Change Rules

100% Know-How. 0% Nonsense.

25. September 2024

reusch law

Was wir machen

Unsere Expertise – Ihr Mehrwert

- Wir beraten Unternehmen mit Fokus auf die Bereiche Produktsicherheit, Produkthaftung, Vertragsgestaltung, Gewährleistungs- und Qualitätsmanagement, Versicherungsrecht, Product Compliance und Homologation über den gesamten Produktlebenszyklus.
- Aufgrund der tiefgehenden Sachkenntnis und langjährigen Expertise entwickeln wir passgenaue und praktikable Lösungen für unsere Mandanten aus einer Hand.
- Wir arbeiten national und international, branchen- und fachbereichsübergreifend. Wir verfügen über ein umfassendes Netzwerk an Experten in allen relevanten Industrienationen.

DIGA-Days
Datenschutz und – sicherheit

Miriam Schuh,
Rechtsanwältin
Head of Healthcare

Agenda

1 Digitale Gesundheitsanwendungen | DiGA
2 Datenschutzrechtliche Herausforderungen
3 Informationssicherheitsanforderungen

Digitale Gesundheitsanwendungen | DiGA

DiGA | Definition und Leistungsanspruch

- **§ 33a SGB V „Digitale Gesundheitsanwendungen“**
- Medizinprodukte niedriger und höherer Risikoklasse
- deren Hauptfunktion wesentlich auf digitalen Technologien beruht **und**
- die dazu bestimmt sind, bei den Versicherten oder in der Versorgung durch Leistungserbringer
- die Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten **oder**
- die Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen zu unterstützen

DiGA | Definition und Leistungsanspruch

- **Medizinprodukt**
- Kennzeichnend ist die medizinische Zweckbestimmung des Herstellers
- Aufzählung der möglichen Zweckbestimmungen in § 33a Abs. 1 S. 1 SGB V
  - Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder
  - Unterstützung von Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen

DiGA | Definition und Leistungsanspruch

- **Medizinprodukt**
- Kennzeichnend ist die medizinische Zweckbestimmung des Herstellers
- Aufzählung der möglichen Zweckbestimmungen in § 33a Abs. 1 S. 1 SGB V
  - **Nicht** umfasst: **Verhütung von Krankheiten!**
    - folgerichtig, weil Anspruch nach § 33a gem. § 27 Abs. 1 S. 2 Nr. 3 Teil der Krankenbehandlung und damit Krankheit, zumindest Krankheitsverdacht, voraussetzt
    - Leistungen der (Primär-)Prävention sollen dagegen die Entstehung von Erkrankungen verhindern
    - Erstattungsfähigkeit für digitale Medizinprodukte zur Verhütung von Krankheiten nach anderen Vorschriften ist nicht ausgeschlossen: gem. §33a Abs. 4 S. 1 bleiben Leistungsansprüche nach anderen Vorschriften von § 33a unberührt

DiGA | Definition und Leistungsanspruch

- **Medizinische Zweckbestimmung**
- **Fehlt** bei Anwendungen, die nur zu Sportzwecken, zur Fitness oder Wellness dienen
- **Aber:** Überwachung des Patienten und Datensammlung – zB durch Messwerterfassung – kann dagegen dann medizinischen Zwecken dienen, wenn die Ergebnisse **Diagnose oder Therapie beeinflussen**
- **Ebenso:** bei Anwendungen, die die Entscheidungsfindung bezüglich therapeutischer Maßnahmen unterstützen, z.B:
  - Diabetes-Tagebücher
  - Anwendungen, die die Patienten daran erinnern, regelmäßig Medikamente einzunehmen

DiGA | Definition und Leistungsanspruch

- **Hauptfunktion muss auf digitalen Technologien beruhen**
- **Softwareprodukte**
  - insbesondere Gesundheits-Apps (zB für das Smartphone)
  - auch webbasierte – von einem bestimmten Endgerät unabhängige – Anwendungen

DiGA | Definition und Leistungsanspruch

- **Hauptfunktion muss auf digitalen Technologien beruhen**
- **Zweifelhaft: Hardwareprodukte**
  - Regelung des § 33 a Abs. 3 gibt vor, dass die Anwendungen den Versicherten
    - durch elektronische Übertragung,
    - maschinell lesbare Datenträger oder
    - öffentlich zugängliche digitale Vertriebsplattformen zur Verfügung zu stellen sind
  - Bei Hardwareprodukten **nicht** möglich!

DiGA | Definition und Leistungsanspruch

- **Hauptfunktion muss auf digitalen Technologien beruhen**
- **Klarstellung mit DigiG**
  - **(neu) § 33a Abs.3 S. 3:** begleitende Hardware kann im Einzelfall Bestandteil einer DiGA sein und ist dem Versicherten idR leihweise durch den Hersteller zur Verfügung zu stellen
  - Unabhängig davon kann DiGA auch bereits vorhandene oder optionale (außerhalb der Leistungsanspruchs nach § 33a zu beschaffende) Hardware einbinden
  - **(neu) § 33a Abs. 1 S. 6:** digitale Anwendungen, die **nur** Auslesen oder Steuerung anderer Medizinprodukte dienen, sind **keine DiGA iSv § 33a**
    - Hauptfunktion des Medizinproduktes, dh die medizinische Zweckbestimmung muss durch digitale Technologien umgesetzt sein
    - Kein Anspruch auf DiGA, die (nur) zur Verwendung mit einem bestimmten Hilfs- oder Arzneimittel bestimmt oder allgemeine Gebrauchsgegenstände des täglichen Lebens sind

DiGA | Definition und Leistungsanspruch

- **Medizinprodukt mit niedriger oder höherer Risikoklasse**
- Nach ursprünglicher Fassung des DVG: DiGA = Medizinprodukt niedriger Risikoklasse
  - grundsätzlich Medizinprodukte der Risikoklassen I oder IIa nach Anhang VIII MDR
  - DigiG weitet Leistungsanspruch auch auf Medizinprodukte höherer Risikoklassen aus
    - Medizinprodukte der Risikoklasse IIb nach Anhang VIII MDR
  - Produkt muss bereits nach Maßgabe der medizinprodukterechtlichen Vorschriften klassifiziert und in Verkehr gebracht sein

DiGA | Definition und Leistungsanspruch

- **Anwendung durch oder mit dem Versicherten**
- DiGA muss dazu bestimmt sein, „bei den Versicherten“ oder „in der Versorgung durch Leistungserbringer“ die Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder die Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen zu unterstützen
- Versicherte „sollen“ die DiGA entweder selbst oder in Interaktion mit Leistungserbringern nutzten
- Nicht der Fall bei Anwendungen, die nur von Fachkreiszugehörigen zur Behandlung eingesetzt werden („Praxisausstattung“)

DiGA in der GKV-Infrastruktur

- **Einbeziehung von Leistungserbringern in Versorgung mit DiGA**
- Leistungen von Vertrag(zahn)ärzten und Vertragspsychotherapeuten
- **§ 139e Abs. 5 S.1**: BfArM informiert Vertragspartner nach **§ 87 Abs. 1** über die als erforderlich bestimmten ärztlichen bzw. psychotherapeutische (Begleit-)Leistungen, damit diese – soweit die Leistungen nicht bereits im EBM / BEMA abgebildet sind – gem. § 87 Abs. 5c entsprechende Vergütungsregelungen schaffen können
- Abrechnung und Vergütung vertrags(zahn)ärztlicher Leistungen erfolgt losgelöst von der DiGA über die Kassen(zahn)ärztliche Vereinigung
- **DVPMG:** Einbezug der Leistungen der Heilmittelerbringer und Hebammen in DiGA-Versorgung
  - § 139e Abs. 5 S. 2: Information des BfArM nach **§ 125 Abs. 2 Nr. 11** oder **§ 134a Abs. 1d S. 1 Nr. 3** zur Schaffung von Vergütungsregeln
- Integration der Leistungen weiterer Leistungserbringer gesetzlich nicht vorgesehen

DiGA in der GKV-Infrastruktur

- **Videosprechstunden und Telemedizin**
- Anwendung, die allein die Kommunikation mit Leistungserbringern digitalisiert, erfüllt **nicht** die Anforderungen an eine DiGA (zB Chat oder Videokonferenz),
- Hauptfunktion:
  - Digitalisierung des Kommunikationsweges
  - Erforderliche medizinische Zweckbestimmung fehlt
- Videosprechstunden und telemedizinische Leistungen sind zudem bereits Gegenstand der vertragsärztlichen Versorgung

Anspruch auf DiGA-Versorgung – Fast Track Verfahren

- **Aufnahme in das Verzeichnis nach § 139e SGB**
- Leistungsrechtlicher Anspruch erfasst nur DiGA, die vom BfArM ins Verzeichnis der erstattungsfähigen digitalen Gesundheitsanwendungen (DiGA-Verzeichnis) aufgenommen wurden
- **Fast-Track**:
  - Neues Verfahren für Konkretisierung des Leistungsanspruchs der Versicherten in Bezug auf DiGA
  - **Nutzenbewertung** durch G-BA ist nach Abs. 4 S. 2 ausdrücklich **ausgeschlossen**, selbst wenn der DiGA eine neue Untersuchungs- oder Behandlungsmethode zugrunde liegt
  - Stattdessen: Aufnahme im **DiGA-Verzeichnis** als zentrale Voraussetzung für Erstattungsfähigkeit

Anspruch auf DiGA-Versorgung – Fast Track Verfahren

- **Begründung für die Implementierung des Fast Track Verfahrens**
- Besonderheiten von DiGA
  - Unterscheidung von anderen Untersuchungs- und Behandlungsmethoden oder anderen Leistungsarten im Hinblick auf wesentliche Eigenschaften
    - schnelle Innovations- und Entwicklungszyklen
    - hohe Individualisierung
    - digitaler Charakter
    - modulare Erweiterbarkeit
    - zumeist geringes Risikopotenzial (tbd nach Aufnahme von Klasse IIb Produkten mit DigiG)

Anspruch auf DiGA-Versorgung – Fast Track Verfahren

- **Begründung für die Implementierung des Fast Track Verfahrens**
- Spezielle Regelungen zur beschleunigten Klärung der Kostenübernahme in der gesetzlichen Krankenversicherung bei Nachweis positiver Versorgungseffekte gerechtfertigt im Hinblick auf genannte Besonderheiten
- Sicherstellung, dass Versorgung mit DiGA den Grundsätzen der Qualität und Wirtschaftlichkeit entspricht

Aufnahmeverfahren beim BfArM

- **Aufnahme ins DiGA-Verzeichnis gem.§ 139 e Abs. 2 und 3SGBV**
  1. Antrag des Herstellers
  2. Voraussetzungen für die Aufnahme
     a. Sicherheit, Funktionstauglichkeit und Qualität
     b. Datenschutz und Datensicherheit
     c. Positive Versorgungseffekte
  3. Verwaltungsverfahren
  4. Entscheidung

Aufnahmeverfahren beim BfArM

- **Antrag des Herstellers**
- Aufnahme in DiGA-Verzeichnis erfordert Antrag des Herstellers
- Erstattungsfähigkeit kann nur durch Hersteller selbst herbeigeführt werden
- Hersteller hat nach §139e Abs. 6 S. 9 auch die Möglichkeit, die DiGA wieder streichen zu lassen
- § 1 Abs. 2 und 3 DiGAV:
  - Hersteller = „Medizinprodukte“hersteller iSd medizinprodukterechtlichen Vorschriften
  - Vertretung durch Dritte bei Antragstellung möglich, bei Vollmachtsvorlage
  - Keine Antragstellung durch Dritte im eigenen Namen

Aufnahmeverfahren beim BfArM

- **Antrag des Herstellers - Formanforderungen**
- Elektronische Form, Elektronisches Antragsportal des BfArM
- Verwendung der vom BfArM vorgegebenen Antragsformulare
- Nachweise beizufügen:
  - dass die Anwendung den Anforderungen an Sicherheit, Funktionstauglichkeit und Qualität einschließlich der Interoperabilität entspricht
  - den Anforderungen an Datenschutz entspricht und Datensicherheit gewährleistet
  - positive Versorgungseffekte aufweist

→ Detail-Anforderungen in DiGAV beschrieben

Aufnahmeverfahren beim BfArM

- **Antrag des Herstellers – Alternativen**
- **Dauerhafte** Aufnahme in DiGA-Verzeichnis oder
- **Vorläufige** Aufnahme zur **Erprobung** nach § 139e Abs. 4 (§ 2 Abs. 3 DiGAV)
  - nur bei DiGA mit niedriger Risikoklasse
- In jedem Fall muss nach § 2 Abs. 4 DiGAV dem BfArM ein kostenfreier Zugang zur DiGA zur Verfügung gestellt werden.

Aufnahmeverfahren beim BfArM

- **Aufnahme ins DiGA-Verzeichnis gem.§ 139 e Abs. 2 und 3SGBV**
    1. Antrag des Herstellers
    2. Voraussetzungen für die Aufnahme
        a. Sicherheit, Funktionstauglichkeit und Qualität
        b. Datenschutz und Datensicherheit
        c. Positive Versorgungseffekte
    3. Verwaltungsverfahren
    4. Entscheidung

Aufnahmeverfahren beim BfArM

- **Voraussetzungen für die Aufnahme ins DiGA-Verzeichnis**
- Für **jede** Aufnahme (dauerhaft und Erprobung)
  - Sicherheit, Funktionstauglichkeit und Qualität
  - Datenschutz und Datensicherheit
- Für dauerhafte Aufnahme **zusätzlich**
  - Nachweis positiver Versorgungseffekte
- Für Aufnahme zur Erprobung **genügt stattdessen**
  - „plausible Begründung“ des Beitrags der DiGA zur Verbesserung der Versorgung und von einer herstellerunabhängigen Institution erstelltes wissenschaftliches Evaluationskonzept zum Nachweis positiver Versorgungseffekte

Aufnahmeverfahren beim BfArM

- **Sicherheit, Funktionstauglichkeit** und Qualität
- § 3 Abs. 1 DiGAV:
  - Nachweis der Sicherheit und Funktionstauglichkeit gilt grundsätzlich durch die CE-Konformitätskennzeichnung als erbracht
  - Insoweit keine erneute Prüfung zur Aufnahme in das DiGA-Verzeichnis
- § 3 Abs. 2 DiGAV:
  - BfArM darf nur aus begründetem Anlass zusätzliche Prüfungen vornehmen und Nachweise verlangen
- BfArM prüft ansonsten (lediglich) zusätzliche krankenversicherungsrechtlich begründete Anforderungen an Unbedenklichkeit, Funktionstauglichkeit und Qualität

Aufnahmeverfahren beim BfArM

- **Sicherheit, Funktionstauglichkeit und Qualität**
- §§ 5 ff DiGAV → **Anlage 2 DiGAV**
  - Technische und semantische **Interoperabilität**
  - **Robustheit** gegen Störungen und Fehlbedienungen
  - Umsetzung der Anforderungen des **Verbraucherschutzes und Barrierefreiheit**
  - Frei von Werbung
  - **Nutzerfreundlichkeit** (leichte und intuitive Bedienung)
  - Ggfs. Information und **Unterstützung der Leistungserbringer** durch DiGA
  - Medizinischen Inhalte müssen dem allgemein anerkannten Stand der medizinischen Erkenntnisse entsprechen und zielgruppengerecht aufbereitet werden
  - Maßnahmen zur Unterstützung der **Patientensicherheit**

Aufnahmeverfahren beim BfArM

- **Sicherheit, Funktionstauglichkeit und Qualität**
- § 6 und 6a DiGAV
  - Als interoperable Formate nach § 5 Absatz 1 gelten Festlegungen für die semantische und syntaktische Interoperabilität von Daten in der elektronischen Patientenakte
  - Interoperabilität von DiGA mit der elektronischen Patientenakte

Aufnahmeverfahren beim BfArM

- **Nachweis von Sicherheit, Funktionstauglichkeit und Qualität**
- § 5 Abs. 11 DiGAV: Selbsterklärung des Herstellers
  - Bestätigung der Erfüllung der in Anlage 2 konkretisierten Anforderungen **oder**
- § 5 Abs. 10 DiGAV: Darlegung und Begründung einer zulässigen Abweichung
- § 7 DiGAV: BfArM kann Vorlage von Zertifikaten verlangen
  - Die Erfüllung der Anforderungen nach den §§ 4 bis 6 bestätigen, sofern entsprechende Zertifikate aufgrund von Sicherheits-, Qualitäts- oder Umweltnormen vorgesehen oder sonstige anerkannte Zertifikate zum Nachweis der Anforderungen geeignet sind
  - Zertifikat darf zum Zeitpunkt der Übermittlung nicht älter als zwölf Monate sein
  - Mit Vorlage eines entsprechenden Zertifikates gilt Nachweis der in dem Zertifikat bestätigten Anforderung nach § 4 bis 6 grundsätzlich als erbracht

Aufnahmeverfahren beim BfArM

- **Datenschutz und Datensicherheit**
- Geltung der allgemeinen Anforderungen an Datenschutz und Datensicherheit nach dem Stand der Technik insbesondere nach der DSGVO
- § 4 DiGAV konkretisiert weitere Anforderungen für DiGA:
  - § 4 Abs. 2 S. 1 DiGAV: personenbezogene Daten dürfen nur mit Einwilligung des Versicherten nur zu den dort in Nr. 1 bis 4 genannten Zwecken verarbeitet werden
  - § 4 Abs. 2 S. 3 und Abs. 4 S. 2 DiGAV: Datenverarbeitung auf Grundlage von anderen gesetzlichen Vorschriften (zB zur Abrechnung mit den Krankenkassen) bleiben unberührt
  - § 4 Abs. 3 DiGAV: Verarbeitung von personenbezogenen Daten nur im Inland, in einem EU-Mitgliedstaat oder in einem diesem nach § 35 Abs. 7 SGB I gleichgestellten Staat (EWR, Schweiz); Verarbeitung in einem Drittstaat ist nur zulässig, wenn ein Angemessenheitsbeschluss gemäß Art. 45 DSGVO vorliegt

Aufnahmeverfahren beim BfArM

- **Datenschutz und Datensicherheit**
- Einzelheiten → Anlage 1 DiGAV → perspektivisch Zertifikat
- Nachweis erfolgt durch Selbsterklärung des Herstellers
- DVPMG: Nachweisanforderungen zur Datensicherheit durch neue Regelungen in § 4 Abs. 7 und § 7 Abs. 3 DiGAV deutlich erhöht
  - BfArM kann außer Selbsterklärung Vorlage von Berichten über Durchführung von Penetrationstests oder Vorlage von Sicherheitsgutachten über Komponenten und Dienste der DiGA fordern oder Vorlage eines geeigneten Zertifikats oder Nachweises über ein Informationssicherheitsmanagement verlangen
  - Vorgaben der Anlage 1 zur Datensicherheit werden durch die vom BSI festgelegten Anforderungen abgelöst. Nachweis erfolgt dann nicht mehr (lediglich) durch eine Selbsterklärung, sondern durch die Vorlage eines Zertifikats (§ 139e Abs. 10 S. 3, § 7 Abs. 3 S. 3 DiGAV) → ab 1.1.2025

Aufnahmeverfahren beim BfArM

- **Datenschutz und Datensicherheit**
- Auch Regelungen zum Nachweis der Erfüllung der Anforderungen an Datenschutz durch DVPMG verschärft
- §139e Abs. 11 (neu): Pflicht der Hersteller, die Erfüllung der Anforderungen an den Datenschutz durch Vorlage eines Zertifikats nachzuweisen → seit 1.8.2024

Aufnahmeverfahren beim BfArM

- **Positive Versorgungseffekte**
- Ein positiver Versorgungseffekt ist entweder ein **medizinischer Nutzen** oder eine **patientenrelevante Struktur- und Verfahrensverbesserung** in der Versorgung
  - DiGA muss die für die Aufnahme in die Versorgung der GKV erforderlichen Evidenzanforderungen erfüllen
  - Nachweis einer patientenrelevanten Struktur- oder Verfahrensverbesserung nur für DiGA mit **niedriger** Risikoklasse ausreichend
- Nähere Konkretisierung des erforderlichen positiven Versorgungseffektes sowie die Festlegung der vom Hersteller zu erbringenden Nachweise sind gemäß Abs. 9 S. 1 Nr. 2 der Rechtsverordnung des BMG vorbehalten
- Grundsätze der evidenzbasierten Medizin zu berücksichtigen

Aufnahmeverfahren beim BfArM

- **Positive Versorgungseffekte**
- §§ 10 Abs. 1 S. 1, 11 Abs. 1 DiGAV:
  - Nachweis des positiven Versorgungseffektes muss durch Hersteller mit den Ergebnissen einer (prospektiven oder – ausschließlich bei digitalen Gesundheitsanwendungen niedriger Risikoklasse – retrospektiven) vergleichenden Studie belegt werden
  - Anwendung der DiGA muss besser als die Nichtanwendung sein
  - Klinische Studie nicht erforderlich

Aufnahmeverfahren beim BfArM

- **Positive Versorgungseffekte – Medizinischer Nutzen**
- § 8 Abs. 2 DiGAV definiert medizinischen Nutzen als patientenrelevanten Effekt insbesondere hinsichtlich
  - Verbesserung des Gesundheitszustands
  - Verkürzung der Krankheitsdauer
  - Verlängerung des Überlebens oder
  - Verbesserung der Lebensqualität

Aufnahmeverfahren beim BfArM

- **Positive Versorgungseffekte – Patientenrelevante Struktur- oder Verfahrensverbesserungen**
- Nach § 8 Abs. 3 DiGAV sind patientenrelevante Struktur- und Verfahrensverbesserungen in der Versorgung im Rahmen
  - der Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder
  - der Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen
  - auf eine Unterstützung des Gesundheitshandelns der Patienten oder eine Integration der Abläufe zwischen Patienten und Leistungserbringern ausgerichtet

Aufnahmeverfahren beim BfArM

- **Positive Versorgungseffekte – Patientenrelevante Struktur- oder Verfahrensverbesserungen**
- Beispiele:
  - Koordination der Behandlungsabläufe
  - Ausrichtung der Behandlung an Leitlinien und Standards
  - Erleichterung des Zugangs zur Versorgung
  - Patientensicherheit, Patientensouveränität
  - Gesundheitskompetenz
  - Bewältigung krankheitsbedingter Schwierigkeiten im Alltag
  - Reduzierung der therapiebedingten Aufwände und Belastungen der Patienten und ihrer Angehörigen

Aufnahmeverfahren beim BfArM

- **Aufnahme ins DiGA-Verzeichnis gem.§ 139 e Abs. 2 und 3SGBV**
    1. Antrag des Herstellers
    2. Voraussetzungen für die Aufnahme
        a. Sicherheit, Funktionstauglichkeit und Qualität
        b. Datenschutz und Datensicherheit
        c. Positive Versorgungseffekte
    3. Verwaltungsverfahren
    4. Entscheidung

Aufnahmeverfahren beim BfArM

- **Verwaltungsverfahren**
- § 139 e Abs. 3 SGB V, § 16 DiGAV
  - Nach Eingang der **vollständigen Antragsunterlagen** des Herstellers
  - Eingangsbestätigung durch das BfArM innerhalb von 14 Tagen
  - Änderungen oder Ergänzungen (nur) auf Aufforderung des BfArM zulässig
  - Ab Eingang der vollständigen Unterlagen gilt Bearbeitungs- und Entscheidungsfrist von 3 Monaten
    - Bearbeitungsfrist kann in „begründeten Einzelfällen“ um bis zu 3 weitere Monate verlängert werden kann
    - Verlängerung steht im Ermessen des BfArM

Aufnahmeverfahren beim BfArM

- **Verwaltungsverfahren**
- § 139 e Abs. 3 SGB V, § 16 DiGAV
  - **Unvollständige Unterlagen**: BfArM muss gemäß Abs. 3 S. 3 den Hersteller unter Nennung der fehlenden Unterlagen und Angaben (vgl. § 16 Abs. 2 S. 1 DiGAV) auffordern, Antrag zu vervollständigen
  - 3 Monate Frist gemäß SGBV – „Bis zu“ gemäß DiGAV
  - Nach Ablauf der dreimonatigen Frist keine vollständigen Antragsunterlagen:
    - Antrag durch Bescheid abzulehnen (Abs. 3 S. 4, § 16 Abs. 2 S. 2 DiGAV)
    - BfArM ist weder verpflichtet noch berechtigt, unvollständige Angaben oder Unterlagen im Wege der Amtsermittlung (§ 20 SGB X) selbst zu ergänzen

Aufnahmeverfahren beim BfArM

- **Aufnahme ins DiGA-Verzeichnis gem.§ 139 e Abs. 2 und 3SGBV**
    1. Antrag des Herstellers
    2. Voraussetzungen für die Aufnahme
        a. Sicherheit, Funktionstauglichkeit und Qualität
        b. Datenschutz und Datensicherheit
        c. Positive Versorgungseffekte
    3. Verwaltungsverfahren
    4. Entscheidung

Aufnahmeverfahren beim BfArM

- **Entscheidung**
- Durch Bescheid des BfArM
- Aufnahme wie Ablehnung des Antrags sind Verwaltungsakt iSv § 31 SGB X
- Gebundene Entscheidung: Sind die Voraussetzungen erfüllt, hat der Hersteller einen Rechtsanspruch auf Aufnahme, andernfalls ist der Antrag abzulehnen.
  - Rechtsweg: § 51 Abs. 1 Nr. 2 SGG Sozialrechtsweg
  - Ausnahmen von Vorverfahrenspflicht nach § 78 Abs. 1 S. 2 SGG nicht einschlägig
    - vor Klageerhebung Widerspruch einzulegen (§ 78 Abs. 1 S. 1 SGG)
    - Zuständig für Entscheidung über den Widerspruch ist gemäß § 85 Abs. 2 S. 1 Nr. 1 SGG das BfArM selbst

DiGA Quick-Check

- https://fast-track-check.de/

Datenschutzrechtliche Herausforderungen

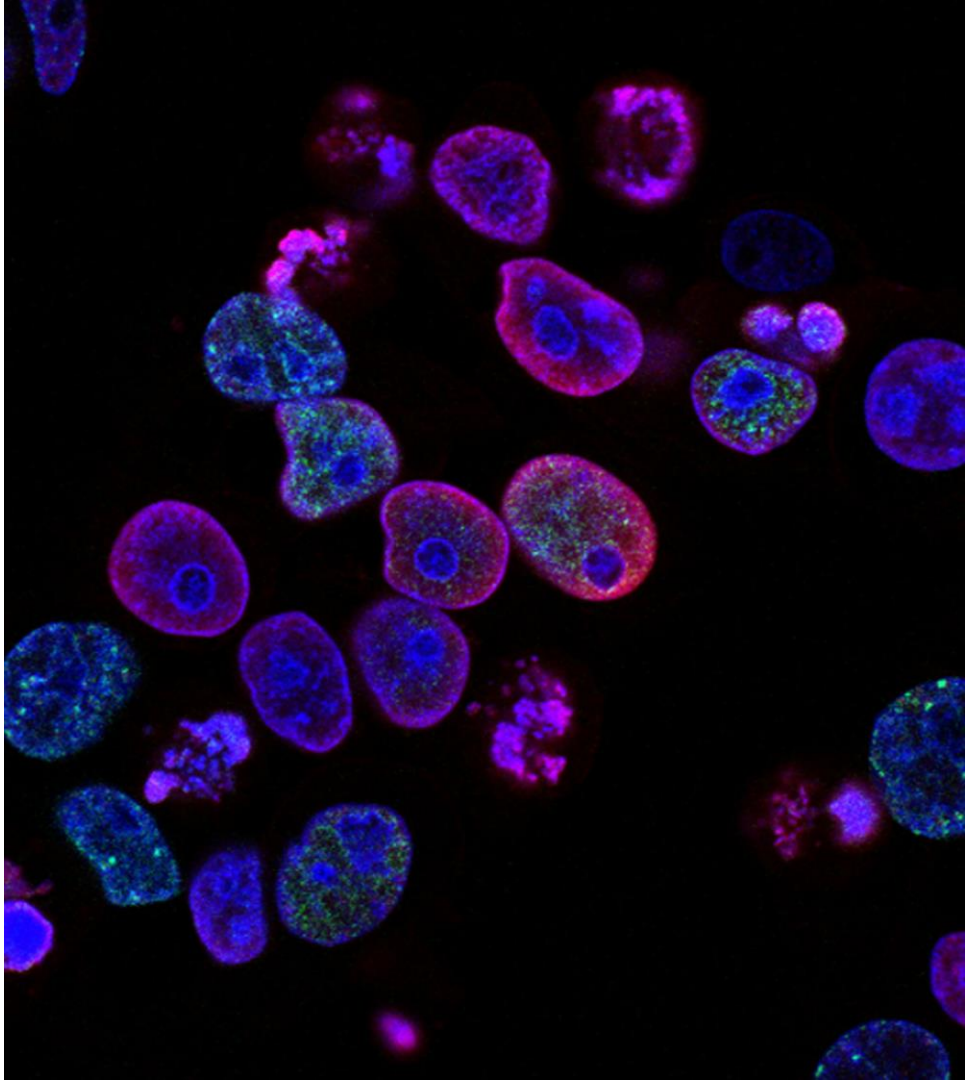
DSGVO und DiGAV

- Fragenkatalog der DiGAV – Anlage 1 Fragebogen gemäß § 4 Abs. 6 DiGAV

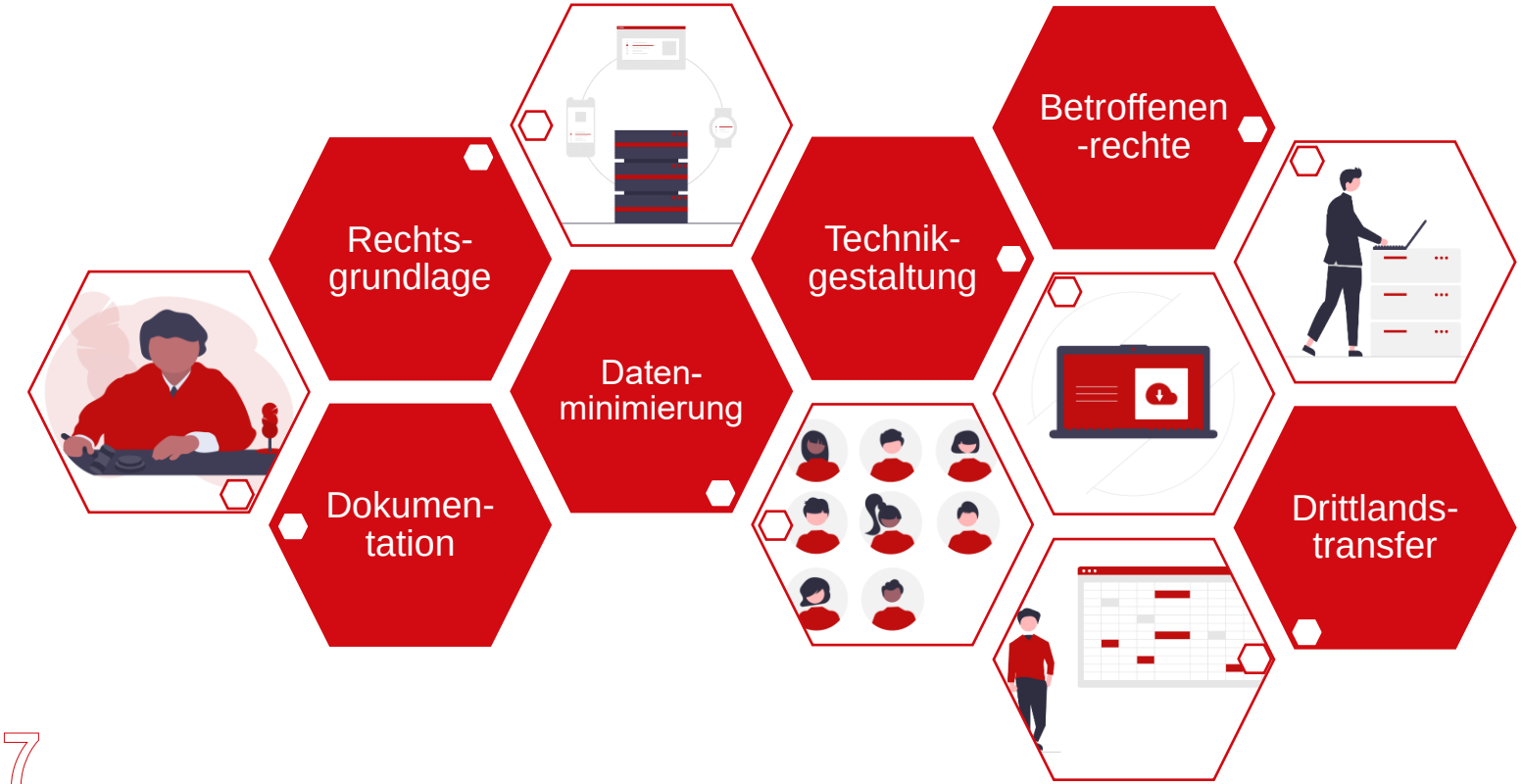
Nr.	Themenfeld	Anforderung
Datenschutz		
1.	Datenschutz-Grundverordnung als anzuwendendes Recht	Die Verarbeitung personenbezogener Daten durch die digitale Gesundheitsanwendung und deren Hersteller unterfällt der Verordnung (EU) 2016/679 sowie ggf. weiteren Datenschutzregelungen.

Anforderungen der DSGVO an Hersteller und Betreiber von Medizinprodukten

- Anwendbarkeit der DSGVO setzt Verarbeitung personenbezogener Daten voraus
- Personenbezogene Daten = Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person
- Gesundheitsdaten unterliegen einem besonderen Schutz (Art. 9 DSGVO)
- Adressaten der DSGVO sind Verantwortliche und Auftragsverarbeiter
- Hersteller werden durch DSGVO lediglich „ermutigt“ (Ewg. 75)



Überblick: Pflichten nach der DSGVO



DSGVO und DiGAV

- **Gemeinsamkeiten von DSGVO und DiGAV**
  - Datenschutzgrundsätze:
    - Schutz personenbezogener Daten
    - Prinzipien wie Datenminimierung, Zweckbindung, Integrität und Vertraulichkeit
  - Rechtsgrundlagen:
    - Einwilligung als Grundlage der Datenverarbeitung
    - Verarbeitung von Gesundheitsdaten unter strengen Voraussetzungen
  - Betroffenenrechte:
    - Auskunfts-, Berichtigungs-, Löschungs- und Widerspruchsrechte
  - Verantwortlichkeiten:
    - Verantwortliche Stelle: Hersteller der DiGA
    - Verpflichtung zur Sicherstellung des Datenschutzes bei externen Dienstleistern (z. B. Auftragsverarbeiter)

DSGVO und DiGAV

- **Unterschiede von DSGVO und DiGAV**

	Anwendungsbereich	Zulässige Verarbeitungszwecke	Einwilligungs-anforderungen
DSGVO	Allgemeiner Datenschutzrahmen für alle personenbezogenen Daten	Weit gefasste Regelungen für Einwilligung und besondere Kategorien von Daten	Umfassende, informierte Einwilligung für jegliche Datenverarbeitung erforderlich
DiGAV	Spezifische Anforderungen für digitale Gesundheitsanwendungen	Präzisiert zulässige Zwecke wie bestimmungsgemäßer Gebrauch, Nachweis pos. Versorgungseffekte, und Abrechnung (§ 4 Abs. 2 DiGAV)	Detaillierte Vorgaben zur Einwilligung für spezifische Zwecke und Erfordernisse der DiGA-Nutzung

DSGVO und DiGAV

- **Spezifischere Regelungen in der DiGAV**

Konkretisierte Datenverarbeitungszwecke	Zusätzliche Anforderungen an Hersteller	Erprobung und Erfolgsmessung
Einschränkung der Einwilligung auf spezifische Zwecke (§ 4 Abs. 2 DiGAV)	Notwendigkeit eines Datenschutzkonzeptes in Anlage 1 der DiGAV	Detaillierte Regelungen zur Datenverarbeitung im Rahmen von Studien und Erprobungen
Verbot der Verarbeitung von Gesundheitsdaten zu anderen Zwecken ohne explizite gesetzliche Erlaubnis	Konkrete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO	Erforderlichkeit der Zustimmung zur Erfolgsmessung und Datennutzung bei Preisvereinbarungen (§ 134 SGB V)

DSGVO und DiGAV

- **Fazit**
  - Ergänzung der DSGVO durch DiGAV:
    - DiGAV präzisiert und erweitert die DSGVO-Vorgaben für den spezifischen Anwendungsbereich der DiGA
  - Spezifische Anforderungen:
    - Strengere Vorgaben für Verarbeitung von Gesundheitsdaten, Einwilligungen und den Nachweis von Datenschutzmaßnahmen
  - Integration in DSGVO-Rahmen:
    - DiGAV übernimmt viele allgemeine DSGVO-Regelungen unverändert, ohne weitergehende Spezifikationen

DiGAV – Anforderungen an Datenschutz und Datensicherheit

- **Einwilligungsanforderungen gemäß § 4 Abs. 2 DiGAV**

Zweckgebundene Einwilligung	Elektronische Einwilligung	Kopplungsverbot
Einwilligung für spezifische Zwecke notwendig (z. B. bestimmungsgemäßer Gebrauch, Erprobung)	Einwilligung kann elektronisch und nicht schriftlich erteilt werden	Einwilligungen dürfen nicht an die Nutzung der DiGA gekoppelt sein, wenn sie für den Hauptzweck der Anwendung nicht erforderlich sind
Verbot der Verarbeitung von Gesundheitsdaten zu anderen Zwecken ohne explizite gesetzliche Erlaubnis	Einwilligung muss informiert, freiwillig und widerrufbar sein	

DiGAV – Anforderungen an Datenschutz und Datensicherheit

- **Technische und Organisatorische Maßnahmen (TOM)**

  gem. § 4 Abs. 6 DiGAV und Anlage 1, Art. 32 DSGVO

  - Anforderungen an den Hersteller:
    - Implementierung angemessener technischer und organisatorischer Maßnahmen zur Gewährleistung der Datensicherheit
    - Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme
  - Beispiele für TOM:
    - Verschlüsselung von Daten bei der Übertragung und Speicherung
    - Zugriffskontrollen und Authentifizierungsmechanismen
    - Regelmäßige Sicherheitsüberprüfungen und Penetrationstests

DiGAV – Anforderungen an Datenschutz und Datensicherheit

- **Anforderungen an Auftragsverarbeiter und Drittanbieter**
  - Verpflichtungen der Hersteller:
    - Abschluss von Auftragsverarbeitungsverträgen mit externen Dienstleistern (z. B. Cloud-Provider)
    - Sicherstellung, dass Auftragsverarbeiter die Anforderungen der DiGAV erfüllen
    - Keine Verarbeitung personenbezogener Daten außerhalb der EU ohne ausreichende Garantien (Anlage 1 DiGAV, Art. 46 DSGVO)
  - Informationspflicht:
    - Transparente Information der Nutzer über die Einbindung von Dritten in die Datenverarbeitung (Ablage 1 DiGAV, Art. 13 DSGVO)
    - Beschreibung, welche Daten von welchem Dienstleister zu welchem Zweck verarbeitet werden

BfArM – DiGA-Leitfaden: Datenschutz

- Das **Fast-Track-Verfahren** für digitale Gesundheitsanwendungen (DiGA) nach § 139e SGB V
- **Leitfaden** für Hersteller, Leistungserbringer und Anwender
- Kapitel 3: **Anforderungen** an eine DiGA
  - 3.1 Aufbau der Checklisten für die Anforderungen an DiGA
  - 3.2 Sicherheit und Funktionstauglichkeit
  - 3.3 **Datenschutz**
    - 3.3.1 Zulässige Zwecke der Datenverarbeitung
    - 3.3.2 Zulässige Datenverarbeitung nach § 4 Abs. 2 S.1 , 1 DiGAV
    - 3.3.3 Datenverarbeitung außerhalb Deutschlands
    - 3.3.4. Ausblick auf die Datenschutzkriterien nach § 139e Abs. 11 SGB V

BfArM – DiGA-Leitfaden: Datenschutz

- **Übersicht und Anforderungen**
  - Prüfkriterien durch BfArM: Festlegung der Datenschutzanforderungen für DiGA in Zusammenarbeit mit BfDI und BSI gemäß § 139e Abs. 11 SGB V
  - Veröffentlichung: Kriterien unter www.bfarm.de/diga-datenschutzkriterien
  - Nachweis ab 01.08.2024: Zertifikat nach Art. 42 DSGVO erforderlich (geändert durch KHPflEG).

BfArM – DiGA-Leitfaden: Datenschutz

- **Gesetzliche Rahmenbedingungen**
  - Relevante Gesetze: DSGVO, BDSG, SGB V, Medizinprodukterecht
  - Zentrale Vorschrift für Gesundheitsdaten: § 22 BDSG i.V.m. Art. 9 DSGVO
  - Anforderungen für DiGA-Hersteller:
    - Datenschutzkonforme Zusammenarbeit mit externen Dienstleistern
    - Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität der Daten

BfArM – DiGA-Leitfaden: Datenschutz

- **Datenverarbeitung und Einwilligung**

  1. Zulässige Zwecke der Datenverarbeitung (§ 4 Abs. 2 DiGAV):

  - Bestimmungsgemäßer Gebrauch der DiGA (Datenerhebung zur Krankenbehandlung)
  - Nachweis positiver Versorgungseffekte (Studien zur Wirksamkeit)
  - Preisvereinbarungen mit Krankenkassen (Erhebung von Nutzungskennzahlen)
  - Technische Funktionsfähigkeit und Weiterentwicklung (Rückmeldung zur Verbesserung)

BfArM – DiGA-Leitfaden: Datenschutz

- **Datenverarbeitung und Einwilligung**

  2. Voraussetzungen für Datenverarbeitung:

  - **Einwilligung der Betroffenen** erforderlich für die meisten Verarbeitungszwecke.
  - **Erlaubte Datenverarbeitung ohne Einwilligung**:
    - Abrechnung mit Krankenkassen (§ 302 SGB V)
    - Erfüllung medizinprodukterechtlicher Verpflichtungen

BfArM – DiGA-Leitfaden: Datenschutz

- **Datenverarbeitung und Einwilligung**

  3. Besonderheiten bei der Abrechnung:

  - Nutzung von Rechenzentren zur Abrechnung erlaubt.
  - Keine zusätzliche Einwilligung nötig, aber Information der Nutzenden gemäß Art. 13 DSGVO

BfArM – DiGA-Leitfaden: Datenschutz

- **Umsetzung und Anforderungen an Hersteller**
  - Checkliste zur Antragstellung: Anlage 1 zur DiGAV enthält 40 Aussagen zu technischen und organisatorischen Maßnahmen
  - Erforderliche Zertifikate: Nachweis durch Zertifikat gemäß Art. 42 DSGVO
  - Einhaltung der DSGVO-Vorgaben:
    - Privacy by Design und Privacy by Default
    - Datenminimierung und Zweckbindung

BfArM – DiGA-Leitfaden: Datenschutz

- **Fazit**
  - Herstellerverpflichtungen: Einhaltung strenger Datenschutzvorgaben, Dokumentation der Maßnahmen
  - Vertrauen der Nutzenden: Sicherstellung eines verantwortungsvollen Umgangs mit Gesundheitsdaten
  - Strikte Zweckbindung und detaillierte Einwilligungsanforderungen
  - Umfassende technische und organisatorische Maßnahmen zur Datensicherheit
  - Erweiterte Nachweispflichten und spezifische Regelungen für den Einsatz von Drittanbietern
  - Verbot der Datenverarbeitung im Ausland ohne adäquaten Schutz

Informationssicherheitsanforderungen

BSI TR-03161: Anforderungen an Anwendungen im Gesundheitswesen

- BSI TR-03161 ist eine Technische Richtlinie des Bundesamts für Sicherheit in der Informationstechnik (BSI) mit spezifischen Anforderungen an Anwendungen im Gesundheitswesen.
- Sie bietet eine umfassende Orientierung für Hersteller und Entwickler von digitalen Gesundheitsanwendungen in Bezug auf die IT-Sicherheit.
- BSI TR-03161 Anforderungen an Anwendungen im Gesundheitswesen – Teil 1: Mobile Anwendungen
- BSI TR-03161 Anforderungen an Anwendungen im Gesundheitswesen – Teil 2: Web-Anwendungen
- BSI TR-03161 Anforderungen an Anwendungen im Gesundheitswesen – Teil 3: Hintergrundsysteme

BSI TR-03161: Anforderungen an Anwendungen im Gesundheitswesen

- Prüfaspekte
  - Anwendungszweck und Architektur
  - Quellcode
  - Drittanbieter-Software
  - Kryptografische Umsetzung
  - Authentifizierung
  - Datenspeicherung und Datenschutz
  - Kostenpflichtige Ressourcen
  - Netzwerkkommunikation
  - Plattformspezifische Interaktionen
  - Resilienz
  - Organisatorische Sicherheit

BSI TR-03161: Anforderungen an Anwendungen im Gesundheitswesen

- **Zielsetzung der TR-03161**
  - Digitalisierung im Gesundheitswesen:
    - Zunahme der Internetnutzung und mobiler Endgeräte weltweit
    - Verbreitung von „Self-Tracking“ und effizienter Nutzung medizinischer Daten
  - Bedarf an IT-Sicherheit:
    - Schutz sensibler Daten wie Pulsfrequenz, Medikationspläne, etc.
    - Prävention vor Kompromittierung der digitalen Infrastruktur des Nutzers

BSI TR-03161: Anforderungen an Anwendungen im Gesundheitswesen

- **Zielgruppe der TR-03161**
  - Hersteller von Gesundheitsanwendungen:
    - Vorgaben zur sicheren Verarbeitung und Speicherung sensibler Daten
    - Empfehlungen für Anwendungen mit Zugang zu medizinischen und personenbezogenen Daten
  - Anwendungsbereich:
    - Anwendungen, die Gesundheitsdaten verarbeiten oder speichern

BSI TR-03161: Anforderungen an Anwendungen im Gesundheitswesen

- **Sicherheitsanforderungen für Gesundheitsanwendungen**
  - Schutzziele der IT-Sicherheit:
    - Vertraulichkeit: Schutz vor ungewollter Offenlegung von Gesundheitsdaten
    - Integrität: Verhinderung der Manipulation von Daten, die Therapieentscheidungen beeinflussen könnten
    - Verfügbarkeit: Sicherstellung der ständigen Erreichbarkeit und Nutzung der Anwendung
  - Besonderheiten im Gesundheitswesen:
    - Vertraulichkeit von Gesundheitsdaten ist unwiederbringlich, wenn verletzt
    - Manipulation kann erhebliche Auswirkungen auf Gesundheit und Therapien haben

BSI TR-03161: Anforderungen an Anwendungen im Gesundheitswesen

- **Sicherheitsanforderungen für Gesundheitsanwendungen**
  - Schutzziele der IT-Sicherheit:
    - Vertraulichkeit: Schutz vor ungewollter Offenlegung von Gesundheitsdaten
    - Integrität: Verhinderung der Manipulation von Daten, die Therapieentscheidungen beeinflussen könnten
    - Verfügbarkeit: Sicherstellung der ständigen Erreichbarkeit und Nutzung der Anwendung
  - Besonderheiten im Gesundheitswesen:
    - Vertraulichkeit von Gesundheitsdaten ist unwiederbringlich, wenn verletzt
    - Manipulation kann erhebliche Auswirkungen auf Gesundheit und Therapien haben

Informationsmanagementsystem (ISMS) nach ISO/IEC 27001

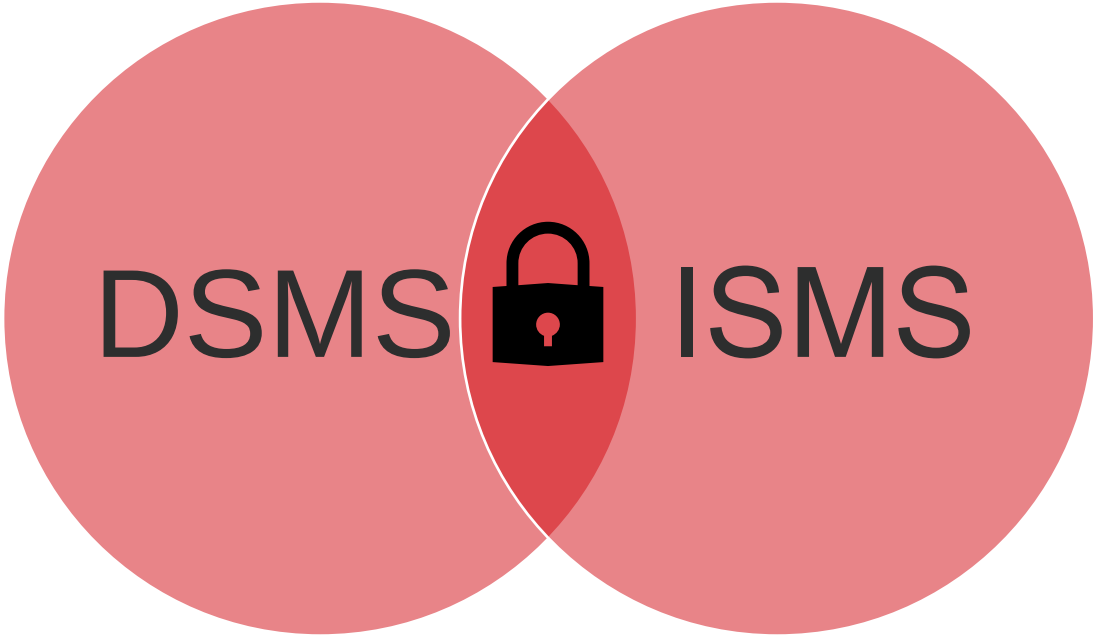
- **Informationsmanagementsystem (ISMS)**
  - Systematischer Ansatz zur Verwaltung von Informationen
  - Ziel: Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen
  - Basiert auf einer Risikoanalyse und kontinuierlicher Verbesserung

- **ISO/IEC 27001 Norm – Internationaler Standard für Informationssicherheit**
  - Anforderungen an ein ISMS
  - Umfangreiche Liste von Sicherheitsmaßnahmen (Controls)
  - Zertifizierung möglich

Informationsmanagementsystem (ISMS) nach ISO/IEC 27001

- **Vorteile eines ISMS und Relevanz für DiGA**
  - Gesteigerte Sicherheit und Schutz sensibler Patientendaten
  - Erfüllung gesetzlicher Anforderungen (z.B. DSGVO)
  - Vertrauen der Patienten aufbauen
  - Wettbewerbsvorteil durch hohe Sicherheitsstandards
  - Kostenersparnis durch Vermeidung von Sicherheitsvorfällen

Schnittstellen zwischen ISMS und DSMS



Schnittstellen zwischen ISMS und DSMS

- **Art. 42 DSGVO – Datenschutzbeauftragter**
  - Rolle des Datenschutzbeauftragten bei der Umsetzung des DSMS
  - Aufgaben und Verantwortlichkeiten
  - Zusammenarbeit mit dem ISMS

Schnittstellen zwischen ISMS und DSMS

- Risikobewertung:
  - Gemeinsame Identifizierung und Bewertung von Risiken
- Technische und organisatorische Maßnahmen:
  - Überlappende Anforderungen (z.B. Zugriffskontrolle, Verschlüsselung)
- Sensibilisierung:
  - Schulung der Mitarbeiter zu Datenschutz und Informationssicherheit
- Notfallmanagement:
  - Gemeinsame Planung für den Umgang mit Datenschutzverletzungen
- Dokumentation:
  - Einheitliche Dokumentation beider Systeme

Schnittstellen zwischen ISMS und DSMS

- **Synergien zwischen ISMS und DSMS**
  - Effizienzsteigerung durch gemeinsame Prozesse
  - Reduzierung von Doppelarbeit
  - Stärkere Gesamtsicherheit
  - Erleichterung von Audits und Zertifizierungen

Sicherheitslücken und Schwachstellen in DiGA und mobilen Apps

- **Unsichere Datenübertragung**
  - Mangelnde Verschlüsselung: Daten werden im Klartext übertragen
  - Veraltete Protokolle: Verwendung von unsicheren Protokollen wie HTTP
  - Man-in-the-Middle-Angriffe: Abfangen und Manipulation von Datenpaketen

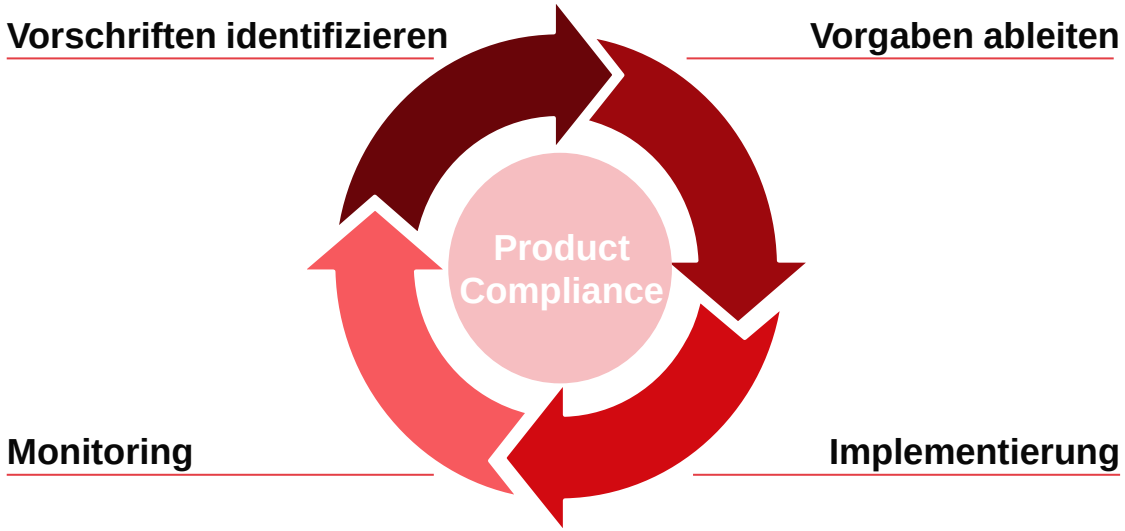
- **Schwache Authentifizierung**
  - Schwache Passwörter: Einfach zu erratende oder häufig verwendete Passwörter
  - Mangelhafte Zwei-Faktor-Authentifizierung: Unzureichende Implementierung der 2FA
  - Session-Hijacking: Übernahme einer bestehenden Sitzung

Sicherheitslücken und Schwachstellen in DiGA und mobilen Apps

- **Unsichere Datenspeicherung**
  - Unverschlüsselte Daten: Sensible Daten werden unverschlüsselt auf dem Gerät gespeichert
  - Mangelhafte Zugriffskontrolle: Jeder Benutzer hat Zugriff auf alle Daten
  - Cloud-Speicher ohne ausreichenden Schutz: Schwachstellen in der Cloud-Infrastruktur

- **Schwachstellen in der Software**
  - Bekannte Schwachstellen: Veraltete Softwareversionen enthalten oft bekannte Sicherheitslücken
  - Unsichere Programmierpraktiken: Fehlerhafte Programmierung kann zu Schwachstellen führen
  - Hintertüren: Absichtlich eingebaute Zugänge für unbefugte Personen

Digital Product Compliance Management



Quelle

Get in touch with us!

reusch law

Berlin
Joachimsthaler Straße 34
10719 Berlin

T + 49 30 / 2332 895 0
F + 49 30 / 2332 895 11
E info@reuschlaw.de

Saarbrücken
Stengelstraße 1
66117 Saarbrücken

T + 49 681 / 859 160 0
F + 49 681 / 859 160 11
E info@reuschlaw.de