HENGELER MUELLER

Hengeler Mueller • Postfach 10 28 21 • 40019 Düsseldorf

European Data Protection Board
Rue Wiertz 60
B-1047 Brussels

- Via Online Submission -

Prof. Dr. Wolfgang Spoerr, LL.M.
Dr. Vera Jungkind
Partner

Direktwahl
Direct Number
+49 211 8304-405
+49 30 20374-161

E-Mail des Absenders
Sender's E-mail
wolfgang.spoerr@hengeler.com
vera.jungkind@hengeler.com

Benrather Straße 18 - 20
40213 Düsseldorf
Telefon +49 211 8304-0
Telefax +49 211 8304-170
www.hengeler.com

Düsseldorf, 21 December 2020
71616956v3

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

Our Comments on Version for Public Consultation of 10 November 2020

Dear Sir or Madam,

We strongly support the EDPB's initiative to provide practical guidance on the implications of the recent CJEU judgement C-311/18 (*Schrems II*). Such Recommendations could guide both companies and data protection authorities to accurately apply the GDPR and implement Schrems II in the field of international data transfers.

We are grateful to be given the opportunity to comment on the public comment version of the Recommendations. Our law firm regularly advises EU-based and international clients on complex cross-border data transfers as part of normal business transactions as well as in the context of transactions, litigation and regulatory investigations. Based on our long-standing professional experience with international data transfers and understanding of the companies' business needs, we would like to share the following legal considerations with you. Our contribution is not made at the request of any client; we comment solely on our own behalf as practitioners and academic contributors to European Data Protection Law:

I. Need for a Risk-Based and Proportionate Approach

In Schrems II, the CJEU clarified that in order to evaluate the legitimacy of international data transfers a case-by-case assessment was required. The need for a case-by-case assessment became specifically clear from the differentiated decision on available safeguards for EU-U.S. data transfers in the underlying case.

The CJEU declared the Privacy Shield Decision, as a general and abstract instrument to justify EU-U.S. data transfers, to be invalid (C-311/18, paragraph 199).

The basis of the CJEU's view was that the Commission's assessment of the surveillance programs based on Section 702 of the Foreign Intelligence Surveillance Act ("FISA") and Executive Order 12333 ("E.O. 12333") was not sufficient to find that these general regulations of the United States of America are limited to what is strictly necessary (C-311/18, paragraph 184). Therefore, "limitations on the protection of personal data arising from the domestic law of the United States on the access and use by U.S. public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law." (C-311/18, paragraph 185).

In contrast, the CJEU reaffirmed at the same time that the EU Standard Contractual Clauses ("SCC") were a valid instrument to justify data exports to non-EU countries, including to the U.S. (C-311/18, paragraph 149), but that additional safeguards were regularly required in the specific case (C-311/18, paragraph 126).

This clear distinction between the U.S. Privacy Shield as an abstract and general instrument and the SCC as an individual instrument tailored to specific cases proves that, where a general and abstract justification fails due to the legal situation in the receiving country, a *case-by-case assessment* is required *in every single case* assessing the risks and proportionality of the specific data transfer.

1. Risk-Based Approach and Proportionality as Core Principles of GDPR

The CJEU's request for a case-by-case assessment and risk-based approach is deeply enshrined in the GDPR: Any data processing under the GDPR requires "*appropriate* security of personal data" and "*appropriate* technical or organizational measures" (Art. 5 (1) f) GDPR), a "level of security *appropriate* to the risk" rather than absolute security (Art. 32 GDPR, Recital 83) or "*appropriate* safeguards" (Art. 46 GDPR). In the GDPR, data security is not an absolute concept but needs to be assessed in the individual

case, in view of the data processing at hand. Art. 24 and Art 32 GDPR are very clear that when determining "*appropriate* technical and organizational measures", the controller needs to take into account "the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons". This is confirmed by Recital 76. In Schrems II, the CJEU did not deviate from this concept. The CJEU did not discuss what "appropriate measures" the data exporter and the data importer could take, and did not restrict them, allowing for any appropriate measure, whether contractual, technical, organizational or of a different nature.

2. Different Structure of Risk Assessments under Art. 45 and Art. 46 GDPR

In our view, it follows from Schrems II that the risk assessments to be undertaken by the Commission under Art. 45 GDPR and the risk assessment under Art. 46 GDPR are not identical. The Commission's assessment under Art. 45 GDPR must necessarily involve a general and abstract assessment based on the non-EU country's legal order and its general enforcement practice. The duty of the controller under Art. 46 GDPR has a different structure. If this was not true, the CJEU would have found that the deficiencies in the legal protection afforded to EU nationals under Section 702 FISA and E.O. 12333 would generally prohibit any data transfer under Art. 46 GDPR.

In our view, the CJEU's decision was no result of timidity but of plain legal logic: While the Commission can and must necessarily assess the abstract conditions since it opens up a general avenue to data transfers, the controller under Art. 46 GDPR may, and must, look at the specific case. The controller may, for example, assess if there have ever been any orders to obtain data for the specific data pool or recipient and if so, with what duration and to what extent.

3. The Risk-Based Approach in the Step Plan of the Recommendations

The Recommendations propose a six-step approach, which explicitly requests a case-by case assessment.

In particular, Step 3 requires the assessment "whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer" and Step 4 "which supplementary measures could be effective". In those sections, it is mentioned several times that a case-by-case assessment is required:

- "in light of all circumstances of the transfer" (heading 2.3)
- "you will need to look into the characteristics of each of your transfers" (mn. 32)
- "The applicable legal context will depend on the circumstances of the transfer" (mn. 33)

- "on a case-by-case basis" (mn. 46)
- "list of factors to identify which supplementary measures would be most effective" (mn. 49)

However, this is less clear from the remaining explanations of Steps 3 and 4. The Recommendations concentrate predominantly on the law or practice of the receiving country, on whether governmental access to the specific data is legally possible and on which supplementary measures would be most effective in protecting the data from such access. The necessary risk-based approach postulated by the GDPR seems to be limited to those aspects while other aspects of the data and transfer do not seem to be considered further.

- The example in margin no. 44[1] could mean that for any data that could fall under Section 702 FISA, only those supplementary measures would be acceptable that make access to the data transferred impossible or ineffective, irrespective of the nature and amount of the data, their sensitivity, purposes of transfer etc.

- The same interpretation could be derived from margin no. 42.[2] It seems that the effectiveness of supplementary measures would have to be assessed exclusively against the level of protection in the country of destination but not the risk profile of the transfer. Following this logic, if access by public authorities was conceivable, regardless how likely the access was and if the typical risks addressed in Schrems II were relevant to the specific data at all, the transfer would be forbidden.

- Margin no. 48 also seems to suggest that the only relevant supplementary measures are those which "impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes", irrespective of the individual circumstances of the data and the data transfers.

---

1 "*This means that the level of protection of the programs authorised by 702 FISA is not essentially equivalent to the safeguards required under EU law. As a consequence, if the data importer or any further recipient to which the data importer may disclose the data falls under 702 FISA, SCCs or other Article 46 GDPR transfer tools may only be relied upon for such transfer if additional supplementary technical measures make access to the data transferred impossible or ineffective*." (mn. 44) In our view, this analysis blurs the lines between an abstract risk – which is not relevant for Art. 46 – and a case-specific risk analysis.

2 "*Your assessment must be based first and foremost on legislation publicly available. However, in some situations this will not suffice because the legislation in the third countries may be lacking. In this case, if you still wish to envisage the transfer, you should look into other relevant and objective factors, and not rely on subjective ones such as the likelihood of public authorities' access to your data in a manner not in line with EU standards.*" (mn. 42.) See comment supra Footnote 1.

We would encourage the EDPB to amend Steps 3 and 4 to clarify that the controller should perform a full case-by-case assessment, which is not limited to the issue of governmental access but takes into account all aspects of the transfer. In doing so, the EDPB would honour the basic principles of the GDPR as well as the distinction made by the CJEU in Schrems II between the Privacy Shield as an abstract decision and the SCCs as an individual solution, thereby avoiding unwanted practical consequences:

- For example, the risk of government access should be compared with many other security risks relevant for the individual data set. While the Schrems II scenario related to data from mass communication, other data sets like financial data (*e.g.*, credit card information) may be more vulnerable with respect to data breaches through private third parties, and for other, more limited data the typical mass surveillance scenario is not relevant at all. The case-by-case assessment should therefore take a broad view on potential risks and not be limited to the government surveillance risk. It should also take a data-specific perspective to check if the mass communications surveillance risk is relevant at all. For example, the protection against significant financial and personal harm that private hackers can cause appears to be just as relevant as the mass surveillance risk in general terms, and it deeply depends on the type and scope of data involved if one or the other or both of the risks are relevant.

- In a risk assessment, the controller should be able to factor in the relevance of the data for untargeted governmental mass surveillance and the likelihood of public authorities' access to the data transferred. Otherwise, data transfers to countries with broad authorities for governmental access would practically be forbidden, regardless of the likelihood of such access. Specifically for the U.S., intra-group data transfers stored in a cloud would be generally forbidden, even if the data were not data from social media and mass communication. Any data transfer to the U.S., where the data should be analysed and worked with in the clear, would be impossible, even if the data were well protected and of no apparent interest to the U.S. government.

- The controller should be able to evaluate whether the risks of governmental access to its data actually stem from the data transfer or rather the use of a service provider headquartered in a non-EU country or a EU-based service provider with sub-processors in a non-EU country, with the data residing in the EU. All these scenarios have a different risk profile, and the safeguards should be selected in accordance with such risk profile.

4. Suggested Clarifications to Steps 3 and 4 of the Recommendations

For all those reasons, we would recommend to implement additional interim steps to reflect the necessary risk-based approach.

Generally, we are of the opinion that the step-approach is an appropriate method for companies to classify and evaluate their international transfers. Multi-step approaches are also codified in the GDPR, for example, the data protection impact assessment in accordance with Art. 35 GDPR ("DPIA"). The concept of the DPIA can be adapted for data transfers to guide data exporters through a risk-based assessment.

The Recommendations partly align with the concept of the DPIA. Step 1 of the Recommendations ("know your transfers") reflects the first step of the DPIA ("systematic description of the envisaged processing operations", *cf.* Art. 35 (7) a) GDPR). Step 4 ("identify and adopt supplementary measures") is identical to the forth step in the DPIA ("the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation", *cf.* Art. 35 (7) d) GDPR).

If the assessment of the laws and the practices of the receiving country concludes that governmental access is legally possible and therefore a risk to the rights and freedoms of natural persons exists, the additional steps of the DPIA should be applied as interim steps of Step 3:

1. an assessment of the necessity and proportionality of the transfer in relation to the purposes (*cf.* Art. 35 (7) b) GDPR);
2. an assessment of the risks to the rights and freedoms of data subjects (*cf.* Art. 35 (7) c) GDPR).

a) Assessment of the Necessity and Proportionality of the Transfer

The Recommendations underline the purpose of Art. 44 GDPR that the GDPR should not be undermined by the transfer (mn. 28). Every transfer of personal data to a non-EU country creates an additional risk. Therefore, a necessity-based analysis is required to assess which data transfers could be suspended or reduced. In this context, alternative data processing options in the EU or the reduction of transferred data must be examined. In practice, the potential of data minimisation should be fully explored (*cf.* Art. 5 (1) c) GDPR).

Nonetheless, there are transfers that cannot be suspended or relocated to countries within the EU. This is specifically true for intra-group transfers to non-EU branches or entities and for the necessary involvement of service providers located outside of the EU. Especially the U.S. are a significant technology market, and U.S. service providers offer various IT services that have no equivalent within the EU (yet).

In the discussion around Schrems II, some requests for a more restrictive approach towards international data transfers seem to be motivated by industry policy considerations or by a desire to export the GDPR not in terms of policy goals but in detail. All this is counter-productive[3] and has no basis in the GDPR. Protectionist considerations that EU companies should rely on EU-based service providers and that newly created demand for EU-based IT and data services would foster innovation and economic growth in the EU should not guide the EDPB. The perceived lack of EU-based IT and data services might be filled more rapidly by U.S. and international service providers than by genuine EU-based service providers. Discouraging EU businesses from purchasing the services of U.S. and international service providers in the field of IT, cloud storage, cybersecurity etc., which often are high performance, both in quality and security, might put the businesses at a competitive disadvantage compared to their non-EU competitors.

b) Assessment of the risks to the rights and freedoms of data subjects

If a transfer is found to be necessary and proportionate, the actual risk assessment needs to be conducted. As part of this assessment, the following factors should be considered:

- type, content and sensitivity of data
- frequency and amount of data
- transfer route
- characterization of data importer
- protective measures during the transfer

(i) The type, content and sensitivity of data are decisive for the risk assessment. All data that can potentially be of interest to the public authorities of the non-EU country because they contain foreign intelligence of any kind (e.g. on the subjects of defence, politics, internal and external security, terrorism, energy supply, narcotics or money laundering) generally incur a higher risk of being accessed by public authorities. Traffic and content data of electronic communication appear to be of greater relevance for foreign intelligence than performance, salary or other

3 *Hennemann*, Wettbewerb der Datenschutzordnungen, RabelsZ 84 (2020), p. 864 et seq.

HR data on employees of EU group companies stored in an intra-group HR database in a non-EU country. The potential relevance of the data for non-EU authorities should be assessed for every country separately.

Special categories of personal data such as health data (*cf.* Art. 9 GDPR), which may be processed only subject to strict requirements, increase the need to protect data subjects and, therefore, have an impact on the data transfer's risk profile. The sensitivity, however, does not *per se* increase the probability of that data being accessed for reasons of foreign intelligence.

(ii) The larger the amount of data, the more frequent the transfers and the less defined the purpose of the processing are, the greater the risk is that the data will be targeted in ongoing surveillance operations or accessed by public authorities. Reducing the volume of the data and the number of data transfers minimises that risk. The same holds true for a clearly defined purpose, which also regularly results in a reduction of the amount and use of data.

(iii) The means of transport influence the risk level as well. For example, the U.S. governmental access rights criticized by the CJEU are aiming at surveilling electronic (mass) communication. The Irish *High Court* found (C-311/18, paragraph 63) that the E.O. 12333 allows U.S. public authorities to access data in underwater cables. Therefore, transfers made via the internet incur a higher risk of access than sending data carriers or hard copies.

(iv) Furthermore, it is relevant who the recipients of the data are. The criticized U.S. surveillance programs focus primarily on large telecommunications companies. Companies that send their data through or to such companies (e.g. via cloud services or external e-mail servers) put their data at a greater risk, whereas internal company-owned servers are likely less exposed. Previous experiences of the recipient must also be taken into account: if it was targeted by surveillance measures in the past, this may *prima facie* be an indication of an increased likelihood of data being accessed in the future. Hence, before transmitting any data, a data controller should ask the data importer whether it is aware of any governmental data access to its database in the past (which is also foreseen in the contractual measures proposed by the Recommendations (mn. 100)).

(v) Not least, data security and encryption mechanisms must be considered already in the risk assessment. Data that has been encrypted in a complex and decentralised way, especially when they appear not to contain any relevant foreign intelligence

– for instance based on their designation as HR, invoice or patient data – are less prone to be accessed by public authorities.

II. Supplementary Measures to Counter Identified Risks

The Recommendations elaborate in much detail on specific examples of technical, contractual and organisational measures. We recommend that the appropriate measures be selected in accordance with the risks identified for each individual transfer, in line with the risk-based approach set out above I.

1. Technical Measures

The Recommendations stress that technical measures are of particular importance to safeguard international data transfers in contrast to contractual and organizational measures:

> "Contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country (where this unjustifiably interferes with the data importer's obligations to ensure essential equivalence). Indeed there will be situations where only technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes." (mn. 48).

However, the demands set by the Recommendations for technical measures are unreasonably high, expecting them to impede or render ineffective any access and aiming not at a reasonable, risk-based approach but at a zero-risk approach.

Following the risk-based approach set out above, technical measures which do not impede or render governmental access ineffective but significantly decrease the likelihood of such access should be seen as appropriate.

Use Cases 1-5 in Annex 2 of the Recommendations are certainly helpful examples. However, their scope of application seems to be rather narrow. In the majority of purposes that companies currently pursue when transferring data to non-EU countries like the U.S., namely general business purposes, it will not be possible to pseudonymize, split or reroute the data, especially if the data is transferred in order to be analysed and used in the receiving country and therefore must be available in the clear. Therefore, Use Cases 6 and 7 should be rewritten in a more hands-on and pragmatic way to describe what can – rather than what cannot – be done in circumstances where supplemental security measures are taken and the risk of governmental access is generally considered low in view of the nature of the data to be transferred.

2. Contractual Measures

We support the numerous examples of detailed supplemental contractual measures in Annex 2 of the Recommendations, which are extremely helpful and will certainly be predominantly used in data transfer agreements in the future.

The important statement that "combining diverse measures in a way that they support and build on each other may enhance the level of protection and may therefore contribute to reaching EU standards" (mn. 47) should be elaborated and put in context with the necessary risk assessment. Margin no. 48[4] should be redrafted to reflect the risk-based approach by clarifying that contractual measures, even if governmental access in the receiving country is generally conceivable, might suffice to justify the transfer in cases where the risk of access is very small and therefore acceptable.

3. Organizational Measures

Similarly, we appreciate the examples of possible organizational measures, especially concerning internal policies for groups of entities. Intra-group transfers to non-EU countries form a significant part of international data transfers and require clear guidance to secure the course of business for many companies.

To implement clear responsibilities and policies regarding international data transfers is key to enable companies to conduct the risk analysis as outlaid above. Nonetheless, the Recommendations seem to neglect that international data transfers are not only an issue for giant international enterprises, but just as well for small and medium-sized businesses that neither have the expertise nor the manpower to build up entire departments or hire law firms to assess those questions. Especially, when it comes to the expectations the Recommendations are currently setting regarding the analysis of the legal situation in the receiving country in mn. 43[5] and Annex 3 of the Recommendations, those expectations should be adjustable to the company size and expertise if the risk profile of the data

---

4 "*Contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country (where this unjustifiably interferes with the data importer's obligations to ensure essential equivalence). Indeed there will be situations where only technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes. In such situations, contractual or organisational measures may complement technical measures and strengthen the overall level of protection of data, e.g. by creating obstacles for attempts from public authorities to access data in a manner not compliant with EU standards." (mn. 48).*

5 "*You may complete your assessment with information obtained from other sources, such as:*

- Elements demonstrating that a third country authority will seek to access the data with or without the data importer's knowledge, in light of reported precedents, legislation and practice;

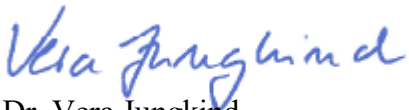
- Elements demonstrating that a third country authority will be able to access the data through the data importer or through direct interception of the communication channel in light of reported precedents, legal powers, and technical, financial, and human resources at its disposal." (mn. 43).

transfers allow for it or the data importer is a highly professional IT service provider supporting the exporter with a convincing legal assessment of the transfer.

We would very much appreciate if the EDPB take our above comments into consideration.

Yours sincerely,

Prof. Dr. Wolfgang Spoerr
Rechtsanwalt



Dr. Vera Jungkind
Rechtsanwältin