German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

"Recommendations 01/2020 of the European Data Protection Board on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" of 10 November 2020

Register of Interest Representatives
Identification number in the register: 52646912360-95

Contact:
Dr. Christian Koch / Wulf Hartmann
Telephone: +49 30 20212321 / +49 30 1663-3140
Telefax: +49 30 2021-192300 /
E-mail: c.koch@bvr.de / wulf.hartmann@bdb.de

Berlin, 18 December 2020

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent approximately 1,700 banks.

Coordinator:
National Association of German Cooperative Banks
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefax: +49 30 2021-1900
www.die-dk.de

Comments „Recommendations 01/2020 of the European Data Protection Board on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" of 10 November 2020

Position of the German Banking Industry Committee on

"Recommendations 01/2020 of the European Data Protection Board on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" of 10 November 2020

Guaranteeing the level of data protection for data transfers to third countries is an important objective of the EU's General Data Protection Regulation (GDPR). Of course we support this goal. However, the principles of proportionality must also be respected and viable solutions must be made available. Consequently, there is a need to improve the recommendations proposed for consultation by the European Data Protection Board (EDPB):

1. **Problem – the approach of the EDPB's recommendations for assessments to be carried out on a case-by-case basis is too complex and means companies have to ensure data protection adequacy on their own**

Firstly, we welcome that the EDPB's recommendations are intended to provide guidance for companies and public bodies as data processors on how to implement the CJEU ruling of 16 July 2020 in Case C-311/18 (Schrems II) when they are exchanging personal data with bodies in third countries and there is no adequacy decision by the European Commission under Article 45 of the GDPR or none of the grounds for exemption under Article 49 of the GDPR apply. However, there is no viable solution for companies to be able to guarantee with proportionate effort the data protection adequacy at data importers in third countries required by the GDPR and emphasised by the CJEU in its ruling of 16 July 2020.

Until now, companies have generally been able to establish data protection adequacy with the help of, among other things, EU standard contractual clauses without having to take supplementary measures. But both the amended EU standard contractual clauses proposed by the European Commission on 11 November 2020 and the EDPB's recommendations of 10 November 2020 turn this principle on its head. They now regularly require an additional case-by-case assessment of the legal situation in the data importer's country (cf. "Step 3" of the recommendations). This would lead to a level of excessive complexity that was not intended by EU legislators when drafting Article 46(2)(c) and (d) of the GDPR to safeguard third-country data transfers using EU standard contractual clauses. This would put companies in a difficult situation, particularly if they did not have the resources to undertake a case-by-case assessment due to their size.

This approach gives the general impression that, since the CJEU judgment of 16 July 2020 at the latest, there has been a trend in data protection legislation away from economic globalisation despite the progressive global interconnectedness of products and services. This is particularly relevant for IT software products and IT services that operate in international markets and do not limit themselves to countries in the European Union. There is also no recognition that – not only in the financial sector – certain high-quality IT products and/or IT services are only offered by providers in certain third countries (e.g. the US). In such cases, the EU single market does not offer solutions of comparable quality. In addition, it is implied that access by public authorities to data in third countries can be controlled or restricted. Even if this were desirable from a data protection perspective, it is unrealistic.

Comments „Recommendations 01/2020 of the European Data Protection Board on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" of 10 November 2020

Shifting the geopolitical problem of differing levels of data protection resulting from the CJEU judgment solely to companies alone cannot be considered a satisfactory solution. This would significantly impair – if not, in some cases, prohibit – data transfers to third counties. In order not to leave companies to deal with this problem on their own, there is a need for robust EU level guidelines and instruments, which businesses can rely on and which allow them to transfer data to a third country on a legally secure basis.

2. Solution – supporting companies in assessing data protection adequacy

The EDPB's chosen approach of case-by-case assessments is too complex and thus unsuitable. Reducing complexity by providing standardised solutions at EU level would help companies produce adequacy assessments.

- **Preserving the function of EU standard contractual clauses**

    - The - revised - EU standard contractual clauses should continue to be sufficient for the purposes of Article 46(2)(c) and (d) of the GDPR to demonstrate the data protection adequacy of the data importer in the third country.

    - Exceptions should only apply if the European Commission explicitly includes certain third countries in a publicly accessible list of states where additional measures are required to ensure data protection adequacy.

- **Supporting the assessment of data protection adequacy through European Commission guidelines**

    - It would be very helpful if the European Commission were to publish data protection information about certain third countries – similar to the way national governments provide security information about travel destinations. A list of this kind would certainly be feasible for the most important third countries (such as China, India, the US, Turkey and Russia). It would assess the data protection level of the respective third country and give recommendations for additional security measures that would be practicable for companies to implement. This might also include clustering third counties by risk class. It would allow companies to conduct a legal assessment of the data protection level in a third country with proportionate effort.

    - In order to reduce the assessment burden on the company exporting the data, consideration should be given to initially permitting the adequacy test to be limited to allowing the data importer in the third country to robustly demonstrate an adequate level of data protection to the data exporting company in the EU.

    - It would be helpful if certain providers in third countries (e.g. providers of cloud services) were to be registered with the European Commission as data protection compliant. Then companies in the EU could rely on this information.

Comments „Recommendations 01/2020 of the European Data Protection Board on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" of 10 November 2020

- **Acceptance of a risk-based approach**

  - A risk-based approach would have to suffice for those third countries where additional safeguards are deemed necessary. This would allow companies to differentiate. The data protection risk might then depend on the

    - type, quality and scope of relevant data,
    - type and method of data access for the importer in a third country,
    - access controls for the data exporter.

  - In terms of technical security measures, the EDPB has set the benchmark too high with its requirement for full encryption. Here, too, it is a matter of differentiating by risk. For lower risks, a simpler type of encryption or even pseudonymisation may also suffice. In terms of technical measures (e.g. encryption), "commercially available solutions" should suffice. The European Commission could also categorise certain encryption standards as sufficient.

- **Transitional solution to changes in the legal situation in a third country**

  - If it is detected in step 3 of the EDPB recommendations that a third country has a lack of data protection in its legislation and if it is not possible to compensate for this lack of data protection in step 4, the data protection supervisory authority should not simply prohibit the data transfer with immediate effect, especially if the legal situation in the third country has just changed. This could leave the company facing insurmountable business continuity difficulties in the short term. Without a fallback solution – which is not usually available immediately – data processing capabilities in the third country that are important for business continuity could suddenly no longer be used. This could jeopardise the viability of the company.

  - If a company can plausibly demonstrate that there is no reasonable backstop solution in the short and medium term to the service provider it uses in the third country, i.e. that it is irreplaceable, it should be possible to put a transitional solution in place. This should be coordinated with the competent supervisory authority.

- **Distinction between transfers of, and access to, personal data**

  - The EDPB does not differentiate between transfers of, and access to, personal data. Mere access by third parties to data stored in the EU or European Economic Area (EEA) is also considered a "transfer" (page 9, paragraph 13 and page 8, footnote 22 of the recommendations). This will have significant practical relevance for many companies in a number of different circumstances, such as if the controller concludes an agreement with a processor established in the EEA, which is in turn a subsidiary of a parent company in a third country. Without making a distinction between a transfer of personal data which are ultimately stored outside the EEA and the granting of third-party access to data stored in the EEA, it will not be possible to apply a risk-based approach focusing on the intensity of the data processing. Access to data stored in the EEA can be granted in many forms, most of which do not present a risk profile even remotely comparable to the situation discussed in the CJEU decision of 16 July 2020.

Comments „Recommendations 01/2020 of the European Data Protection Board on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" of 10 November 2020

- The EDPB recommendations should therefore clarify that the mere possibility of being able to access data stored in the EEA is subject to less stringent restrictions than the physical transfer of personal data and their storage in a third country. It would also be helpful if the recommendations clarified that data transfers to a recipient in the EEA do not fall within the scope of the CJEU ruling of 16 July 2020 even if the recipient's parent company is domiciled in a third country.