasing the technology divide and the costs for EU SMEs that rely on the Internet and SaaS technologies to levy the playing field, and

- risking the exposure of data to cybercriminals and other bad actors as EU companies may be forced to use less sophisticated, secure, and reliable services.

We respectfully urge the EDPB to revisit the draft Recommendations to set forth illustrative use cases involving the transfer of personal data in a manner that can be addressed by supplementary measures. One way forward is for the Board to take a new approach with respect to technical measures by setting forth clear technical requirements that not only account for the categories of data at issue, but also the threat that organizations need to protect against, and also allow a combination of controls to neutralize a threat. In addition to encryption, these technical controls could include access controls, escorted access, and policy systems. The Board can also improve the technical feasibility of the measures by eliminating the call for "flawless" encryption and instead aligning encryption standards, definitions, and controls with international standards and other industry-accepted encryption terms. Lastly, the Board should consider additional supplementary measures for (1) supervised access to personal data by an authorized European third party to ensure the processing is limited to the data exporter's instructions, and (2) that allow plain text access with mitigation measures.

**Conclusion**

On behalf of SIIA, thank you again for the opportunity to provide these written comments and suggestions. We look forward to engaging with the Board as this process moves forward, and in particular if you have any questions or concerns relating to our comments

**Dated: December 21, 2020**

Respectfully submitted,

**Sara C. DePaul**
Associate General Counsel & Senior Director for Technology Policy
Software & Information Industry Association