RATAJCZAK & PARTNER mbB

DigA und der Datenschutz – „Blackbox-Reloaded“

13.05.2022

Ihr Referent

Gerald Spyra, LL.M.

- Rechtsanwalt / Partner bei RP
- Hohe Affinität für die Informationssicherheit

Spezialisiert auf

- das Informations- / Datenschutzrecht,
- das „Software-Medizinprodukterecht“ und
- die „IT-Forensik“

- Externer betrieblicher Datenschutzbeauftragter

RP RECHTSANWÄLTE

APPS SIND „IN“…

- Es gibt **sehr viele Apps**, die in den **unterschiedlichen App-Stores angeboten** werden.
- Auch immer **mehr Apps** rund um die **„Gesundheit“** werden dort angeboten (**Gesundheit** ist **„IN“**).
- **Anerkannte, einheitliche Standards**, wie eine **Gesundheits-App „rechtskonform“ entwickelt** und **betrieben** werden soll, **gibt** es bisher **nicht**.
- Viele **App-Anbieter**, die in **anderen Sparten** aktiv waren, **entwickeln** daher auch **mal „eben“** eine **Gesundheitsapp**, um damit **schnell Geld** zu **verdienen**.
- Gerade weil **Gesundheit „in“** ist, werden auch immer mehr **Apps** mit **„Behandlungs- / Diagnosefähigkeiten“** entwickelt, die u.a. die **Sensoren / Funktionalitäten** des **Smartphones nutzen**.
- Diese **Apps** sind dann möglicherweise als **Medizinprodukte einzustufen**, die dann wiederum **besondere Anforderungen** zu **erfüllen** haben…

Was macht Software-Medizinprodukte (Apps) aus?

- Immer **mehr Apps** stellen **Medizinprodukte** dar bzw. werden als **Medizinprodukte** in den **Verkehr** gebracht.
- Dieses insbesondere deshalb, weil sie auch für die **Behandlung**, **Diagnose**, **Überwachung** etc. eines **Patienten genutzt** werden (können).
- Da von diesen **Apps** (ihrer **Datenverarbeitung**) ein **nicht** zu **unterschätzendes Risiko** für die **Gesundheit** und sogar **Leben** des **Patienten ausgeht**, sind diese **Apps** besonders **gesetzlich reguliert**.
- Daher müssen sie **entsprechend** ihrer **Risikoklasse** die **gesetzlichen Anforderungen** der **EU-Medizinprodukteverordnung** (MDR) erfüllen und einen **Nachweis** für eine **ausreichende „Sicherheit“** erbringen.
- Dieses betrifft insbesondere die **„Sicherheit** der **Funktionsfähigkeit** (**safety**) und die **IT-Sicherheit** (**security**)
- Gerade weil die **Anforderungen** und der **Aufwand** für die **Entwicklung**, in **Verkehrbringung** und **Betreiben** einer solchen **App sehr hoch** ist, fragen sich **Anbieter**, wie sie diese Apps **finanzieren** sollen…

Finanzierung von Apps

- Gerade weil die **Entwicklung** und das **Betreiben** von **Software-Medizinprodukte-Apps** / Plattformen **teuer** ist, stellt sich die **Frage**, wie man sie **finanziert**.
- Es gibt **diverse Möglichkeiten**, die natürlich auch mit **diversen rechtlichen Implikationen** verbunden sind:
  - Kosten der App sind **„Werbekosten“**;
  - App wird gemeinsam mit **„Produkt** (oftmals **auch** ein **Medizinprodukt**) **vertrieben“**;
  - Mittels der App werden die **Daten** des **Nutzers kommerzialisiert**;
  - Man holt sich **Sponsoren**;
  - Man nutzt die vom **Gesetzgeber** geschaffene Möglichkeit eine **Digitale Anwendung** (DigA) **zuzulassen**, was jedoch mit **hohen Anforderungen verbunden** ist.
- Daher schauen wir uns diese **DigA-Möglichkeit** mal an…

DigA- Was ist das?

- Der deutsche **Gesetzgeber** will die **Digitalisierung voranbringen** (jedenfalls zu Zeiten von Spahn) und sieht daher für **DIGA(s) entsprechende Fördermöglichkeiten** vor.
- **DigA** sind letzten Endes, **„Apps** auf **Rezept“** (vgl. §§33a, 139e SGB V i.V.m. der DigAV) und werden auch **ähnlich abgerechnet** (bekommen auch eine **PZN**)!
- Die **Hürden**, um in das **DigA-Verzeichnis** aufgenommen zu werden sind **hoch** (und damit der zu betreibende **Aufwand**), was auch ganz im **Sinne** von gewisser **„Institutionen“** sein dürfte, die auf **DigA keine „Lust“** haben!
- Daher wurden bisher auch noch **nicht** so wirklich **viele DigA bisher zugelassen**.
- Eine **Zulassung** und **Aufnahme** in das **DigA-Verzeichnis** erfolgt nach entsprechendem **Antrag** beim Bundesinstitut für Arzneimittel und Medizinprodukte (**BfArM**) und wird **nur gewährt**, wenn die **DigA** entsprechende **Anforderungen erfüllt…**

Was sind die wesentlichen Anforderungen an DiGA

- Da **DiGA Medizinprodukte** sind, die vom Gesetzgeber bzw. den Krankenkassen gefördert werden können, müssen diese das in sie **gesetzte Vertrauen erfüllen**.
- Daher müssen diese **Anwendungen** die **Anforderungen** der **DiGAV** (§§ 3 – 6a DigaV) **erfüllen**. Diese sind:
  - **Sicherheit** und **Funktionstauglichkeit** (safety)
  - **Qualität**, insbesondere **Interoperabilität**
  - **Datenschutz** und **Informationssicherheit** (security).
- **Unabhängig** von der **Prüfentscheidung** des **BfArM** ist der **Hersteller** einer **DigA** jederzeit **VERANTWORTLICH**!! für die **Gewährleistung** aller **datenschutz-** (§ 4 Nr. 7 DSGVO) und **informationssicherheitsbezogenen** sowie sonstigen **rechtlichen Anforderungen** an sein **Medizinprodukt** und natürlich auch, dass sein **Antrag** der **„Wahrheit“** entspricht ;).
- Dem Antrag wird nur vom **BfArM stattgegeben**, wenn insbesondere die **Datenverarbeitung** die **rechtlichen Anforderungen** an die **„Rechtmäßigkeit“** erfüllt...

Rechtmäßigkeit / Zulässige Zwecke der Datenverarbeitung

- Grundsätzlich bedarf die Datenverarbeitung einer DigA **einer Einwilligung** (Art. 9 Abs. 2 a) DSGVO), die auf **bestimmte Zwecke beschränkt** ist (vgl. § 4 Abs. 2 DigAV). Diese sind:
  - **bestimmungsgemäßer Gebrauch** der DigA durch die Nutzer,
  - Zur **Nachweisführung positiver Versorgungseffekte** im Rahmen einer Erprobung nach § 139e Abs. 4 SGB V,
  - zur **Nachweisführung** bei **Vereinbarungen** nach § 134 Abs. 1 S. 3 SGB V (**GKV** und **Hersteller**);
  - zur dauerhaften **Gewährleistung** der **technischen Funktionsfähigkeit**, der **Nutzerfreundlichkeit** und der **Weiterentwicklung** der DigA (bedarf aber einer separaten / getrennten Einwilligung)
- Auch **ohne Einwilligung** dürfen Daten verarbeitet werden, wenn andere Rechtsvorschriften dies erlauben oder anordnen. Das betrifft insbesondere:
  - Die **Abrechnung** des **DigA-Herstellers** gegenüber der **Krankenkasse** gemäß § 302 SGB V
  - Die **Erfüllung medizinprodukterechtlicher Verpflichtungen** z. B. gemäß MDR (bzw. im Rahmen der Übergangsregelungen MDD/MPG)
- Eine **eingeholte** ausdrückliche **Einwilligung**, mit der eine Verarbeitung von Gesundheitsdaten zu **anderen** als den in **§ 4 Abs. 2 S. 1 DiGAV** genannten **Zwecken** legitimiert werden soll, ist **nicht zulässig**!!!
- Was der **Hersteller** für die **Zulassung angeben** muss, findet sich in den **Anlagen** zur **DigaV…**

Die Anlagen / Fragebögen…

- Zur **Antragstellung** muss der **Hersteller** einen **Wust** an **Fragen beantworten**, die aus **Anlage 1** und **2** der DigaV stammen:
  - **Anlage 1**: **Anforderungen** an **Datenschutz** und **Datensicherheit**
  - **Anlage 2**: **Anforderungen** an **Interoperabilität**, **Robustheit**, **Verbraucherschutz**, **Nutzerfreundlichkeit**, Unterstützung von Leistungserbringenden, **Qualität** medizinischer Inhalte und **Patientensicherheit**
- Die jeweiligen Bereiche und diesebezüglichen Anforderungen werden mittels **„Ja/Nein“**- und **„Nicht-zutreffend“**-) **Kästchen abgefragt**.
- Eine **„Nicht zutreffend“-Antwort** erfordert eine **schriftliche Begründung** darüber, warum die **Anforderung** dennoch **erfüllt** wird.
- **Fehlt** eine solche **Begründung**, gilt der Antrag als **unvollständig** – Antwort muss in einer kurzen **Frist nachgereicht** werden. Falls **keine plausible Begründung** erfolgt, lehnt **BfArM** den ganzen Antrag ohne **weitere Prüfung ab**!!!
- Der Inhalt der **Anlagen** sind **m.A. nach** durchaus **„verbesserungswürdig“**, denn die **Fragen** sind **manchmal sehr offen und oftmals** sehr **spezifisch formuliert**.
- Es sei darauf hingewiesen, dass es sich um **Minimalanforderungen** handelt, so dass durchaus **weitere Anforderungen** erfüllt werden müssen, um **„rechtskonform“** zu sein.
- Schauen wir uns mal **Anlage 1** an…

Anlage 1 – Datenschutz - Einwilligung

- **Anlage 1** beinhaltet die **wesentlichen datenschutzrechtlichen Fragen** und stellt klar, dass die **Regeln** der **DSGVO** maßgeblich sind, jedoch auch **weitere Gesetze** (wie bspw. das **TTDSG**) **Anwendung** findet.
- **„Einwilligungen“** werden von der **DigAV** als **Mittel** der **Wahl** angesehen und **müssen entsprechende Anforderungen erfüllen** (Fragen 2 – 7):
  - **Informiertheit** der **Einwilligung**
  - **Informiertheit** über **Art** und **Weise**, **Umfang** der **Datenverarbeitung**
  - **Ausdrücklichkeit**
  - **Barrierefreiheit** und **Einfachheit**
  - Hinweis auf **Widerrufbarkeit**
  - **Abrufbarkeit** der **Einwilligung**
- Und eng damit verbunden ist die **Zweckbindung**…

Anlage 1 – Datenschutz – Zweckbindung / Datenminimierung / Angemessenheit

- Die **Zweckbindung** und **Datenminimierung** als ganz wesentliche datenschutzrechtliche Grundprinzipien werden auch von Anlage 1 adressiert (Frage 8 – 13)
  - Erfolgt **Verarbeitung ausschließlich** zu **Zwecken** in **§ 4 Abs. 2 DigAV** oder sonstiger **Datenverarbeitungsbefugnisse**?
  - Sind die **Daten** auf das **notwendige Maß beschränkt**?
  - Ist die **Datenverarbeitung „angemessen“** oder könnten die **Zwecke** der **Datenverarbeitung** auch auf **andere Weise erreicht** werden?
  - Erfolgt eine **Datentrennung** (gesundheitsbezogene Daten getrennt von Daten für Leistungsabrechnung)?
  - Existieren **ausreichende Zugriffsberechtigungen**, damit etwaige nicht **zugriffsberechtigte Mitarbeiter** auch **keinen Zugriff** auf die **Daten** nehmen können.
  - Falls die **DigA nicht** nur auf **Smartphone** des **Nutzers** verwendet werden soll, wurde das in der **DSFA berücksichtigt**? Wird **Nutzer hingewiesen**, dass Nutzung in einer potenziell **unsicheren Umgebung** erfolgt und der **Hersteller** dieses **nicht vollständig adressieren** kann – wird bzw. kann die (temporäre) **Speicherung** auf diesen **Systemen unterbunden**?
- Und dann gibt es ja noch die **Integrität** und **Vertraulichkeit**…

Anlage 1 – Datenschutz – Integrität und Vertraulichkeit

- Gerade die **Gewährleistung** der **Integrität** und **Vertraulichkeit** sind gerade bei der **„BlackBox“ Smartphone** sehr **wichtig** und werden **nochmals getrennt / individuell** von Anlage 1 **adressiert** (Fragen 14 und 15):
  - Sieht die **DigA angemessene technische** und **organisatorische Maßnahmen** vor, um personenbezogene **Daten** gegen unbeabsichtigte oder unzulässige **Zerstörung**, **Löschung**, **Verfälschung**, **Offenbarung** oder nicht legitimierte **Verarbeitungsformen** zu **schützen**?
  - Ist der durch die **DigA** gesteuerte **Austausch** von **Daten** zwischen dem Endgerät der betroffenen Person und externen Systemen **durchgängig** gemäß dem Stand der Technik **verschlüsselt**?
- Und eng mit der Integrität der Daten steht auch die „**Richtigkeit**“ in Verbindung…

Anlage 1 – Datenschutz – Richtigkeit

- Gerade weil die **Verarbeitung** von Daten bei **DigA** extreme **Auswirkungen** auf den **Nutzer** haben kann, sind die **„Integrität“** aber auch die **„Richtigkeit“** der Daten absolut **essenziell** (Frage 16 – 18):
  - Sieht die **DigA technische** und **organisatorische Maßnahmen** vor, die **sicherstellen**, dass die über die **DigA verarbeiteten** personenbezogenen **Daten sachlich richtig** und auf dem **neuesten Stand** sind?
  - Trifft der **Hersteller alle angemessenen Maßnahmen**, damit personenbezogene **Daten**, die im Hinblick auf die **Zwecke** ihrer **Verarbeitung unrichtig** sind, **unverzüglich gelöscht** oder **berichtigt** werden?
- Und natürlich muss die **„Erforderlichkeit“** gewahrt sein…

Anlage 1 – Datenschutz – Erforderlichkeit / Speicherbegrenzung/ Datenportabilität

- Aufgrund der **Relevanz** der **Datenverarbeitung** und **Sensibilität** der Daten muss auch die **Erforderlichkeit** gewahrt bleiben (Frage 18 – 19):
  - Werden **Daten** nur so **lange gespeichert**, wie sie für die **Zwecke „erforderlich“** sind?
  - Werden entsprechende **Daten nach Erfüllung** der **Zwecke** in **§ 4 Abs. 1 Nr. 1 - 4 DigaV** entsprechend **nicht länger gespeichert** – **gelöscht**?
  - Ist der durch die **DigA** gesteuerte **Austausch** von **Daten** zwischen dem **Endgerät** der betroffenen Person und **externen Systemen durchgängig** gemäß dem Stand der Technik **verschlüsselt**?
- Daten sollen auch immer **„übertragen“** (Datenportabilität) werden können (Frage 20):
  - Hat **Hersteller Mechanismen** für die **Ausübung** des Rechts auf **„Datenportabilität“** getroffen – **Portierbarkeit** der Daten?
- Und über alles muss natürlich auch **aufgeklärt** / **informiert** werden…

Anlage 1 – Datenschutz – Informationspflichten / Transparenz / Berichtigung

- Aufgrund der **Sensibilität** der **Datenverarbeitung** muss der **Nutzer** auch **umfänglich** über die **Datenverarbeitung aufgeklärt** werden (Frage 21 – 27):
  - Ist die **DigA-Datenschutzerklärung einfach**, **barrierefrei auffindbar** und frei **einsehbar**?
  - Erhält die **Datenschutzerklärung** die entsprechend **gesetzlich geforderten Angaben** (**Art. 13 – 14 DSGVO**)?
  - Ist die **DS-Erklärung** auch **nach Installation** der App noch **einfach auffindbar**?
  - Kann **Betroffener Auskunft** gem**. Art .15 erhalten**?
  - **Existiert** ein entsprechendes **Lösch- / Sperrkonzept** (**Widerruf** der **Einwilligung** / **Löschen** der App – **Daten-Sperrung)**?
  - Kann **Berichtigung** der **unrichtigen Daten** verlangt werden und wird sie auch entsprechend **umgesetzt**?
  - Wird **Person** vor **Löschung** auf **Recht** auf **Datenübertragung hingewiesen**?
- Und all das erfordert ein entsprechendes **Datenschutz-Management**…

Anlage 1 – Datenschutz – Datenschutzmanagement

- Die Rechtskonformität der Datenverarbeitung macht ein entsprechendes **Datenschutzmanagement** erforderlich (Frage 28 – 29):
  - Hat der **Hersteller** der **DigA** ein **Verfahren** zur **regelmäßigen Überprüfung**, **Bewertung** und **Evaluierung** der **Wirksamkeit** der **technischen** und **organisatorischen Maßnahmen** zur **Gewährleistung** der **Sicherheit** der **Verarbeitung** umgesetzt, mit dem **ALLE** im **Zusammenhang** mit der **DigA eingesetzten Systeme** und **Prozesse** erfasst sind?
  - Hat der **Hersteller** der **DigA alle Personen**, die aus ihrer **Tätigkeit** heraus **Zugang** zu personenbezogenen **Daten** haben, auf die **Verschwiegenheit** verpflichtet?
- Und all das erfordert ein **Datenschutzfolgenabschätzung**…

Anlage 1 – Datenschutz – Datenschutzfolgenabschätzung / Risikomanagement

- Gerade weil sehr **sensible Daten** verarbeitet werden und **systemimmanent** ein **großes Risiko** entsteht, ist ein **Risikomanagement** und **Datenschutzfolgenabschätzung durchzuführen** (Frage 30 – 32):
  - Hat der **Hersteller** der **DigA** für diese **Anwendung** eine **Datenschutz-Folgenabschätzung** durchgeführt und die hierbei durchgeführte **Risikoanalyse** in die **dokumentierten Prozesse** eines **Risikomanagements** überführt, nachdem eine **kontinuierliche Neubewertung** von **Bedrohungen** und **Risiken** erfolgt?
  - Stellt der **Hersteller** der **DigA** sicher, dass die **Meldung** von **Verletzungen** des **Schutzes** personenbezogener **Daten innerhalb** von **72 Stunden** nachdem ihm die **Verletzung bekannt wurde**, **an** die **Aufsichtsbehörde** erfolgt?
  - Setzt der Hersteller der **DigA** die **Vorgaben** nach **Artikel 34 DSGVO** zur Information Betroffener bei **Datenschutzvorfällen** um?
- Und all das muss **nachgewiesen** werden…

Anlage 1 – Datenschutz – Nachweispflicht

- Dem Grundsatz der **Rechenschaftspflicht** folgend, muss der Hersteller sicherstellen, dass er die **„Datenschutzkonformität“** jederzeit **nachweisen** kann (Frage 33- 36):
  - Hat der Hersteller die für das **Unternehmen geltenden Datenschutzleitlinien dokumentiert** und seine **Mitarbeiter** in deren **Umsetzung geschult**?
  - **Realisiert** der **Hersteller** der DigA **Maßnahmen**, die gewährleisten, dass **nachträglich überprüft** und **festgestellt** werden kann, **ob** und **von** wem bei dem Hersteller **gespeicherte** personenbezogene Daten **eingegeben**, **verändert** oder **entfernt** worden sind (Protokollierung)?
  - Kann der **Hersteller** der DigA jederzeit **nachweisen**, dass zu einer durchgeführten Verarbeitung personenbezogener Daten die **erforderliche Einwilligung** der betroffenen Person **vorlag**, **soweit** die **Datenverarbeitung nicht** auf anderer **rechtlicher Grundlage** erfolgt?
- Und auch die **Verarbeitung** durch **„Externe“** bedarf entsprechender Aufmerksamkeit…

Anlage 1 – Datenschutz – Verarbeitung durch Externe / im Ausland

- Gerade durch die **Einschaltung Externer**, besonders wenn sie im **Ausland** sind, bestehen besondere **Risiken**, die der **Hersteller** adressieren muss (Frage 36- 38):
  - Werden über die **DigA** oder den **Hersteller** der **DigA** personenbezogene **Daten** gar **nicht** an **Auftragsverarbeiter** oder **ausschließlich** an **Auftragsverarbeiter weitergegeben**, die über eine **ausreichende Vertrauenswürdigkeit** und **Haftbarkeit!!! verfügen**, **angemessene Mechanismen** zum **Schutz** übernommener Daten **realisieren** und mit dem **Hersteller** in einem **verpflichtenden vertraglichen Verhältnis** stehen, das eine **Abschwächung** der dem **Versicherten** gegenüber gemachten **Zusagen ausschließt**?
  - Werden über die **DigA** oder den **Hersteller keine** personenbezogenen **Daten** an **Dritte weitergegeben**, sofern dies nicht unmittelbar für die Erfüllung von Zwecken nach **§ 4 Abs. 2 Satz 1 Nr. 1** oder die **Erfüllung gesetzlicher Vorschriften erforderlich** und auf diese **Zwecke beschränkt** ist?
  - Erfolgt die **Verarbeitung** von **Gesundheitsdaten** sowie personenidentifizierbaren **Bestands-** und **Verkehrsdaten ausschließlich** im **Inland**, in einem anderen **Mitgliedstaat** der **EU**, in einem diesem nach § 35 Abs. 7 SGB I **gleichgestellten Staat**, oder auf Grundlage eines **Angemessenheitsbeschlusses** gemäß Art. 45 DSGVO?
- Weitere **Gewährleistungsziele**?…

Anlage 1 – Datenschutz –Weitere Gewährleistungsziele

- Ferner gibt es **weitere Gewährleistungsziele**, die man bspw. aus dem SDM kennt ;) (Frage 39- 40):
  - Ist die **Verkettung** von personenbezogenen **Daten** über **zwei** oder **mehr DigA** hinweg **technisch ausgeschlossen** oder muss die **betroffene Person** für eine **Verkettung** von Daten über **zwei** oder **mehr DigA hinweg** eine **explizite**, **gesondert** eingeholte, informierte **Einwilligung** abgeben?
  - Ist **sichergestellt**, dass eine **Offenbarung** von **Informationen** der betroffenen Person oder über die betroffene Person für die Öffentlichkeit oder eine für die betroffene Person nicht eingrenzbare Personengruppe **gar nicht** oder **immer** nur infolge einer **expliziten**, **aktiven Handlung** der **betroffenen Person erfolgt**, der eine **zielgruppengerechte Information** über die **Art** der **offenbarten Informationen** und den **möglichen Kreis** der **Empfänger zugrunde** liegt?

- Und dann enthält Anlage 1 noch sehr detaillierte (**weitere**) **Anforderungen** an die **Daten-** / **IT-Sicherheit**…

Anlage 1 – Daten- / IT-Sicherheit (1)

- Anlage 1 enthält teilweise **sehr detaillierte Fragen** zur **Daten- / IT-Sicherheit**, um **„CIA“** bei einer **DigA** zu **gewährleisten** (Fragen 1- 37 - Zusammenfassung):
  - **Betreiben** eines **ISMS** (ISO 27001 – BSI-GRS) und **entsprechende Prozesse** – **Schutzbedarfsanalyse** – **Release- Changemanagement-Prozesse**;
  - **Verhinderung** des **Datenabflusses** – **Einschränkung** der **Kommunikationsmöglichkeiten** – **Transportverschlüsselung** - **Zugriffsprüfung** – **keine ungewollten Log-** oder **Hilfsdateien** – **keine Fehlermeldungen** mit **vertraulichen** Infos;
  - Personen müssen sich alle entsprechend **authentisieren**, bevor **Zugriff gestattet** wird – **keine Gestattung** des **unverschlüsselten Datenaustauschs** – **Authentifizierung** über (akkreditierte) **Standardkomponenten** – **Datenveränderung** nur nach **entsprechender Authentisierung** möglich – **Verwendung** / Durchsetzung **sicherer Passwörter** – **keine Klartextspeicherung** / **Verarbeitung** der **Passwörter** – **Protokollierung** der **Passwortänderung** – falls **Speicherung** der **Authentifizierungsdaten** auf Gerät / **Hinweis** auf **Risiko** – **Schutz** der Session / **Sessiondaten** – **Invalidierung** der Daten nach **Beendigung** / **Abbruch** der **Session** – **maximale Sitzungsdauer** der Sessions – **Authentisierung** mit **eGK**;
  - **Zugriffskontrolle** – **umfassende Berechtigungsprüfung** insbesondere bei **Herstellerpersonen** – **restriktive Zugriffsrechte** und Prüf- / **Kontrollmechanismen** bei Hersteller (**4-Augen**) – bei verschiedenen **Nutzerrollen** nur **Zugriff entsprechend** der **Rechte** – führen **Fehler** beim **Zugriff** zur **Ablehnung**;
  - **Einbinden** von **Daten** und **Funktionen** – **Nutzung nur** innerhalb der **„Vertrauensdomäne“ möglich** –**Uploadfunktion** entsprechend **restriktiv;**
- Und noch **mehr**…

Anlage 1 – Daten- / IT-Sicherheit (2)

- Und **weiter**:
  - **Protokollierung**: **Vollständige Protokollierung** entsprechend des **Zwecks** – **automatische Auswertung** um **sicherheitsrelevante Ereignisse** zu erkennen / verhindern – Beschränkung des **Zugriff** auf Protokolle;
  - **Aktualisierung** – **Information** über (sicherheitsrelevantes) **Updates** z. B. via **PUSH;**
  - Sichere **Deinstallation** – **Rückstandslose Entfernung** aller **Daten** bei **Deinstallation**;
  - **Härtung** – **Restriktion** der **nicht benötigten Dienste** / **Protokolle** – **Einschränkung** der **Zugriffsversuche** (**Bruteforceschutz- keine Offenbarung sicherheitsrelevanter Informationen** – **Löschung nicht benötigter Daten** – **keine Pfadangaben** – **keine Indexierung** in **Suchmaschinen** – Unterbinden Quelletextabruf – restriktive Handhabung von Daten aus externen Quellen – **Prüfung** auf **vertrauenswürdige Systemen** – **Verhinderung Missbrauch** von **Fehleingaben** – **Datentrennung** – **adäquate Fehlerbehandlung** – erforderliche **Schutzmechanismen** – **Schutz** von **Konfigurationsdateien;**
  - Wurden **Penetrationstests** für **Anwendung** und **Backend durchgeführt** entsprechend **BSI-Vorgaben;**
  - **Nutzung Sensoren**, externen **Geräten** - Fremdsoftware – wurde **Nutzung** und **Rechte entsprechend festgelegt** entsprechend **Sicherheitsrichtlinie** – **Datenaustausch** erst bei **Freigabe** und **Abschluss** der **Installation** – ausreichende **Information** / Dokumentation - müssen **externe Sensoren Geräte** sich entsprechend **authentisieren** (**wechselseitige Authentisierung**)- Führung einer **vollständigen Auflistung** der **Bibliotheken** / weiteren **Software-Produkte** usw. – ausreichende **Marktbeobachtung** / erforderliche Maßnahmen bei Feststellung eines Sicherheitsrisikos (z. B. Sperrung der App, Benachrichtigungen usw.
- Und dann noch **Zusatzanforderungen** für **DigA** mit **sehr hohem Schutzbedarf**…

Anlage 1 – Daten- / IT-Sicherheit – Zusatzanforderungen

- Für **DigA** mit **besonders hohem Risiko** gibt es noch **zusätzliche Anforderungen** (Fragen 1 – 9)
  - **Verschlüsselung aller** gespeicherter **Daten**
  - **Authentifizierungen** / Zwei-Faktor – **„Rückfallauthentisierung** (1-Faktor) und Hinweis auf Risiken – **Möglichkeit** der **Rückkehr** zu **2-Faktor**?
  - **Bei Beteiligung von Ärzten usw. - Einbindung einer HBA-Schnittstelle?**
  - **DDOS** (Distributed Denial Of Service)-**Schutzmaßnahmen** bei **„offener Kommunikation“**
  - **Eingebetteter Webserver** (restriktive Konfiguration) – **Härtung** – **Betreiben** des **Servers** mit **minimalen Zugriffsmöglichkeiten** - **Zugang** nur nach **Authentisierung** – **durchgehende Verschlüsselung**

- Aufgrund der fortgeschrittenen Zeit kommen wir nun zum **Fazit**…

FAZIT

- Bei der **Entwicklung** von **Apps** und insbesondere **Gesundheits-** / **medizinische Apps**, gibt es **einiges** zu **berücksichtigen**.
- Oftmals fehlen den **Herstellern klare Vorgaben**, was eine **App**, die **Gesundheitsdaten verarbeitet** alles an **Voraussetzungen** zu **erfüllen** hat.
- Gerade weil für **DigA** etwaige **Anforderungen** (**nicht abschließend**) **formuliert** sind, können diese **Vorgaben** einen **ersten Anhaltspunkt** geben, eine **App „rechtskonform“** zu **entwickeln** und zu **betreiben**.
- Jedoch sei **nochmals** darauf **hingewiesen**, dass diese Anforderungen **nicht** als **abschließend** zu **verstehen** sind und daher nur als **„Anregung“** verstanden werden sollten.
- Gerade aufgrund der **„Smartphone-BlackBox“** sollte für die **App** ein **individuelles Datenschutzkonzept erarbeitet** werden, in dem natürlich die **DigA-Anforderungen**, darüber hinaus aber auch noch **intensiver** die **datenschutzrechtlichen Grundprinzipien** gem. **Art. 5 DSGVO adressiert** werden.
- **Gerade** bei diesen **Anwendungen** ist ein **erheblicher Aufwand notwendig**, um die **Anforderungen „rechtskonform“ abzubilden**.
- Doch dieser **Aufwand** ist **notwendig**, um dem **Betroffenen** (das kann jeder von uns sein) und **seinen Daten**, den notwendigen **Respekt entgegenzubringen** sowie das **nötige Vertrauen** zu **erfüllen**.

Gibt es noch Fragen?

Gerald Spyra, LL.M.
Rechtsanwalt,
Externer Datenschutzbeauftragter

https://www.rpmed.de/

spyra@rpmed.de

Partner bei
RATAJCZAK & PARTNER mbB
Zollstockgürtel 59 / Atelier 25
50969 Köln

Vielen Dank für Ihr Interesse!