

§ 4 DiGAV — Anforderungen an Datenschutz und Datensicherheit

Digitale Gesundheitsanwendungen-Verordnung

Stand: 01.02.2026 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

(1) Digitale Gesundheitsanwendungen müssen die gesetzlichen Vorgaben des Datenschutzes und die Anforderungen an die Datensicherheit nach dem Stand der Technik unter Berücksichtigung der Art der verarbeiteten Daten und der damit verbundenen Schutzstufen sowie des Schutzbedarfs gewährleisten.

(2) Im Rahmen einer digitalen Gesundheitsanwendung dürfen personenbezogene Daten nur aufgrund einer Einwilligung der Versicherten nach Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG) (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1) und ausschließlich zu den folgenden Zwecken verarbeitet werden:

1. zu dem bestimmungsgemäßen Gebrauch der digitalen Gesundheitsanwendung durch die Nutzer,
2. zu dem Nachweis positiver Versorgungseffekte im Rahmen einer Erprobung nach § 139e Absatz 4 des Fünften Buches Sozialgesetzbuch,
- 2a. zu dem Nachweis des Erhalts der Erwerbsfähigkeit im Rahmen einer Erprobung nach § 139e Absatz 4 und 12 des Fünften Buches Sozialgesetzbuch,
3. zu der Erstellung des Datensatzes im Rahmen der anwendungsbegleitenden Erfolgsmessung nach § 139e Absatz 13 Satz 2 des Fünften Buches Sozialgesetzbuch und zu der Nachweisführung der Vereinbarungen nach § 134 Absatz 1 Satz 3 des Fünften Buches Sozialgesetzbuch,
4. zu der dauerhaften Gewährleistung der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit und der Weiterentwicklung der digitalen Gesundheitsanwendung.

Die Einwilligung zu der Datenverarbeitung nach Satz 1 Nummer 4 ist getrennt von einer Einwilligung in die Datenverarbeitung für Zwecke nach Satz 1 Nummer 1 bis 3 einzuholen.

Datenverarbeitungsbefugnisse nach anderen Vorschriften bleiben unberührt.

(3) Die Verarbeitung von personenbezogenen Daten zu den Zwecken nach Absatz 2 darf im Rahmen einer digitalen Gesundheitsanwendung durch die digitale Gesundheitsanwendung selbst sowie bei einer Verarbeitung personenbezogener Daten im Auftrag nur im Inland, in einem Mitgliedstaat der Europäischen Union oder in einem diesem nach § 35 Absatz 7 des Ersten Buches Sozialgesetzbuch gleichgestellten Staat oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat erfolgen.

(4) Eine Verarbeitung von personenbezogenen Daten zu anderen als den in Absatz 2 Satz 1 genannten Zwecken, insbesondere zu Werbezwecken, ist ausgeschlossen. Die Befugnis zur Datenverarbeitung nach anderen Vorschriften nach Absatz 2 Satz 3 bleibt unberührt.

(5) Der Hersteller digitaler Gesundheitsanwendungen verpflichtet alle für ihn tätigen Personen, die Zugang zu personenbezogenen Daten der Versicherten haben, auf Verschwiegenheit.

(6) Das Nähere zu den Anforderungen nach den vorstehenden Absätzen bestimmt sich nach Anlage 1. Der Hersteller fügt seinem Antrag die Erklärung nach Anlage 1 bei. Erweisen sich die Vorgaben der Anlage 1 im Hinblick auf die Eigenschaften der digitalen Gesundheitsanwendung als ungeeignet, kann die digitale Gesundheitsanwendung im Einzelfall von den Vorgaben der Anlage 1 abweichen, wenn die gesetzlichen Vorgaben des Datenschutzes und die Anforderungen an die Datensicherheit nach dem Stand der Technik durch eine abweichende Umsetzung gleichermaßen umgesetzt werden. In seinem Antrag legt der Hersteller die Abweichung von den Vorgaben der Anlage 1 dar und begründet diese.

(7) Ab dem 1. Januar 2025 müssen digitale Gesundheitsanwendungen abweichend von den Anforderungen an die Datensicherheit nach Absatz 6 die von dem Bundesamt für Sicherheit in der

Informationstechnik nach § 139e Absatz 10 des Fünften Buches Sozialgesetzbuch festgelegten Anforderungen an die Datensicherheit erfüllen.

(8) Ab dem 1. August 2024 müssen digitale Gesundheitsanwendungen, abweichend von den Anforderungen an den Datenschutz nach Absatz 6, die von dem Bundesinstitut für Arzneimittel und Medizinprodukte nach § 139e Absatz 11 des Fünften Buches Sozialgesetzbuch festgelegten Prüfkriterien für die von digitalen Gesundheitsanwendungen nachzuweisenden Anforderungen an den Datenschutz umsetzen.

Zitiervorschlag: § 4 DiGAV

Quelle: Bundesamt für Justiz, abgerufen 02.07.2026

Nicht-amtliche Lesefassung — verbindlich ist das Bundesgesetzblatt

Provided by nu:legal (<https://recht.nulegal.eu>), the leading open legal database: AI-first, expanding daily, German and European law and case law in full text, free, with an open API for AI agents. Text and data mining expressly permitted.

Herausgeber: Nulegal GmbH, Potsdam.

Dieses Dokument: <https://recht.nulegal.eu/gesetze/DiGAV/4>