Verbot von Datentransfers in die USA?

Ein Beitrag von Dr. Carlo Piltz und Stefan Hessel

Der aktuelle DiGA-Leitfaden ist eine Herausforderung für Anbieter von Gesundheits-Apps & Co.

Dass für die Anbieter von Gesundheits-Apps und anderen DiGA bei Datentransfers in die USA wegen der Aufhebung des EU-US Privacy Shield harte Zeiten anbrechen, hatten wir bereits in einem unserer letzten Newsbeiträge erläutert. Nun hat das BfArM seinen offiziellen "Leitfaden zum Fast-Track-Verfahren für digitale Gesundheitsanwendungen (DiGA) nach § 139e SGB V" an die Vorgaben des jüngsten Urteils des Europäischen Gerichtshofs (EuGH) angepasst.

Mit seinem Urteil in der Rechtssache C 311/18 ("Schrems II"-Fall) hatte der EuGH am 16. Juli 2020 den für Datenübertragungen zwischen der EU und den USA bestehenden Angemessenheitsbeschluss für Datenübermittlungen, das EU-US Privacy Shield, für ungültig erklärt. Gleichzeitig hat das Gericht auch für Datenübertragung auf Basis von Standardvertragsklauseln hohe Anforderungen aufgestellt.

Keine Datenübermittlung in die USA?

Datenübermittlungen in Drittstaaten wie die USA sind in § 4 Abs. 3 der Digitale-Gesundheitsanwendungen-Verordnung (DiGAV) geregelt. Danach dürfen Daten in Drittstaaten ausschließlich übertragen werden, wenn ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt. Mit dieser Regelung hat das nach § 139e Abs. 9 SGB V zuständige Bundesministerium für Gesundheit die Vorgaben der DSGVO, die Datenübermittlungen in Drittstaaten auch auf Basis anderer Mechanismen erlaubt, verschärft. Als Argument hierfür wird auf Seite 45 des DiGA-Leitfadens ein regelhaft anzunehmender besonders hoher Schutzbedarf ins Feld geführt. Ob diese Abweichung von der DSGVO, die eine Vollharmonisierung des Datenschutzrechts in der EU zum Ziel hat, zulässig ist, erscheint jedoch fraglich. Der deutsche Gesetzgeber scheint insoweit auf einen wichtigen Grund des öffentliches Interesses nach Art. 49 Abs. 5 DSGVO zu berufen (vgl. Gesetzesbegründung zu § 80 Abs. 2 SGB 10, S. 115). Ob dieser jedoch tatsächlich vorliegt und in dieser Pauschalität begründet ist, kann man jedoch durchaus in Zweifel ziehen. Geht man jedoch davon aus, dass die vom deutschen Gesetzgeber

vorgenommene Einschränkung von Transfermodalitäten der DSGVO zulässig ist, hat dies gravierende Folgen für DiGA-Anbieter. Ihnen ist eine Datenübermittlung in die USA infolge der Aufhebung des EU-US Privacy Shield dann schlicht nicht mehr möglich.

Der aktualisierte DiGA-Leitfaden

Vor diesem Hintergrund ist es wenig verwunderlich, dass das BfArM in seiner aktualisierten Version des DiGA-Leitfadens (laut Metadaten vom 31.07.2020) auf S. 45 zum EU-US Privacy Shield feststellt: "Eine Verarbeitung von personenbezogenen Daten in den USA ist auf seiner Grundlage folglich nicht mehr zulässig." Die erstmals erschienene englische Version (laut Metadaten vom 07.08.2020) des DiGA-Leitfadens (PDF) wird auf Seite 43, ebenfalls bezogen auf das EU-US Privacy Shield, sogar noch deutlicher: "Processing of health data in the USA is therefore not permissible for a DiGA." Vergleicht man beide Formulierungen, fällt zunächst auf, dass sich die deutsche Version allgemein auf personenbezogene Daten bezieht, während in der englischen Übersetzung ausschließlich auf Gesundheitsdaten abgestellt wird.

Vor diesem Hintergrund ist derzeit unklar, ob das BfArM bei DiGA von einem kompletten Übermittlungsverbot personenbezogener Daten in die USA ausgeht oder die Beschränkung nur für Gesundheitsdaten gelten soll. In letzterem Fall könnte man etwa noch technische Daten zur Nutzung einer App in die USA übertragen. Selbst wenn man jedoch – anbieterfreundlich – von der englischen Version ausgeht, ist das Übermittlungsverbot weitreichend. Dies liegt nicht zuletzt darin begründet, dass die Datenschutzaufsichtsbehörden eine eher weite Auslegung von besonders sensiblen Daten vornehmen. So soll nach der Ansicht der Datenschutzkonferenz (DSK) in ihrem Kurzpapier Nr. 17 bereits der regelmäßige Besuch einer bestimmten Kirche als besonders sensibel und damit von den strengen Verarbeitungsanforderungen des Art. 9 DSGVO erfasst sein. Übertragen auf Gesundheits-Apps könnte dies bedeuten, dass schon die Installation der App als Gesundheitsdatum zu qualifizieren wäre. Hieraus könnte sich dann im worst case ein Verbot für die Nutzung von Appstores, wie z.B. dem Google Playstore oder dem iStore von Apple, ergeben.

Was Anbieter jetzt tun sollten

Für Anbieter von Gesundheits-Apps bleibt die Situation damit auch weiterhin rechtlich unsicher. Neben einer Überprüfung, inwieweit die eigene Anwendung überhaupt der DiGAV unterfällt, sollten sie prüfen, ob Daten an US-Anbieter übermittelt werden. Hierbei sollte auch an Anbieter gedacht werden, die Daten zwar in Deutschland speichern, aber deren Muttergesellschaft bzw. Hauptsitz sich in den USA befindet. Ein erster Schritt ist etwa, ein internes Mapping der Datenflüsse in Drittstaaten durchzuführen. Schlussendlich müssen sich DiGA-Anbieter auch bewusst sein, dass das BfArM die bestehenden Vorgaben im Rahmen der Zulassung

prüfen wird. Auf Non-Compliance kann man als Anbieter daher nicht setzen, sondern muss die strengen Vorgaben umsetzen oder gegebenenfalls bei Beanstandungen im Zulassungsverfahren rechtliche Schritte erwägen. Unabhängig vom gewählten Weg sollten die rechtlichen Vorgaben schon bei der Entwicklung der DiGA berücksichtigt werden, damit ein etwaiger Ablehnungsbescheid des BfArM nicht zu einem bösen Erwachen führt.

[September 2020]

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