vAItality – Gesundheitswesen

Datenweitergabe an Dritte für KI-basierte Vitalfunktionsoptimierung

Das Med-Tech-Start-up vAItality hat einen KI-basierten Vitalfunktionsoptimierer zur Überwachung des Schlafverhaltens entwickelt, der einen direkten (Daten-)Austausch zur Vorsorge und Therapie zwischen Patientinnen/Patienten und Ärztinnen/Ärzten ermöglicht. Die damit erhobenen PatientInnen-Gesundheitsdaten dienen vor allem der Behandlung für einen gesunden Schlaf und sind nicht nur für die weitere Optimierung des KI-basierten Modells von Belang, sondern bieten auch anderen Akteuren aus dem Gesundheitswesen – wie universitäre Forschungsprojekte oder Pharmaunternehmen – enormes Potenzial für innovative gesundheitsfördernde Geschäftsmodelle und Produkte.

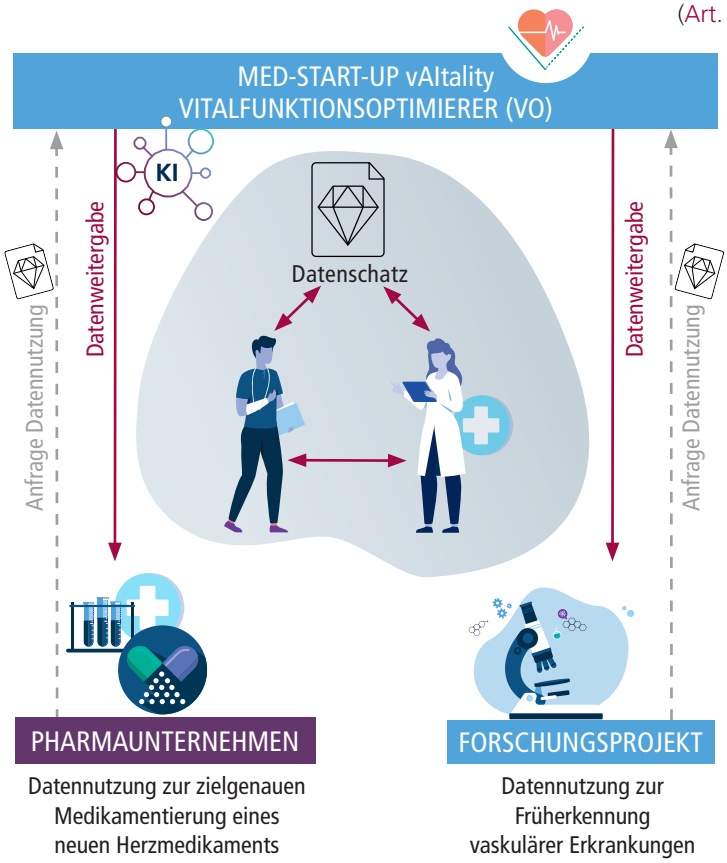
Datenschatz
Gesundheitsdaten

- vergangene, gegenwärtige oder zukünftige Gesundheitsdaten
- körperliche/geistige Gesundheit einer Person
- bei Anmeldung/Erbringung von Gesundheitsdienstleistungen
- Fitness-Apps
- medizinische intelligente Implantate
- etc.

Datenschutz
Datenweitergabe an Dritte

Bei der Weitergabe der persönlichen Daten von PatientInnen an Dritte für weitere innovative Geschäftsmodelle und Produkte, gemeinwohlorientierte Zwecke (z. B. Forschungszwecke) ist zu beachten:

- Einwilligung der betroffenen Personen (Art. 4 Nr. 11 DSGVO)
- Informiertheit der betroffenen Personen (Art. 13 DSGVO)
- Zweckbindung der Datenerhebung (Art. 5 Abs. 1 lit. b) DSGVO)



Datennutzung zur zielgenauen Medikamentierung eines neuen Herzmedikaments

Datennutzung zur Früherkennung vaskulärer Erkrankungen

KI-basierter Vitalfunktionsoptimierer überwacht und stimuliert die Vitalfunktionen (Atmung, Kreislauf, Körpertemperatur) während des Schlafes.
Auf Basis der Vitalfunktionsaufzeichnung können ÄrztInnen die Behandlung abstimmen bzw. sogar nach Notruf durch das Tool informiert werden.

INFO

Technische Ansätze

Differential Privacy (DP):
Verfahren zur Anonymisierung der Daten für den Trainingsdatensatz

☞ Verrauschung führt zu einer signifikanten Reduktion der Genauigkeit der über das ML-Modell erfolgten Klassifikation der PatientInnen.

Federated Learning:
Datenschutzkonformes Training aller KI-Elemente, bei dem die verwendeten Daten auf den Endgeräten der UserInnen (nicht zentral!) gebündelt werden und damit bei diesen verbleiben. (Mehr zu Federated Learning)

☞ Neue Angriffspunkte für Cyberkriminelle

Federated Learning + Differential Privacy (Hybride Modelle):
Absicherung des Austausches des Wights

☞ Fehlkassifikationen/gesundheitsschädliche Fehlstimulierungen aufgrund der signifikanten Reduktion der Datengenauigkeit

Unabhängige Vermittler-Instanzen, eigenverantwortliche Datenorganisation

Personal Information Management Systems (PIMS):
Stärkung der Souveränität von PatientInnen hinsichtlich ihrer Gesundheitsdaten aufgrund privatwirtschaftlichen Interesses

Datentreuhänder mit Datenenklave:
Stärkung der Forschungs-/Gemeinwohlzwecke sowie Datensouveränität von PatientInnen

Anton Merk, 65 Jahre, hat kürzlich seinen Lungenkrebs besiegt; dies mithilfe KI-gestützter Methoden der Krebserkennung, -behandlung und -therapie. Da ihn seit Jahren Schlaf- und Herzrhythmusstörungen plagen, fühlt er sich oft schlapp und schwach. Seine Hausärztin rät ihm, den in Kürze auf den Markt kommenden KI-basierten Vitalfunktionsoptimierer des Med-Tech-Start-up vAItality zu nutzen, der das Schlafverhalten nicht nur überwacht, sondern auch optimieren kann. Anton ist begeistert von dieser Empfehlung und registriert sich als Nutzer des Vitalfunktionsoptimierers ab Produktstart.

vAItality, ein Med-Tech-Start-up, hat sein erstes KI-Produkt entwickelt: den KI-basierten Vitalfunktionsoptimierer. Dieser soll in Kürze auf dem Markt eingeführt werden. Im Vorfeld gilt es für das junge Start-up-Unternehmen noch einiges abzuklären: insbesondere datenschutzrechtliche Vorgaben. Da es sich beim Vitalfunktionsoptimierer um eine KI-basierte Technologie handelt, zu der bisher kaum Gerichtsentscheidungen oder Leitlinien vorliegen, kann der Einsatz mit einem gewissen Risiko verbunden sein. Daher holt sich vAItality vor Einsatz des Vitalfunktionsoptimierers rechtlichen wie technischen Rat ein.

UNIVERSITÄRES FORSCHUNGSPROJEKT

vAItality-Gesundheitsdaten zur Früherkennung vaskulärer Erkrankungen nutzen

Vor Projektstart erhält vAItality eine Anfrage aus der medizinischen Forschung zur entgeltfreien Nutzung der potenziellen PatienInnendaten für ein großes universitäres Forschungsprojekt zur Früherkennung vaskulärer Erkrankungen.

DATEN-WEITERGABE AN DRITTE

PHARMAUNTERNEHMEN

vAItality-Gesundheitsdaten zur Entwicklung eines neuen Herzmedikaments nutzen

Ein Pharmaunternehmen wird aufgrund der erfolgreichen Markteinführung und der positiven Resonanz seitens der PatientInnen und ÄrztInnen auf den Vitalfunktionsoptimierer aufmerksam und sieht in den vAItality-Gesundheitsdaten wirtschaftliches Potenzial. Das Pharmaunternehmen fragt daher bei vAItality an, ob die Gesundheitsdaten für eigene medizinische Zwecke käuflich zu erwerben sind.

Ziele des Unternehmens, auch mit KI-Einsatz

- **Entwicklung eines KI-Vitaloptimierers**
- **Weitergabe der Gesundheitsdaten als Datenschatz für das Gemeinwohl**
- **Generierung neuartiger Geschäftsmodelle mit Dritten**

Datenerhebung für den Vitalfunktionsoptimierer und Datenteilung mit universitärem Forschungsprojekt

SZENARIO 1

Ausgangssituation

Vor Markteinführung des Vitalfunktionsoptimierers hat vAItality u. a. rechtliche Fragen zum Einsatz KI-basierter Anwendungen zu klären. Vor Projektstart erhält vAItality eine **Anfrage aus der medizinischen Forschung zur entgeltfreien Nutzung** der potenziellen PatientInnendaten für ein großes universitäres Forschungsprojekt zur Früherkennung vaskulärer Erkrankungen.

Rechtliche Lage

Bei der Datenerhebung für die **Datennutzung und Datenteilung** gelten folgende Datenschutzauflagen:

- Einwilligung der betroffenen Personen (Art. 4 Nr. 11 DSGVO)
- Informiertheit der betroffenen Personen (Art. 13 DSGVO)
- Zweckbindung der Datenerhebung (Art. 5 Abs. 1 lit. b) DSGVO)

☞ Beide Zwecke – Datennutzung wie Datenteilung (Forschungsprojekt) – sind datenschutzkonform abzudecken.

☞ vAItality erstellt ein Informationsblatt, bei dem die Nutzenden nicht einem einzelnen Zweck, sondern nur beiden gemeinsam (gekoppelt) zustimmen können.

☞ **Frage nach Zweckbindung/„richtigem" Informationsgrad:** Die Formulierung zur Zweckbindung lautet: *„Ihre Gesundheits- und Bewegungsdaten werden für die Optimierung Ihrer Vitalfunktionen mittels eines KI-Systems sowie für ein medizinisches Forschungsprojekt zur Früherkennung von Krankheiten verwendet."*

- Einwilligung zum Forschungszweck nicht ausreichend: kein „broad consent"
- Forschungsprojekt darf die von vAItality erhobenen Daten nicht verwenden
- vAItality darf den Vitalfunktionsoptimierer weiter anbieten
- Informationspolitik von vAItality transparent

Datennutzung: Einwilligung notwendig – Informationsgrad angemessen und verständlich?

nein

Technische Umsetzung: Datenschutz über Datenzugriff-Managementsysteme sichergestellt?

Datentreuhänder mit Datenenklave: Stärkung der Datensouveränität von PatientInnen zu Forschungs-/Gemeinwohlzwecken

☞ PatientInnen können personenbezogene Daten (z. B. Vorerkrankungen) in die Datenenklave hochladen und geben breite Einwilligung für die Datenverwertung zu gemeinwohlorientierten, privatwirtschaftlichen sowie Forschungszwecken, damit Entscheidungs- oder Wahlfreiheit für oder gegen.

ja

DSGVO-konforme Datennutzung für KI-System

vAItality versendet das Informationsblatt zusammen mit der Zweckbindung an alle den Vitaloptimierer vertreibenden ÄrztInnen, die es an ihre PatientInnen austeilen. vAItality entstehen dadurch Administrationskosten im fünfstelligen Bereich. Viele PatientInnen – wie Anton – stimmen der Datennutzung für beide Zwecke zu; viele geben aber die Datennutzung für das Forschungsprojekt nicht frei und können den Vitalfunktionsoptimierer daher nicht nutzen.

(-) PatientInnenvorteil
> Wechsel (-)
> Steigerung der Gesundheit (+)

(/) Unternehmensvorteil
> hohe Investitionskosten (-)
> kein vollumfänglicher KI-Einsatz (-)
> Reduzierung des PatientInnenstamms (-)
> reduzierte Datenqualität (-)

(+) Datenschutz

(/) Gemeinwohl

nein

Keine Datenteilung mit dem Forschungsprojekt

Das Forschungsprojekt wird aufgrund des rechtlichen Verbots der Datennutzung abgebrochen und muss alle personenbezogenen Daten löschen. Der Forschungsfortschritt ist dahin, weitere potenzielle Fortschritte bei der Erkennung vaskulärer Erkrankungen bleiben aus. Aufgrund begrenzter Fördermittel kann der Forschungsrückstand nicht mehr auf-, auch die nachträgliche Einwilligung nicht mehr eingeholt werden.

(/) Forschungsprojekt
> keine medizinischen Fortschritte (-)
> keine finanzielle Förderung (-)

ja

Datenzugriff-Managementsysteme zur DSGVO-konformen Datennutzung für KI-System

vAItality registriert sich beim Datentreuhänder Data4Health, der dem Start-up aufgrund der Verbesserung der individuellen PatientInnensituation Gemeinwohlorientierung bescheinigt. vAItality verknüpft in der Datenenklave die dort abgespeicherten personenbezogenen PatientInnendaten des Vitalfunktionsoptimierers mit ihren selbst gesammelten Daten und trainiert die KI-Elemente des Optimierers.

(+) PatientInnenvorteil
> Datensouveränität (+)
> Steigerung der Gesundheit (+)

(+ Unternehmensvorteil
> Umsatzsteigerung (+)

(+) Datenschutz
(+) Gemeinwohl

Auch das Forschungsprojekt registriert sich beim Datentreuhänder und nutzt die dort gespeicherten Daten in der Trusted Execution Environment der Enklave für ihr Forschungsvorhaben.

(+) Forschungsprojekt
> Forschungsergebnisse (+)

Datenschützende Datennutzung über DSGVO-Ansatz

Datenschützende Datennutzung über technischen Ansatz

Datenerwerb für Produktentwicklung eines Pharmaunternehmens

SZENARIO 2

Ausgangssituation

Ein Pharmaunternehmen möchte die **Gesundheitsdaten für die Entwicklung eines neuen Herzmedikaments (bereits in der Klinikphase) kaufen**, um mit diesen eine individualisierte Medikamentierung zu erzielen. Dies verspricht u. a. einen Innovationssprung in der Prävention von Herzinfarkten. vAltality erkennt den gesellschaftlichen Mehrwert, schließt einen Vertrag mit dem Pharmaunternehmen über den Datenaustausch und erhält einen siebenstelligen Betrag – PatientInnen profitieren monetär nicht von der Weitergabe ihrer Daten.

Rechtliche Lage

Für die Verwendung der Gesundheitsdaten stehen dem Pharmaunternehmen zwei Möglichkeiten zur Verfügung:

a) Einholung einer aufwändigen **nachträglichen Einwilligung** (DSGVO Art. 6 Abs. 4) aller vAltality-PatientInnen
b) Vollzug einer **individuellen Interessenabwägung** (DSGVO Art. 6 Abs. 1 S. 1 lit. f)

☞ Beim Datenerwerb besteht in der Umsetzung Interpretationsunsicherheit.

Technische Umsetzung: Datenschutz über Datenzugriff-Managementsysteme sichergestellt?

Personal Information Management Systems (PIMS) ermöglichen die Stärkung der Souveränität von PatientInnen hinsichtlich ihrer Gesundheitsdaten, vor allem bei privatwirtschaftlichem Interesse.

☞ Missbrauch der Machtposition seitens der Datentreuhänder möglich; Datenschutz sollte daher per By-Design-Ansatz (z. B. bei PIMS) auf Gemeinwohl ausgerichtet sein.

nein / ja

- Prüfschritt 1: **Plausibilität** Innovationssprung in der Herzinfarktprävention? Eher hoch.
- Prüfschritt 2: **Rechtssicherheit** Gemeinwohlvorrang vor Einzelfallentscheidung?

Höherwertigkeit Gemeinwohlinteresse?

nein/unklar / ja

Keine DSGVO-konforme Aktion notwendig

Entscheidung Kosten/Nutzen bei Datennutzung für KI-System

nein / ja

DSGVO-konforme Aktion notwendig: Nachträgliche Einwilligung

Keine Datennutzung für KI-System

Das Pharmaunternehmen verzichtet wegen der teuren und aufwändigen Einholung der Einwilligungen aller PatientInnen auf die Gesundheitsdaten zur Entwicklung eines neuen Herzmedikaments.

(-) PatientInnenvorteil
(-) Unternehmensvorteil
(+) Datenschutz
(/) Gemeinwohl

DSGVO-konforme Datennutzung für KI-System

Das Pharmaunternehmen holt die Einwilligungen aller PatientInnen ein. Einige PatientInnen verweigern die Einwilligung aber.

(+) PatientInnenvorteil
> Wechsel (-)
> Verbesserung (+)
(-) Unternehmensvorteil
> Einsatz (+)
> Aufwand (-)
> Reduzierter PatientInnenstamm
(+) Datenschutz
(+) Gemeinwohl

DSGVO-konforme Datennutzung für KI-System

Das Pharmaunternehmen entscheidet sich für die individuelle Interessenabwägung, da mit dem Medikament ein Innovationssprung in der Herzinfarktprävention wahrscheinlich ist. Dies verspricht eine Steigerung der gesamtgesellschaftlichen Gesundheit. Die Daten der PatientInnen werden somit ohne nachträgliche Einwilligung genutzt.

(+) PatientInnenvorteil
(+) Unternehmensvorteil
(+) Datenschutz
(+) Gemeinwohl

Datenzugriff-Managementsysteme zur DSGVO-konformen Datennutzung für KI-System

Das Pharmaunternehmen – und auch weitere privatwirtschaftliche Gesundheitsakteure fragen direkt in der PIMS-App zur PatientInnen-Datennutzung an.

(+) PatientInnenvorteil
- Stärkung der Datensouveränität
(+) Unternehmensvorteil
- Datenteilung (+)
- Umsatzsteigerung (+)
(+) Datenschutz
- gleichberechtigte Akteure in der Datenökonomie (+)
(+) Gemeinwohl

☞ **vAltality** empfiehlt seinen PatientInnen, sich auf der PIMS-App sovereign.data zu registrieren und ihre personenbezogenen Daten dort zu hinterlegen: PatientInnen entscheiden selbst, ob sie ihre Daten – entgeltlich oder unentgeltlich – zur Verfügung stellen oder für privatwirtschaftliche Zwecke grundsätzlich ausschließen.

Datenschützende Datennutzung über DSGVO-Ansatz

Datenschützende Datennutzung über Datenzugriff-Managementsysteme

Datennutzung mit technischen Verfahren flexibilisieren

SZENARIO 3

Ausgangssituation

Um den Datenschutz bei der Anwendung des Vitalfunktionsoptimierers sicherzustellen, lässt vAItality technische Aspekte von seinem Entwicklungspartner überprüfen. Dieser empfiehlt, verschiedene **technische Verfahren (auch KI-basierte)** in die Entwicklung des Vitalfunktionsoptimierers einzubeziehen. Dadurch soll eine **datennutzungsorientierte Flexibilität für KI-Systeme** gefördert werden, die dem Gemeinwohl dient, während gleichzeitig die Kontrolle der datengebenden Personen in der Datenökonomie gestärkt wird.

Rechtliche Lage

Einhaltung (datenschutz-)rechtlicher Vorgaben:

☞ Bei der **Datenprozessierung** und **Datenerhebung** ist eine Identifizierbarkeit von Personen bei der Datenverarbeitung zu vermeiden (Art. 4 Nr. 5 DSGVO).

☞ Die **Datenverknüpfung** unterliegt dem Grundsatz der Datenminimierung (Art. 5 Abs.1 lit. c).

☞ In den verschiedenen Daten-Lebenszyklusphasen sind die für den Trainingsdatensatz der KI-Elemente des Vitalfunktionsoptimierers verwendeten PatientInnendaten datenschutzkonform zu gestalten. Ebenso eine datenschutzkonforme Absicherung des Datenaustausches.

Datenschutz technisch sichergestellt?

Differential Privacy (DP) zur Anonymisierung der PatientInnendaten, um den Trainingsdatensatz für KI-Elemente des Vitalfunktionsoptimierers datenschützend auszugestalten.

Neben allen biografischen Daten im vorbereiteten Trainingsdatensatz sind auch einige Vitalfunktionsdaten zu verrauschen, da diese in ihrer Zusammensetzung Identifizierbarkeit erlauben könnten.

Eine mit Intensitätsintervallen trainierende Spitzensportlerin, die den Vitalfunktionsoptimierer nutzt, könnte fälschlicherweise als ältere Frau mit Herzrhythmusstörungen klassifiziert werden, was gesundheitsschädliche Fehlstimulierungen durch den Vitalfunktionsoptimierer provozieren könnte.

☞ **Verrauschung** führt zur signifikanten Reduktion der Genauigkeit der über das ML-Modell erfolgten Klassifikation der PatientInnen.

☞ Datenschutzkonformität beim Training wird so sichergestellt, vAItality kann die individuellen personenbezogenen Daten der PatientInnen nicht einsehen.

Federated Learning zum datenschutzkonformen Training aller KI-Elemente des Vitalfunktionsoptimierers.

vAItality entwickelt zentral ein ML-Modell, bei dem Vitalfunktionswerte von PatientInnen abhängig von ihren biografischen Daten (z. B. Vorerkrankungen, Ernährungs-/Bewegungsgewohnheiten, Alter, Gewicht etc.) klassifiziert werden.

Das auf dem vAItality-Server gespeicherte ML-Modell wird von den Vitalfunktionsoptimierern der PatientInnen heruntergeladen und mit deren Gesundheitsdaten und anderen personenbezogenen Daten lokal trainiert. Nur die Ergebnisse (Weights) des lokal trainierten Modells werden an den zentralen Server zurückgesendet. Dieser aggregiert die Weights aller Vitalfunktionsoptimierer der PatientInnen und aktualisiert damit das ML-Modell.

☞ **Bösartige Extraktionsangriffe** möglich, bei denen ein Server jedem Client zum Training andere Updates der Weights schickt, was die Modellgüte signifikant reduzieren kann.

Federated Learning + Differential Privacy als hybride Modelle zur Absicherung des Austausches der Weights bei Federated Learning.

Die lokalen Trainingsdaten der in den Vitalfunktionsoptimierern individueller PatientInnen trainierten KI-Elemente könnten so weit verändert werden, dass Identifizierbarkeit individueller PatientInnen beim Weight-Austausch nicht mehr möglich ist, sodass Datenschutz sichergestellt wäre.

☞ **DP-Einsatz** führt zur signifikanten Reduktion der Genauigkeit der über das ML-Modell erfolgten Klassifikation der PatientInnen.

nein | ja | ja

Datenschutz rechtlich anerkannt

nein | ja | ja

Keine Datennutzung für KI-System

Die Ungenauigkeit des KI-Modells über die Differential-Privacy-Komponente würde einen Einsatz unrentabel machen. vAItality verzichtet deshalb auf den Einsatz und damit auf die Verbesserung der Nutzererfahrung.

(-) PatientInnenvorteil
(-) Unternehmensvorteil
(-) Datenschutz
(/) Gemeinwohl

Technische Sicherstellung einer DSGVO-konformen Datennutzung für KI-System

vAItality setzt voll auf verteiltes Lernen und geht damit bewusst ein Datenschutzrisiko hinsichtlich möglicher Angriffe auf den Weight-Austausch oder auf die Endgeräte ein.

(+) PatientInnenvorteil
  > Steigerung der Datensouveränität
  > hohe Genauigkeit des KI-Modells
  > Angriff auf Endgeräte (-)
(+) Unternehmensvorteil
  > Umsatzsteigerung (-)
(+) Datenschutz
  > mögliche Angriffe auf Weight-Austausch/ die Endgeräte
(/) Gemeinwohl

Datennutzung für KI-System

vAItality setzt das hybride Modell ein und schützt somit das KI-Modell vor Angriffen; nimmt dafür die leichten Genauigkeitsverluste des KI-Modells in Kauf.

(+) PatientInnenvorteil
  > leichte Reduktion der Genauigkeit des KI-Modells durch Verrauschung
  > Steigerung der Souveränität
  > Schutz vor Angriff auf Endgeräte (+)
(+) Unternehmensvorteil
  > Umsatzsteigerung (-)
  > Rücklagen (-)
(+) Datenschutz
  > Schutz vor Angriffen auf Weight-Austausch
(+) Gemeinwohl

Datenschützende Datennutzung über technischen Ansatz