

## Ban on data transfers to the USA?

**Article by Dr. Carlo Piltz and Stefan Hessel**

The current Digital Health Applications Guide is a challenge for providers of health apps and other digital helpers

We already explained in one of our last [newsletters](#) that hard times are ahead for providers of digital health applications (DHAs) and other digital helpers with respect to data transfers to the USA due to the annulment of the EU-US Privacy Shield. Now the Federal Institute for Drugs and Medical Devices has adapted its [official guide](#) (PDF), The Fast Track Process for Digital Health Applications according to Section 139e SGB V (the “DHA Guide”), to the requirements of the latest ruling of the European Court of Justice (ECJ).

On 16 July 2020, by way of its [judgment in case C 311/18 \("Schrems II"\)](#), the European Court of Justice annulled the existing EU-US Privacy Shield adequacy finding for data transfers between the EU and the US. At the same time, the Court also set high standards for data transmission based on standard contractual clauses.

### No data transfers to the USA?

Data transfers to third countries such as the USA are regulated in Section 4(3) of the Digital Health Applications Ordinance (DiGAV). According to this provision, data may only be transferred to third countries if an adequacy decision has been issued by the European Commission. By way of this Ordinance, the Federal Ministry of Health, which is competent under Section 139e(9) of Title V of the Social Code, has tightened the requirements of the General Data Protection Regulation (GDPR), which also permits data transfers to third countries on the basis of other mechanisms. As an argument for this, [page 45 of the DHA Guide](#) mentions a very high need for protection to be assumed as a rule.

However, it seems questionable whether this deviation from the GDPR, which aims at full harmonisation of data protection law in the EU, is permissible. In this respect, German legislators appear to be invoking important reasons of public interest in accordance with Article 49(5) GDPR ([cf. legislative intent to Section 80\(2\) of Title 10 of the Social Code, p. 115](#)).

However, whether this is actually the case and whether this is justified in such general terms can be doubted. If one assumes, however, that the limitation of the transfer modalities in the GDPR made by German legislators is permissible, this has serious consequences for DHA providers. You will then simply no longer be able to transfer data to the United States due to the annulment of the EU-US Privacy Shield.

### The updated DHA Guide

In this light, it is not surprising that the Federal Institute states on page 45 of the [updated German version of the DHA Guide \(metadata dated 31 July 2020\)](#) concerning the EU-US Privacy Shield that: "Processing of personal data in the USA is therefore no longer permissible on this basis." The recent official [English version \(metadata dated 7 August 2020\)](#) of the DHA Guide is even clearer on page 43 with reference to the EU-US Privacy Shield: "Processing of health data in the USA is therefore not permissible for a [DHA]." When one compares the two formulations, it is immediately noticeable that the German version refers generally to personal data, while the English translation refers exclusively to health data.

In this light, it is currently unclear whether the Federal Institute assumes with respect to DHAs a complete ban on the transfer of personal data to the USA or whether the restriction is only to apply to health data. In the latter case, technical data for the use of an app could be transferred to the USA. However, even if the English version is taken as the starting point - in a supplier-friendly manner - the ban on transmission would be far-reaching.

This is not least due to the fact that data protection authorities tend to have a rather broad interpretation of particularly sensitive data. For example, in the opinion of the [Data Protection Conference \(DSK\) in its Short Paper No 17](#) regular attendance at a particular church is already considered to be particularly sensitive and thus covered by the strict processing requirements of Article 9 GDPR. Applied to health apps, this could mean that the very installation of the app would qualify as health data. In the worst case, this could result in a ban on the use of app stores, such as the Google Playstore or Apple's iStore.

## What providers should do now

The situation therefore remains legally uncertain for providers of health apps. In addition to checking the extent to which their own applications are at all subject to the Digital Health Applications Ordinance, they should also check whether data are being transferred to US providers. Providers who store data in Germany but whose parent company or registered office are located in the US should also be considered. A first step, for example, would be to internally map data flows to third countries. Finally, DHA providers must also be aware that the Federal Institute will examine the existing requirements in the context of approvals. As a provider, therefore, you cannot rely on non-compliance, but must implement the strict requirements or, if necessary, be ready for legal action in the event of complaints during the approval procedure. Regardless of the path chosen, the legal requirements should be taken into account in the development of DHAs, so that a possible rejection notice from the Federal Institute does not lead to a rude awakening.

[September 2020]



### About us:

reuschlaw Legal Consultants advise companies active on a national and international scale in more than 30 countries in the areas of product liability, product safety law, recall management, insurance law, cybersecurity and data protection, compliance management and contract law.

**Company contact:** Melanie Schaumann | Head of Marketing & Communications | T > +49 30 / 2332895 0 | E > [melanie.schaumann@reuschlaw.de](mailto:melanie.schaumann@reuschlaw.de)