Prescription apps: new information concerning data transfers to the US

Article by Dr. Carlo Piltz and Stefan Hessel

Special requirements apply for data transfers to third countries by digital health applications, i.e. health apps which can be prescribed by physicians and which are eligible for statutory health insurance coverage. In accordance with § 4(3) of the Digital Health Applications Ordinance, personal data may only be transferred to countries outside the European Economic Area (EEA) if an adequacy decision has been issued by the European Commission. Since the EU-US Privacy Shield was struck down by Judgment of the ECJ in Case No. C 311/18 (the "Schrems II" case), that is no longer the case for the US as of 16 July 2020. This poses enormous challenges for manufacturers of digital health applications, as we reported before the Judgment, and even raises the question as to whether digital health applications can be offered in the Google and Apple app stores.

The Federal Institute for Drugs and Medical Devices (BfArM) has issued guidance for digital health applications in which it discussed the challenges associated with data transfers to the US and more recently, on 28 January 2021, the authority published separate information concerning the lawfulness of data transfers to countries outside Germany (only in German), which we will explain in greater detail below.

No violation of European law because the provision does not relate to data protection law?

Right at the start, BfArM clarified that its assessment relates only to the eligibility of digital health applications for insurance coverage and that it is not binding upon the data protection authorities. It goes on to say the following: "Should the data protection authorities take a different legal view in the course of their supervisory activities, a technical adjustment to ensure proper data processing activities within the app may be necessary to avoid removal of the app from the directory."

In other words, the value of this official statement for manufacturers of digital health applications is considerably diminished right at the start, as there is always a possibility that a data protection authority will take a stricter view than that of BfArM, which would render this information moot. But this statement is also of interest in light of the possibility that § 4(3) of the Ordinance could violate European law. After all, this requirements specified in that provision are narrower than those provided in the GDPR beginning with Article 44, under which data transfers to third countries are generally allowed based on other safeguards, such as

standard contractual clauses, particularly in cases where an adequacy decision from the European Commission does not exist. In accordance with Article 49(5) of the GDPR, member states may only deviate from this rule for important reasons of public interest.

In such a case, however, the European Commission would have to be notified, something which the competent authority, the Federal Ministry of Health, has apparently failed to do (only in German). In light of the information which has been published to date, one possible explanation for this course of action is that the Federal Ministry of Health, as well as BfArM (a subordinate office attached to the Ministry of Health), interpret § 4(3) of the Digital Health Applications Ordinance not as a rule of data protection law but rather solely as a provision relating to coverage under the statutory health insurance scheme. However, such an interpretation is questionable from the viewpoint of European law since the provision in question, § 4(3) of the Digital Health Applications Ordinance, effectively prevents full harmonization of the GDPR in cases not covered by Article 49(5) of the GDPR.

BfArM: data transfers to establishments and subsidiaries of US companies may be lawful

But the substantive statements by BfArM are no less interesting. For example, the authority makes it very clear that "for all tools which may be used in connection with use of the app, the flow of personal data to the US must be completely ruled out." However, the authority takes the view that US service providers "with (independent) establishments in the EU but parent companies in the US," such as e.g. Google Limited Ireland or AWS Luxembourg, may be used provided that "personal data are encrypted and that the keys are managed or stored by the app manufacturers in the EU itself." In cases where the relevant entity is not an establishment but rather a European subsidiary, BfArM goes even further, stating that it is enough if the processor "gives assurance that no data transfer to the US will take place and that no data will be processed in the US."

In addition, the processor is required to confirm "that, even in case of a surrender request from the US authorities, no data will be made available, not even to the parent company." The subsidiary is also required to give assurance that it will take legal action to oppose any request for surrender of the data, exhausting all avenues of appeal all the way to the supreme court. Even if such a ruling were to be issued, the data may only be surrendered if "it is based on an international agreement currently in effect between the third country seeking the information and the EU, or an individual member state, such as a mutual legal assistance treaty." BfArM does not address the question as to how companies with a US parent company can confidently provide such an assurance in light of the foreseeable conflict of laws. Since the authority itself does not seem sure that such

assurances are legally valid, it requires manufacturers of digital health applications to "report any surrender requests from US authorities to BfArM."

Insured persons in the US and app stores

Also notable from the viewpoint of data protection law are the statements made by BfArM with regard to cases where an insured person is physically located in the US upon using the app. Specifically, the authority assumes that US law would apply in such a case, and "particularly for the processing of personal data." The question as to how this opinion can be reconciled with Article 3(1) of the GDPR, which expressly states that the GDPR applies to data processing "in the context of the activities of an establishment of a controller [...] in the Union, regardless of whether the processing takes place in the Union or not" is left unanswered. A data transfer under such circumstances could typically be based on Article 49 of the GDPR, but such a transfer would be impermissible in accordance with § 4(3) of the Digital Health Applications Ordinance.

The authority's reasoning is also inconsistent as it relates to the use of app stores, which it fortunately considers to be permissible provided that the "log-in data is kept separate from the app's health data." Accordingly, the provisions of the GDPR apply without qualification for the use of app stores, so that data transfers can take place even in the absence of an adequacy decision. But the authority does not address the fact that, regardless of how the app is structured, the processing of data via the app store nevertheless likely qualifies as processing of health data, certainly from the viewpoint of the data protection authorities, since it creates a clear link between a user and a specific ailment. It is also questionable whether BfArM's interpretation is consistent with the wording of § 4(3) of the Ordinance, which expressly relates to processing "within the framework of a digital health application."

Conclusion

The new information provided by BfArM does not afford manufacturers of digital health applications an adequate degree of legal certainty with regard to the conflict between the Digital Health Applications Ordinance and the GDPR. Rather, the Ordinance's deviation from the provisions of the GDPR means that BfArM will have to create a "parallel universe of data protection law" in order to account for the drastic impact of the "Schrems II" decision on data transfers to the US by manufacturers of digital health applications.

The novel interpretation of data protection law which is required for this purpose may create problems with data protection authorities for manufacturers of digital health applications. Accordingly, it would generally be desirable for the Federal Ministry of Health to back away from its deviation from the GDPR, which is questionable in terms of European law, by making changes to the Digital Health Applications Ordinance. Until this occurs, manufacturers have no choice but to subject their data flows to careful factual and legal review, while at the same time assuming substantial risks, whenever they use non-European providers or their subsidiaries.

[February 2021]

Company contact: Melanie Schaumann I Head of Marketing & Communications I T > +49 30 / 2332895 0 I E > melanie.schaumann@reuschlaw.de