Apps im Gesundheitswesen

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

3. Fachtagung Datenschutz im Gesundheitswesen
07. Mai 2021

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)
  - Fachverband Biomedizinische Technik e.V. (fbmt)
  - HL7 Deutschland e.V.
  - IHE Deutschland e.V.
- Beruflich angestellt bei
  Deutsche Telekom Healthcare HEALTHCARE SOLUTIONS

Agenda

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

Was möchte ich heute vorstellen?

- Rechtliche Einordnung von mobilen Anwendungen
- (Einige wenige ausgewählte) Begriffsbestimmungen
- Zweckbestimmung
- Privacy by design/Default
- Betroffenenrechte
- Sicherheit der Verarbeitung
- Verzeichnis der Verarbeitungstätigkeiten
- Spezialfall: DiGA gemäß § 33a SGB V
- Checkliste: Hab ich an alles gedacht?

Grundsätzlicher Hinweis

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

Virtuelle Seminare und Interaktion

Virtuelle Seminare stellen besondere Herausforderungen an die Interaktion miteinander.

Daher ein paar Worte vorab:

- Nach etwa der Hälfte der Zeit gibt es eine kurze Pause
- Einzelne Themenblöcke sind abgetrennt voneinander (Trennfolie mit Überschrift des folgenden Blockes)
- Bitte über Chat Verständnisfrage stellen
  - Nach jedem Block gibt es Zeit, **Verständnisfragen** zu dem gerade besprochenen Block zu stellen
- Grundsätzliche Fragen zum Thema „Mobile Apps“ bitte auch in den Chat
  - Sie werden aber am Ende besprochen

→ Aufgrund der hohen Anzahl Teilnehmer wird es absehbar nicht möglich sein, alle Fragen zu besprechen.

→ Bitte nutzen Sie auch die Mailadresse und kontaktieren Sie mich nach der Veranstaltung per E-Mail

Rechtliche Einordnung

Rechtliche Einordnung …?

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

Apps = Software-Produkt

- Mobile App:= Software für Mobilgeräte beziehungsweise mobile Betriebssysteme
- D.h.: ALLE Regelungen, die für Software gelten, gelten 1:1 auch für mobile Apps

Mobile App = Software

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

Dementsprechend gelten beispielsweise

- Persönlichkeitsrechte
- Urheberrecht
- Vertragsgestaltung
- Ggf. Telekommunikationsrecht
- Telemedienrecht
- Werbung
- Haftungsfragen
- Strafrecht
- Bei „medical Apps“ ggf. Medizinprodukterecht

→ Und natürlich: **Datenschutz** – Unser heutiges Thema

→ Hinweis: Aufgrund der Kürze der Zeit können auch zum Thema Datenschutz nur einige ausgewählte Aspekte vorgestellt werden

(Einige wenige ausgewählte) Begriffsbestimmungen

Begriffsbestimmungen (Art. 4)

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

Art. 4 Ziff. 7: Verantwortlicher

„Verantwortlicher"

- die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,
- die allein oder gemeinsam mit anderen über
- die **Zwecke und Mittel** der
- Verarbeitung von personenbezogenen Daten **entscheidet**

Grundsätzliche Frage im Datenschutz:

- Wer ist Verantwortlicher im Datenschutzrechtlichem Sinne?

→ Der ist verantwortlich für die Einhaltung der datenschutzrechtlichen Vorgaben

Begriffsbestimmungen (Art. 4)

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

Art. 4 Ziff. 1: Personenbezogene Daten (pbD)

"personenbezogene Daten"

- alle Informationen,
- die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen;
- als identifizierbar wird eine natürliche Person angesehen,
- die direkt oder indirekt,
  - insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind,

  identifiziert werden kann;

Begriffsbestimmungen (Art. 4)

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

Art. 4 Ziff. 5: Pseudonymisierung

„Pseudonymisierung"

- **Verarbeitung** personenbezogener Daten in einer Weise, dass die personenbezogenen Daten
- ohne **Hinzuziehung zusätzlicher Informationen**
- nicht mehr einer **spezifischen** betroffenen Person **zugeordnet werden können**,
- **sofern** diese zusätzlichen Informationen
  - **gesondert aufbewahrt** werden und
  - **technischen und organisatorischen Maßnahmen unt**erliegen,
  - die **gewährleisten**, dass
  - die personenbezogenen Daten **nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden**

Begriffsbestimmungen (Art. 4)

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

Art. 4 Ziff. 5: Pseudonymisierung

Folgerungen:

- Pseudonymisierung (und auch Anonymisierung) stellt eine Verarbeitung personenbezogener Daten dar
- Pseudonyme Daten sind personenbezogene Daten
- Für pseudonyme Daten gelten alle Bestimmungen aus dem Datenschutzrecht

Begriffsbestimmungen (Art. 4)

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

Art. 4 Ziff. 2: Verarbeitung

"Verarbeitung"

- jeden
- mit oder ohne Hilfe automatisierter Verfahren
- ausgeführten Vorgang oder
- jede solche Vorgangsreihe
- im Zusammenhang mit personenbezogenen Daten wie
  - das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

} Beispielhafte Aufzählung

Begriffsbestimmungen (Art. 4)

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

Art. 4 Ziff. 15: Gesundheitsdaten

"Gesundheitsdaten"

- personenbezogene Daten, die
- sich auf die körperliche oder geistige Gesundheit einer natürlichen Person,
  - einschließlich der Erbringung von Gesundheitsdienstleistungen,
- beziehen
- und
- aus denen Informationen über deren Gesundheitszustand hervorgehen;

Begriffsbestimmungen (Art. 4)

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

Art. 4 Ziff. 15: Gesundheitsdaten

- Gesundheitsdatum: sehr weit gefasster Begriff
- Umfasst weitaus mehr als nur (Einzel-) Angaben über Erkrankungen
- Alles, was mit dem Gesundheitszustand zu tun hat, wie beispielsweise
  - positive, neutrale oder negative Informationen zum Gesundheitszustand
  - Informationen zum früheren, gegenwärtigen und zukünftigen physischen oder geistigen Gesundheitszustand

  ist davon erfasst
- Beispiele
  - Tatsache, dass jemand ein Patient ist (so sind dementsprechend bspw. auch administrative Daten Gesundheitsdaten)
  - Fitnessdaten wie z.B. Pulsschlag beim Laufen, Gehen usw.

Zweckbestimmung

Zweckbestimmung: Beispiel „Corona-Warn-App“

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

Zweckbestimmung Corona-Warn-App

Zur Erinnerung: Was sollte die Corona-Warn-App leisten?

- Identifizieren, wenn Personen in der Nähe sind
- Festhalten, welche Personen dies sind
- Wenn eine Person an Corona erkrankt
  - → Alle Personen mit Kontakt warnen (Zweck)

Mehr nicht!

Insbesondere nicht:

- Nutzungsstatistiken ermöglichen
- Festhalten, wer wann wo gewesen ist („Hotspot“ Identifizierung)

} Spätere Kritikpunkte

Zweckbestimmung: Beispiel „Corona-Warn-App“

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

Zweckbestimmung Corona-Warn-App

Zweckbestimmung: Beispiel „Corona-Warn-App“

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

Zweckbestimmung Corona-Warn-App

- Am Anfang wurden unzureichende Vorgaben gemacht
  - Pandemie auf Welt keine Neuheiten
    - Hotspot-Identifizierung, Nachverfolgung Ansteckungsverlauf usw.
    - wesentlicher Teil jeder Pandemie-Bekämpfung
  - → Vorgaben RKI von Anfang an unzureichend!
- Entwickler entwickeln entsprechend ihrer Aufgabe
  - Fehlende Funktionenwenn Anforderungen nicht vorhanden Erwartungskonform!
- Suche nach „Schuldigen“ statt Korrekturen
  - Schlagzeilen wie „Politiker fordern Korrekturen“?
  - Politiker legen die Anforderungen an App fest

→ Was kann, was sollte man daraus lernen?

Zweckbestimmung: Beispiel „Corona-Warn-App“

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

Corona-Warn-App: Lessons Learned

- Zweckbestimmung zuvor sehr gut überlegen
- Nachträgliche Änderungen/Anpassungen
  a) schwierig, vielleicht sogar nicht umsetzbar
  b) (meistens) sehr kostenintensiv
- Zweckbestimmung = Welche Daten dürfen überhaupt verarbeitet werden?

Zweckbestimmung: Grundlage jeder Verarbeitung pbD

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

Art. 5 Abs. 1 lit. b, c sowie Abs. 2 DS-GVO

Art. 5 DS-GVO

1. Personenbezogene Daten müssen
   b) für **festgelegte, eindeutige und legitime Zwecke erhoben** werden und **dürfen nicht** in einer mit diesen Zwecken **nicht zu vereinbarenden Weise weiterverarbeitet werden** […] ("Zweckbindung");
   c) dem Zweck angemessen und erheblich sowie **auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein** ("Datenminimierung");
2. Der Verantwortliche ist für die **Einhaltung** des Absatzes 1 **verantwortlich** und muss dessen **Einhaltung nachweisen können** ("Rechenschaftspflicht").

Zweckbestimmung: Grundlage jeder Verarbeitung pbD

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

Zweckbestimmung: Auch an Geschäftsmodell denken!

- Personenbezogene Daten dürfen
  - nur im erforderlichen Umfang
  - nur zu festgelegten Zwecken

  verarbeitet werden

→ Womit wird die App finanziert?
  - Staatlich finanziert?
  - Gesetzliche Krankenversicherung?
  - Anwender zahlt?
  - Werbung?
  - Durch personenbezogene Daten („Handel mit Daten“)?

→ Zweckbestimmung muss Verarbeitung auch hinsichtlich Geschäftsmodell beinhalten

Zweckbestimmung: Geschäftsmodelle beachten

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

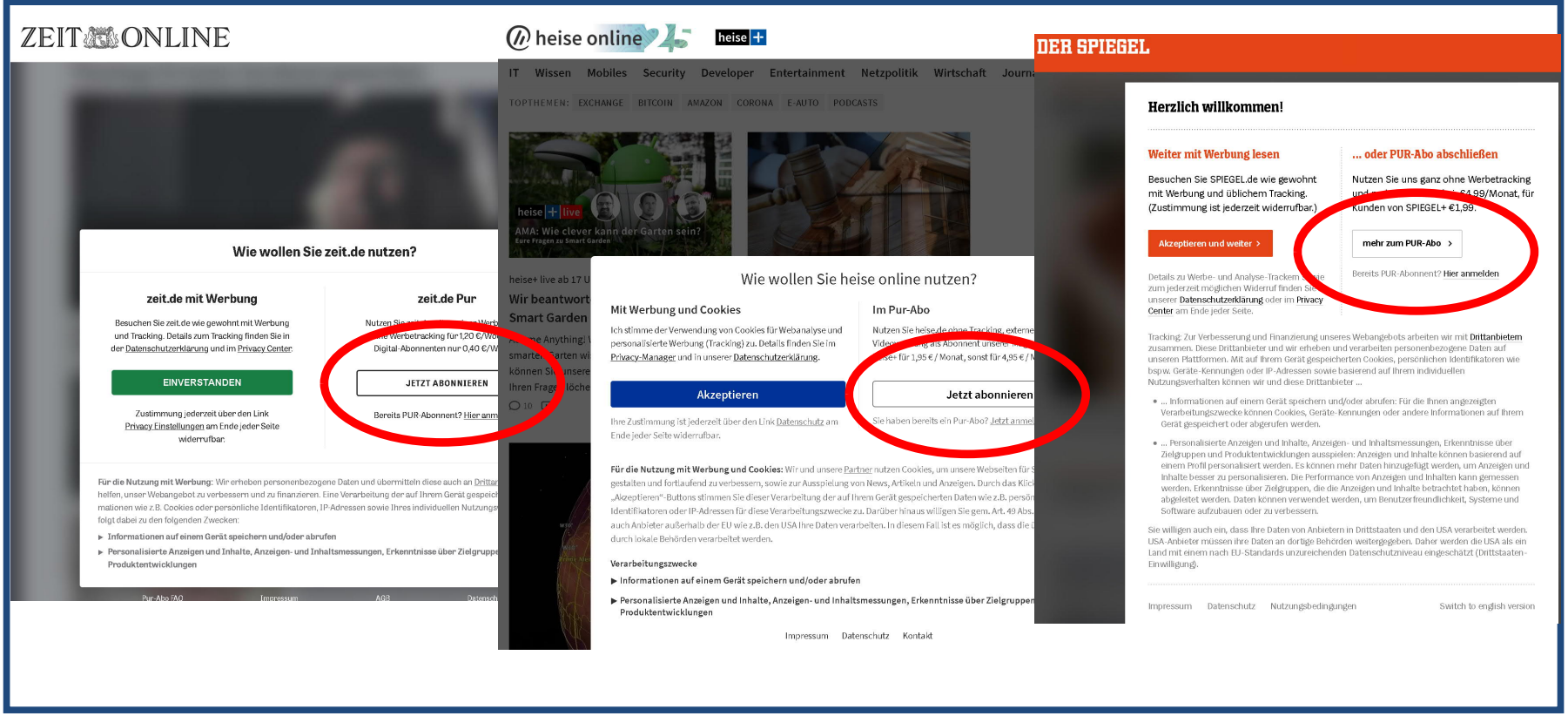
Geschäftsmodell: Beispiel Werbefinanzierung

- Werbefinanzierte Apps legal?
- Ja, aber…
  - Verarbeitung personenbezogener Daten beruht auf Einwilligung
  - Einwilligung muss freiwillig erteilt werden
  - Herausforderung: Werbung für eigentliche Verarbeitung nicht erforderlich
  - Freiwillig: „Echte“ Alternative muss vorhanden sein
  - → In diesen Fällen App immer auch als Bezahlmodell anbieten
  - → Wie beispielsweise verschiedene Online-Zeitschriften

Zweckbestimmung: Geschäftsmodelle beachten

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

Geschäftsmodell: Beispiel Werbefinanzierung – Online-Zeitschriften



Zweckbestimmung: Geschäftsmodelle beachten

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

Geschäftsmodell: Beispiel Forschung

- App erhebt Daten zur Forschung
- Grundlage „Handel mit Daten“
- Ja, aber…
  - Daten sind für App und Forschung gleichermaßen erforderlich
  - Verarbeitung personenbezogener Daten beruht auf Einwilligung
  - Herausforderung: Bei Widerruf Einwilligung Weiterverarbeitung unzulässig, Daten müssen gelöscht werden
- Rahmenbedingungen
  - Forschung: Pseudonyme Daten, App: Personenbeziehbare Daten
  - → Bei Widerruf: Löschung App auf Smartphone/Tablet = Zuordungsvorschrift gelöscht
  - → Folge: Daten anonym, Daten können anonym für Forschung weiter genutzt werden

Zweckbestimmung: Geschäftsmodelle beachten

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

Geschäftsmodell: Beispiel Forschung – App für Diabetiker

- Beispiel: App für Diabetiker
  - Erfasst, was wann zu welchem Zeitpunkt gegessen, getrunken wird
  - Diabetiker
    - Erfasst Daten per Eingabe (was wann zu sich genommen wurde; keine Standortdaten!)
    - Gibt zusätzlich Kalorien an
    - Macht Foto von Nahrung
    - Bei Messung Blutzucker: ebenfalls dokumentiert
- Zweckbestimmung
  1. Diabetiker-Tagebuch
  2. Entwicklung eines KI-gestützten Tools zur Ermittlung der Kalorienzahl basierend auf Fotografien von Nahrungsmitteln
  3. Entwicklung eines KI-gestützten Tools zur Ermittlung zur Abschätzung der Zunahme bestimmter Nahrungsmittel auf den Verlauf des Blutzuckerwertes

Zweckbestimmung: Geschäftsmodelle beachten

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

Geschäftsmodell: Beispiel Forschung – App für Diabetiker

- Beispiel: App für Diabetiker
- Grundlage:
  - Diabetiker/-in bekommt App, wenn sie ihre pseudonymen Daten zur Forschung bereitstellt
  - Pseudonym: Nachfolgende Daten müssen zuordenbar sein, da Nahrungszunahme und Auswirkung auf den Blutzucker abhängig von Person ist
  - Zuordnung Person-Daten nur auf mobilen Gerät möglich
    - ➢ Für Forschung genaue Person uninteressant
  - Für Dauer der Nutzung „zahlt“ Anwender mit Daten: dies wird Anwendern transparent dargestellt
    - ➢ Vertrag, z.B. in Form AGB

Zweckbestimmung: Geschäftsmodelle beachten

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

Geschäftsmodell: Beispiel Forschung – App für Diabetiker

- Beispiel: App für Diabetiker
- Bei Widerruf:
  - App wird auf mobilen Gerät gelöscht
    - Zuordnungsvorschrift gelöscht
    - Für niemanden auf der Welt ist Zuordnung zu einer „spezifischen betroffenen Person“ möglich → Keine pseudonymen Daten mehr
  - Folge
    - Daten bei Forschern sind anonyme Daten
    - Löschung der Daten durch Anonymisierung erfolgt
  - Hinweis
    - „Nette“ Forscher ermöglichen vor Löschung App Export der Daten für Anwender

Privacy by Design/Default

Privacy by Design/Default

Art. 25 DS-GVO

Art. 25

- Unter **Berücksichtigung** des
- **Stands der Technik**, der Implementierungskosten und der
- Art, des Umfangs, der Umstände und der **Zwecke der Verarbeitung** sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die
- **Rechte und Freiheiten natürlicher Personen**
- trifft der Verantwortliche sowohl
- zum **Zeitpunkt der Festlegung** der Mittel für die Verarbeitung als auch
- zum **Zeitpunkt der eigentlichen Verarbeitung**
- **geeignete** technische und organisatorische Maßnahmen
- die dafür ausgelegt sind, die **Datenschutzgrundsätze wirksam umzusetzen** und
- die notwendigen **Garantien** in die Verarbeitung aufzunehmen

Privacy by Design/Default

Art. 25 DS-GVO

- Zeitpunkt der Festlegung:
  Vor Beginn der Verarbeitung = schon bei Planung
- Zeitpunkt der eigentlichen Verarbeitung:
  Für den gesamten Lebenszyklus der Daten = Erhebung bis Löschung
- geeignete technische und organisatorische Maßnahmen
  - Datenschutzgrundsätze wirksam umzusetzen = Art. 5 DS-GVO muss umgesetzt werden
  - Garantien in die Verarbeitung aufzunehmen
    - Einhaltung der Anforderungen der DS-GVO muss garantiert werden
    - Rechte der betroffenen Personen müssen garantiert werden

Privacy by Design/Default

Art. 25 DS-GVO: Anforderungen Art. 5 DS-GVO müssen umgesetzt werden

- Privacy by Default:= Datenschutz per „Voreinstellung“
- Zielsetzung
  - Zu beachten: Datenschutz ist ein wesentlicher Bestandteil des Systems, ohne Abstriche bei der Funktionalität
  - Einzelperson muss nichts für den Schutz leisten
  - Schutz ist systemimmanent als Standardeinstellung vorhanden
  - → Einzelperson kann entsprechend eigenem Wunsch den Schutz verringern
    - ➢ Keine „Bevormundung“ betroffener Personen
    - ➢ Kein „Zwang“ zu Datenschutz
  - → Interessen der betroffenen Person stehen immer an erster Stelle
    - ➢ Aber: Einhaltung rechtlicher Vorgaben (z.B. Drittstaatentransfer) müssen natürlich eingehalten werden

Privacy by Design
Beispiel: Luca-App

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

Privacy by Design: **Kompetentes** Team zwingend erforderlich…

Corona-Nachverfolgung

Luca-App – neue Mängel und immer noch intransparent

heise online

IT Wissen Mobiles Security Developer Entertainment Netzpolitik

TOPTHEMEN: EXCHANGE BITCOIN AMAZON CORONA E-AUTO PODCASTS

heise online ⟩ News ⟩ 04/2021 ⟩ Luca first, Bedenken second: Pandemiebekämpfung mit lückenhaf

Luca first, Bedenken second: Pandemiebekämpfung mit lückenhafter Software

Süddeutsche Zei

SZ.de Zeitung Magazi

Meinung Panorama Sport München Bayern

App: Das Problem mit den Schlüsselanhängern

RT DE Aktuell Viral Meinung Videos Karriere

Hauptseite / Coronavirus

Kritik an der Luca-App: Chaos Computer Club kritisiert Verfahren und Finanzierung aus Ste

heise online

IT Wissen Mobiles Security Developer Entertainment Netzpolitik

TOPTHEMEN: EXCHANGE BITCOIN AMAZON CORONA E-AUTO PODCASTS

heise online ⟩ News ⟩ 04/2021 ⟩ Sicherheitsforscher: Risiken der Luca-App "völlig unverhältnismäßig"

Sicherheitsforscher: Risiken der Luca-App "völlig unverhältnismäßig"

70 Sicherheitsforschende haben eine gemeinsame Stellungnahme veröffentlicht, in der sie der Luca-App weder Nutzen noch Sicherheit zusprechen.

taz

POLITIK ÖKO GESELLSCHAFT KULTUR SPORT BERLIN

Streit um Luca-App in Berlin

Sicher ist anders

Stundenlang befragen Abgeordnete den Senat, Datenschützer, Entwickler

13. April 2021, 22:42 Uhr Check-in-App gegen Corona

"Luca" und das Problem mit Schlüsselanhängern

14.04.2021, 12:05 Uhr

Bewegungsdaten von Luca-Usern abrufbar - CCC fordert "Notbremse"

Wer kein Smartphone hat, kann d

Doch diese Lösung birgt laut Expe

Nutzer. Der CCC fordert derweil ei

Corona-Kontaktnachverfolgung

Schwere Sicherheitsmängel bei Luca-App

14. April 2021, 09:44 Uhr | dpa | Kommentar(e)

heise online

IT Wissen Mobiles Security Developer Entertainment Netzp

TOPTHEMEN: EXCHANGE BITCOIN AMAZON CORONA E-AUTO PODCASTS

heise online ⟩ News ⟩ 04/2021 ⟩ Corona-Tracking: Luca-Überwachung lässt sich mit Fake-Daten

Corona-Tracking: Luca-Überwachung lässt sich mit Fake-Datenmüll aushebeln

home

Club

CCC Regional

2021-04-13 21:04:42, linus

Privacy by Design
Beispiel: Luca-App

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

Luca-App: Lessons Learned

- Schwachstellen
  - Zentrale Speicherung:
    - Gesteigerte Motivation für Angreifer
    - Bei Kompromittierung alle Daten auf einmal zugreifbar
  - Verschlüsselungskonzept
    - Alle Gesundheitsämter haben einen Schlüssel
  - …
- Einsatz von Software Development Kits zur Verschlüsselung reichen nicht
  - Technik alleine unzureichend
  - Sicherheitskonzept erforderlich
- Vermutung: Mit Beteiligung entsprechender Experten zur IT-Sicherheit hätten die „Anfänger“-Fehler vermieden werden können

Privacy by Design

Umsetzung Privacy by Design

1. Team bilden
   - Projektleiter
   - Anforderungsanalyst
   - Entwickler
   - IT-Sicherheits-Experte
     (mit sehr guten Kenntnissen in Kryptographie)
   - Datenschutz-Experte
   - Usability Experte
     (idealerweise spezialisiert auf Mobile Devices)
   - Jurist
     (sollte auch Medizinprodukterecht abdecken)
   - (Anwender)

Privacy by Design

Umsetzung Privacy by Design

2. Aus „Zweck“ bzw. Zwecken erforderliche Daten ableiten
   - Keine Legaldefinition in DS-GVO oder BDSG
   - Verarbeitung insbesondere erforderlich, wenn
     - der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann (Erwägungsgrund 39) oder
     - der Zweck der Verarbeitung im lebenswichtigen Interesse der betroffenen Person liegt (Erwägungsgrund 112)
   - → Erforderlich:= Verarbeitung ist ohne diese Daten **nicht möglich**

Privacy by Design

Umsetzung Privacy by Design

3. Methode der Verarbeitung beschreiben/festlegen („wie erfolgt Verarbeitung“)
   - Verarbeitung muss zur Erreichung des Zweckes erforderlich sein
   - Verarbeitung erforderlich:
     - Verarbeitung muss geeignet sein, den Zweck zu erreichen
     - Es gibt kein milderes (= in die Rechte Betroffener weniger eingreifendes) Mittel, welches den gleichen Erfolg mit vergleichbarem Aufwand erzielt.
   - Beantwortung von drei Fragen zur Bestimmung, welche Verarbeitung „mildestes“ Mittel ist:
     - Gibt es überhaupt ein anderes Mittel?
     - Ist dieses in gleicher Weise geeignet, den Zweck zu erreichen?
     - Ist dieses Mittel ein milderes, also die Rechte der betroffenen Person weniger belastendes Mittel?

     Cave: Ist ein anderes Mittel finanziell unattraktiver, ist dies kein Ausschlusskriterium!

Privacy by Design

Umsetzung Privacy by Design

4. Aus Bestimmung Daten und Verarbeitungsmethode folgt
   - Beschränkung der Datenmenge
   - Beschränkung Art und Umfang der Verarbeitung
   - Beschränkung der Speicherfristen
   - Beschränkung der Zugänglichkeit

Maximum=
Zweck muss damit erreicht werden können
(Maximum=Minimum)

Privacy by Design

Umsetzung Privacy by Design

5. Festlegung, wie Betroffenenrechte gewährleistet werden
   - Transparenzvorgaben (Art. 12): Informationen müssen präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache gegeben werden
   - Informationspflichten (Artt. 13, 14)
   - Recht aus Auskunft (Art. 15)
   - Recht auf Kopie der Daten (Art. 15)
   - Recht auf Berichtigung (Art. 16)
   - Recht auf Löschung (Art. 17)
   - Recht auf Einschränkung der Verarbeitung (Art. 18)
   - Recht auf Datenübertragbarkeit (Art. 20)
   - Widerspruchsrecht (Art. 21)
   - Keine (ausschließliche) automatisierte Entscheidungen im Einzelfall einschließlich Profiling
   - Recht auf Beschwerde bei Aufsichtsbehörde

Privacy by Design

Umsetzung Privacy by Design

6. Risiko für „Rechte und Freiheiten der betroffenen Person ermitteln
   - ErwGr. 75 DS-GVO:
     Zu welchem physischen, materiellen oder immateriellen Schaden könnte die Verarbeitung der personenbezogenen Daten führen?
     - Beispiele aus ErwGr. 75: Diskriminierung, Identitätsdiebstahl oder -betrug, finanzieller Verlust, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, unbefugte Aufhebung der Pseudonymisierung
   - Voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen:
     - Datenschutz-Folgenabschätzung
     - (Auch an die anderen Vorgaben insbesondere an nationale Vorgaben denken)
   - Maßnahmen zum Schutz entsprechend Risikoanalyse erforderlich
     - Risiko muss soweit gesenkt werden, dass maximal ein Risiko des täglichen Lebens* verbleibt

* Bzgl. Lebensrisiko siehe auch: BGH Urt. V. 1993-05-04, AZ VI ZR 283/92. Online, zitiert am 2021-04-28; Verfügbar unter https://dejure.org/1993,1128

Privacy by Design

Umsetzung Privacy by Design

7. Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung festlegen
   - Grundsätzlich: Art. 32 DS-GVO muss eingehalten werden (dazu später mehr)
   - Weiterhin denken an
     - Rollen- und Berechtigungskonzept
     - Protokollierungskonzept (an Anforderungen von § 22 Abs. 2 BDSG denken)
     - Archivierungs- und Löschkonzept
     - Datenschutzkonzept
     - IT-Sicherheitskonzept

Privacy by Design

Umsetzung Privacy by Design

8. Verarbeitung in Drittstaaten
   - Mobile Apps laufen typischerweise auf iOS oder Android
   - Hersteller von Android und iOS haben Zugriff auf Gerät
   - EuGH Schrems II Urteil zu Drittstaatenverarbeitung beachten
     - Personenbezogene Daten müssen vor Zugriff durch Hersteller Google oder Apple geschützt werden
     - Insbesondere Gesundheitsdaten
   - Bei „Digitalen Gesundheitsanwendungen“ (DiGA) nach § 33a SGB V daran denken
     - § 4 Abs. 3 DiGAV: Nur zulässig, wenn Angemessenheitsbeschluss der EU Kommission nach Art. 45 DS-GVO vorliegt; für USA liegt keiner vor
     - Kommentierung siehe https://www.reuschlaw.de/news/apps-auf-rezept-neue-informationen-zur-datenuebermittlung-in-die-usa/

Privacy by Design

Umsetzung Privacy by Design

9. Prozess zum Umgang mit Datenpannen festlegen
   - Meldung von Datenpannen (intern) und Dokumentation
     - Cave: Alle Datenpannen müssen dokumentiert werden (Art. 33 Abs. 5 DS-GVO(
   - Definition Datenpanne: (siehe Art. 4 Ziff. 12 DS-GVO)
     - Ereignis, welches
     - unbeabsichtigt oder unrechtmäßig,
     - zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt
   - Datenpanne z.B.: jemand, der auf personenbezogene Daten ohne Erfordernis zugreift
   - Prozess zur Meldung an Datenschutzaufsicht (Art. 33) und betroffene Personen (Art. 43) festlegen
     - Wer meldet an wen?
     - Wer unterstützt, liefert Informationen?...

Privacy by Default

Umsetzung Privacy by Default

Anforderungen Art. 5 DS-GVO müssen umgesetzt werden

- Abs. 1
  - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz Rechtsgrundlage (Artt. 6-11), Rechte der betroffenen Person“ (Artt. 12-23), Drittlandverarbeitung (Artt. 44-49)
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit (Art. 25, 32)
  - Speicherbegrenzung (Art. 25, 32)
  - Integrität und Vertraulichkeit (Artt. 25, 32 bis 39)
- Abs. 2: Einhaltung Art. 5 Abs. 1 muss nachgewiesen werden

Betroffenenrechte

Gewährleistung Betroffenenrechte

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

Betroffenenrechte müssen gewährleistet werden, d.h. …

- Transparenzvorgaben (Art. 12): Informationen müssen präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache gegeben werden

Gewährleistung Betroffenenrechte

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

Betroffenenrechte müssen gewährleistet werden, d.h. …

- Art. 12 DS-GVO: Informationen müssen
  - präziser,
  - transparenter,
  - verständlicher und
  - leicht zugänglicher Form in einer
  - klaren und einfachen Sprache
  - und kostenlos
  - gegeben werden.
- Vorgaben von Art. 12 gelten für **alle** in Artt. 13-22 genannten Betroffenenrechte

Gewährleistung Betroffenenrechte

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

Betroffenenrechte müssen gewährleistet werden, d.h. …

- Transparenzvorgaben (Art. 12): Informationen müssen präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache gegeben werden
- Informationspflichten (Artt. 13, 14):

Informationspflichten: Artt. 13, 14 DS-GVO

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

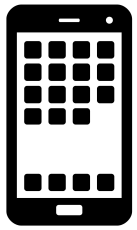
Informationspflicht	Art. 13	Art. 14
Kontaktdaten Verantwortlicher	Abs. 1	Abs. 1
Kontaktdaten Datenschutzbeauftragter	Abs. 1	Abs. 1
Zwecke Verarbeitung	Abs. 1	Abs. 1
Rechtsgrundlage Verarbeitung	Abs. 1	Abs. 1
Kategorien der Daten	-	Abs. 1
Empfänger der Daten	Abs. 1	Abs. 1
Drittstaatentransfer	Abs. 1	Abs. 1
Speicherdauer	Abs. 2	Abs. 2
Information bzgl. Betroffenenrechte	Abs. 2	Abs. 2
Widerruf Einwilligung	Abs. 2	Abs. 2
Einzelfallentscheidung	Abs. 2	Abs. 2
Angabe Quelle	-	Abs. 2

Informationspflichten: Artt. 13, 14 DS-GVO

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

Bei Mobile Apps: in der Regel „Direkterhebung“, also Art 13

- Im Rahmen von Mobile Apps
  - Regelhaft Direkterhebung: Apps werden direkt bei der betroffenen Person erhoben
  - Cave: Gerade im medizinischen Kontext werden ggf. via Fragen Daten über Dritte erhoben
    Beispiel: Hält Ihr Lebensabschnittgefährte sie für cholerisch und alkoholsüchtig?
- „Herausforderung“
  - Menge an bereitzustellen Informationen ggf. umfangreich
  - Begrenzter Platz zur Darstellung der Informationen



Informationspflichten: Artt. 13, 14 DS-GVO

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

Umgang mit Informationspflichten bei Mobile Apps: Herausforderung Platz

- Artikel29-Datenschutzgruppe: WP 260 rev. 01
  - Leitlinien für Transparenz gemäß der Verordnung 2016/679
  - Zuletzt überarbeitet und von EDSA angenommen am 11. April 2018
  - https://edpb.europa.eu/endorsed-wp29-guidelines_de
- Somit „offizielle“ Empfehlung des EDSA zum Umgang mit Betroffenenrechte

Informationspflichten: Artt. 13, 14 DS-GVO

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

Aussagen EDSA in WP 260 rev. 01 der Art.-29-Datenschutzgruppe

- Rn. 33: „[…] Verantwortliche selbst aktiv werden muss, um der betroffenen Person die Information bereitzustellen oder sie aktiv zu der Stelle zu leiten, wo die Angaben zur Verfügung stehen […]“
- Rn. 35: „Angesichts der Menge an Informationen, die der betroffenen Person übermittelt werden müssen, kann von den Verantwortlichen im digitalen Bereich ein Mehrebenen-Ansatz verfolgt werden […]“
- Rn. 35: „[…] zu beachten, dass es sich bei Mehrebenen-Datenschutzerklärungen / -hinweisen nicht bloß um verschachtelte Seiten handelt, die erst über mehrere Klicks zu den maßgeblichen Informationen führen […]“

Informationspflichten: Artt. 13, 14 DS-GVO

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

Aussagen EDSA in WP 260 rev. 01 der Art.-29-Datenschutzgruppe

- Rn. 35: „Die Gestaltung und Gliederung der ersten Ebene der Datenschutzerklärungen / -hinweise sollten der betroffenen Person einen klaren Überblick über die ihr hinsichtlich der Verarbeitung ihrer personenbezogenen Daten zur Verfügung stehenden Informationen liefen und aufzeigen, wo / wie sie die einzelnen Informationen auf den jeweiligen Ebenen der Datenschutzerklärungen / -hinweise finden kann […]“
- Rn. 35: „[…] wichtig, dass die auf den verschiedenen Ebenen eines Mehrebenen-Hinweises enthaltenen Informationen konsistent sind und sich nicht in widersprüchlicher Weise von Ebene zu Ebene unterscheiden.“

Informationspflichten: Artt. 13, 14 DS-GVO

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

Umgang mit Informationspflichten bei Mobile Apps: Herausforderung Platz

- Möglichkeit des Mehrschichten-Ansatzes berücksichtigen*
  - Auf der ersten Stufe müssen immer die Informationen zur Identität des Verantwortlichen und zu den Zwecken der Verarbeitung gegeben werden.
  - Auf zweiter Stufe müssen dann alle Informationen nach Art. 13 bzw. 14 DS-GVO für die betroffene Person erhältlich sein bzw. gegeben werden.
  - Dies kann bspw. per Link zu der entsprechenden Website erfolgen, auf der alle Informationen vorgehalten werden.
  - Möglich ist auch das Bereithalten eines dementsprechenden Informationsblattes, das jederzeit ausgehändigt bzw. übergeben oder zugesandt werden kann.
- Aber beachten: Informationspflichten von Art. 13 DS-GVO muss **vor Beginn der Verarbeitung** oder **spätestens zum Zeitpunkt der Erhebung** genügt werden

* Bayerisches Landesamt für Datenschutzaufsicht: Informationspflichten. Online, zitiert am 2021-04-28; Verfügbar unter https://www.lda.bayern.de/de/thema_informationspflichten.html

Gewährleistung Betroffenenrechte

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

Betroffenenrechte müssen gewährleistet werden, d.h. …

- Transparenzvorgaben (Art. 12): Informationen müssen präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache gegeben werden
- Informationspflichten (Artt. 13, 14)
- Recht aus Auskunft (Art. 15)
- Recht auf Kopie der Daten (Art. 15)
- Recht auf Berichtigung (Art. 16)
- Recht auf Löschung (Art. 17)
- Recht auf Einschränkung der Verarbeitung (Art. 18)
- Recht auf Datenübertragbarkeit (Art. 20)
- Widerspruchsrecht (Art. 21)
- Keine (ausschließliche) automatisierte Entscheidungen im Einzelfall einschließlich Profiling
- Recht auf Beschwerde bei Aufsichtsbehörde

Gewährleistung Betroffenenrechte

Beispiel für Umsetzung Betroffenenanfragen

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

Prozess als PDCA-Zyklus etablieren

- Plan
  Planung der Verarbeitung inkl. Risikomanagement
- Do
  Umsetzung geeigneter technisch-organisatorischer Maßnahmen
- Check
  Überwachung/Monitoring der Maßnahmen hinsichtlich der Wirksamkeit bzgl. der Risiken (inkl. Ggf. neu aufgetretener Risiken)
- Act
  Anpassung/Aktualisierung Maßnahmen

Gewährleistung Betroffenenrechte

Beispiel für Umsetzung Betroffenenanfragen

Prozess als PDCA-Zyklus etablieren

- Prozessbeschreibung inkl. Verfahrens-/Arbeitsanweisungen
- Regelmäßige Prüfung der Prozesse sowie Dokumentation der Prüfungsergebnisse
- Dokumente Reaktion auf bei Prüfungen festgestellte Abweichungen

Gewährleistung Betroffenenrechte

Beispiel für Umsetzung Betroffenenanfragen

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

Erforderlich: Etablierung strukturierter Prozesse

1 Annahme einer Anfrage

- Darstellung, *wo* Anfragen im Unternehmen eingehen können
  - Identifizierung der „Entry-Points“ wie Telefonzentrale, Kontaktformular Internet, E-Mail-Kommunikationsadressen des Unternehmens, z. B. Impressum, …
- Schulung der die Anfragen entgegennehmenden Personen
  - Welche Informationen müssen erfragt werden?
  - An wen wird die Anfrage weitergeleitet?

Gewährleistung Betroffenenrechte

Beispiel für Umsetzung Betroffenenanfragen

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

Erforderlich: Etablierung strukturierter Prozesse

2 Umgang mit einer Anfrage

2.1 Eingangsprüfung

- Überprüfung, ob es sich tatsächlich um eine datenschutzrechtliche Anfrage handelt
- Erfassung der Anfrage in einem geeigneten Dokumentationssystem
- Überprüfung, worum es sich handelt (Auskunftsersuchen, Korrekturanfrage, Löschungsersuchen, …)
- Versendung einer Eingangsbestätigung an den Antragssteller
- Prüfung der Identität des Antragsstellers
- Prüfung, ob
  - unbegründete Antrag i.S.v. Art. 12 Abs. 5 DS-GVO
  - exzessiven Anträgen einer betroffenen Person vorliegen
- Kann Antrag nicht sofort bearbeitet werden: Information betroffene Person ohne Verzögerung

Gewährleistung Betroffenenrechte

Beispiel für Umsetzung Betroffenenanfragen

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

Erforderlich: Etablierung strukturierter Prozesse

2 Umgang mit einer Anfrage

2.2 Inhaltliche Prüfung

- Prüfung, ob personenbezogene Daten der betroffenen Person verarbeitet werden/wurden
- Wenn keine Daten vorhanden sind:
  Negativmitteilung an den Betroffenen versenden !
- Wenn Daten vorhanden sind: Abarbeiten

Gewährleistung Betroffenenrechte

Beispiel für Umsetzung Betroffenenanfragen

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

Erforderlich: Etablierung strukturierter Prozesse

2 Umgang mit einer Anfrage

2.3 Beantwortung

- Auskunftsersuchen:
  - Zusammenstellung
  - Unverzügliche Beantwortung
    a) Innerhalb eines Monats
    b) Wenn auf Grund Komplexität nicht innerhalb von einem Monat möglich
       - Innerhalb von 3 Monaten nach Antragstellung zwingend umzusetzen
       - Person muss innerhalb der ersten Monats über Verzögerung informiert werden
  - Beachten: Elektronische Antragstellung = Unterrichtung auch elektronisch, wenn betroffene Person nichts anderes verlangt
- Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit
  - Weiterleitung an entsprechende Stellen zwecks Umsetzung
  - Sobald Umsetzung erfolgt → Information betroffene Person (siehe Auskunftsersuchen)

Gewährleistung Betroffenenrechte

Beispiel für Umsetzung Betroffenenanfragen

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

Erforderlich: Etablierung strukturierter Prozesse

2 Umgang mit einer Anfrage

2.3 Beantwortung

- Widerspruch Verarbeitung, Widerruf einer Einwilligung
  - Information der Stelle, welche
    a) die Verarbeitung (z.B. Forschung) durchführt
    b) die Einwilligung erhob
  - Verarbeitung einstellen
  - Prüfen, ob Daten gelöscht werden müssen (Art. 17 Abs. 1 lit. b, c DS-GVO)
  - Information betroffene Person über erfolgte Maßnahmen, ggf. auch über Löschung
    (siehe Auskunftsersuchen)

Sicherheit der Verarbeitung

Sicherheit der Verarbeitung

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

Anforderungen Art. 32 DS-GVO

Treffen geeigneter technisch-organisatorische Maßnahmen (Art. 32 Abs. 1)

- um ein dem Risiko angemessenes Schutzniveau zu gewährleisten
- unter Berücksichtigung (Art. 32 Abs. 1)
  - des Stands der Technik
  - der Implementierungskosten
  - der Art, Umfang, Umstände und Zwecke
  - der Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen

Sicherheit der Verarbeitung

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

Art. 32 DS-GVO fordert „angemessene“ Maßnahmen

- Die Beurteilung der Angemessenheit ist eine Abwägung beinhaltend
  - Stand der Technik
  - Implementierungskosten
  - Art, Umfang, Umstände und Zwecke der Verarbeitung
  - Eintrittswahrscheinlichkeit
  - Schwere des Risikos für die persönlichen Rechte und Freiheiten

Sicherheit der Verarbeitung

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

Mobile Apps müssen Sicherheit der Verarbeitung gemäß Art. 32 gewährleisten

Insbesondere heißt dies

- Privacy by Design/Default
- Maßnahmen u.a.
  - Pseudonymisierung
  - Verschlüsselung
- Gewährleistung von
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Belastbarkeit/Ausfallsicherheit
  - Wiederherstellbarkeit
  - Notfallmanagement
- Verfahren
  - Überprüfbarkeit
  - Bewertung
  - Evaluierung

Unter Berücksichtigung

→ Stand der Technik
→ Implementierungskosten
→ Art, Umfang, Umstände und Zwecke der Verarbeitung
→ Risiko der Verarbeitung

Sicherheit der Verarbeitung

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

Technisch-organisatorische Maßnahmen (TOM)

Diese Maßnahmen schließen u.a. Folgendes ein:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- […]

→ D.h. Pseudonymisierung und Verschlüsselung gefordert

→ Begründung erforderlich, wenn darauf verzichtet wird

Sicherheit der Verarbeitung

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

Technisch-organisatorische Maßnahmen (TOM)

Diese Maßnahmen schließen u.a. Folgendes ein:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer **sicherzustellen**;
- die Fähigkeit, die **Verfügbarkeit** der Daten und den **Zugang** zu ihnen bei einem physischen oder technischen Zwischenfall **rasch wiederherzustellen**;
- ein Verfahren zur **regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit** der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Sicherheit der Verarbeitung Cloud

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

Speicherort der Daten

„[…] speichern wir die Daten verschlüsselt in der Cloud, so dass ein Backup immer vorhanden ist […]“

Frage 1: Verschlüsselte Daten – anonym oder pseudonym?

- Artikel-29-Gruppe zu RL 95/46
  - Verschlüsselte Daten können als anonym angesehen werden, wenn
    a) Der Schlüssel vernichtet wurde und
    b) eine Entschlüsselung der Daten in absehbar endlicher Zeit nicht möglich ist.
  - Backup: Daten können und sollen bei Bedarf entschlüsselt werden. Also pseudonym?
- Pseudonyme Daten: Anwendungsbereich der DS-GVO gegeben

Frage 2: Welche Cloud von wem und vor allem wo?

Sicherheit der Verarbeitung: Cloud Computing

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

Speicherort der Daten: Die „Cloud“

Dienst	Standort (Mutter-) Unternehmen
1. Apple iCloud	1. Apple, USA
2. Amazon Cloud Drive	2. Amazon, USA
3. Dropbox	3. Dropbox, USA
4. Google Drive	4. Google, USA
5. HiDrive	5. Strato, Deutschland
6. luckycloud	6. Luckycloud, Deutschland
7. LeitzCloud	7. LeitzCloud, Deutschland
8. Mega	8. Mega, USA
9. Microsoft OneDrive	9. Microsoft, USA
10. pCloud	10. pCloud, Schweiz
11. Your Secure Cloud	11. Your Secure Cloud, Deutschland
12. Telekom MagentaCLOUD	12. Telekom, Deutschland

Sicherheit der Verarbeitung: Cloud Computing

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

- **Preiswerter Cloud-Speicher der „üblichen Verdächtigen“**
  - **Anbieter mit Sitz in USA:**
    Auch bei Speicherort „Europa“ Zugriff durch Anbieter möglich
- **Entsprechend EuGH Schrems II-Urteil: EU- Datenschutz muss „gewährleistet werden“**
- **D.h. Voraussetzungen für Drittland-Verarbeitung müssen eingehalten werden, z.B.**
  - **Binding Corporate Rules**
  - **Standardvertragsklauseln der EU Kommission**
  - **Genehmigung durch die zuständige Aufsichtsbehörde**

  Und je nach Rechtslage ergänzt durch Maßnahmen wie Verschlüsselung, Anonymisierung oder Pseudonymisierung

Sicherheit der Verarbeitung: Vorgehen…

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

Technisch-organisatorische Maßnahmen (TOM)

- Risikoevaluierung und –beurteilung
- Darstellung eines Maßnahmenkatalogs
- (Interne) Audits inkl. Managementbewertung
- Verfahren zur Korrektur/Anpassung von ergriffenen Maßnahmen („PDCA-Zyklus“)
- Managementsystem inkl.
  - Datenschutzkonzept
  - IT-Sicherheitskonzept
  - Rollen- und Berechtigungskonzept
  - Protokollierungskonzept
  - Löschkonzept
  - …

Technisch-organisatorische Maßnahmen (TOM)

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

Darstellung eines Maßnahmenkatalog für Apps, z.B.

Authentifizierung

- Die Applikation muss mit unprivilegierten Benutzerrechten auskommen, um auf dem Endgerät lauffähig zu sein.
- Falls ein dauerhaftes Login benötigt wird, dann sichere Mechanismen verwendet werden. Zur zeit bspw. OAuth-2.0-Refresh-Token.
- Falls eine App die Möglichkeit bietet, ein Login dauerhaft zu speichern, so muss diese Option für den Benutzer an- und abwählbar sein.
- Das System muss Benutzern ermöglichen sich von ihrer Sitzung abzumelden und die Applikation zu beenden.
- …

Kommunikation

- Falls SSL/TLS-Server-Zertifikate verwendet werden, müssen diese von einer App auf Gültigkeit und Revocation-Status überprüft werden. Bei Ungültigkeit oder Verbindungs-Timeout zum Revocation- oder OCSP-Server, muss der Verbindungsaufbau abgebrochen und der Benutzer informiert werden.
- Falls ein SSL/TLS-Server-Zertifikat verwendet wird und dieses als ungültig erkannt wurde, so muss die Verbindung unterbrochen werden.
- …

Technisch-organisatorische Maßnahmen (TOM)

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

Darstellung eines Maßnahmenkatalog für Apps, z.B.

Vorschläge hinsichtlich zu treffender IT-Sicherheitsmaßnahmen
(„Rad nicht neu erfinden“)

- Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kataloge. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
- Deutsche Telekom: Privacy and Security Assessment Verfahren – Technische Sicherheitsanforderungen https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/sicherheit/privacy-and-security-assessment-verfahren-342724
- National Institute of Standards and Technology (NIST): Special Publications (SP) http://csrc.nist.gov/publications/PubsSPs.html

Verzeichnis der Verarbeitungstätigkeiten

Art. 30: „Verzeichnis von Verarbeitungstätigkeiten“

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

Ich hab doch nur eine App …

- Nicht jeder muss ein Verzeichnis der Verarbeitungstätigkeiten führen
- Prüfen, ob man muss
- Je nach Verarbeitung muss man ggf. auch als App-Anbieter ein entsprechendes Verzeichnis führen
  - Wird dann halt nur kleiner ausfallen ;-)

Art. 30: „Verzeichnis von Verarbeitungstätigkeiten“

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

Wer braucht ein „Verzeichnis der Verarbeitungstätigkeiten“?

Das Verzeichnis von Verarbeitungstätigkeiten **muss aufgestellt werden**, wenn

- das Unternehmen mindestens 250 Mitarbeiter hat

oder

- Daten mit Risiken für die Rechte und Freiheiten der betroffenen Personen verarbeitet werden

oder

- eine **Verarbeitung besonderer Datenkategorien erfolgt**

oder

- eine Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen durchgeführt wird

oder

- die Datenverarbeitung nicht nur gelegentlich erfolgt.

Art. 30: „Verzeichnis von Verarbeitungstätigkeiten“

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

Ich hab doch nur eine App …

- Verarbeitet die App die in Art. 9 Abs. 1 genannten Datenkategorien **UND** der App-Anbieter ist Verantwortlicher
  - → Verzeichnis der Verarbeitungstätigkeiten muss geführt werden
- In Art. 9 Abs. 1 genannte Datenkategorien
  - rassische und ethnische Herkunft
  - politische Meinungen
  - religiöse oder weltanschauliche Überzeugungen
  - Gewerkschaftszugehörigkeit
  - **genetischen Daten**
  - biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
  - **Gesundheitsdaten**
  - **Daten zum Sexualleben** oder der sexuellen Orientierung

Art. 30: „Verzeichnis von Verarbeitungstätigkeiten“

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

Wer ist verantwortlich für das Verzeichnis?

- Verantwortlich für
  - die Erstellung bzw.
  - das Vorhandensein des Verzeichnisses sowie
  - der entsprechenden Aktualisierungen

  „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“
- Letztlich: Führung des Unternehmens / Organisation (Geschäftsführer, Vorstand, …)
- Cave Auftragsverarbeitung:
  - Gilt für Verantwortlichen aber auch für Auftragsverarbeiter

Art. 30: „Verzeichnis von Verarbeitungstätigkeiten“

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

Wozu dient dieses Verzeichnis?

- Primäres Ziel
  - Aufsichtsbehörde Möglichkeit bieten, „die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse“ kontrollieren zu können
- Sekundär: Arbeitshilfe für den Datenschutzbeauftragten
  - Übersicht der im Unternehmen eingesetzten Verarbeitungsvorgänge, bei denen personenbezogene Daten verarbeitet werden

→ Primäres Ziel verlangt, dass im Verzeichnis alle Verfahren geführt werden müssen

→ Umfasst neben den automatisierten Verarbeitungen auch manuelle

→ DS-GVO fordert in Art. 30, dass in dem Verzeichnis alle Verarbeitungstätigkeiten aufgeführt werden müssen

Art. 30 Abs. 1: Verantwortlicher

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

Mindestinhalte des Verzeichnisses
Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen
Namen und die Kontaktdaten eines etwaigen Datenschutzbeauftragten
Zwecke der Verarbeitung
Beschreibung der Kategorien betroffener Personen
Beschreibung der Kategorien personenbezogener Daten
Kategorien von Empfängern […], einschließlich Empfänger in Drittländern oder internationalen Organisationen
die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
Kategorien von Empfängern […], einschließlich Empfänger in Drittländern oder internationalen Organisationen
eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32

Art. 30 Abs. 2: Auftragsverarbeiter

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

Mindestinhalte des Verzeichnisses
Namen und Kontaktdaten des Auftragsverarbeiters, sowie gegebenenfalls des Vertreters des Auftragsverarbeiters
Namen und Kontaktdaten eines jeden Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen
den Namen und die Kontaktdaten eines etwaigen Datenschutzbeauftragten des Auftragsverarbeiters **und des Verantwortlichen**
Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden
gegebenenfalls Übermittlungen von personenbezogenen Daten an ein **Drittland** oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien
eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32

Art. 30: „Verzeichnis von Verarbeitungstätigkeiten“

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

Rahmenbedingungen

- Tätigkeit
  - Begriff „Tätigkeit“ in DS-GVO nicht definiert
- Verantwortlicher
  - Definition in Art. 4 Abs. 7 DS-GVO
- Zweck
  - Begrifflichkeit in DS-GVO nicht definiert
  - Umgang mit Zweck aber in Kommentaren dargelegt (z.B. Simitis)
- Verletzung des Schutzes personenbezogener Daten
  - Definition in Art. 4 Abs. 12 DS-GVO
- Stand der Technik
  - In DS-GVO nicht definiert
  - Siehe z. B. § 3 Abs. 6 Bundes-Immissionsschutzgesetz, IT-Sicherheitsgesetz

Art. 30: „Verzeichnis von Verarbeitungstätigkeiten“

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

Rahmenbedingungen

- Es existiert genau **ein Verzeichnis**, in dem **alle Verarbeitungs**tätigkeiten für jeden
- Verantwortlichen (Art. 30 Abs. 1 DS-GVO) bzw. Auftragsverarbeiter (Art. 30 Abs. 2 DS-GVO) müssen Verzeichnis führen

  („Jeder Verantwortliche und gegebenenfalls sein Vertreter führen *ein* Verzeichnis […]“)
- Das genannte Verzeichnis ist **schriftlich** zu führen, was **auch in einem elektronischen Format** erfolgen kann. (Art. 30 Abs. 3 DS-GVO)
- Auf Anfrage muss der Verantwortliche bzw. der Auftragsverarbeiter der Aufsichtsbehörde das Verzeichnis zur Verfügung stellen (Art. 30 Abs. 4 DS-GVO)
- Eine Verfügbarmachung für Jedermann ist nicht vorgesehen
  (Aber natürlich auch nicht verboten)

Art. 30: „Verzeichnis von Verarbeitungstätigkeiten“

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

Sanktionen: Art. 83 Abs. 4 lit. a DS-GVO

Bei Verstößen gegen die Pflicht:

- Geldbußen von bis zu 10.000.000 EUR oder
- im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs
- je nachdem, welcher der Beträge höher ist

Merke: Einen Verstoß kann auch ein

- unvollständiges Verzeichnis
- fehlerhaft geführtes Verzeichnis
- nicht aktuelles Verzeichnis

darstellen.

Spezialfall:
DiGA gemäß § 33a SGB V

Digitale Gesundheitsanwendungen (DiGA) nach § 33a SGB V

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

DiGA ist zwingend ein Medizinprodukt

- DiGA gemäß § 33a Abs. 2 SGB V: Medizinprodukte der Klasse I oder IIa
- DiGA muss vom BfArM zugelassen sein, Zulassungsvoraussetzung regelt Digitale Gesundheitsanwendungen-Verordnung (DiGAV) (http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl120s0768.pdf)
  - § 4 DiGAV: Anforderungen an Datenschutz und Datensicherheit
  - Bewertung erfolgt durch Fragebogen zu § 4 Abs. 6 in der DiGAV selbst
    - Datenschutz: 46 Fragen
    - Datensicherheit: 37 Fragen
    - Zusatzanforderungen bei digitalen Gesundheitsanwendungen mit sehr hohem Schutzbedarf: 9 Fragen

DiGAV
Fragebogen § 4

- DiGA-Leitfaden des BfArM dient als Auslegungshilfe (https://www.bfarm.de/SharedDocs/Downloads/DE/Service/Beratungsverfahren/DiGA-Leitfaden.pdf;jsessionid=10D072DCF8CFA5203144BD7BF0FC8428.1_cid506?__blob=publicationFile&v=11)

Digitale Gesundheitsanwendungen (DiGA) nach § 33a SGB V

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

DiGA: Drittstaaten

Besonderheit bei Verarbeitung in Drittstaaten

- § 4 Abs. 3 DiGAV: Nur zulässig, wenn Angemessenheitsbeschluss der EU Kommission nach Art. 45 DS-GVO vorliegt
- Für USA liegt kein Angemessenheitsbeschluss vor
  - Google, Apple & Co. Dürfen daher keinerlei Zugriff auf personenbezogene Daten haben
  - Kommentierung siehe https://www.reuschlaw.de/news/apps-auf-rezept-neue-informationen-zur-datenuebermittlung-in-die-usa/

Checkliste: Hab ich an alles gedacht?

Vorgehen bei einer Prüfung: Verarbeitung ok?

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

Prüfung Einhaltung Datenschutz-Vorgaben bei einer Mobile App

1. Sind Zwecke und Vorgehen der geplanten Verarbeitung so dokumentiert, dass durch den Datenschutzbeauftragten eine Begutachtung erfolgen kann?
   - Sind Verarbeitungszwecke ausreichend klar beschrieben?
   - Ist die Methodik der Verarbeitung klar beschrieben?
2. Allgemeine Anforderungen
   - Alle Anforderungen Art. 5 DS-GVO werden eingehalten?
   - Gewährleistung Betroffenenrechte erfolgt?
   - Prozess zur Dokumentation und Meldung von Datenpannen etabliert?
   - Sind vorhersehbaren Risiken und Nachteile bei der Nutzung der App für die betroffene Person beschrieben und wurde das Risiko voraussichtlich auf ein vertretbares Maß reduziert?
     (Es müssen Belege vorliegen, welche alles nachweisen)

Vorgehen bei einer Prüfung: Verarbeitung ok?

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

Prüfung Einhaltung Datenschutz-Vorgaben bei einer Mobile App

3. Erlaubnistatbestand
   - Gesetzlicher Erlaubnistatbestand ohne Einwilligung vorhanden?
     - Wenn ja: Welcher?
   - Wird Einwilligung bei vorhandenem anderem gesetzlichen Erlaubnistatbestand eingeholt?
     - Wenn ja: Vorgaben EDSA beachtet?
     - Wenn ja: Wird insbesondere bei Widerruf Verarbeitung inkl. Speicherung eingestellt?
   - Verarbeitung basiert ausschließlich auf Einwilligung
     - Alle Vorgaben für Einwilligung eingehalten?
     - Einwilligungsformular und Informationen geprüft?

Vorgehen bei einer Prüfung: Verarbeitung ok?

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

Prüfung Einhaltung Datenschutz-Vorgaben bei einer Mobile App

4. Datenerhebung/-Verarbeitung
   - Nachweis bzgl. Erforderlichkeit der verarbeiteten Datenarten vorhanden?
   - Nachweis bzgl. Erforderlichkeit von Art und Umfang der Verarbeitung vorhanden?
   - Nachweis, dass kein „milderes“ Mittel existiert, vorhanden?
   - Wurde der Zeitraum der Verarbeitung (= Zeitraum von Erhebung bis Löschung der Daten) festgelegt?
   - Keine Zweckänderung möglich?
     - Wenn Zweckänderung: Werden betroffene Personen über die Zweckänderung bei der Verwendung der Daten informiert?

Vorgehen bei einer Prüfung: Verarbeitung ok?

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

Prüfung Einhaltung Datenschutz-Vorgaben bei einer Mobile App

5. Sicherheit der Verarbeitung
   - Sind angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorgesehen?
   - Sind alle am Projekt beteiligten Personen auf das Datengeheimnis verpflichtet?
   - Wird nachweisbar Privacy by Design/Default eingehalten? (Art. 25 eingehalten?)
   - Wurde geprüft, ob eine Datenschutz-Folgenabschätzung durchgeführt wurde? (Art. 35 eingehalten?)
   - Sind angemessene und spezifische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung vorgesehen? (Art. 32 eingehalten?)
     - Insbesondere: Erfolgt (regelmäßig) eine Auditierung aller Maßnahmen zum Nachweis der Umsetzung und Einhaltung?
   - Dokumentation im Verzeichnis der Verarbeitungstätigkeiten erfolgt? (Einhaltung Art. 30?)

Vorgehen bei einer Prüfung: Verarbeitung ok?

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

Prüfung Einhaltung Datenschutz-Vorgaben bei einer Mobile App

6. Zusammenarbeit mit Dritten
   - Falls Verarbeitung in Drittstaaten:
     Anforderungen DS-GVO sowie ggf. nationale Vorgaben berücksichtigt?
   - Bei Auftragsverarbeitern
     - Zusatzvertrag zur Auftragsverarbeitung abgeschlossen und Vertrag liegt unterschrieben vor?
     - AV-Dienstleister erfüllen Verpflichtung zur Wahrung Datengeheimnis und – falls erforderlich – unterliegen der Schweigepflicht nach § 203 StGB?
   - Bei gemeinsamer Verantwortlichkeit nach Art. 26 DS-GVO
     - Zusatzvertrag zur gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO abgeschlossen und Vertrag liegt unterschrieben vor?
     - Information betroffener Personen entsprechend Art. 26 Abs. 2 S. 2 DS-GVO wird gewährleistet?

Fazit

Datenschutz in mobilen Anwendungen

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

Mobile App: Alle Datenschutzanforderungen müssen eingehalten werden

- Bzgl. Mobiler Apps gibt es keine Sonderstellung:
  Alle Anforderungen aus dem Datenschutzrecht müssen eingehalten werden
- Die Art des Endgerätes enthält hingegen besondere Herausforderungen, z. B.:
  - Informationsbereitstellung im Rahmen der Betroffenenrechte:
    Kleines Display verhindert eine übersichtliche Darstellung aller benötigten Informationen
  - Mobile Endgeräte können leichter gestohlen/verlegt werden:
    Datenverlust oder unbefugte Offenbarung erfordern ggf. Meldung an Aufsichtsbehörde
  - Bezug eher regelhaft über Store eines US-Anbieters:
    Umgang mit Drittstaaten-Verarbeitung
- Nachweispflichten erfordern entsprechende Dokumentation
- Cave: Wenn Datenschutz-Folgenabschätzung erforderlich:
  Pflicht zur Benennung eines Datenschutzbeauftragten nach § 38 Abs.. 1 S. 2 BDSG

Fragen / Diskussion

Kontakt:

Dr. Bernd Schütze

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

mailto:schuetze@medizin-informatik.org

https://gesundheitsdatenschutz.org