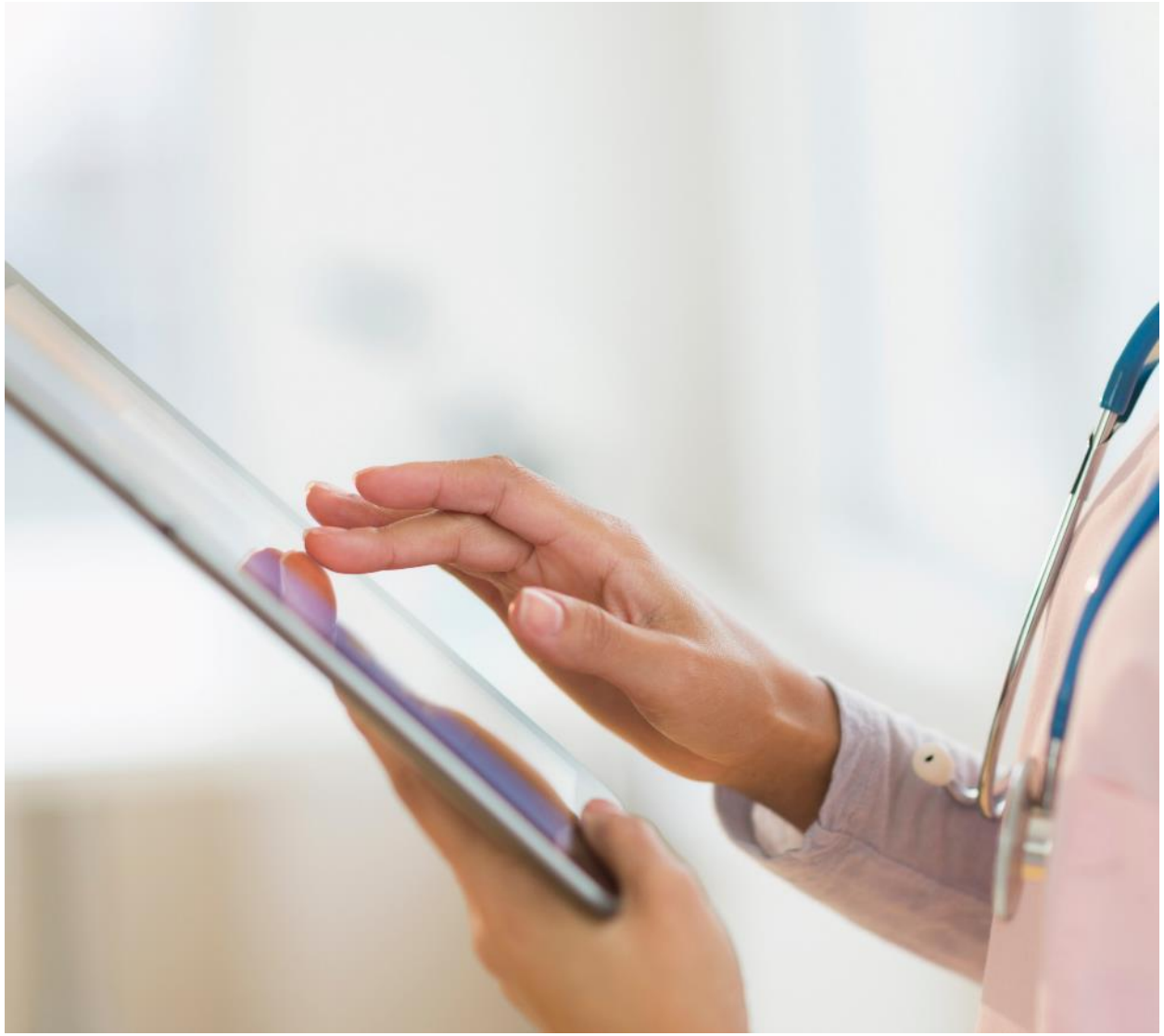
Digital gut unterwegs sein

Praktische Tipps für den Alltag

Dezember 2025

Egbert Zwerschke

PC-Treff 55+



Wer sind wir vom PC-Treff 55+?

(ehrenamtliche Mentoren)

Horst Höfer

Rainer Pluschys

Dorothea Reichenbauer

Rainer Kaiser

Richard Weitz

Egbert Zwerschke

Quelle Stadt Wendlingen a.N.

Heike Hauß
Leiterin MIT

Unser Ziel von PC-Treff 55+

Fakt ist, die Menschen ohne Zugang zur digitalen Welt werden gesellschaftlich ausgeschlossen!

Wir möchten gerne **die Digitale Kompetenz älterer Menschen fördern** durch:

- Vermitteln von grundlegenden Hard- und Software Kenntnissen im Umgang mit den elektronischen Möglichkeiten
- Die Ängste vor der Nutzung digitaler Geräte reduzieren
- z.B. komplexe Online-Anmeldungen oder Registrierungen zu ermöglichen
- Seriöse Quellen erkennen und somit Schaden an der eigenen Gesundheit oder den Geldbeutel abwenden

Worüber wir heute sprechen wollen

- Digital gut unterwegs sein
- WIN10 Upgrade auf WIN 11
- IT-Sicherheit
  - Deep Fake
  - KI, ist alles real?
  - Grundlegende IT-Sicherheit, Passwortmanager
- Einkaufen im Internet
  - Amazon, eBay, Shein, AliExpress, TEMU und Co.
- Gesundheits-Apps
  - DoctoLib
  - Telemedizin
  - Elektronische Patientenakte
- Digitales Erbe

Quelle: Microsoft

Digital gut unterwegs sein

SICHER UND KOMPETENT IM UMGANG MIT SMARTPHONES UND PC‘S

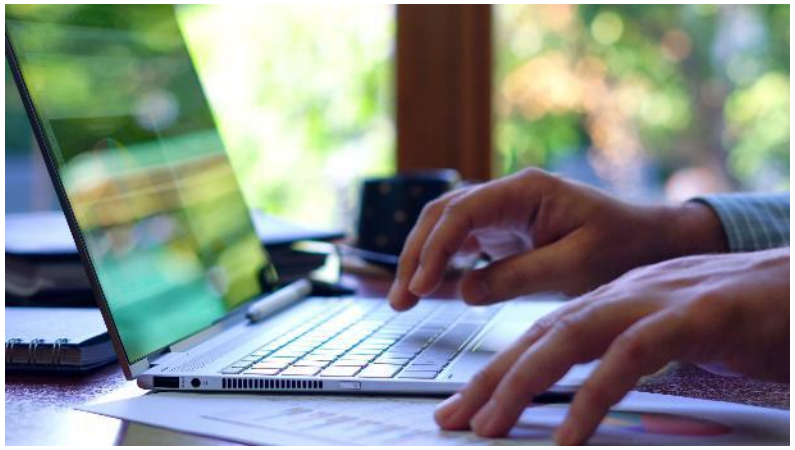
Die wichtigsten Voraussetzungen

Benutzerfreundliche Geräte:

- Geräte mit intuitiven Benutzeroberflächen und großen, klaren Displays sind entscheidend. Viele Hersteller bieten spezielle Senioren-Modelle an, die einfacher zu bedienen sind.

Schulungen und Unterstützung:

- Regelmäßige Schulungen oder Workshops können älteren Menschen helfen, digitale Fähigkeiten zu erlernen. Unterstützung durch Familie oder Freunde ist ebenfalls wichtig, um Fragen zu klären und Unsicherheiten abzubauen.



Quelle: Microsoft

Die wichtigsten Voraussetzungen

Zugängliche Apps und Programme:

- Die Auswahl von Apps, die speziell für Senioren entwickelt wurden, kann den Einstieg erleichtern. Diese Apps sind oft einfacher zu navigieren und bieten Funktionen, die auf die Bedürfnisse älterer Nutzer zugeschnitten sind.

Sicherheit und Datenschutz:

- Ein grundlegendes Verständnis von Online-Sicherheit ist unerlässlich. Ältere Menschen sollten über sichere Passwörter, Phishing und den Schutz ihrer persönlichen Daten informiert werden.

Soziale Vernetzung:

- Die Nutzung von sozialen Medien oder Kommunikations-Apps kann helfen, den Kontakt zu Familie und Freunden aufrechtzuerhalten. Dies fördert nicht nur die digitale Kompetenz, sondern auch das soziale Wohlbefinden.

Quelle: Microsoft

WIN 10 Upgrade auf WIN 11

WIN11 Upgrade

- Der Support für WIN10 endet im Oktober 2026
- Lt. Microsoft ist ein Upgrade auf Windows 11-PC ist nicht geeignet, wenn die Mindestanforderungen nicht erfüllt sind.
- Die Mindestvoraussetzungen sind:
  - Prozessor: max. 2 Jahre alt
  - TPM 2.0: das Trusted Platform Module (TPM 2.0) ist vorhanden und aktiviert
  - Secure Boot: der PC startet nur mit vertrauenswürdiger Software
  - Arbeitsspeicher: mindestens 4GB RAM

Quelle: Microsoft

WIN11 Upgrade

- Die Mindestanforderungen sind erfüllt
- Das Update auf WIN11 wird angeboten → Prozess starten
- Oder gehen zur MS-Webseite „Windows 11 herunterladen“
  - Installationsassistenten laden und starten
  - oder Windows 11-Installationsmedium erstellen und starten

Quelle: Microsoft

WIN11 Upgrade bei älteren PC‘s?

- Alle WIN10 Updates laden
- Backup persönlicher Daten erstellen
- PC-Integritätsprüfung durchführen → die Software ist auf der Microsoft Support Seite zu finden
- Falls OK → Download und Installation starten
- Falls nicht OK:
  - USB Installations-Stick mittels RUFUS erstellen und Installieren
  - oder mittels Registry Tweak: „AllowUpgradesWithUnsupportedTPTOrCPU“ und Installationsassistent für WIN11

Quelle: Microsoft

IT-Sicherheit

Bedrohungen aus dem Internet

- **Schadsoftware** auch Malware genannt
  - Computerviren, Trojaner, Spyware und Würmer
- **Ransomware**
  - eine besondere Form von Schadsoftware, die den Zugriff auf Daten und Systeme einschränkt und dessen Ressourcen erst gegen Zahlung eines Lösegelds wieder freigibt
- **Social Engineering**, das Erschleichen von persönlichen Daten in den sozialen Medien
- **Unerwünscht zugesandte E-Mails** wie
  - klassischer Spam
  - Schadprogramm-Spam
  - Phishing

Bedrohungen aus dem Internet

- Botnetze
- Überlastung einer IP-Adresse durch Distributed-Denial-of-Service-(DDoS)-Angriffe
- Ausnutzen von Schwachstellen in Browser, Browser-Plug-ins oder Betriebssystemen
- Identitätsdiebstahl, wie zum Beispiel
  - Pharming → umleiten auf eine gefälschte Webseite
  - Spoofing → vortäuschen einer falschen Identität
  - Phishing → sammeln von persönlichen schützenswerten Daten
- Keylogger

Als Schutzmechanismen dienen u.a. eine Firewall und eine aktuelle Anti-Viren-Software

Deep-Fake

Deep Fake

- **Politische Deepfakes**
  - Gefälschte Videos von Politikern, die kontroverse oder falsche Aussagen machen, um Desinformation zu verbreiten oder politische Gegner zu diskreditieren.
    Beispiel: Ein manipuliertes Video, in dem ein Politiker scheinbar eine radikale oder beleidigende Aussage macht.

- **Prominente in gefälschten Videos**
  - Deepfakes von Schauspielern oder prominente Menschen, die z-B. in Filmen oder Clips auftreten, die so nie gedreht wurden.
    Beispiel: Ein Deepfake-Video, das einen berühmten Schauspieler in einer neuen Filmszene zeigt, die nie existierte.

Quelle: Pixabay, Geralt

Deep Fake

- **Stimmen-Imitation**
  - Deepfake-Technologie kann auch Stimmen nachahmen, um gefälschte Audioaufnahmen zu erzeugen, die so klingen, als kämen sie von einer bestimmten Person.
    Beispiel: Ein gefälschtes Telefonat, in dem die Stimme eines Bekannten oder Prominenten verwendet wird, um Menschen zu manipulieren.

- **Unterhaltung und Kunst**
  - Deepfakes werden auch kreativ genutzt, um historische Figuren in neuen Kontexten darzustellen oder um Schauspieler digital zu verjüngen / altern.
    Beispiel: Ein Film, in dem eine verstorbene Schauspielerin (z.B. Carrie Fisher) durch Deepfake-Technologie wieder zum Leben erweckt wird, um ihre Rolle weiter in eine Serie zu spielen.

Quelle: Pixabay, Geralt

Deep Fake erkennen

- Auf unrealistische Versprechen achten
- Vorsicht, wenn vorab bezahlt werden soll
- Kein oder nicht aussagekräftiges Impressum
- Rechtschreibe- und Grammatikfehler
- Suspekte Kundenbewertungen und Berichte
- Unnatürliche Mimik oder Lippenbewegungen
- Im Zweifel
  - Im **Fakeshop-Finder** die URL prüfen lassen
  - **Correctiv.Faktencheck** oder **Mimikama** nutzen

Quelle: © ProPK, SID-Logos: Klicksafe

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Informationen

Von der EU-Kommission und BSI zu KI-Systemen wird gefordert, dass alle mit der Deep-Fake-Technologie erstellten Materialien auch als solche gekennzeichnet werden müssen.

- **Erkennen von Deep-Fake bei Bildern**
  - Sichtbare Übergänge, unscharfe Konturen
  - begrenzte Mimik, Augenbewegung und Blinzeln
  - unstimmige Beleuchtung

- **Erkennen von Deep-Fake bei Tönen**
  - Metallischer Sound
  - Falsche Aussprache oder Sprechweise
  - Monotone Sprachausgabe
  - Unnatürliche Geräusche

- **Technische Tools und Software**

Quelle: Microsoft

Künstliche Intelligenz

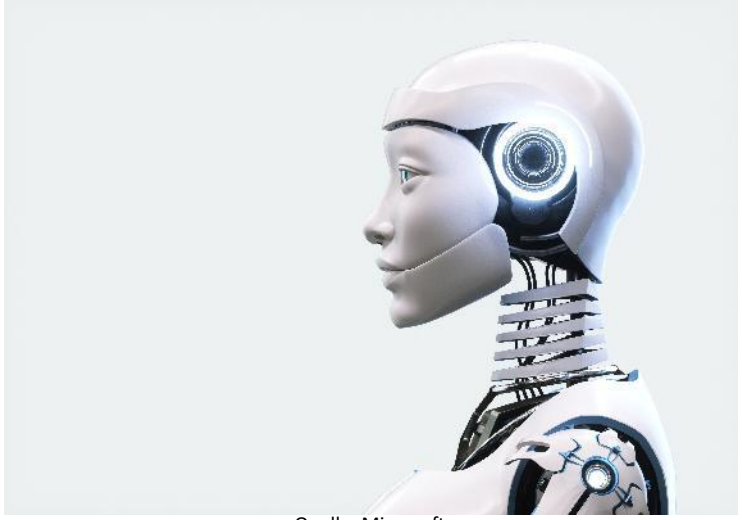
Künstliche Intelligenz

Quelle: Plattform Lernende Systeme

Künstliche Intelligenz KI

Was ist KI?

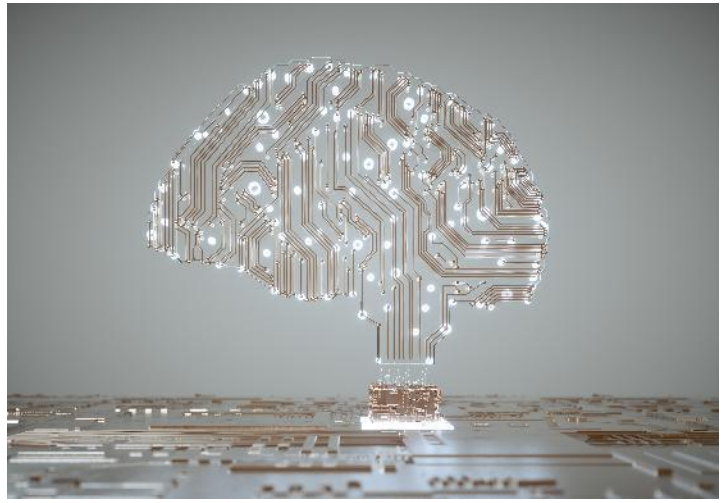
- die Wissenschaft hat bereits in den 1950er Jahren den Begriff Künstliche Intelligenz geprägt
- KI besteht aus Software- und Robotik-Systeme, die sich wie menschliche Intelligenz verhalten sollen
- In viele verschiedenen Bereichen werden KI-basierte Techniken mittlerweile eingesetzt z.B. Bilderkennung, Sprachverarbeitung, Informationen sammeln…



Quelle: Microsoft

Wofür wird KI eingesetzt?

- **Alltag:** Übersetzungstools, Sprachassistenten (**z.B. Siri, Alexa, Google Assistant**) und personalisierte Empfehlungen nutzen KI bereits heute. Aber auch bei Rettungseinsätzen nach Katastrophen, Bild- und Gesichtserkennung, maschinelle Übersetzung (z.B. Google Translate)
- **Wirtschaft:** In der Produktion hilft KI bei der Optimierung von Prozessen durch die Analyse von Sensordaten. In der IT-Sicherheit wird sie zur Erkennung von Cyberkriminalität und autonomes Fahren eingesetzt.
- **Gesundheitswesen:** KI kann bei der Analyse von medizinischen Bildern und der Entwicklung individueller Behandlungspläne unterstützen z.B. im Kampf gegen Krebs



Quelle: Microsoft

Wie funktioniert KI?

- **Maschinelles Lernen**: Die meisten modernen KI-Systeme basieren auf maschinellem Lernen (ML), bei dem Algorithmen Muster in großen Datenmengen erkennen und daraus lernen, ohne explizit für jede einzelne Aufgabe programmiert zu werden.
- **Training:** Ein KI-Modell wird mit vielen Beispieldaten trainiert. Durch dieses Training lernt es, beispielsweise auf einem Bild eine Katze von einem Hund zu unterscheiden.
- **Anwendungen:** Nach dem Training kann die KI diese Muster auf neue Daten anwenden. Beispiele sind die Erkennung von Objekten durch Sensoren in Fahrzeugen oder die Analyse medizinischer Bilder zur Krankheitsfrüherkennung

Quelle: Microsoft

Wichtige Hinweise zur KI

- **Mustererkennung:**

Auch wenn KI menschenähnliche Texte oder Bilder erstellen kann, basiert dies auf der Erkennung von Mustern in den Trainingsdaten und nicht auf echtem Verständnis oder Bewusstsein.

- **Computer versus Menschen:**

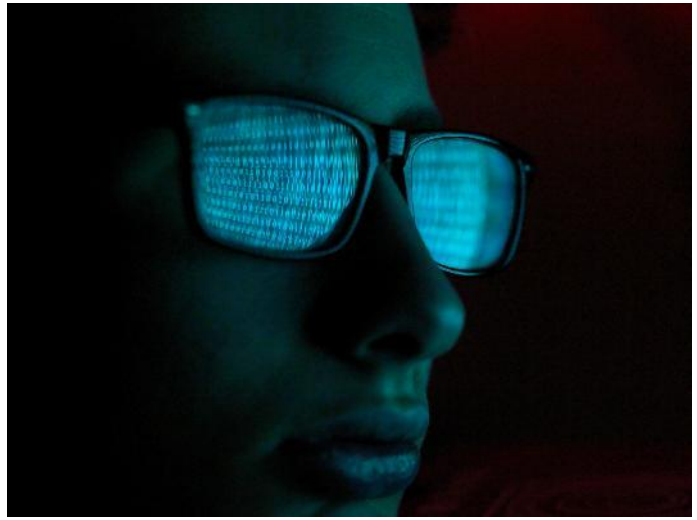
Da KI von Daten lernt, kann sie auch menschliche Vorurteile oder Charakteristiken übernehmen, wenn diese in den Trainingsdaten vorhanden sind.

Quelle: Microsoft

IT-Sicherheitsmaßnahmen

Grundlegende IT-Sicherheitsmaßnahmen

- **Sichere Passwörter**: Nutzen Sie starke, einzigartige Passwörter für jedes Konto. Sie können Passwörter auch sicher aufschreiben und verwahren, jedoch nicht direkt am Gerät.
- **Zwei-Faktor-Authentifizierung (2FA):** Aktivieren Sie diese, um eine zusätzliche Sicherheitsebene zu schaffen. Viele Konten bieten diese Option an.
- **Updates**: Halten Sie Betriebssystem und Programme stets aktuell, um Sicherheitslücken zu schließen.
- **Vorsicht bei E-Mails**: Seien Sie misstrauisch bei E-Mails, die Dringlichkeit vortäuschen oder nach persönlichen Daten fragen. Klicken Sie nicht vorschnell auf Links.
- **Antivirus und Firewall:** Installieren Sie eine zuverlässige Antivirus-Software und aktivieren Sie die Firewall, um Ihren PC zu schützen.



Quelle: Microsoft

Weitere IT-Sicherheitsmaßnahmen

- **Datensicherung und -verwaltung**
  - **Regelmäßige Backups**: Erstellen Sie regelmäßig Sicherungskopien wichtiger Daten auf einer externen Festplatte oder in der Cloud, um sie im Falle eines Systemabsturzes oder Angriffs zu sichern.
  - **Sichere Cloud-Speicher**: Speichern Sie wichtige Dokumente in einem sicheren Cloud-Speicher, um Datenverlust vorzubeugen.
- **Privatsphäre und Online-Verhalten**
  - **Vorsicht bei Veröffentlichungen**: Überlegen Sie gut, was Sie online teilen. Einmal veröffentlichte Informationen können schwer wieder zu entfernen sein.

Quelle: Microsoft

Weitere IT-Sicherheitsmaßnahmen

- **Persönliche Daten**: Geben Sie persönliche Daten nur an vertrauenswürdige Anbieter weiter.
- **Browser-Sicherheit**: Sichern Sie Ihren Browser und akzeptieren Sie nur notwendige Cookies.

- **Zusätzliche Hilfe**
  - Unterstützung suchen: Scheuen Sie sich nicht, sich bei Fragen oder Unsicherheiten an Familienmitglieder oder Bekannte zu wenden.
  - Es gibt auch spezielle Beratungsangebote für Senioren (z. B. Familienportal des Bundes oder **PC-Treff 55+**).

Quelle: Microsoft

Passwortmanager

Was ist ein sicheres Passwort?

- Sichere Passwörter erfinden
  - z.B. **AdTs1sekm$**
  - mind. 8 Zeichen, Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen

- Passwortmanager

Ein Passwortmanager ist eine Softwareanwendung, die dazu dient, Passwörter sicher zu speichern, zu verwalten und zu organisieren. Man muss sich nur ein Master-Passwort merken, um Zugriff auf den Passwortmanager zu erhalten.

Quelle: Microsoft

Hauptfunktionen eines Passwortmanagers

- **Sichere Speicherung**: Passwörter werden verschlüsselt gespeichert, sodass nur der Nutzer mit dem Master-Passwort darauf zugreifen kann.
- **Passwort-Generierung**: Automatische Erstellung starker, zufälliger Passwörter, die schwer zu knacken sind.
- **Automatisches Ausfüllen**: Der Manager kann Login-Daten automatisch in Webseiten oder Apps einfügen.
- **Synchronisation**: Viele Passwortmanager synchronisieren Daten über verschiedene Geräte hinweg (Smartphone, PC, Tablet).
- **Sicherheitsüberprüfung**: Einige bieten Funktionen zur Überprüfung der Passwortstärke oder warnen vor kompromittierten Passwörtern.

Quelle: Microsoft

Wie wird ein Passwortmanager benutzt?

- Software Auswahl und Installation
- Einrichtung eines Master-Passworts
- Passwörter speichern
- Passwörter verwalten
- Automatisches Ausfüllen
- Synchronisieren und Backup

Quelle: Microsoft

Die besten Passwortmanager (Testsieger) sind **1Password** und **Dashlane**. **Keeper** und **NordPass**
Kostenlose Alternativen sind **Bitwarden** und **NordPass**

Mein persönlicher Passwortmanager

Quelle: Microsoft

Bundesamt
für Sicherheit in der
Informationstechnik

Weitere hilfreiche Informationen rund um das Thema „Sicherheit im Internet“ finden Sie auf den Seiten des Bundesamts für Sicherheit in der Informationstechnik.

Aktuelle Themen und Vorfälle | Tipps für den digitalen Alltag | Kooperationen und Forschung

Verbraucherschutz-Newsletter 'Einfach • Cybersicher'

Passkey - Anmeldung ohne Passwort

Bericht zum Digitalen Verbraucherschutz

IT-Sicherheitskennzeichen

Sie haben einen IT-Sicherheitsvorfall?

Internet der Dinge / Smart Home / vernetztes Fahren

Wie Sie eine Cloud für Ihre Daten sicher nutzen

Identitätsdiebstahl und seine Folgen

Einkaufen im Internet

AMAZON, EBAY UND CO

Tipps für den Online Einkauf

- **Sichere Websites:** Unbedingt darauf achten, dass die gewählte Website sicher ist. Das wird an der Webadresse (URL) erkannt, die mit "**https**://" beginnt. Das "**s**" steht für „gesicherte Verbindung".
- **Nur bekannten Anbietern vertrauen:** Nur bei vertrauenswürdigen und bekannten Online-Händlern einkaufen. Zuerst recherchieren, wenn bei neuen Anbietern eingekauft werden soll.
- **Phishing vermeiden:** Sehr kritisch sein bei E-Mails oder Nachrichten, die auffordern, persönlichen Daten einzugeben oder zu bestätigen. Diese könnten Phishing-Versuche sein.
- **Zahlungsmethoden:** Nur sichere Zahlungsmethoden nutzen, wie Kreditkarten oder Zahlungsdienste, die Käuferschutz bieten. Vorab Überweisung von Geld vermeiden.
- **Passwortsicherheit:** Nur starke und einzigartige Passwörter für die Online-Konten einsetzen und regelmäßig ändern. Wenn möglich, eine Zwei-Faktor-Authentifizierung nutzen.

amazon.de

OTTO

Thalia

breuninger

Shop Apotheke

ebay

Weitere Verbrauchertipps

Preise: Diese sollten nicht nur realistisch, sondern auch inklusive Versand-, Rücksende- und möglicher Zusatzkosten transparent aufgeschlüsselt sein.

Domain: Mitunter ändern Kriminelle die Adresse eines bekannten Onlineshops nur minimal ab, um Kundinnen und Kunden hinters Licht zu führen.

Impressum: Dort sollten Telefonnummer und E-Mail-Adresse ebenso wie eine vollständige Anschrift und weitere Informationen wie etwa die Rechtsform zu finden sein.

Gütesiegel: Dieses sollte ein bekanntes Siegel eines größeren Anbieters sein. Ein Klick auf das Siegel sollte zu weiteren Informationen führen. Betrügerinnen und Betrüger erfinden oft neue Siegel oder kopieren ein bestehendes. In dem Fall ist dies meist nicht anklickbar.

Zahlungsmöglichkeiten: Kundinnen und Kunden sollten darauf achten, welche Daten sie angeben und ob diese an mögliche Dienstleister weitergegeben werden. Einige speichern Daten und werten diese gegebenenfalls auch aus.

Quelle: Microsoft

Tipps für asiatische Anbieter

- Preise vergleichen
- Kundenbewertungen und Händlerprofil gründlich prüfen
- Auf die Aktualität und Inhalte der Rezessionen achten
- Auf CE-Kennzeichnung / Produktsicherheit achten
- Mit längeren Lieferzeiten rechnen
- Rückgabe und Garantie oft eingeschränkt
- Auf finanzkonforme Rechnungen achten

TEMU

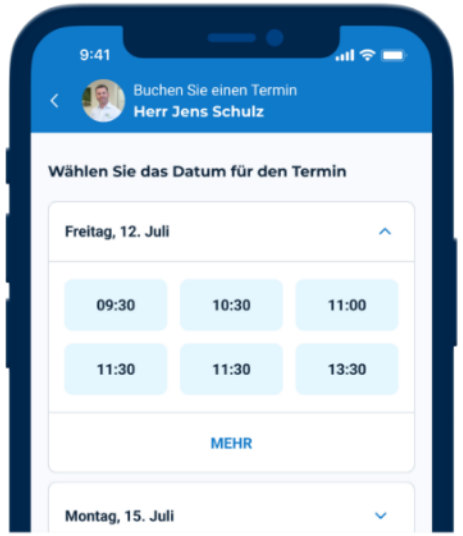
SHEIN

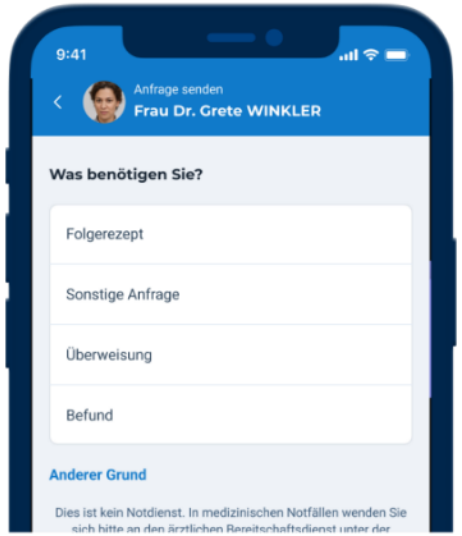
AliExpress

Gesundheits-Apps

Doctolib-App

- Terminbuchung
- Terminerinnerungen
- Digitale Warteliste
- Anfragen





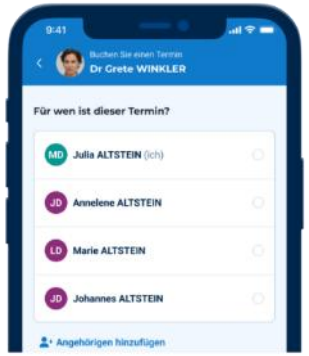
Laden im App Store

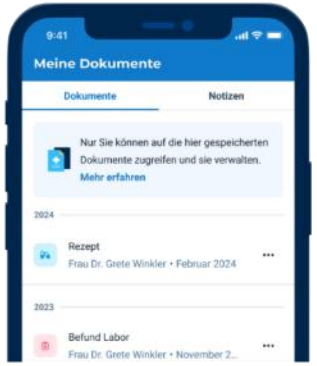
JETZT BEI Google Play

Quelle: Doctolib

Doctolib-App

- Kartenfunktion
- Management für Angehörige
- Dokumente übermitteln
- Videosprechstunde
- Mehrsprachig



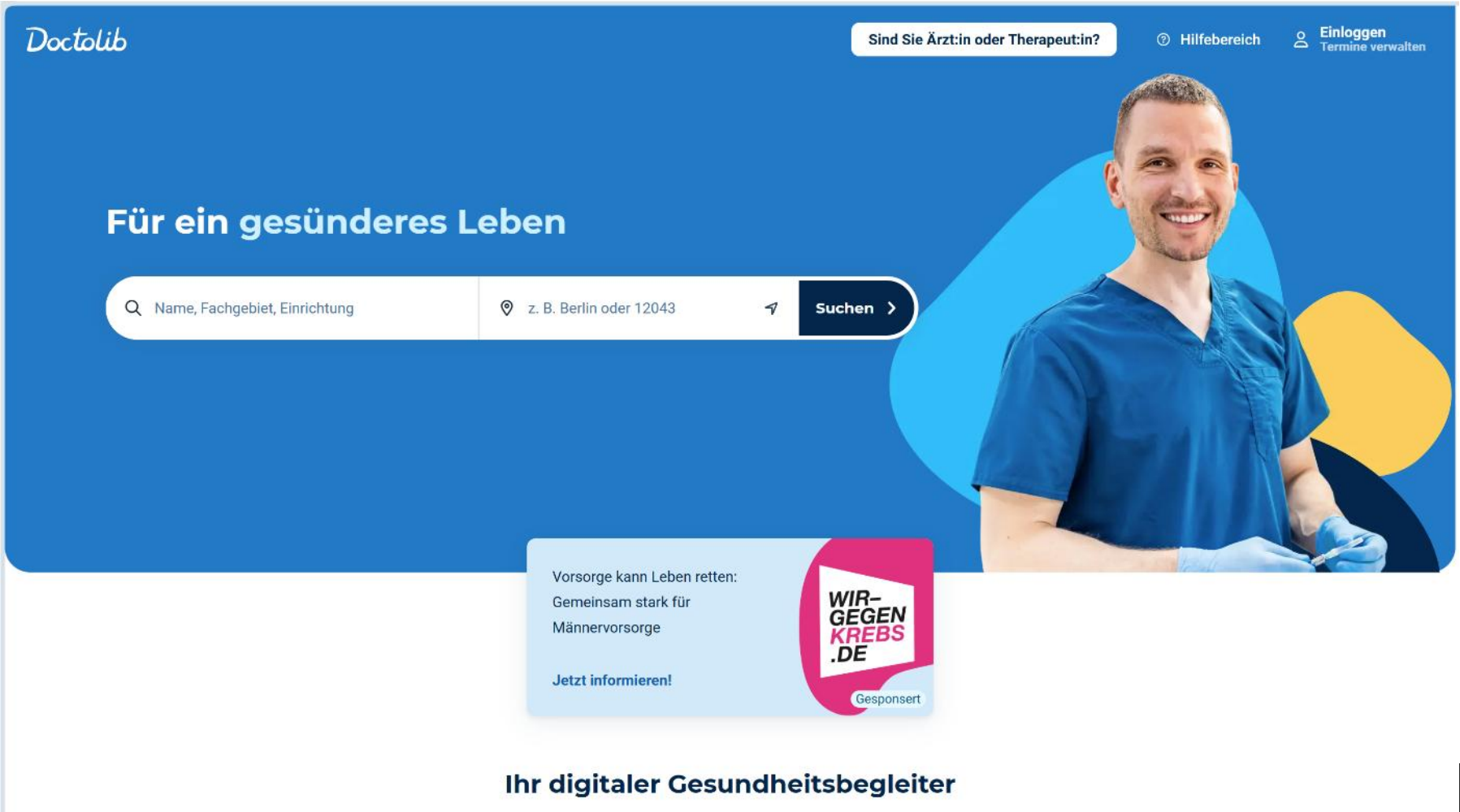


Laden im App Store

JETZT BEI Google Play

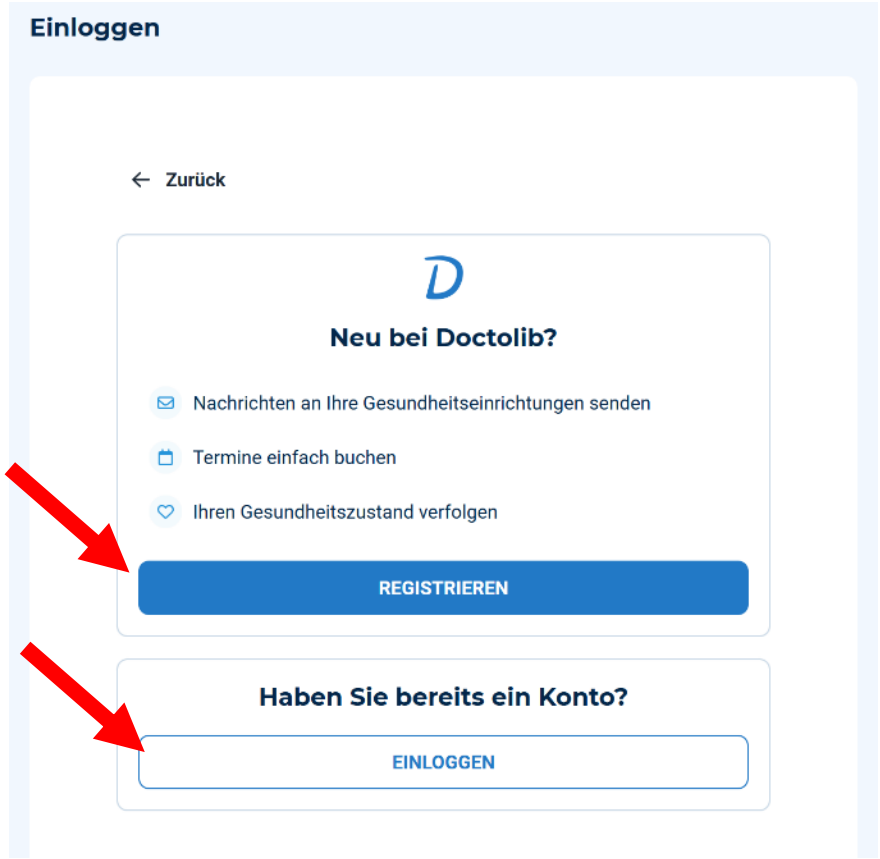
Quelle: Doctolib

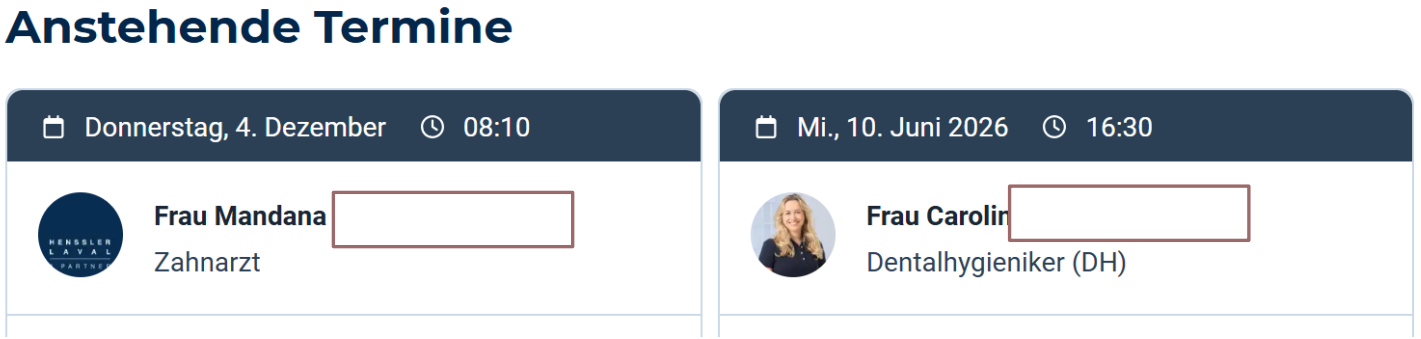
Doctolib-Webseite



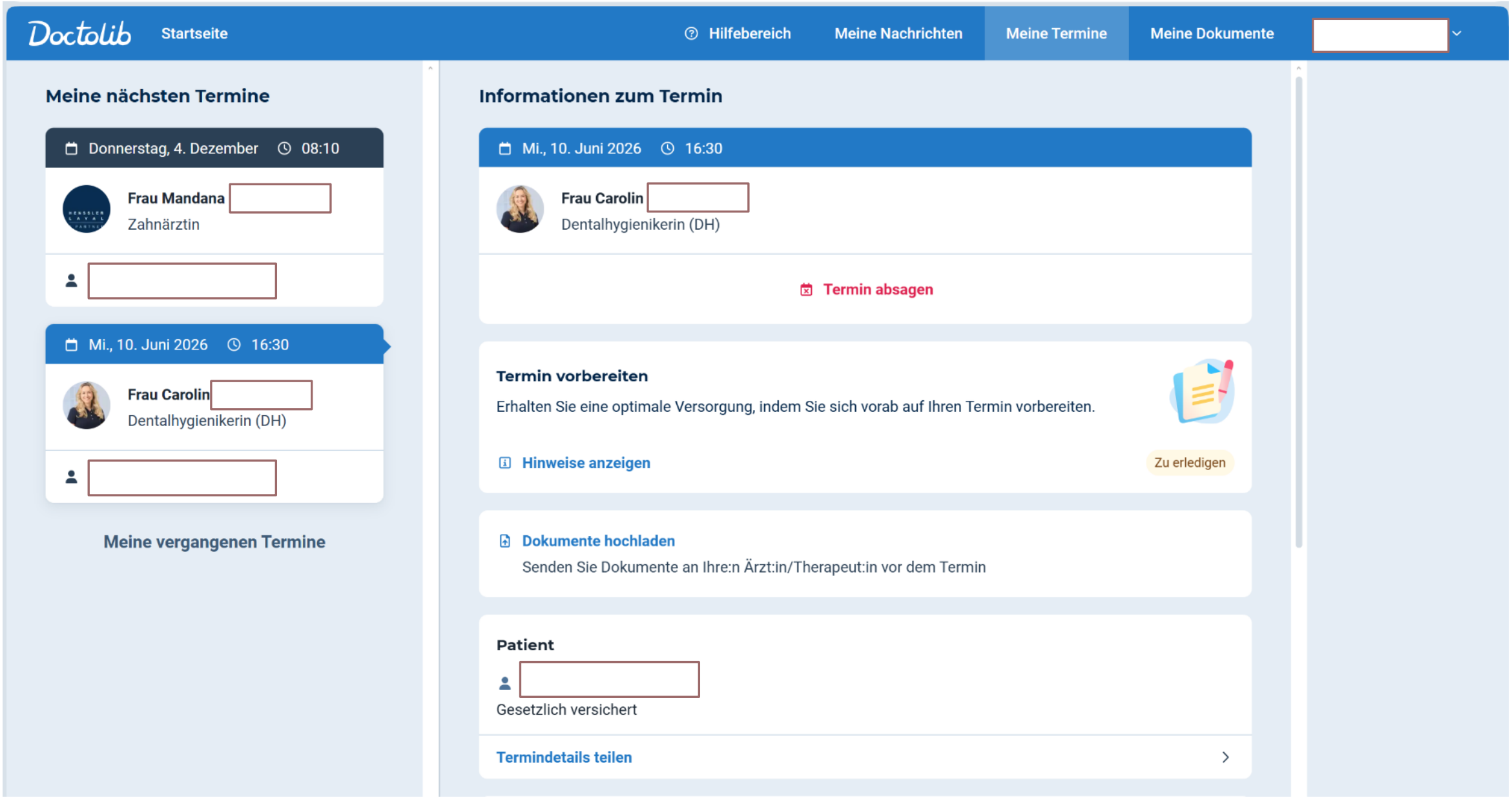
Quelle: Doctolib

Anmeldung / Termine

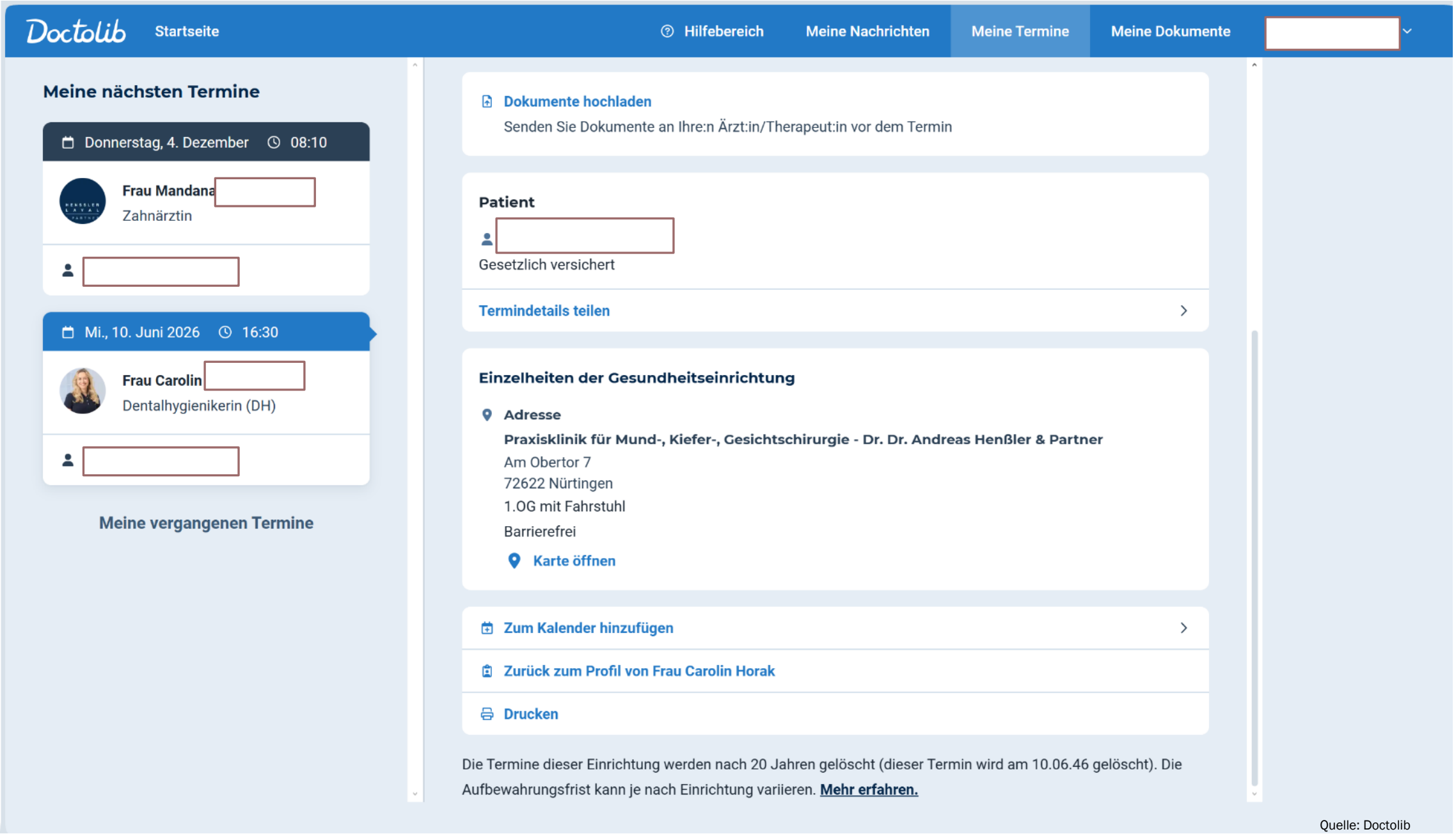




Quelle: Doctolib



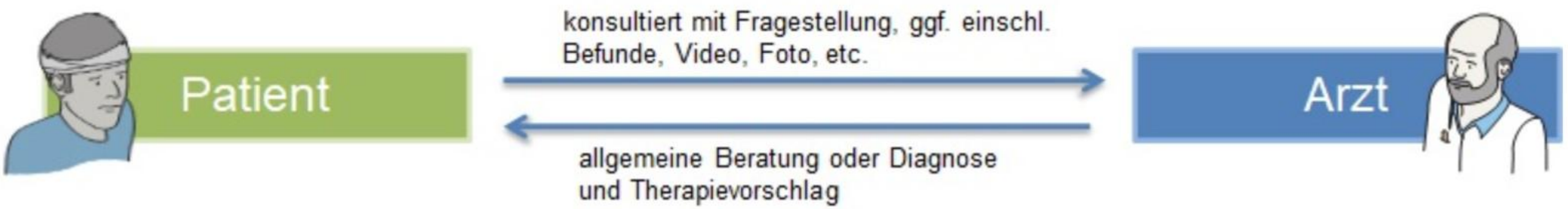
Quelle: Doctolib



Quelle: Doctolib

Video Sprechstunde

Video Sprechstunde



Telekonsultation-Patient mit Ärztin/Arzt © *Bundesärztekammer*

Telemedizin kurz beleuchtet

- **Videotelefonie** ist auch bei Seniorinnen und Senioren recht bekannt und beliebt, z.B. das sprechen mit den Kindern und Enkeln oder Freunden über WhatsApp oder anderer Software.
- Diese Kompetenz hilft auch dabei Ängste und Bedenken zu reduzieren an einer Videosprechstunde teilzunehmen.
- Eine Videosprechstunde kann eine Behandlung begleiten, ohne dass Patientinnen / Patienten im kranken Zustand zur Arztpraxis kommen müssen.
- Seit 2018 dürfen Ärzte und Psychotherapeuten grundsätzlich Telemedizin und Videosprechstunden anbieten.
- Termine können auch über die Krankenkassen oder Notfall Rufnummer 116117 organisiert werden

Quelle: Microsoft.com

Wie funktioniert eine Videosprechstunde?

- **Arzt kontaktieren**: fragen Sie Ihren Arzt / Ärztin, ob sie Videosprechstunden anbieten. Viele Ärzte haben mittlerweile diese Möglichkeit integriert.
- **Terminvereinbarung**: Wenn Ihr Arzt Videosprechstunden anbietet, wird er Ihnen einen Termin für die Sprechstunde geben.
- **Einwilligung**: Sie müssen in der Regel eine Einwilligung für die Videosprechstunde abgeben. Dies kann oft direkt beim Arzt oder online erfolgen.
- **Zugangs-PIN**: Nach der Terminvereinbarung erhalten Sie eine Zugangs-PIN, die per E-Mail oder SMS zugesendet wird. Diese wird benötigt, um an der Videosprechstunde teilzunehmen.
- **Technische Voraussetzungen**: Stellen Sie sicher, dass die notwendige Technik zur Verfügung steht, wie ein Smartphone, Tablet oder Computer mit Kamera und Mikrofon sowie eine stabile Internetverbindung.
- **Privatsphäre**: Achten Sie darauf, dass die Videosprechstunde in einem ruhigen und ungestörten Raum stattfindet kann.

Vorteile der Telemedizin

- Zeitliche und örtliche Flexibilität:
  - Die **Telemedizin** ermöglicht es Patienten, medizinische Hilfe zu erhalten, ohne das Haus verlassen zu müssen.
  - Geeignet für den ländlichen Raum und Gebiete mit weniger Praxen
- Evtl. schnellere Genesung:
  - Durch die virtuelle Arztkonsultation kann der Arzt schnell weitere Behandlungen empfehlen.
- Gesetzliche Krankenkassen übernehmen die Kosten für den Online-Arztbesuch.

Quelle: Microsoft.com

Welche Einschränkungen gibt es?

- Ärzte dürfen per Videosprechstunde keine Diagnosen stellen.
- Die Behandlung darf nur bei Patienten erfolgen, die zuvor schon persönlich von dem betreffenden Arzt behandelt wurden.
- Jedoch dürfen Ärzte alle Patienten medizinisch beraten und sie über bestimmte Verfahren und Behandlungen informieren.

Quelle: Microsoft.com

Die elektronische Patientenakte

ePA-Übersicht

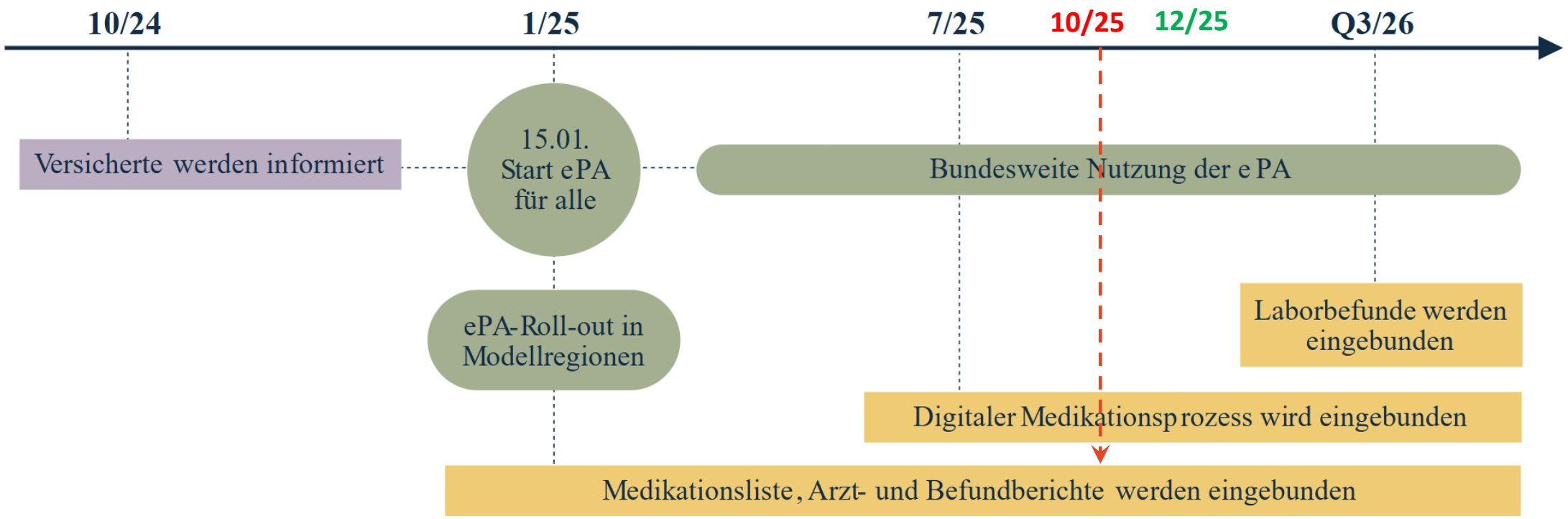
Bundesministerium für Gesundheit

Die ePA für alle

- Die ePA für alle kann seit dem 29. April 2025 für rund 73 Millionen gesetzlich Versicherte bundesweit genutzt werden. Sie wird den Austausch und die Nutzung von Gesundheitsdaten vorantreiben und die Versorgung gezielt unterstützen.
- Die Krankenkassen stellen ihren Versicherten dann ohne deren Zutun eine ePA zur Verfügung. **Wer dies nicht möchte, kann dem ganz einfach widersprechen**.
- Die ePA wird den Austausch und die Nutzung von Gesundheitsdaten zwischen allen behandelnden Ärztinnen, Krankenhäusern oder Praxen verbessen und so gezielt die Versorgung der Patientinnen und Patienten unterstützen.
- Die ePA wird zurzeit (Dezember 2025) nur von ca. 3 % der Versicherten genutzt

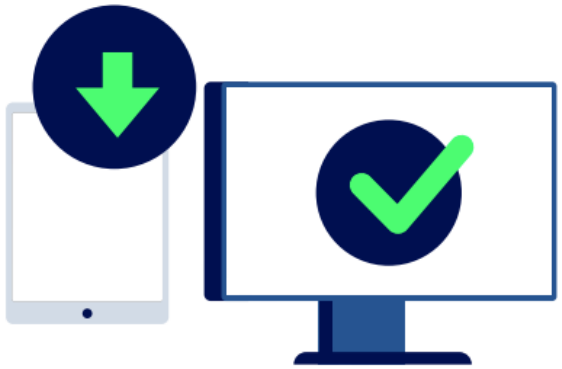
Bundesministerium
für Gesundheit

Zeitplan der ePA



gematik
Nationale Agentur für Digitale Medizin

Wie funktioniert die ePA?



Schritt 1: Laden Sie die App herunter

Laden im App Store JETZT BEI Google Play

Schritt 2: Beantragen Sie die ePA bei Ihrer Krankenkasse

Schritt 3: Registrieren Sie sich in der App

1. mit der neuen NFC-fähigen elektronischen Gesundheitskarte und der dazugehörigen PIN

gematik
Nationale Agentur für Digitale Medizin

Wie funktioniert die ePA?

2.) **mit einer Zwei-Faktor-Authentisierung**

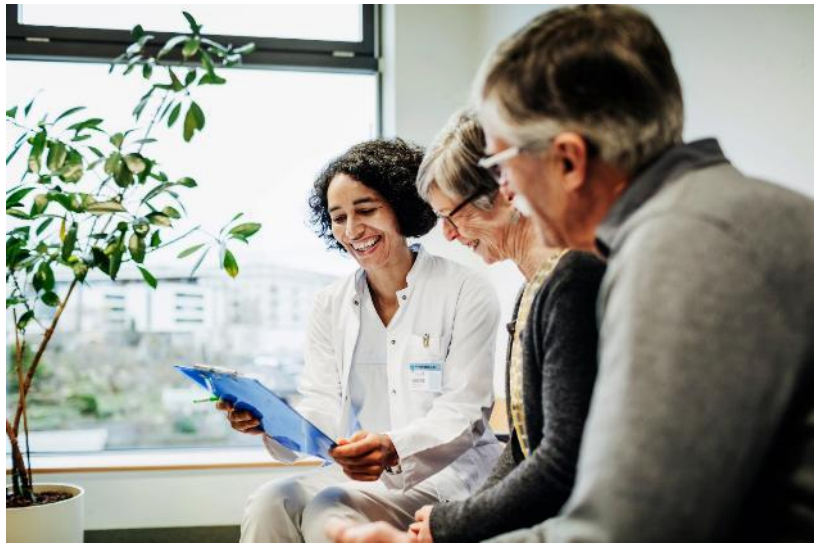
Schritt 4: Lassen Sie die ePA befüllen

Schritt 5: Sie entscheiden, wer zugreifen darf

Die Vorteile der elektronischen Patientenakte

Bundesministerium für Gesundheit

- Der Einblick in Ihre ePA bringt **mehr Transparenz beim Arzt**. Doppeldiagnosen werden vermieden
- Ihre Ärztin hat Ihre **Medikamente sofort im Blick**
- Sehen Sie Ihre Krankendaten ein, wann und wo Sie möchten
- Lästiges Suchen in der Krankengeschichte gehört (hoffentlich bald) der Vergangenheit an
- Wer Ihre ePA lesen darf, können **Sie selbst bestimmen**
- Arztbriefe, Krankengeschichte und Medikationsliste werden einfach in Ihre ePA eingefügt
- Die Daten in Ihrer **ePA sind sicher und geschützt** durch die Telematikinfrastruktur und VPN



Quelle: Microsoft.com

Wichtigsten Merkmale der ePA I

Digitale Gesundheitsakte: Die ePA ist ein digitaler Ordner, in dem persönliche Gesundheitsdaten der Versicherten gespeichert werden. Dies umfasst Informationen zu Behandlungen, Diagnosen, Medikamenten und Impfungen.

- **Versichertengeführte Akte**: Die ePA wird von den Versicherten selbst geführt. Sie haben die Kontrolle darüber, welche Daten gespeichert werden und wer darauf zugreifen kann.

- **Lebenslange Nutzung**: Die ePA ist potenziell lebenslang und begleitet die Versicherten durch ihre gesamte Gesundheitsgeschichte.
- **Unterstützung der Versorgung**: Die ePA fördert den Austausch und die Nutzung von Gesundheitsdaten, was die medizinische Versorgung gezielt unterstützt und verbessert.

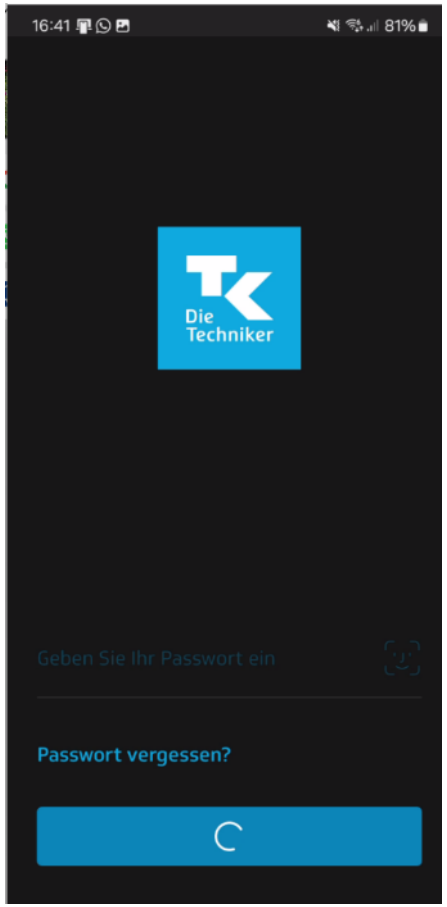
Wichtigsten Merkmale der ePA II

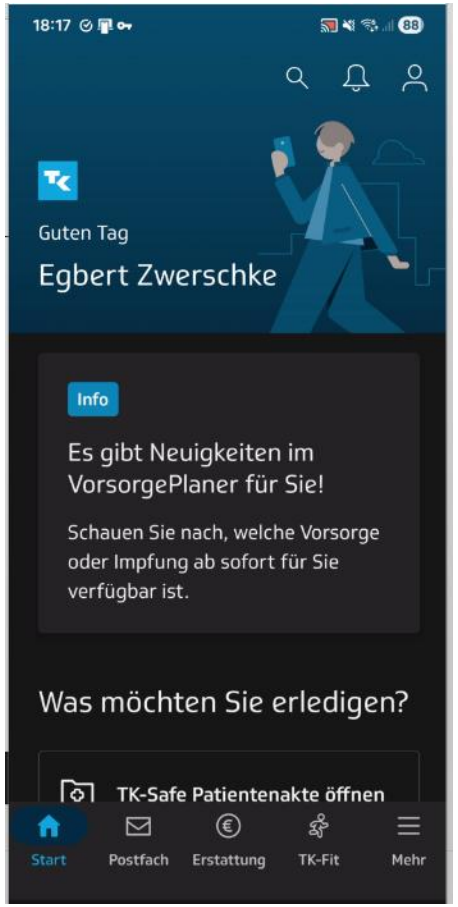
- **Zentrale Rolle in der Telematikinfrastruktur**: Die ePA ist ein zentrales Element der vernetzten Gesundheitsversorgung und spielt eine wichtige Rolle in der Telematikinfrastruktur, die verschiedenen Aktionen im Gesundheitswesen miteinander verbindet.
- **Zugriff durch Fachkräfte**: Ärzte und andere Gesundheitsdienstleister können mit Zustimmung der Versicherten auf die ePA zugreifen, was eine bessere Koordination der Behandlung ermöglicht.

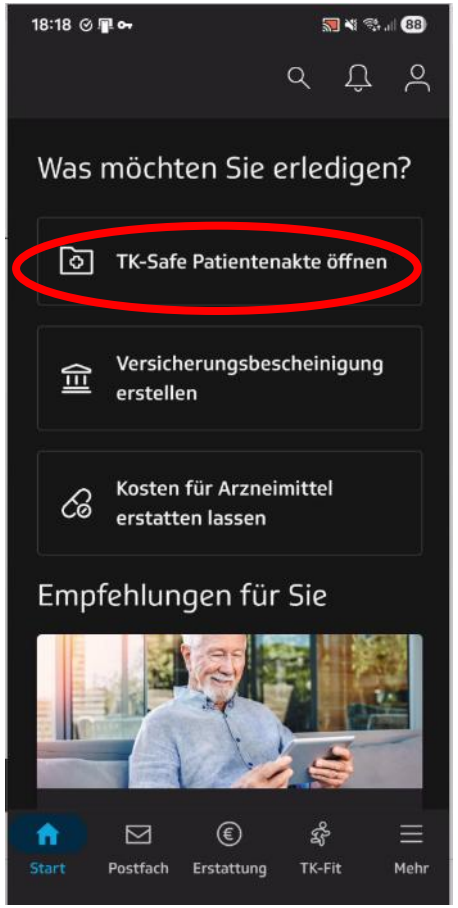
- Die Einführung der ePA zielt darauf ab, die Qualität der Gesundheitsversorgung zu verbessern und **den Patienten mehr Kontrolle über ihre Gesundheitsdaten** zu geben.

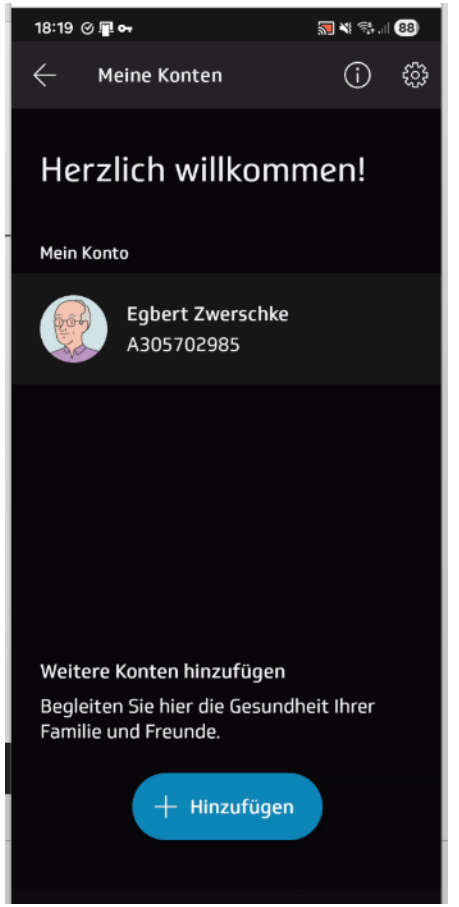
ePA-Beispiel (TK) I

Laden im App Store JETZT BEI Google Play

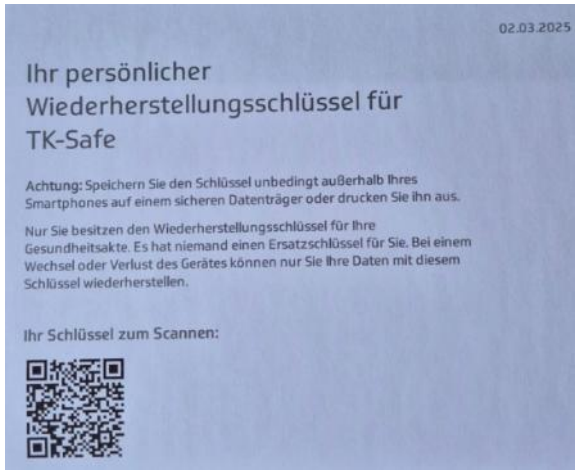




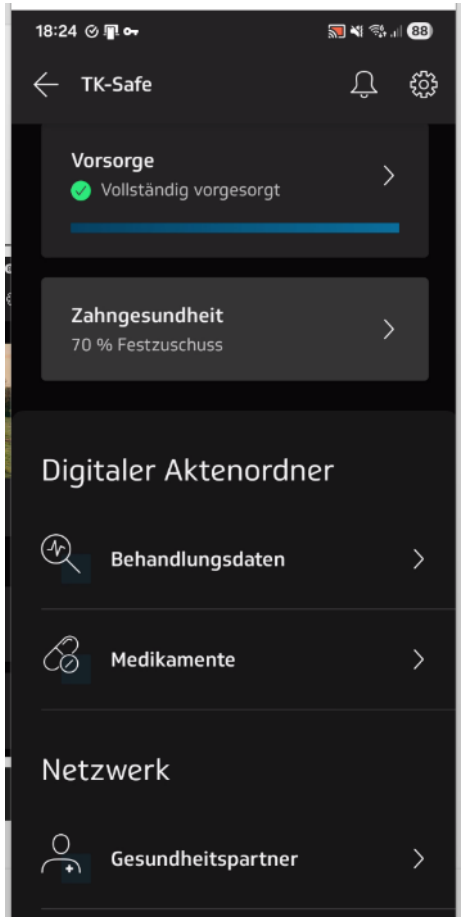




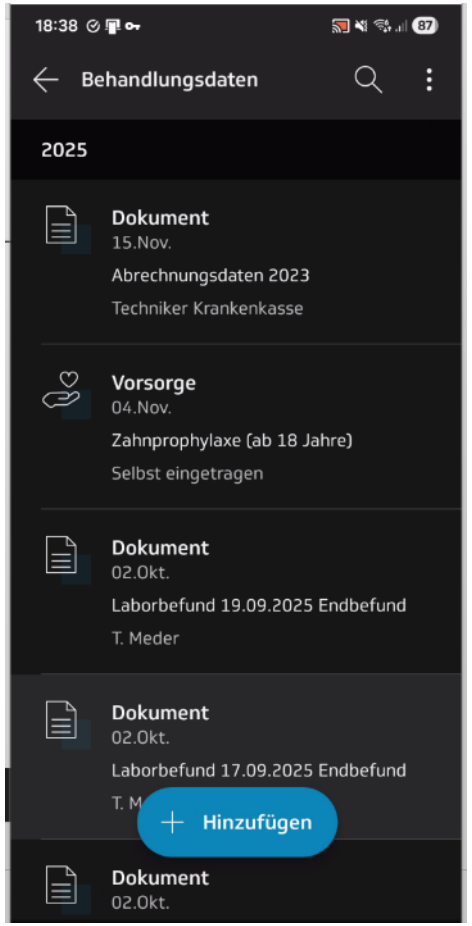
ePA-Beispiel (TK) II



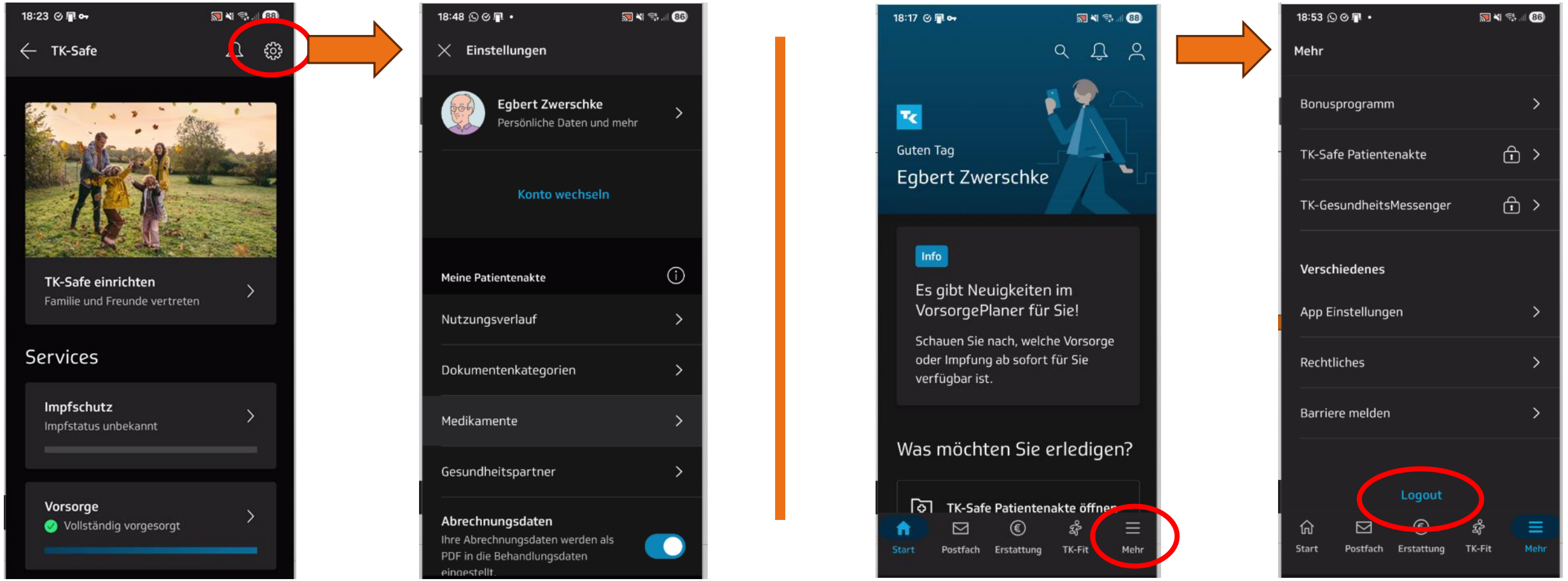
Sicherheitsschlüssel an einem sicheren Ort speichern!



ePA-Beispiel (TK) III



ePA-Menü Beispiel (TK)



Diese Daten müssen Praxen in die ePA einpflegen

Gesetzliche Pflicht ab 1. Oktober 2025, sofern Patienten **nicht** widersprochen haben:

- Befundberichte aus selbst durchgeführten invasiven oder chirurgischen sowie aus nichtinvasiven oder konservativen diagnostischen und therapeutischen Maßnahmen
- eigene Befunddaten aus bildgebender Diagnostik
- Laborbefunde
- Arztbriefe

Quelle: Microsoft.com

Auf Wunsch des Patienten

Patientinnen und Patienten haben Anspruch darauf, dass die Praxen ihre ePA auf Nachfrage mit weiteren Daten befüllen. Gesetzlich festgelegt sind unter anderem:

- Daten aus Behandlungsprogrammen chronischer Krankheiten
- eAU-Bescheinigungen (Patienten-Kopie)
- Daten zu Erklärungen zur Organ- und Gewebespende
- Vorsorgevollmachten und Patientenverfügungen
- Kopie der vom Arzt oder Psychotherapeuten geführten Behandlungsdokumentation

Quelle: Microsoft.com

Widerspruchsmöglichkeiten der Versicherten

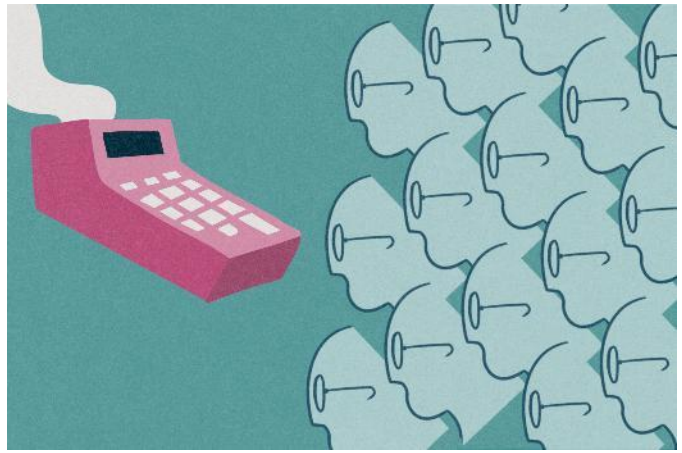
- Gegen die Bereitstellung der ePA
- Gegen den Zugriff einer Praxis auf die ePA
- Gegen die Bereitstellung der Medikationsliste
- Gegen das Einstellen von Dokumenten in einer Behandlungssituation
- Gegen das Einstellen von Abrechnungsdaten
- Gegen die Nutzung der ePA-Daten zu Forschungszwecken

Quelle: Microsoft.com

Digitales Erbe

Was gehört alles zum digitalen Erbe?

- **Online-Konten**
  - Online-Banking
  - Versicherungen
  - Internet Kundenkonten
  - Smartphone-, TV-, Internet-Vertrag
  - Sozialmedia Konten



Quelle: Microsoft.com

Was gehört alles zum digitalen Erbe?

- **Persönliche Daten**
  - E-Mail-Konten und Adressen
  - alle digital gespeicherten Daten auf allen PC‘s, Smartphones etc.
  - Dokumente, Dateien, Fotos…
  - Messenger Daten wie z.B. WhatsApp, Instagram, X, Facebook etc.
  - Daten in einer persönlichen Cloud

Quelle: Microsoft.com

Was gehört alles zum digitalen Erbe?

- **Digitale Produkte und Werte**
  - Gekaufte Software, auch Software Abonnements z.B. Office 365
  - Erworbene Musik und Video Dateien
  - Produkte, die mit einem Nutzerkonto verknüpft sind oder der Käufer nur ein persönliches Nutzungsrecht hatte
  - Kryptowährungen (Zugang und Schlüssel notwendig)

Quelle: Microsoft.com

Wie vererbe ich meinen digitalen Nachlass?

- Zunächst mal einen Überblick verschaffen und schon zu Lebzeiten entscheiden, was mit Daten nach dem Tod passieren soll
- Bestimmen Sie jemanden, der ihren digitalen Nachlass regeln darf.
- Machen Sie von ihren Accounts eine detaillierte Liste
- Halten Sie diese Liste immer aktuell.
- Teilen Sie der bevollmächtigten Person mit, wo sie die Liste finden kann.
- „Inaktivitätsmanager“ bei Google oder "Gedenkstatus" bei z.B. Facebook / Meta einstellen
- Mit den Angehörigen über das digitale Erbe und Wünsche sprechen. Dies kann Missverständnisse und Konflikte im Erbfall vermeiden.
- **….**und, das beste Speichermedium für Zugänge und Passwörter ist immer noch **Papier!**

Quelle: Microsoft.com

Fazit

Auch wenn Sie Virenscanner, VPN, Passwortschutz, Firewall etc. zum Schutz in der Internetnutzung einsetzen,

bleiben Sie kritisch und wachsam!

Vielen Dank für Ihre Aufmerksamkeit

Quellen

Internet:

- https://www.digital-mobil-im-alter.de/fileadmin/dmia/documents/Leitfaden_Digitale-Kompetenzen-fuer-aeltere-Menschen.pdf
- https://www.aok.de/pk/magazin/wohlbefinden/motivation/welche-apps-fuer-senioren-und-seniorinnen-sinnvoll-und-nuetzlich-sind/
- https://www.swr.de/swraktuell/digitales-erbe-nachlasseinstellungen-vollmacht-gedenkzustand-daten-nach-dem-tod-100.html
- https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html
- https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html
- https://de.wikipedia.org/wiki/Kennwortverwaltung
- https://correctiv.org/faktencheck/
- https://www.mimikama.org

Bildquellen:

iStock.com/Extreme Media
Pixabay
BMI
MicroSoft 360
wie unter dem Bild angegeben