Bundesverband E-Commerce und
Versandhandel Deutschland e.V.
www.bevh.org

- Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh) -

Position on the EDPB's Reccomendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Berlin, 21 December 2020

Contact: Alien Mulyk, Manager Public Affairs EU & International, am@bevh.org

1. Introduction

In its Schrems II ruling, the European Court of Justice held that businesses relying on standard contractual clauses (SCCs) to transfer data to non-EU countries may need to adopt additional safeguards to protect personal data from being accessed by public authorities in these countries. Especially for SMEs it is not feasible to ensure that third country authorities can really not access the data that they transferred to their business partners in third countries. However, data transfers, also to countries outside the EU for which the European Commission has not yet taken an adequacy decision, is essential for international trade in general and e- commerce in particular as it is data-driven and not place-bound. Therefore, pragmatic and practical measures are needed to allow businesses to comply with the Court's decision. Thus bevh[1] welcomes the opportunity to provide feedback from the point of view of the German e-commerce industry on the Recommendations of the EDPB.

2. Need for legal certainty

It is the European Commission's responsibility to decide with their knowledge and experience if a country provides an adequate level of data protection. However, the EDPB Recommendations are putting this responsibility on businesses. The proposed assessment process is very complex even for big multinational companies. SMEs which only dispose of very limited resources and rely on solutions of business partners to process and store data are however particularly affected. Therefore, they will be particularly affected by the requirement that EU companies have to undertake their own analysis of the laws and practices of dozens of non-EU countries (i.e., those not subject to an EU adequacy decision), which is very costly for them as it will also require significant legal assistance. Moreover, it is questionable that this approach will lead to a better level of protection of personal data in third countries. In addition, as companies may have to face fines up to 4% of their annual turnover when using online services to process and transfer data e.g. for email, hosted applications or any other online service, selling to or having relations with

[1] The German E-Commerce and Distance Selling Association (bevh) represents a dynamically growing membership of large and small distance selling businesses using the internet, catalogues, direct sales and TV as sales channels. The members of bevh represent more than 75% of the total industry turnover in Germany. In addition, more than 130 service providers from the e-commerce sector are affiliated to the association.

companies outside the EU becomes very risky as a consequence. This could have a dissuasive effect, which would eventually lead to an isolation from global trade and economy of European businesses like in a pre-Internet era with enormous negative effects on EU competitiveness, innovation, and society.

3. Need for a proportionate, risk-based approach

Whereas a risk-based approach is provided for in the Schrems II ruling, the EDPB Recommendations seem to ignore it. Instead, the EDPB would require companies to take measures irrespective of the likelihood that a public authority in any third country would ever access the data in question. Where real-world risks are low, the Recommendations should not require organisations to adopt supplemental measures, as set out in Articles 32 and 35 of the GDPR. Additionally, the compliance checks should also be based on real risks incurred.
Moreover, not all information is relevant / could be subject to law enforcement requests (e.g. processing of employee credentials or limited profiles to provide access to a technical solution that does not process personal data as its primary function). Therefore, the full context of data transfers must be taken into account, which means also the nature of the data being transferred and not only the data protection legislation in the respective third country. When assessing potential risks and considering additional measures the principle of proportionality needs to be equally taken into account and needs to be based on the importance of the personal data affected and the parties involved.
The lack of such risk-based approach in the Recommendations will cause high administrative burden and harm the EU economy and society: EU researchers sharing health data with foreign partners to fight COVID-19, EU companies engaging in routine communications with employees outside the EU, and even simple commercial transactions with non-EU entities would all be fraught with substantial risk or even be made impossible without this being required by the Schrems II ruling.

4. Need for technical measures that are workable in practice

The case studies presented in the Recommendations to illustrate the non-exhaustive list of measures that can be taken to supplement the SCCs, are not workable in practice.
For instance, the Recommendations suggest that organisations can rely on encryption as a safeguard in most cases only if the data never appears in an unencrypted form in the third country and if the decryption keys are held only within the EU (or an adequate jurisdiction) (see, e.g., ¶¶ 79(6), 89(2-3), 84(11)). They also suggest that encryption almost never provides sufficient protection where data is accessible “in the clear” in the third country, including where an EU organisation uses an online service that may process the data in the third country (¶¶ 88-89), or where employees or others in the third country can access the data on a shared IT system (e.g., human resources data) (¶¶ 90-91).
Moreover, because the Recommendations state that even remote access by an entity in a third country to data stored in the EU constitutes a “transfer” (e.g., footnote 22, ¶ 13), organisations in many cases would need to apply these technical safeguards to EU-stored data as well. This fact underscores the impracticality of the Recommendations and their incompatibility with other

important EU interests, such as promoting open global trade and research necessary to protect vital interests. At a time when policymakers across the world, including in Europe, are pressing companies to provide greater access to encrypted communications in order to help governments more effectively fight terrorism and other threats, the proposed Recommendations seem to penalise companies for making such access possible.

More pragmatically, the Recommendations' positions on technical measures would render the SCCs virtually worthless as a transfer mechanism. In the vast majority of cases, the reason companies transfer data to third countries is to communicate and share information with people in those countries. If those people cannot access the information—as the Recommendations require— there is no point in transferring the data. Similarly, many online services that EU businesses rely on today must be able to process the information in unencrypted form in order to work properly; given the nature of the Internet and the global economy, this might entail some processing that occurs outside the EU, irrespective of where the data controller or data processor is based. The Recommendations would prohibit EU organisations from engaging in these commonplace and essential business activities.
In reality, most EU organisations would not be able to cease these activities entirely while still remaining economically competitive. Instead, many would likely turn to other legal mechanisms, such as the derogations set out in Article 49 of the GDPR. Because organisations adopting this approach might transfer data to non-adequate jurisdictions without even adopting SCCs (to say nothing of additional safeguards), this outcome would leave EU data subjects worse off because their data would be subject to fewer protections than they are today. However, the EDPB also noted that such derogations (which would include data subject consent) must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive.
To avoid these consequences, the EDPB should revise the Recommendations to ensure that the proposed technical measures are workable in practice and should leave it to data exporters to determine whether any particular measure adequately protects the transferred data. The Recommendations should not prohibit all access to data in the third country; doing so will discourage organisations from adopting technical measures, such as encryption, that in fact provide meaningful safeguards against unauthorised access.

5. Need for clarification that contractual measures may provide sufficient safeguards

Although the Recommendations propose a non-exhaustive list of contractual measures that can offer additional safeguards, they also include language suggesting that contractual or organisational measures on their own (i.e. without additional technical measures) cannot provide the level of data protection that EU law requires (¶ 48). This seems to be based on the assumption that the mere theoretical possibility of access by third-country authorities—even if the practical risk is very small—renders a transfer unlawful.
This constitutes an overly restrictive reading of the Schrems II judgement in which the ECJ held that data transfers to third countries should be prohibited only "in the event of the breach of [the SCCs] or it being impossible to honour them" (¶ 137). This suggests that, as long as the data importer does not disclose data to third-country authorities (or, if it does, notifies the data exporter accordingly), the two parties may rely on SCCs (¶ 139). In this case, contractual measures alone

can provide the additional safeguards needed to safely transfer data to a non-adequate jurisdiction. Thus, to be in line with the Schrems II judgement, the Recommendations should remove all language suggesting that contractual measures alone are insufficient safeguards to satisfy EU law. The Recommendations should instead bring forward several possible contractual measures that EU organisations may consider when transferring data to a non-adequate jurisdiction, then leave it to data exporters and importers to evaluate which measures are appropriate in context and "in the light of all the circumstances of that transfer" (Schrems II, ¶¶121, 146).

6. Need for a transition period

The Recommendations imply that supervisory authorities should move directly to "corrective measure[s] (e.g. a fine)" if they determine that a data transfer does not comply with the Recommendations (¶ 54). However, the Recommendations require companies to prepare new data transfer impact assessments and, in certain cases, to overhaul aspects of their data transfers. In many cases, these efforts require changes not only to contracts, but also to underlying infrastructure, software, and systems. Undertaking these changes is a complex task that often will involve many different parties, both inside and outside an organisation. Therefore, this will lead EU organisations to rush through changes to their data transfer practices—making it far less likely that organisations address these issues carefully and precisely. Therefore, instead, the Recommendations should expressly advise supervisory authorities, when they determine that a specific data transfer does not comply with EU law, to work with data exporters to find acceptable safeguards, and give them sufficient time to implement such solutions. In this sense, we would also call for a transition period of at least 1 year.

7. Need for correct legal basis

The EDPB's Guidance goes beyond the actual GDPR text. Although it is factually only a non-binding guidance, it will have a far-reaching effect, especially for the interpretation and enforcement by EU data protection authorities and finally result in a change in the politically agreed system of the GDPR. In our view, the EDPB's mandate is on enforcing the GDPR and not on changing it unilaterally. Therefore, it should be made clear that the provisions in the EDPB's guidance are only recommendations. In the same logic, it is important to note that companies that rely on Binding Corporate Rules (BCRs) have invested a significant amount of time, effort and money in their approval. The EDPB guidance now adds additional assessment requirements to BCRs even though these additional requirements are not covered by the GDPR, which is thus disproportionate.

8. Need for further clarification

There are also several elements in the Recommendations that require further clarification. First, the division of responsibilities between two or more data exporters in a joint controllership setting should be clarified and examples of such a scenario should be provided. The example in the box following paragraph 44 should be clarified, notably with regards to whether data exporters are

exempt from the obligation to undertake and document transfer impact assessment pursuant to paragraphs 34-43, in case they ascertain that a data importer falls under Section 702 FISA. The way the Recommendations transpose the requirements of Schrems II could lead to a de-facto prohibition of use of U.S.-based telecom, cloud and other service providers subject to FISA 702, significantly altering existing relationships. For this reason, only the largest and most sophisticated businesses could comply with the Recommendations and this may therefore amount to a non-tariff trade barrier on data flows, which only a political solution (and not the industry itself) would solve. On this issue, the EDPB has included some examples of supplementary measures but it would be helpful if the EDPB would provide practical examples on how to shape this process/ analysis in practice and in writing, especially in the situation where an EU-based controller is transferring personal data to a U.S. processor subject to FISA 702.

- Use case 6 should clarify whether EDPB Recommendations apply when cloud service providers do not need continuous access to the data. Data is often primarily hosted in an encrypted form within the EU and will most likely only be subject to access from a third country in specific and limited cases.
- Use case 7 should specify whether the use of personal data by the exporter 'for its own purposes' is a relevant criterion for the scenario assessment, especially given outsourced business services are typically provided under instruction of the data controller.
- The EDPB should clarify in use cases 6 and 7 the meaning of "the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society" as a criterion. Further clarification is notably needed on whether EDPB conclusions apply in situations where third-country laws prevent data importers from fulfilling their obligations under a data transfer tool (e.g. a third country does not permit encryption at rest) and how to assess whether public authorities' powers are deemed as not going beyond what is necessary and proportionate. We would also welcome further clarification on whether this criterion would also apply in use cases 1 to 5.
- The EDPB should introduce specific non-US examples to understand how different criteria should be interpreted in the context of jurisdictions which have not come under CJEU scrutiny.

Moreover, there is also a need for more clarity in the guidelines on the division of responsibilities between data exporter and importer that should consider which of the involved parties is in a better position to conduct assessments both from competence and scalability standpoints. Introducing requirements upon data exporter only would most likely create extensive administrative burdens for companies that might not operate in the specific jurisdiction they are required to assess the judicial privacy remedies, but consequently not able to do so. As data importers mostly are in a better position to know which laws apply to them in both import and export markets, and as they often typically serve multiple exporters, standardised assessments performed by the data importer could benefit all of their exporter customers and consequently should be supported in the EDPB guidelines. The same clarity is needed to allocate responsibilities among joint controllers and processors, especially in cases where only one of them is basically determining the purpose and the functioning of the data transfer service which

is offered to the joint controller on a ready tailored and non-negotiable basis. Examples of such scenarios would be more than welcome and should preferably focus on most common cases.
Furthermore, any suggestion that controllers are liable for sub-processors' supplemental measures appears to be inconsistent with the requirements in the GDPR. In relation to this, the contractual relationship between the exporter and the importer must consequently be considered as a relevant factor. When it comes to the many vendors on which retailers rely, the bargaining power of each individual business, no matter how large, vis-à-vis the vendor is limited. This contractual imbalance is being addressed in certain sectors, such as financial services (where specific contractual clauses are being drafted to reduce risk of vendor lock-in) but is not currently available in the retail content. It is therefore likely, on the basis of the Recommendations as drafted, that such vendors will also insist on an agreement from retailers that these measures are sufficient on a take-it-or-leave-it basis. In line with the practical realities and contractual imbalances noted above, we would like the Recommendations to direct greater responsibility towards these vendors.