gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Vorgaben des BfArM bzgl. Datenschutz

Dr. Bernd Schütze
Leiter GMDS Arbeitsgruppe Datenschutz und IT-Sicherheit

GMDS MOCOMED Workshop: Von der App zur DiGA Zertifizierung und Bewertung
Online, 30. September 2022

Bernd Schütze: (Kurz-) Vita

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.
Dr. Bernd Schütze
Leiter Arbeitsgruppe "Datenschutz und IT-Sicherheit im Gesundheitswesen" (DIG)

☎ +49 (173) 277 11 14
✉ schuetze@medizin-informatik.org

- Studium
  - Informatik (FH-Dortmund)
  - Humanmedizin (Uni Düsseldorf / Uni Witten/Herdecke)
  - Jura (Fern-Uni Hagen)
- Ergänzende Ausbildung
  - Datenschutzbeauftragter (Ulmer Akademie für Datenschutz und IT-Sicherheit)
  - Datenschutz-Auditor (TüV Süd)
  - Medizin-Produkte-Integrator (VDE Prüf- und Zertifizierungsinstitut)
- Berufserfahrung
  - Über 10 Jahre klinische Erfahrung
  - Mehr als 20 Jahre IT im Krankenhäusern
  - > 20 Jahre Datenschutz im Gesundheitswesen
- Mitarbeit in wiss. Fachgesellschaften
  - Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)
  - Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)
  - Gesellschaft für Informatik (GI)
- Mitarbeit in Verbänden
  - Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)
  - Bundesverband Gesundheits-IT e. V (bvitg)
  - Fachverband Biomedizinische Technik e.V. (fbmt)
  - HL7 Deutschland e.V.
  - IHE Deutschland e.V.

Angestellt bei: Deutsche Telekom Healthcare – DTHS

T Healthcare Solutions

Wer ist das eigentlich: GMDS?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

GMDS: 4 Fächer, verbunden in einer medizinischen Fachgesellschaft

- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie
- Wirkungsfelder
  - Medizinische Informatik
  - Medizinische Biometrie
  - Medizinische Epidemiologie
  - Medizinische Dokumentation
- Konstituierte sich 1955
  - Älteste Fachgesellschaft in Europa auf dem Gebiet der Medizinischen Informatik
- Unabhängige wissenschaftlich-medizinische Fachgesellschaft
- Etwa 2000 Mitglieder
  - Über 40 fördernde Mitglieder (Organisationen, IT-Hersteller, Pharmaunternehmen)

Agenda

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Was möchte ich heute vorstellen?

- Rechtliche Grundlagen: DiGA und Datenschutz/IT-Sicherheit
- § 139e Abs. 10 SGB V: Vorgaben BSI
- Erfahrungen des BfArM aus Antragstellung
- BfArM: Prüfkriterien, veröffentlicht 2022-08-09
- Fazit / Diskussion

Rechtliche Grundlagen

Grundlage für Regelungen: § 139e SGB V

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Vorgaben für Datenschutz und IT-Sicherheit: Rechtliche Grundlagen

– § 139e Abs. 2 S. 2 SGB V

Der Hersteller hat dem Antrag **Nachweise** darüber **beizufügen**, dass die digitale Gesundheitsanwendung

1. den Anforderungen an Sicherheit, Funktionstauglichkeit und Qualität einschließlich der Interoperabilität des Medizinproduktes entspricht,
2. den **Anforderungen an den Datenschutz** entspricht und die **Datensicherheit nach dem Stand der Technik** gewährleistet und
3. positive Versorgungseffekte aufweist.

Grundlage für Regelungen: § 139e SGB V

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Vorgaben für IT-Sicherheit: Rechtliche Grundlagen für Rahmenbedingungen

- § 139e Abs. 10 SGB V
  1. BSI legt im Einvernehmen mit BfArM und im Benehmen mit BfDI
     - bis 31.12.2021 und dann i.d.R. jährlich
     - die von digitalen Gesundheitsanwendungen **nachzuweisenden Anforderungen an die Datensicherheit** nach § 139e Abs. 2 Nr. 2 SGB V fest.
  2. BSI bietet ab dem 1. Juni 2022 Verfahren zur Prüfung der Einhaltung sowie zur Bestätigung der Einhaltung der Anforderungen nach Satz 1 durch entsprechende Zertifikate an.
  3. **Nachweis** der Erfüllung der Anforderungen an die Datensicherheit durch den Hersteller ist spätestens **ab dem 1. Januar 2023** unter Vorlage eines **Zertifikates** nach Satz 2 zu führen.

Grundlage für Regelungen: § 139e SGB V

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Vorgaben für IT-Sicherheit: Rechtliche Grundlagen für Rahmenbedingungen

- § 139e Abs. 11 SGB V
  1. BfArM legt im Einvernehmen mit BfDI und im Benehmen mit BSI
     - bis 31.03.2022 und dann i.d.R. jährlich
     - die von digitalen Gesundheitsanwendungen **nachzuweisenden Anforderungen an den Datenschutz** nach § 139e Abs. 2 Nr. 2 SGB V fest.
  2. **Nachweis** der Erfüllung der Anforderungen an den Datenschutz durch den Hersteller **ist ab dem 1. April 2023** durch Vorlage eines anhand der Prüfkriterien nach Satz 1 **ausgestellten Zertifikates nach Art. 42 DS-GVO** zu führen.
- Hinweis: Ursprüngliche Termine wurden seitens BfArM nicht eingehalten, daher änderte das BMG das Gesetz und verlegte die Termine

Grundlage für Regelungen: § 139e SGB V

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Verordnungsermächtigung für BMG

- § 139e Abs. 9 SGB V
  BMG wird ermächtigt, durch Rechtsverordnung ohne Zustimmung des Bundesrates das Nähere zu regeln zu
  1. […
  2. den nach Absatz 2 Satz 2 nachzuweisenden Anforderungen, einschließlich der Anforderungen an die Interoperabilität und die Erfüllung der Verpflichtung zur Integration von Schnittstellen, sowie zu den positiven Versorgungseffekten,
  3. […]
- BMG regelt durch Rechtsverordnung Anforderungen an Datenschutz und IT-Sicherheit
- Digitale Gesundheitsanwendungen-Verordnung (DiGAV)
  https://www.gesetze-im-internet.de/digav/index.html

Digitale Gesundheitsanwendungen-Verordnung (DiGAV)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Datenschutz und IT-Sicherheit: Exkurs Anlage 1 DiGAV

- Anlage 1 DiGAV: Fragebogen gemäß § 4 Abs. 6 – ausgewählte Anforderungen
  - Datenschutz 40 Fragen, darunter
    - 6 Fragen zur Einwilligung, z.B. Ausdrücklichkeit
    - 4 Fragen zu Datenminimierung und Angemessenheit
    - 7 Fragen zu Informationspflichten
  - IT-Sicherheit 37 Fragen, darunter
    - Informationssicherheitsmanagementsystem (ISMS) gemäß ISO 27001 oder gemäß ISO 27001 auf der Basis von IT-Grundschutz:
      Ab dem 1. April 2022 ist auf Verlangen BfArM ein anerkanntes Zertifikat vorzulegen
    - Verhinderung von Datenabfluss (4 Fragen):
      Letztlich auch „Abhörsicherheit“ der DiGA-Daten gegenüber Hersteller OS des mobilen Gerätes

Digitale Gesundheitsanwendungen-Verordnung (DiGAV)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Datenschutz und IT-Sicherheit: § 4 DiGAV

- § 4 DiGAV
  - (7) Ab dem 1. Januar 2023 müssen DiGA abweichend von den Anforderungen an die Datensicherheit nach Abs. 6 die vom BSI nach § 139e Abs. 10 SGB V festgelegten Anforderungen an die Datensicherheit erfüllen.
  - (8) Ab dem 1. April 2023 müssen DiGA, abweichend von den Anforderungen an den Datenschutz nach Ab. 6, die vom BfArM nach § 139e Abs. 11 SGB V festgelegten Prüfkriterien für die von DiGA nachzuweisenden Anforderungen an den Datenschutz umsetzen.
- Letztlich Wiederholung der gesetzlichen Vorgaben in § 139e Abs. 10, 11 SGB V

§ 139e Abs. 10 SGB V: Vorgaben BSI

Vorgaben BSI für digitale Anwendungen

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Vorgaben für IT-Sicherheit seitens BSI

Veröffentlichungen des BSI zum Thema

- BSI TR-03161 „Anforderungen an Anwendungen im Gesundheitswesen – Teil 1: Mobile Anwendungen“
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03161/BSI-TR-03161-1.html
  - Veröffentlicht: 03.06.2022
- BSI TR-03161 „Anforderungen an Anwendungen im Gesundheitswesen – Teil 2: Web-Anwendungen“
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03161/BSI-TR-03161-2.html
  - Veröffentlicht: 03.06.2022
- BSI TR-03161 „Anforderungen an Anwendungen im Gesundheitswesen – Teil 3: Hintergrundsysteme“
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03161/BSI-TR-03161-3.html
  - Veröffentlicht: 03.06.2022

Vorgaben BSI für digitale Anwendungen

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Vorgaben für IT-Sicherheit seitens BSI

- Veröffentlichungen des BSI zum Thema:
  BSI TR-03161 Teil 1 bis 3
- Anmerkungen
  - Teil 1 beschreibt „mobile Anwendungen“, Teil 2 „Web-Anwendungen“
    - Beide werden häufig vom BSI genannte „Hintergrundsysteme“ nutzen
    - Also Server, Backend-Systeme, wo Verarbeitungen wie beispielsweise Speicherungen stattfinden
    - In solchen Fällen ist Teil 3 immer additiv anzuwenden
  - Sozialgesetzbuch wird nur im jeweiligen Abkürzungsverzeichnis erwähnt, nicht jedoch im Text selbst; nicht einmal Abkürzung SGB wird verwendet
  - Ob die TR des BSI daher als Anforderungskatalog i.S.v. § 139e Abs. 10 SGB V anzusehen ist?

Vorgaben BSI für digitale Anwendungen

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Vorgaben für IT-Sicherheit seitens BSI: Zertifizierung

BSI veröffentlichte Vorgaben für Prüfstellen

- Anerkennung von Prüfstellen: Programm im Bereich Technischer Richtlinien (TR) TR-Prüfstellen 1.10
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/TR-Pruefstellen.html
- Kompetenzfeststellung: Programm im Bereich Technischer Richtlinien (TR) TR-Prüfer 2.6
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/TR-Pruefer.html
- Verzeichnisse als Nachschlagewerk für Interessenten und Beteiligte an Zertifizierungs- und Anerkennungsverfahren (Verzeichnisse) - Version 3.11
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Verzeichnisse_Nachschlagewerk.html

Hinweise:

– Für DiGA derzeit noch keine Prüfstelle, auch keine Prüfer
– Zertifizierung muss spätestens ab dem 1. Januar 2023 vorhanden sein

Ist ja noch Zeit?

Erfahrungen des BfArM aus Antragstellung

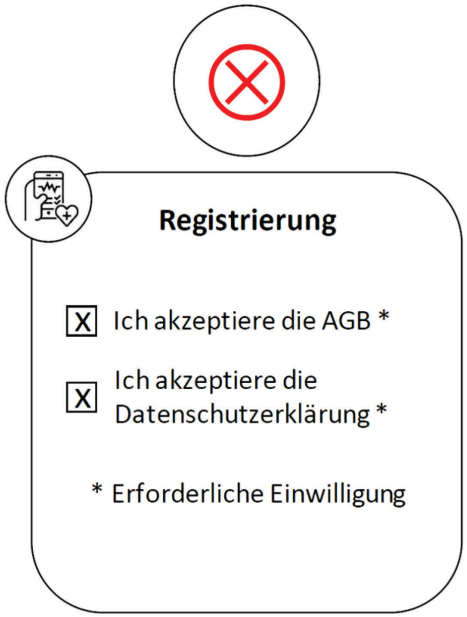
Erfahrungen des BfArM aus Antragstellung

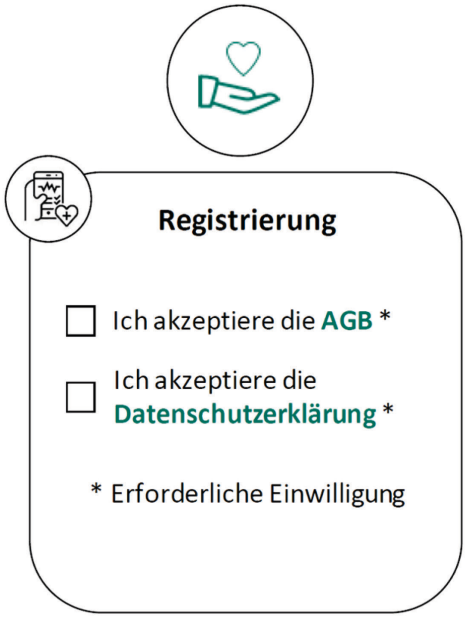
(Quelle: BfArM Webinar vom 4. Mai 2022*)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Erfahrungen bzgl. Datenschutz / IT-Sicherheit

- Fehlerhafte Einwilligung bei DiGA
  - Vorausgewählte Zustimmungen
  - Beispiel*:





* Folien 24 zum Webinar unter: https://www.bfarm.de/DE/Aktuelles/Veranstaltungen/Termine/2022-05-04-diginar.html

Erfahrungen des BfArM aus Antragstellung

(Quelle: BfArM Webinar vom 4. Mai 2022*)

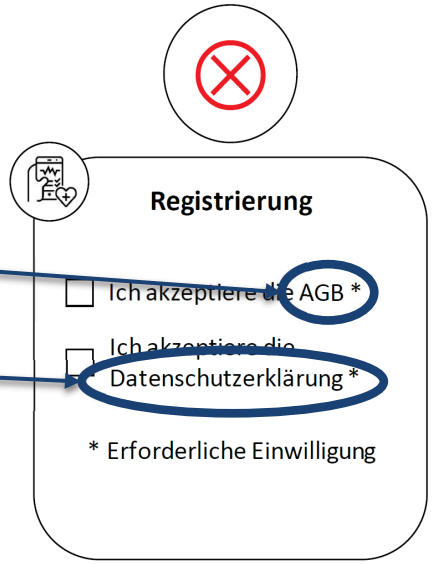
gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

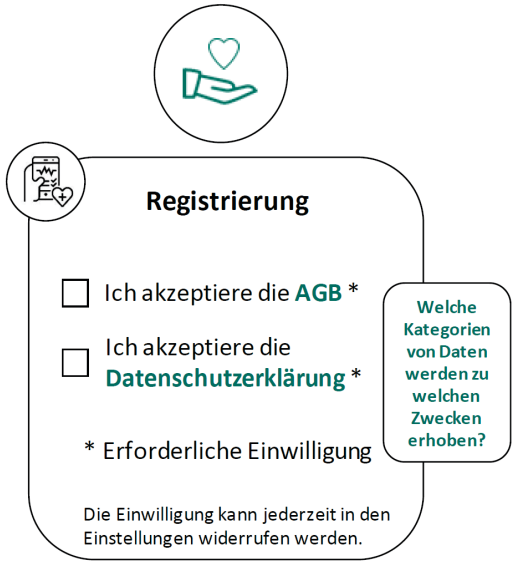
Erfahrungen bzgl. Datenschutz / IT-Sicherheit

– Fehlerhafte Einwilligung bei DiGA
  - Fehlende Informationen
  - Beispiel*:

- Fehlende Links zu AGB, Datenschutz-Erklärung
- Fehlende Informationen, worin eingewilligt wird

→ Erst nach Erteilung Einwilligung Infos abrufbar





* Folien 26 zum Webinar unter: https://www.bfarm.de/DE/Aktuelles/Veranstaltungen/Termine/2022-05-04-diginar.html

Erfahrungen des BfArM aus Antragstellung

(Quelle: BfArM Webinar vom 4. Mai 2022*)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Erfahrungen bzgl. Datenschutz / IT-Sicherheit

- Fehlerhafte Einwilligung bei DiGA
  - Fehlende separate Einwilligung zur Verarbeitung nach § 4 Abs. 2 Nr. 4 DiGAV**
  - Beispiel*:

* Folie 31 zum Webinar unter: https://www.bfarm.de/DE/Aktuelles/Veranstaltungen/Termine/2022-05-04-diginar.html

** Dauerhaften Gewährleistung techn. Funktionsfähigkeit, Nutzerfreundlichkeit und Weiterentwicklung der DiGA

Erfahrungen des BfArM aus Antragstellung

(Quelle: BfArM Webinar vom 4. Mai 2022*)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Erfahrungen bzgl. Datenschutz / IT-Sicherheit

– Vorgaben bzgl. Verarbeitung Drittland nicht beachtet

- Beispiel*:

Im Rahmen der inhaltlichen Prüfung werden die IP-Adressen überprüft, zu denen die App bzw. Anwendung eine Verbindung aufbaut.

Folgende Erfahrungen zu ungewollten Datenabfluss wurden hierbei schon gesammelt:

Unternehmen	Ursache
Google LLC	Google Schriftarten
Amazon.com, Inc.	Dienst „*Branch.io*“
Microsoft Corporation	Dienstleister Selligent GmbH Dienst „*CodePush*“

* Folie 77 zum Webinar unter: https://www.bfarm.de/DE/Aktuelles/Veranstaltungen/Termine/2022-05-04-diginar.html

Erfahrungen des BfArM aus Antragstellung

(Quelle: BfArM Webinar vom 4. Mai 2022*)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Fazit BfArM Workshop Mai 2022

- Die meisten eingereichten Apps fallen beim Datenschutzvorgaben durch
- BfArM muss den Antrag dann schon aufgrund dieses Umstandes ablehnen
  - Unabhängig von der evtl. vorhandenen qualitativ besseren Versorgung von Patienten

Folien zum Webinar unter: https://www.bfarm.de/DE/Aktuelles/Veranstaltungen/Termine/2022-05-04-diginar.html

BfArM: Datenschutzkriterien, veröffentlicht 2022-08-09

Prüfkriterien für die von digitalen Gesundheitsanwendungen (DiGA) und digitalen Pflegeanwendungen (DiPA) nachzuweisenden Anforderungen an den Datenschutz*

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Datenschutz-Prüfkriterien als pdf veröffentlicht (Version 0.1 vom 09.08.2022)

- 80 Seiten
  - Inhaltsverzeichnis (3 Seiten), Definitionen (3 Seiten), Literatur (3 Seiten)
  - Ca. 70 Seiten mit Anforderungen und die Anforderungen erläuterndem Text
- Schlüsselwörter angelehnt an RFC2119**, d.h.
  - Muss/Müssen (must)
  - Soll (should)
  - …
- Grundsätzlicher Aufbau
  - Regulatorische Grundlagen,
  - Gegenstandsbereich und Motivation,
  - Kriterien,
  - Allgemeine Erläuterungen,
  - Spezifische Erläuterungen

* BfArM: Datenschutzkriterien nach § 139e Absatz 11 SGB V und § 78a Absatz 8 SGB XI. https://www.bfarm.de/DE/Medizinprodukte/Aufgaben/DiGA-und-DiPA/Datenschutzkriterien/_node.html

** RFC 2119: Key words for use in RFCs to Indicate Requirement Levels. https://www.rfc-editor.org/rfc/rfc2119

BfArM Datenschutz-Prüfkriterien

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Datenschutz-Prüfkriterien: Ein Beispiel zur Einwilligung

- Prüfkriterium:
  CNST_1 Rechtmäßigkeit durch Einwilligung
- Anforderungen (exemplarisch):
  - CNST_1.1 Jegliche mit der digitalen Anwendung verfolgten Zwecke einer Verarbeitung personenbezogener Daten MÜSSEN auf einer informierten Einwilligung der betroffenen Person nach Art. 9 Absatz 2 Buchstabe a DSGVO basieren oder durch eine Befugnis aus einer Rechtsvorschrift gedeckt sein.
  - CNST_1.2 Einwilligungen DÜRFEN NICHT zu anderen als den rechtmäßigen Zwecken der digitalen Anwendung eingefordert werden. Die mit den Einwilligungen verbundenen Erklärungen DÜRFEN KEINE über die zulässigen Zwecke hinausgehenden Sachverhalte enthalten.
  - …

BfArM Datenschutz-Prüfkriterien

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Datenschutz-Prüfkriterien als pdf veröffentlicht

Anforderungen bzgl. datenschutzrechtlicher Grundsätze (85 Kriterien)

- Rechtmäßigkeit (15 Kriterien)
- Verarbeitung nach Treu und Glauben (4 Kriterien)
- Transparenz (17 Kriterien)
- Nichtverkettbarkeit (5 Kriterien)
- Datenminimierung und Speicherbegrenzung (12 Kriterien)
- Intervenierbarkeit (14 Kriterien)
- Integrität, Richtigkeit und Vertraulichkeit (9 Kriterien)
- Rechenschaftspflicht (9 Kriterien)

BfArM Datenschutz-Prüfkriterien

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Datenschutz-Prüfkriterien als pdf veröffentlicht

Anforderungen bzgl. Verantwortlicher und Auftragsverarbeiter (53 Kriterien)

- Wahrnehmung von Verantwortung (11 Kriterien)
- Auftragsverarbeitung und Datenübermittlung (12 Kriterien)
- Datenschutz-Folgenabschätzung und Verzeichnis von Verarbeitungstätigkeiten (12 Kriterien)
- Technische und Organisatorische Maßnahmen (18 Kriterien)

BfArM Datenschutz-Prüfkriterien

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Datenschutz-Prüfkriterien als pdf veröffentlicht

- Insgesamt 138 Kriterien
- Ein Kriterium beinhaltet 1…n Anforderungen
- Beispiel TOM_2.2:

TOM_2.2 Der Verantwortliche der digitalen Anwendung MUSS alle verwendeten kryptografischen Dienste zusammen mit ihrem Einsatzzweck und den verwendeten Algorithmen und vorgegebenen Schlüssellängen in einem Kryptografiekonzept dokumentieren. Das Kryptografiekonzept MUSS Maßnahmen beschreiben, wie Schlüssel und Zertifikate ausgetauscht werden können.

a) Jegliche Kommunikation zwischen Komponenten der digitalen Anwendung, zu Komponenten der digitalen Anwendung und aus Komponenten der digitalen Anwendung heraus MUSS verschlüsselt erfolgen.

b) Jegliche Speicherung von personenbezogenen Daten auf dem Endgerät der betroffenen Person MUSS verschlüsselt erfolgen.

c) Jegliche Speicherung von personenbezogenen Daten auf Hintergrundsystemen der digitalen Anwendung MUSS verschlüsselt erfolgen.

d) Für die Authentisierung und Autorisierung genutzte Sicherheitstoken MÜSSEN digital signiert sein. Die digitale Anwendung MUSS die Integrität und Authentizität dieser Signaturen prüfen.

e) Auf Hintergrundsystemen angesiedelte Dienste MÜSSEN sich gegenüber anfragenden Systemen authentisieren. Anfragende Systeme DÜRFEN KEINE personenbezogenen Daten an Dienste auf Hintergrundsystemen übermitteln, deren Authentizität sie nicht zuvor geprüft haben.

f) Alle verwendeten Zertifikate und Schlüssel MÜSSEN dem Stand der Technik entsprechen.

Fazit

Fazit

Datenschutz und IT-Sicherheit von Anfang an einplanen !!!

- Vorgaben von BSI und BfArM schon in der Planungsphase berücksichtigen
- Und natürlich umsetzen
- Dokumentation für Nachweise der Erfüllung der Anforderungen ist ein MUSS-Kriterium
  - Auch wenn immer noch unklar ist, wie eine Zertifizierung aussieht: Zertifizierung muss Einhaltung gesetzlicher Vorgaben prüfen
  - → Daher muss Zertifizierung Einhaltung der Vorgaben BSI prüfen
  - → Daher muss Zertifizierung Einhaltung der Vorgaben BfArM prüfen
  - Wie soll eine Prüfung ohne Dokumentation möglich sein?
- Unabhängig von den Vorgaben von BSI und BfArM sind natürlich alle gesetzlichen Anforderungen einzuhalten, also Vorgaben beachten z.B. von
  - Datenschutz-Grundverordnung
  - Bundesdatenschutzgesetz
  - … (wir haben gar nicht zu wenig Gesetze 😉)

Online-Literatur

Leitfäden & Co von Datenschutz-Aufsichtsbehörden, BSI usw. beachten

Neben den bei DiGA erwähnten BSI Leitfäden gibt es z.B.:

- WP 202 der Artikel-29-Datenschutzgruppe: „Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten“
- BSI: IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Gesundheits-Apps. Stand: 2021-06-06
- BSI: Grundschutz-Kompendium - APP.1.4 Mobile Anwendungen (Apps) (Edition 2022). Stand: 01.02.2022
- EDPS: Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions. Stand: 2016-11-07
- EDPS: Mobile-Health-Dienste. Stellungnahme 1/2015, 2015-05-21
- FDA: Policy for Device Software Functions and Mobile Medical Applications. Stand: 2019-09
- National Institute of Standards and Technology (NIST): Special Publications (SP), insbesondere
  - Securing Electronic Health Records on Mobile Devices. Stand: 2018-07-27
  - Securing Telehealth Remote Patient Monitoring Ecosystem. Stand: 2022-02-22

„Werbung“

Praxishilfe in Entwicklung: „Mobile Apps im Gesundheitswesen“

- Praxishilfe in Entstehung
  „Mobile Apps im Gesundheitswesen: Anforderungen aus dem Datenschutz“
- 9 Menschen arbeiten an der Praxishilfe
- Beteiligte kommen aus 3 Verbänden:
  - Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)
  - Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD)
  - Berufsverband der Datenschutzbeauftragten Deutschlands e. V. (BvD)
- Praxishilfe wird u.a. Anhänge enthalten, z.B.
  - Beispiel für Datenschutzerklärung / Datenhinweise für Medical Apps
  - Hinweise zur Planung von Maßnahmen zur Umsetzung der Anforderungen von Datenschutz und IT-Sicherheit
  - Beispiel für Maßnahmen hinsichtlich IT-Sicherheit

„Werbung“

Praxishilfe in Entwicklung: „Mobile Apps im Gesundheitswesen“

- Praxishilfe in Entstehung
  „Mobile Apps im Gesundhe … s dem Datenschutz“
- 9 Menschen arbeiten an de …
- Beteiligte kommen aus 3 Ve …
  - Deutsche Gesellschaft … Biometrie und Epidemiologie e. V. (G …
  - Gesellschaft für Daten … . V. (GDD)
  - Berufsverband der Da … chlands e. V. (BvD)
- Praxishilfe wird u.a. Anhäng …
  - Beispiel f … Apps
  - Hinweise … orderungen von Datensch …
  - Beispiel f …


Mobile Apps im Gesundheitswesen:
Anforderungen aus dem Datenschutz

Erarbeitet von

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

Gesellschaft für Datenschutz und Datensicherheit e. V.
Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“

Berufsverband der Datenschutzbeauftragten Deutschlands e. V.

Erscheinen voraussichtlich
Ende Oktober 2022

Fragen / Diskussion

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Kontakt:

Dr. Bernd Schütze

Leiter GMDS AG „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

mailto:schuetze@medizin-informatik.org

https://gesundheitsdatenschutz.org