Business Roundtable Comments on Recommendations 01/2020 of the European Data Protection Board (EDPB)

December 21, 2020

Business Roundtable is an association of chief executive officers of leading global companies, working to promote a thriving global economy and expanded opportunity for all through sound public policy.

We thank you for the opportunity to contribute the following comments regarding the EDPB recommendations on measures that supplement data transfer tools to ensure compliance with the EU level of protection of personal data. We appreciate the hard work that has gone into developing the draft recommendations, understand that developing consensus within the EDPB is a complex process, and hope you find these targeted comments helpful in finalizing an agreed position that sustains critical data flows in ways that are respectful of the fundamental rights and freedoms of individuals.

1. Ensuring recommendations are consistent with the *Schrems II* decision

We welcome recognition that supplementary measures may enhance the level of protection afforded to a transfer of personal data and that these measures may be of a contractual, technical, or organizational nature. It is also helpful to see the referenced examples in Annex 2.

We are concerned that the EDPB recommendations present certain technical measures as a pre-requisite to transfers in any case where there is a mere theoretical possibility of access by public authorities under relevant surveillance regimes. This approach precludes an exporter from considering whether contractual, organizational or (other lesser) technical measures may, taken as a whole, provide an appropriate level of protection and/or whether there is any likelihood of access by public authorities to the personal data being transferred.

We submit that this approach is at odds with the Court of Justice of the European Union (CJEU) decision, which does not state that the abstract right of the public authorities to obtain to personal data is *per se* determinative of the safeguards to be adopted. Instead, the CJEU decision directs a specific, risk-based analysis based upon access to "the personal data". The CJEU notes that consideration should be of "the relevant aspects of the legal

regime of th[e] third country" but only as regards to "*any access* by the public authorities of that third country *to the personal data transferred*" (emphasis added).[1]

Companies should be allowed to form an assessment of the efficacy of supplementary measures on a holistic basis, having regard to the totality of organizational, contractual and technical measures being adopted. The EDPB recommendations should not constrain transfers by prescribing the adoption of specific technical measures based upon a theoretical risk of access. Rather, the EDPB recommendations should anticipate that it may be feasible for other measures to provide an appropriate level of protection proportionate to the risk posed by the data transfer, as assessed on a case-by-case basis. By way of example, if an importer can demonstrate to the exporter that no public authority access has occurred or is likely to occur and can provide contractual assurances that support this position, then the transfer should be permitted to safely proceed without necessarily requiring full encryption or pseudonymization, provided appropriate supporting technical measures are in place, such as robust access controls.

We believe this approach is consistent with the CJEU decision and aligns well with the principles of necessity, proportionality and rationality embedded in the Charter of Fundamental Rights of the European Union and the General Data Protection Regulation (GDPR). Moreover, we are concerned that placing such a significant emphasis on the adoption of technical measures for transfers to service providers who are subject to Section 702 of the U.S.'s Foreign Intelligence Surveillance Act (FISA) risks undermining the use of organizational and contractual protections. These measures can also bring important protections to safeguard data and deter excessive and disproportionate access and should be given appropriate prominence alongside technical measures.

2. Recognizing the risk-based approach inherent in the General Data Protection Regulation

We ask the EDPB to recognize that the *likelihood* of risk of harm to the rights and freedoms of the data subjects arising from a proposed transfer is a relevant factor for the data exporter to take into account when assessing whether the level of protection guaranteed to the data subject under the GDPR may be undermined as a result of a proposed transfer.

Adopting a significant risk-based element in the assessment is important and relevant, because the legal protections guaranteed to data subjects under the GDPR are not absolute, but rather subject to proportionality thresholds.

By way of example, Article 24 of GDPR provides that controllers are expected to implement technical and organizational measures to ensure compliance with the GDPR in a manner that "*tak[es] into account [of] the nature, scope, context and purposes of processing as well*

[1] *Case C-311/18 Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems ("Schrems II")* at paragraphs 104 & 105.

as the risks of varying likelihood and severity for the rights and freedoms of data subjects." Moreover, the rights afforded to data subjects to secure compensation following an infringement of the GDPR do not apply *per se* to all data subjects, but rather to those "*who have suffered material or non-material damage*" (Article 82). Similar principles run through other provisions (e.g., Article 34 (notification of data breaches), Article 35 (conduct of DPIA)).

Business Roundtable submits that as the protections afforded to data subjects under the GDPR are inherently proportionate, it is entirely logical and consistent with GDPR that any assessment as to whether those safeguards are undermined in the context of a particular transfer should also be considered through a proportionate (risk-based) lens. This is particularly pertinent to business operations, as the current application of the EDPB recommendations may restrict transfers in many cases where a transfer of data to a third country involves no meaningful risk to data subjects.

For example, much of the data that multi-national companies transfer from the EU to the U.S. is very different from the personal social media user data at issue in the *Schrems II* decision. Businesses often transfer data for ordinary operational purposes (e.g., human resources, service quality assurance, and security) to cloud environments located across the Atlantic. Such transferred data include business contact information, client data, employee contact information and employee work product that contain limited personal information. Much of these data are entirely innocuous, in the sense that the exporter could establish that the data was highly unlikely to be of any interest to any public authority in the third country (e.g., where there was evidence that authorities had never shown any prior interest in such data) and/or unlikely to cause any risk of harm to the data subject (e.g., if the data is in no way related to an individual's private life or is widely available on a public website or record). Logically, a transfer of such innocuous data should be treated differently from transfers where there are genuine risks of harm to the data subject.

A risk-based approach accounting for these proportionality considerations would be both consistent with the CJEU decision, which advocates any assessment be undertaken on a 'case by case' basis, and consistent with the underlying principles of the GDPR noted above.

If incorporated into the EDPB recommendations, this approach would provide that exporters consider all factors associated with the specific circumstances associated with a particular transfer, including (i) the specific nature of the data being transferred, and (ii) the likely risk of surveillance for the type of data being transferred. Such an approach would be fully consistent with the European Commission's interpretation in the recently published draft Standard Contractual Clauses (12 November 2020), which refers in Clause 2(b) to an assessment that takes into account the specific circumstances associated with a particular transfer.

It is essential that the new Standard Contractual Clauses (SCC) and the EDPB supplementary measures operate consistent with one another. The proposed supplementary measures should be consistent with GDPR and the proposed SCCs in allowing a data exporter to take into account the nature of the data transferred and the likelihood of actual (as opposed to theoretical) government access.

The fact in some situations that the data to be transferred may be of no interest to surveillance authorities, accounting for the circumstances of the transfer, including the nature of the transferred data and whether a data importer has ever received requests for disclosure from public authorities, is material to any risk-based cross border data transfer assessment. The approach proposed within the draft SCCs allowing for such a risk assessment to be undertaken should be reflected in the EDPB recommendations which seems to suggest that this kind of approach is not possible.

We urge the EDPB to align the recommendations to reflect the position set out in the draft Standard Contractual Clauses.

3. Considering feasibility of technical measures

We further note the substantial challenges for many businesses in adopting the measures set out in the recommendations. The last 10 years have seen a major shift in the business IT environment toward a reliance on externally hosted, typically cloud-based, solutions, as well as the development of agile services delivered by subprocessors. This infrastructure has been widely adopted by many multi-national businesses and is simply not practical to operate on a completely encrypted or pseudonymized basis, where no access to data or encryption key may be permitted in the U.S. The only feasible alternative involves migrating EU personal data to EU cloud solutions (a marketplace which does not yet have sufficient capacity to accommodate this approach), or to have U.S.-held data processed 'off-cloud' in an on-premise environment. Very few organizations have the resources to accommodate this model. Moreover, we believe this approach exposes data subjects to higher risks, given that cloud-based solutions often offer superior security architectures and controls. This is very likely to be a particular concern in the case of small and medium sized enterprises (SMEs), who will have more limited resources to invest in robust on-premise solutions.

4. Compliance timeframe

In light of these and other operational challenges, we encourage the EDPB to allow businesses reasonable time to implement the necessary technical, organizational, and contractual measures, prior to enforcement actions based on its guidance. Changing data flows to comply with the supplementary measures set out in the EDPB recommendations is by no means an overnight process and will not be practicably feasible for most organizations, particularly SMEs, to adopt immediately. We would suggest taking an approach consistent with the new version of the Standard Contractual Clauses, which envisions a 12-month compliance period.

5. Balancing examples of regimes that may require technical safeguards

We note that offering only FISA in the U.S. as an example of a legal regime that imposes a direct obligation to turn over data to public authorities has the effect of creating a confusing and incomplete view of the implications on rights of EU data subjects with regard to their personal data transferred to other countries and appears to imply that FISA is somehow unique. In fact, many countries that are significant trading partners with the EU either afford fewer procedural protections than does FISA or in no way limit surveillance by their governments. We suggest that if the EDPB addresses FISA as an example, it should provide more varied examples. Focusing specifically on the challenges arising from one particular country's well understood, rule of law-based statutory approach to surveillance risks making the guidance unduly narrow and approaches legal formalism.

On behalf of the 215 companies that are members of Business Roundtable, we thank you for the opportunity to comment. Business Roundtable respectfully requests incorporation of these factors within the assessment model set out in the EDPB's final recommendations.