Informationen zur Zulässigkeit der Datenverarbeitung außerhalb Deutschlands im Zusammenhang mit dem Prüfverfahren des BfArM gemäß § 139e Fünftes Buch Sozialgesetzbuch (SGB V)

Stand 11.10.2023

Die nachfolgenden Ausführungen geben eine Einschätzung der Rechtsauffassung des BfArM im Rahmen des Verfahrens zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen (DiGA) nach § 139e Absatz 3 und 4 SGB V wieder. Diese Einschätzung entfaltet keine Bindungswirkung für die Datenschutzbehörden. Sollten die Datenschutzbehörden im Rahmen ihrer Aufsichtstätigkeit eine abweichende Rechtsauffassung vertreten, ist zur Gewährleistung einer ordnungsgemäßen Datenverarbeitungstätigkeit innerhalb der DiGA ggf. eine technische Anpassung zur Vermeidung der Streichung einer Anwendung aus dem Verzeichnis erforderlich.

Die DSGVO erlaubt grundsätzlich eine Datenverarbeitung personenbezogener Daten innerhalb der Europäischen Union (EU). Eine Verarbeitung außerhalb der EU in einem sog. Drittstaat ist zulässig, sofern ein vergleichbares Schutzniveau im Drittstaat besteht (Angemessenheitsbeschluss nach Artikel 45 Datenschutz-Grundverordnung, DSGVO).

Die Digitale Gesundheitsanwendungen-Verordnung (DiGAV) beschränkt analog zu den für Krankenkassen geltenden Regeln (§ 80 SGB X) den Ort der Datenverarbeitung für die von der DiGA nach § 4 Abs. 2 DiGAV verarbeiteten Daten auf die Bundesrepublik Deutschland, die Mitgliedstaaten der EU, die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR) und die Schweiz und Staaten, für die ein Angemessenheitsbeschluss nach Artikel 45 DSGVO vorliegt. Eine Verarbeitung personenbezogener Daten außerhalb der EU allein auf Basis von Artikel 46 DSGVO (Standardvertragsklauseln) oder Artikel 47 (Binding Corporate Rules) ist für DiGA nicht zulässig (vgl. § 4 Abs. 3 DiGAV).

Mit der Annahme des Angemessenheitsbeschlusses für den Datenschutzrahmen EU-USA durch die Europäische Kommission können seit dem 10.07.2023 personenbezogene Daten aus der Europäischen Union (sowie aus Norwegen, Liechtenstein und Island) in die USA übermittelt werden. Hierfür müssen sich allerdings die betreffenden US-Unternehmen dem Datenschutzrahmen EU-USA anschließen, indem sie sich zur Einhaltung detaillierter Datenschutzpflichten verpflichten. Auf der Seite der US-Handelskammer sind die US-Unternehmen „*aktiv*“ gelistet, die sich dem Datenschutzrahmen EU-USA angeschlossen haben.

Referenzen

- **Liste der US-Handelskammer über US-Unternehmen, die sich dem Datenschutzrahmen EU-USA angeschlossen haben.** Online unter: https://www.dataprivacyframework.gov/s/participant-search

Dienstleister (z. B. Betreiber von Rechenzentren) aus den USA mit (selbständiger) Niederlassung in der EU, aber einem Mutterkonzern in den USA, die sich nicht dem Datenschutzrahmen EU-USA anschließen, dürfen aufgrund des EuGH-Urteils und den Vorgaben der DiGAV nur unter bestimmten Voraussetzungen für die Verarbeitung von personenbezogenen Daten herangezogen werden: Eine Inanspruchnahme kommt allein unter Beachtung strenger Anforderungen in Betracht, die hinreichende Gewähr für die Unterbindung einer Datenübertragung aus dem Geltungsbereich der DSGVO an das Mutterunternehmen bieten (s. FAQ). Auch für jegliche Tools, die im Rahmen der Nutzung der DiGA ggfs. zum Einsatz kommen, sind im Falle einer

Übermittlung von personenbezogenen Daten in die USA die unten genannten Voraussetzungen zu beachten.

Der Hersteller einer DiGA ist verantwortlich für die Gewährleistung aller datenschutz- und datensicherheitsbezogenen sowie sonstigen rechtlichen Anforderungen an sein Medizinprodukt. Deren Einhaltung bei der Nutzung der DiGA gemäß dem aktuellen Stand der gesetzlichen und technischen Anforderungen sowie die wahrheitsgemäße Bestätigung deren entsprechenden Einhaltung gegenüber dem BfArM im Rahmen des Antragsverfahrens zur Aufnahme in das Verzeichnis des BfArM nach § 139e SGB V liegen ebenfalls in seiner Verantwortung. Jegliche nachträgliche Veränderung mit Bezug zu diesem Thema ist als wesentliche Veränderung im Sinne von § 18 Abs. 1 DiGAV anzusehen und entsprechend dem BfArM unverzüglich anzuzeigen.

Referenzen

- **Liste der Staaten, für die ein Angemessenheitsbeschluss vorliegt.** Online unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Als DiGA-Hersteller haben wir einen Vertrag zur Datenverarbeitung (Data Processing Agreement, DPA) mit einem Dienstleister mit Niederlassung in der EU, aber einem Mutterkonzern in den USA (z. B. Google Limited Ireland oder AWS Luxemburg) geschlossen oder nutzen Services eines solchen Anbieters. Gibt es Voraussetzungen, unter denen diese Datenverarbeitung zulässig ist?

Dienstleister mit Sitz in den USA können für die Speicherung und Verarbeitung personenbezogener Daten herangezogen werden, sofern sie sich dem Datenschutzrahmen EU-USA anschließen, der sie zur Einhaltung detaillierter Datenschutzpflichten verpflichtet.

Für Dienstleister mit Sitz in den USA, die sich nicht dem Datenschutzrahmen EU-USA anschließen, gilt:

- Sofern die personenbezogenen Daten nach dem Stand der Technik im Sinne von Artikel 25 und 32 DSGVO verschlüsselt sind und die Schlüssel vom DiGA-Hersteller in der EU oder einem Drittland, für welches ein Angemessenheitsbeschluss nach Artikel 45 DSGVO besteht, selbst verwaltet und gespeichert werden, dürfen Dienstleister mit Niederlassung in der EU, aber einem Mutterkonzern in den USA, herangezogen werden. Eine Aufbewahrung der Schlüssel kann auch durch einen Dritten (Treuhanddienstleister) durchgeführt werden, wenn sich dessen Sitz in der EU bzw. einem Drittstaat mit Angemessenheitsbeschluss befindet. Eine Aufbewahrung der Schlüssel beim Dienstleister mit US-Mutterkonzern selbst wird explizit ausgeschlossen. Darüber hinaus muss der jeweilige Dienstleister dem DiGA-Hersteller zusichern, dass kein Datentransfer und auch keine Datenverarbeitungen in den USA durchgeführt werden.
- Sofern Dienstleister und DiGA-Hersteller bestätigen, dass auch im Fall von Herausgabeverlangen von US-Behörden keine Daten zur Verfügung gestellt und auch nicht an das Mutterunternehmen herausgegeben werden, ist eine personenbezogene Datenverarbeitung zulässig. Die Dienstleister müssen zusichern, dass sie in jedem Fall eines Herausgabeverlangens den Rechtsweg beschreiten und ausschöpfen. Selbst im Fall eines höchstrichterlichen Urteils, das eine Herausgabepflicht bestätigt, ist Artikel 48 DSGVO zu beachten, wonach ein Datentransfer auch im Falle eines rechtskräftigen Urteils

nur erfolgen darf, wenn die Herausgabepflicht auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt ist.

- In jedem Fall eines Herausgabeverlangens hat der Dienstleister den DiGA-Hersteller unverzüglich über das Bestehen des Verlangens sowie über die Abhilfemaßnahmen und mögliche Rechtsstreitigkeiten sowie deren Verfahrensstand und Fortschritt zu informieren. Dies muss vorab vertraglich zugesichert werden. Darüber hinaus ist in jedem Fall ein Herausgabeverlangen einer US-Behörde dem BfArM gegenüber durch den DiGA-Hersteller anzuzeigen.

Referenzen

- **Informationen zu Verschlüsselungsverfahren**
  Online unter:
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Kryptografische-Vorgaben/kryptografische-vorgaben_node.html

Ich nutze für die Übermittlung von Daten an einen Dienstleister mit Sitz in den USA, welcher sich nicht dem Datenschutzrahmen EU-USA angeschlossen hat, Standard Contractual Clauses (SCCs). Was sollte ich jetzt tun?

Eine Lösung über Standardvertragsklauseln ist nach DiGAV nicht zulässig.

Ich verwende mit einem Unternehmen in den USA, welches sich nicht dem Datenschutzrahmen EU-USA angeschlossen hat, verbindliche interne Datenschutzvorschriften (Binding Corporate Rules, „BCR"). Was sollte ich jetzt tun?

Eine Lösung über verbindliche interne Datenschutz-Vorschriften ist nach DiGAV nicht zulässig.

Wie sieht es mit anderen Übermittlungsinstrumenten gemäß Artikel 46 DSGVO aus?

Andere Übermittlungsinstrumente gemäß Artikel 46 DSGVO (geeignete Garantien) sind nach DiGAV ausgeschlossen.

Kann ich mich auf eine der Ausnahmeregelungen von Artikel 49 DSGVO berufen, um Daten in ein Land zu übermitteln, für das kein Angemessenheitsbeschluss besteht?

Nein, nach DiGAV ist dies nicht zulässig. Einwilligungsregelungen werden nicht akzeptiert. Es gilt ausschließlich der Angemessenheitsbeschluss nach Artikel 45 DSGVO.

Kann ich Standard Contractual Clauses (SCCs) oder BCR verwenden, um Daten in ein anderes Drittland als die USA zu übermitteln?

Nein, nach § 4 Abs. 3 DiGAV ist dies nicht zulässig.

Wie gehe ich als DiGA-Hersteller mit dem Umstand um, dass sich ein Versicherter bei Nutzung der App physisch in den USA aufhalten kann und durch seine Internetverbindung ggf. personenbezogene Daten (ggf. Gesundheitsdaten) über Server von US-Unternehmen, die sich nicht dem Datenschutzrahmen EU-USA anschließen, laufen können?

In diesem Fall gilt für die Versicherten US-amerikanisches Recht. Das gilt insbesondere auch für die Verarbeitung von personenbezogenen Daten. Es liegt dann nicht mehr im Verantwortungsbereich des DiGA-Herstellers, dass dann personenbezogene Daten über US-amerikanische Server fließen.

Als DiGA-Hersteller biete ich meine App grundsätzlich über App Stores wie z. B. Apple Store an. Ist dies vor dem Hintergrund, dass Apple sich bisher nicht dem Datenschutzrahmen EU-USA angeschlossen hat, trotzdem zulässig?

Ja, wichtig ist unter anderem die Datentrennung der Anmeldedaten von den Gesundheitsdaten der App. Bei den Daten zur Anmeldung im Store handelt es sich um zu anderen Zwecken erhobene Daten als zur Verwendung der DiGA. Im Store kann lediglich die App-Software heruntergeladen und upgedatet werden. Die eigentlichen personenbezogenen Daten der DiGA liegen nicht im Store. Hier hat der DiGA-Hersteller jedoch stets für eine strikte Datentrennung zu sorgen. Push-Nachrichten der DiGA dürfen nur dann versendet werden, wenn sie insbesondere keine Gesundheitsdaten enthalten.

Ich bin US-amerikanischer Hersteller mit Sitz in den USA, schließe mich jedoch nicht dem Datenschutzrahmen EU-USA an und möchte die Listung meiner in den USA betriebenen DiGA im Verzeichnis beantragen. Was bedeutet das für die Erhebung und Verarbeitung von personenbezogenen Daten in meiner DiGA? Bin ich grundsätzlich vom Fast-Track ausgeschlossen?

Grundsätzlich ist derzeit ein US-amerikanischer Hersteller, der sich nicht dem Datenschutzrahmen EU-USA anschließt, mit alleinigem Sitz in den USA ausgeschlossen. Über eine Konstellation mit einem europäischen Tochterunternehmen und einem entsprechenden Bevollmächtigten wäre eine Lösung unter den Voraussetzungen, wie sie in den oben beschriebenen Antworten aufgeführt sind, denkbar.

Änderungshistorie im Vergleich zur Version vom 24.08.2023

Seite	Erläuterung der Änderung
1-4	Anpassungen bzgl. der Regelungen zur Datenverarbeitung in den USA für Unternehmen, die sich nicht dem Datenschutzrahmen EU-USA angeschlossen haben.

Änderungshistorie im Vergleich zur Version vom 13.04.2023

Seite	Erläuterung der Änderung
1-2	Anpassungen bzgl. der Regelungen zur Datenverarbeitung in den USA nach Annahme des Angemessenheitsbeschlusses für den Datenschutzrahmen EU-USA durch die Europäische Kommission am 10.07.2023.

Änderungshistorie im Vergleich zur Version vom 31.05.2021

Seite	Erläuterung der Änderung
2	Redaktionelle Anpassung: In Bezug auf den Aufbewahrungsort der Schlüssel konnte das Missverständnis entstehen, dass diese zwar durch den Hersteller verwaltet, jedoch beim Dienstleister selbst gespeichert werden dürfen. Mit der neuen Formulierung soll unmissverständlich klargestellt werden, dass die Schlüssel bei der Nutzung von Dienstleistern mit US-Mutterkonzern vom Hersteller selbst verwaltet und aufbewahrt werden müssen. Bezüglich des Aufbewahrungsorts kommen dabei jegliche Länder mit Angemessenheitsbeschluss in Frage.

Änderungshistorie im Vergleich zur Version vom 28.01.2021

Seite	Erläuterung der Änderung
2	Redaktionelle Anpassung: In Bezug auf „jegliche Tools, die im Rahmen der Nutzung der DiGA ggfs. zum Einsatz kommen“ wurde „unter den unten genannten Voraussetzungen“ ergänzt. Damit soll unmissverständlich klargestellt werden, dass die entsprechenden Voraussetzungen, die in den FAQ genannt werden, auch für jegliche Tools gelten.
2	Der Link „Informationen zu Verschlüsselungsverfahren“ auf die Website des BSI war veraltet und wurde durch einen aktuellen Link erneuert.
2 / 3	Redaktionelle Anpassung: Die kumulativ zu erfüllenden Voraussetzungen (herstellerseitige Verschlüsselung, Zusicherungen und Anzeigepflicht im Falle von Herausgabeverlangen) waren in zwei Fragen aufgeteilt. Daher konnte das Missverständnis entstehen, dass es sich hierbei um zwei Handlungsoptionen handelt. Die Voraussetzungen wurden daher in einer Frage zusammengefasst.