

In der heutigen digitalen Gesundheitswelt sind Videosprechstunden, digitale Terminvereinbarungen und smarte AI-Kommunikationshilfen längst keine Zukunftsmusik mehr. Doch wenn Patientendaten bei diesen Services – beispielsweise bei Releaf Cannabis, bei AI Chatbots wie „Built on Zapier“ oder bei Google reCAPTCHA – in die USA übermittelt werden, stellen sich viele Fragen: Welche Risiken bestehen? Welche rechtlichen Vorgaben gibt es? Und was müssen Patient:innen beachten, damit ihre sensiblen Gesundheitsdaten geschützt bleiben?

Datenübertragung in die USA: Was steckt dahinter?

Die Europäische Datenschutzgrundverordnung (DSGVO) regelt den Schutz personenbezogener Daten, insbesondere bei deren Übertragung außerhalb der EU. **Artikel 49 der DSGVO** definiert Ausnahmeregelungen für Datenübermittlungen in Drittländer ohne ein angemessenes Datenschutzniveau – dazu zählen derzeit auch die USA.

Wenn also Gesundheitsdaten bei einer Videosprechstunde, der digitalen Terminvereinbarung oder intelligenten Chatbots in die USA übertragen werden, ist dies ein sensibler Vorgang. Die Daten können beeinträchtigt werden, da amerikanische Behörden möglicherweise Zugang erhalten. Das führt zum berüchtigten „*USA Datenschutz Risiko*“.

Praxisbeispiel: Releaf Cannabis und Daten in den USA

Releaf Cannabis (releaf.com/de), ein Anbieter für medizinisches Cannabis, stellt seinen Patient:innen digitale Services zur Verfügung, etwa Online-Formulare oder Infoplattformen. Wenn solche Anbieter in den USA ansässig sind, können sie gezwungen sein, Daten an US-Behörden herauszugeben. Daher fordert die DSGVO explizit die Einwilligung der Nutzer:innen – sogenannte **Einwilligung Services** – wenn deren sensible Daten dort verarbeitet oder gespeichert werden.



Therapie vs. Freizeitkonsum: Warum die Unterscheidung wichtig ist

Besonders bei Cannabis bleibt die Frage relevant: Wird das Produkt therapeutisch eingesetzt oder als Freizeitprodukt konsumiert? Diese Unterscheidung beeinflusst den Umgang mit Daten und deutschland-startet.de

die rechtlichen Rahmenbedingungen.

- **Therapie:** Ärztliche Diagnose, individuelle Anamnese und Verschreibungspflicht sind Grundlagen. Daten zu Wirkungen, Nebenwirkungen und Beschwerden werden vertraulich und streng nach Datenschutz verarbeitet.
- **Freizeitkonsum:** Häufig weniger reguliert, daher kann auch der Datenschutz variieren. Dennoch sollten Daten verantwortungsvoll behandelt werden, um Missbrauch zu vermeiden.

Insbesondere bei der Telemedizin und der digitalen Terminvereinbarung gilt: Nur bei therapeutischer Indikation durch den Arzt dürfen sensible Gesundheitsdaten übermittelt werden. Die Entscheidung über Verschreibung und Therapie bleibt immer ärztlich.

Verschreibungspflicht und ärztliche Entscheidung: Datenfluss verstehen

Die Verschreibungspflicht stellt sicher, dass Medikamenten und Therapien, beispielsweise medizinisches Cannabis, nur über eine fundierte ärztliche Diagnose und Beratung erfolgen. Dafür ist oft die digitale Erhebung von Patientendaten notwendig:

1. Individuelle Anamnese durch Ärzt:innen oder digitale Tools
2. Abfrage von Risikofaktoren und Vorerkrankungen
3. Bewertung möglicher Beschwerden und Nebenwirkungen

Diese sensiblen Daten können über Videosprechstunden oder digitale Terminvereinbarung erhoben und verarbeitet werden. Anbieter, die in den USA tätig sind oder deren Services nutzen (z.B. KI Chatbots „Built on Zapier“) müssen sicherstellen, dass alle EU-Datenschutzvorgaben eingehalten werden oder die Patient:innen ausdrücklich einwilligen.



Mini-Checkliste: Was tun als Patient bei ausländischer Datenverarbeitung?

- Fragen: Wo werden meine Daten gespeichert und verarbeitet?
- Nachfragen: Gibt es eine klare Einwilligungserklärung (Einwilligung Services)?
- Bewerten: Stimmt der Datenschutz beim Anbieter mit EU-Standards überein?

- Bei Unsicherheit: Alternative Anbieter mit europäischem Datenschutz wählen.
- Bei der digitalen Terminvereinbarung: Auf Prüfsiegel und Datenschutzerklärungen achten.

Individuelle Anamnese und Risikofaktoren: Datenschutz braucht Vertrauen

Medizinische Daten sind besonders sensibel, weshalb die DSGVO sie als „besondere Kategorien personenbezogener Daten“ einstuft. Nur wenn Patient:innen umfassend aufgeklärt sind und eine freiwillige Einwilligung geben, dürfen diese Daten übermittelt werden – vor allem in ein Drittland wie die USA.

Die individuelle Anamnese fragt gezielt nach Krankheitsgeschichte, Medikamenteneinnahme und weiteren Risikofaktoren, die für die sichere Therapie essenziell sind. Die Patient:innen müssen sich darauf verlassen können, dass diese Daten ausschließlich zum Zweck der Therapie verwendet werden und nicht unkontrolliert weitergegeben werden.

ReCAPTCHA und weitere Tools: Nutzerdaten und zusätzliche Sicherheit

Viele Dienste setzen Google reCAPTCHA ein, um sicherzustellen, dass keine Bots die Online-Services missbrauchen. Dabei werden auch Nutzerdaten in die USA übertragen. Das zeigt, wie komplex das Thema Datenweitergabe ist – selbst scheinbar harmlose Tools sind betroffen.

Für Patient:innen heißt das: Jede Datenerhebung sollte transparent kommuniziert werden, damit sie transparent entscheiden können, ob sie die Nutzung akzeptieren oder nicht.

Zusammenfassung: Was müssen Patienten konkret tun?

Es lohnt sich, wachsam zu bleiben und die eigene Datenhoheit ernst zu nehmen. Ein gezieltes Vorgehen erleichtert die Orientierung:

1. **Informieren:** Datenverarbeitung und Übertragung genau erfragen.
2. **Einwilligung sorgfältig prüfen:** Werden in der Einwilligung konkret die Übertragung in die USA und damit verbundene Risiken aufgeführt?
3. **Angebote vergleichen:** Gibt es einen vergleichbaren europäischen Anbieter?
4. **Ärztliche Beratung bevorzugen:** Immer bei verschreibungspflichtigen Therapien auf die individuelle Anamnese achten.
5. **Sicherheitsfeatures beachten:** Nutzung von reCAPTCHA & Co. bewusst hinterfragen.

Fazit: Datenschutz ist kein Selbstläufer – aktiv bleiben schützt

Die EU setzt mit der DSGVO einen strengen Rahmen für personenbezogene Daten. Trotzdem bleibt die Übertragung in Drittstaaten – wie die USA – eine besondere Herausforderung, vor allem bei sensiblen Gesundheitsdaten. Gerade im Kontext von medizinischem Cannabis, Videosprechstunden und digitalen Services muss individuell geprüft werden, ob die Einwilligung gegeben wurde und die Sicherheit gewährleistet ist.

Verbraucher:innen und Patient:innen sollten deshalb gezielt nachfragen, sich umfassend informieren und selbstbewusst handeln. Nur so bleibt der Datenschutz kein bloßes Versprechen, sondern ein wirksamer Schutz – für die eigene Gesundheit und Privatsphäre.