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

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

Position on the European Commission's draft implementing decision on standard contractual clauses

Berlin, 10 December 2020

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

1. Introduction

In light of the Schrems II ruling, in which the European Court of Justice held that businesses transferring data outside the EU cannot only rely on standard contractual clauses but need to adopt additional safeguards to protect personal data from being accessed by third countries' authorities, bevh[1] welcomes the swift proposal of the European Commission of new standard contractual clauses. 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 that is data-driven and not place-bound in particular. As the European Data Protection Board is working in parallel on recommendations on how to supplement data transfer tools to ensure compliance of third country parties with EU data protection standards, it is essential for reasons of clarity and legal certainty to align their work with the future SCCs. We welcome the opportunity to provide comments from the point of view of the German e-commerce industry on the Commission's draft implementing decision on standard contractual clauses.

2. Need for legal certainty

It is crucial that companies can really rely on the new SCCs. They need the necessary legal certainty that the new SCCs are sufficient, and that the validity of data transfers will be ensured. It is also important that data protection authorities do not impose additional requirements at national level that are going beyond the SCCs, which might lead to contractionary requirements, legal uncertainty and confusion for businesses. Moreover, it is important that the new SCCs will not be subject to additional contractual clauses for compliance with privacy law, that they can be used for transfers to any data importers in third countries and that any provisions in agreements that are conflicting with obligations in the SCCs are void. Additionally, we ask the Commission to clarify that service providers cannot seek to decrease the protections of such SCCs (e.g., in provisions in other agreements that sit outside the SCCs, such as "For purposes of clarification,

[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.

the data importer's obligation to allow an audit under GDPR will be satisfied by data exporter requesting data importer to provide written information about data importer's security practices").

3. Modular approach

In general, we welcome the modular approach that tries to cover various scenarios. On the one hand, this is beneficial as, unlike in the past, this allows for flexibility and the SCCs can individually be adapted to the requirements of a particular data transfer. On the other hand, however, this leads to more complexity for companies as this entails an assessment of each individual case. Thus, particularly for SMEs, it will be very difficult to apply. Moreover, it is unclear how this approach will exactly work in practice. Consequently, it is essential that the Commission creates final and clean drafts of the SCCs for each of the processing scenarios and the use of SCCs beyond the four relationship scenarios identified. This will be the only way to provide legal certainty to the businesses involved.

4. Need for a risk-based approach

We welcome the European Commission's risk-based approach which should also be reflected in the recommendations on supplementary measures. In line with the Schrems II ruling, businesses should rely on their own practical experience when assessing the specific circumstances of data transfers. However, the proposed SCCs require the data exporter and data importer to declare that they have no reason to believe that the laws in the third country will prevent the data importer from fulfilling the obligations under the SCCs. However, it remains unclear if they have to do so jointly. As both parties naturally have different levels of knowledge about the law applicable in the third country, the Commission should clarify that they only have to do so separately since for the data exporter, this warranty can only be based on his or her knowledge of requests for disclosure from third country authorities. Thus, the "relevant practical experience" needs to be applied in a risk-based way to the obligations laid down in the SCCs, especially when it comes to warranties that a controller / data exporter has to make.

5. Need for full consistency with the GDRP

The modernised SCCs should be fully aligned and consistent with the GDPR as any contradictions or inconsistencies will lead to legal uncertainty. This particularly applies to the controller-to-processor scenario as in accordance with the GDPR, it should be the processor who is responsible to ensure the adequate behaviours of the sub-processor and not the controller / exporter. The obligations to provide data subjects with a copy of SCCs and inform them about any changes of purpose and / or identity of a third-party data recipient should be proportionate and also aligned with the GDPR as it already defines these information obligations. Therefore, it should be clarified that the data exporter only needs to provide copies upon request to the extent it is required by the GDPR. This is part of the discretion of companies to determine in line with the GDPR the necessary actions to meet the obligations of the SCCs. In this sense, the European Commission should also clarify that data importers only need to challenge government requests where this would be considered reasonable after a careful assessment since according to the draft data importers would need to "exhaust all available remedies to challenge" a request if there

"are grounds under the laws of the country of destination to do so." Read broadly, this could require data importers to challenge requests even where there is no reasonable possibility, or no possibility at all, of success. Such a stance could impose legal costs on data importers with no real benefit to data subjects.

6. Need for a longer transition period

The 12 months transition period foreseen in the proposal is not sufficient for e-commerce sellers as they have a complex framework of data transfer agreements that they have to review, cancel and replace. Moreover, following the Schrems II ruling, in parallel companies have to assess if they would need to adopt additional measures to transfer data to third countries, which is particularly challenging for SMEs. Therefore, the transition period should be extended to at least 24 months (in line with the GDPR implementation period of 2 years+), existing SCCs should remain valid during this transition period and the duration of the data transfer agreement (with additional safeguards taken where necessary) i.e., the new SCCs are only required for new data transfer arrangements.