

dsc-Paper
16.04.2026

DSGVO-Zertifizierung als Wettbewerbsvorteil für eHealth-Anbieter: Compliance nachweisen und Reputation stärken mit dem Zertifizierungsstandard „DSGVO – information privacy standard“

1. Executive Summary

eHealth-Anbieter – von spezialisierten SaaS¹- und Plattformanbietern über Videosprechstunden- und Telemedizin-Provider bis hin zu Anbietern von Gesundheits-Apps, Patientenportalen sowie Termin- und Abrechnungsdiensten – verarbeiten entlang des Patienten- und Versorgungszyklus in großem Umfang sensible personenbezogene Daten. Zu den besonders geschützten Gesundheitsdaten² zählen etwa Diagnosen, Befunde (Laborwerte, Vitalparameter), Therapie- und Medikationsdaten (Verordnungen, Dosierungen), OP-/Behandlungsberichte und Bilddaten (Röntgen/CT/MRT³ inkl. DICOM⁴-Metadaten) sowie Abrechnungs- und Leistungsdaten mit Gesundheitsbezug. Dabei erfolgt die Datenverarbeitung vermehrt unter Zuhilfenahme von KI (z. B. zur automatisierten Symptom-Vorsortierung sowie zur Personalisierung und Adhärenz-Unterstützung in Gesundheits-Apps). Aufgrund der mit der Verarbeitung verbundenen Risiken drohen bei DSGVO-Verstößen im eHealth-Kontext hohe Bußgelder von bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes und Schadensersatzansprüche betroffener Personen. Vor diesem Hintergrund verlangen Auftraggeber von eHealth-Anbietern zunehmend objektive, unabhängige Nachweise zur Einhaltung des Datenschutzes, bevor sie sich für eine Zusammenarbeit mit ihnen entscheiden. Auch im Rahmen von Ausschreibungen spielen solche Nachweise eine immer größere Rolle.

Hier bietet die DSGVO mit der genehmigten Zertifizierung nach Artikel 42 ein optimales, passgenaues Tool zum Nachweis von Compliance. Der Zertifizierungsstandard „DSGVO – information privacy standard“ ist eine solche genehmigte Zertifizierung, mit der Verantwortliche und Auftragsverarbeiter den Nachweis erbringen können, dass ihre IT-gestützten Verarbeitungsvorgänge DSGVO-konform sind. Ein Zertifizierungsverfahren erfolgt unparteilich, transparent und qualitätsgesichert in einem zweistufigen Verfahren. Ein erteiltes Zertifikat ist drei Jahre gültig und kann im Rahmen von Rezertifizierungen um jeweils drei weitere Jahre verlängert werden. Zertifizierte eHealth-Anbieter profitieren von Wettbewerbsvorteilen, der Reduktion von Haftungsrisiken, einem gesteigerten Vertrauen ihrer Kunden und der von der jeweiligen Datenverarbeitung betroffenen Patient*innen sowie einem Reputationszuwachs.

¹ Software-as-a-Service

² Vgl. Art. 4 Nr. 15 sowie Art. 9 Abs. 1 DSGVO

³ Computertomographie/Magnetresonanztomographie

⁴ Digital Imaging and Communications in Medicine

2. Ausgangslage: eHealth als Datenschutz-Hochrisikobereich

Im eHealth-Kontext wird eine Vielzahl personenbezogener Daten verarbeitet, womit regelmäßig ein hohes Risiko einhergeht. Als Beispiele hierfür können die Profilbildung und Nutzungs-/Interaktionsanalyse in Gesundheits-Apps und Patientenportalen, KI-gestützte Auswertungen und (teil-)automatisierte Entscheidungs- bzw. Empfehlungssysteme (z. B. Risikoklassifikationen oder Analysen bildgebender Daten zur automatisierten Erkennung und Markierung auffälliger Strukturen als Befundhinweis) sowie die Verarbeitung von Bild-, Audio- und Videodaten im Rahmen von Videosprechstunden genannt werden. Verarbeitet werden dabei so sensible Informationen wie Angaben zu Symptomen und anamnestischen Details, Protokolle aus Chats zwischen Patient*innen und Ärzt*innen oder Therapeut*innen sowie Sensor- und Wearable-Daten zu Vitalparametern.



Neben den jeweiligen Leistungserbringern bzw. Verantwortlichen im Versorgungskontext sind hier auch die von diesen beauftragten eHealth-Anbieter in der Pflicht: Je nach Art der konkret erbrachten Dienstleistung werden diese als Auftragsverarbeiter oder Verantwortliche im Sinne der DSGVO tätig und sind deshalb selbst Adressaten datenschutzrechtlicher Pflichten (vgl. hierzu auch Anhang 1).

So müssen Auftragsverarbeiter u.a. den folgenden Rechtspflichten nachkommen:

- Verarbeitung personenbezogener Daten nur auf dokumentierte Weisung des Verantwortlichen (Auftraggebers) – Artikel 29 DSGVO;
- Treffen geeigneter technischer und organisatorischer Maßnahmen zur Sicherheit der Verarbeitung – Artikel 32 DSGVO;
- Inanspruchnahme weiterer Auftragsverarbeiter nur nach vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung des Verantwortlichen – Artikel 28 Abs. 2 DSGVO;
- Beachtung der Regeln für Übermittlungen personenbezogener Daten in Drittländer außerhalb EU/EWR – Artikel 44 ff. DSGVO;
- Unverzügliche Meldung an den Verantwortlichen bei einer Verletzung des Schutzes personenbezogener Daten („Data Breach“) – Artikel 33 Absatz 2 DSGVO.

eHealth-Anbieter, die ihre Leistungen als Verantwortliche erbringen, treffen noch sehr viel weitergehende Pflichten, z. B.:

- Rechenschaftspflicht: Verantwortliche müssen nachweisen können, dass sie die Grundsätze für die Verarbeitung personenbezogener Daten einhalten – Artikel 5 Abs. 2 DSGVO;
- Treffen von Maßnahmen zur Umsetzung von Privacy by Design and by Default – Artikel 25 DSGVO;
- Gewährleistung von Transparenz: Informationspflichten und Auskunftsrecht gegenüber den von der Verarbeitung betroffenen Personen – Artikel 13 ff. DSGVO;
- Beachtung der rechtlichen Vorgaben der DSGVO zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling – Artikel 22 DSGVO;
- Durchführung einer Datenschutzfolgen-Abschätzung bei Verarbeitungen mit hohem Risiko für Rechte und Freiheiten natürlicher Personen – Artikel 35 DSGVO.

Die Durchführung einer Datenschutzfolgenabschätzung wird im eHealth-Kontext u. a. auch dann oftmals erforderlich sein, wenn KI eingesetzt wird. Als Beispiel sei insoweit der Einsatz eines KI-gestützten Triage- oder Risiko-Scorings genannt, etwa zur Priorisierung von Patienten, zur Empfehlung bestimmter Versorgungspfade oder zur automatisierten Einschätzung von Behandlungsdringlichkeiten. Vielfach wird beim Einsatz von KI auch ein besonderes Augenmerk auf die Einhaltung der Vorgaben von Artikel 22 DSGVO zu legen sein. Ist diese Vorschrift anwendbar, trifft den Verantwortlichen zudem die Pflicht, den betroffenen Personen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung zur Verfügung zu stellen.⁵

3. Risiko: Bußgelder, Schadensersatzansprüche und Vertrauensverlust

Bekanntermaßen drohen Verantwortlichen und Auftragsverarbeitern bei DSGVO-Verstößen Bußgelder von bis zu 20 Mio. € oder 4 % des welt- und konzernweiten Jahresumsatzes. Auf dem Vormarsch sind außerdem Schadensersatzansprüche von Personen, denen wegen eines Verstoßes ein materieller oder immaterieller Schaden entstanden ist.

Im eHealth-Bereich sind bereits Bußgelder in Millionenhöhe erteilt worden. So wurde etwa gegen einen Anbieter aus dem Umfeld medizinischer IT/Labordienstleistungen ein Bußgeld in Höhe von 1,50 Mio. € verhängt, nachdem Gesundheitsdaten von nahezu 500.000 Personen ohne hinreichenden Zugangsschutz auf einem Webserver und damit für jedermann abrufbar gespeichert waren.⁶ Des Weiteren wurde ein Bußgeld in Höhe von 1,19 Mio. € gegen den Betreiber einer Gesundheits-Hotline ausgesprochen, weil Gesprächsaufzeichnungen ungeschützt auf einem Webserver abgelegt wurden.⁷ Weitere Bußgelder wurden beispielsweise wegen wiederholten Falschversands von Arztbriefen und fehlender Protokollierungsfunktionen für Zugriffe auf Patientendaten⁸ sowie wegen einer (auch Patienten betreffenden) Videoüberwachung in einem Unternehmen aus der Gesundheitsbranche⁹ verhängt.



Die Anforderungen an Datenverarbeitungen im Gesundheitsumfeld haben sich durch die jüngere Rechtsprechung des Europäischen Gerichtshofs noch weiter verschärft: Der EuGH interpretiert den Begriff der Gesundheitsdaten weit und erfasst damit auch schon solche Informationen, aus denen nur mittels gedanklicher Kombination oder Ableitung auf den Gesundheitszustand einer Person geschlossen werden kann.¹⁰

Sei es durch ein Bußgeld, Schadensersatzansprüche von betroffenen Personen oder einen Data Breach: Häufig wiegen der Vertrauensverlust bei Kunden und sonstigen Stakeholdern sowie der daraus resultierende Reputationsschaden mindestens ebenso schwer wie der unmittelbare finanzielle Schaden.

⁵ Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO.

⁶ <https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-dedalus-biologie-2022-04-15-FR-1961.php>

⁷ <https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-medhelp-ab-2021-06-08-SE-1328.php>

⁸ <https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-betrieb-im-gesundheitswesen-2022-01-27-DE-1845.php>

⁹ <https://www.dsgvo-portal.de/bussgelder/dsgvo-bussgeld-gegen-unternehmen-aus-2023-03-10-DE-2960.php>

¹⁰ <https://curia.europa.eu/site/upload/docs/application/pdf/2024-10/cp240159de.pdf>

4. Lösung: Zertifizierung nach Artikel 42 DSGVO

Mit der Zertifizierung gemäß Artikel 42 stellt die DSGVO ein verlässliches und praktikables Instrument zum Nachweis von Datenschutz-Compliance zur Verfügung. Zertifiziert werden können Verarbeitungsvorgänge von Verantwortlichen und Auftragsverarbeitern. Das bedeutet im Umkehrschluss, dass reine IT-Produkte wie etwa Software, die erst noch „on-prem“ installiert werden muss, Personen und Management-Systeme nicht in den Anwendungsbereich dieser Vorschrift fallen. So handelt es sich beispielsweise bei der Zertifizierung eines Datenschutz-Managementsystems nach ISO/IEC 27701 oder bei einer Personenzertifizierung, durch die die Fachkunde eines betrieblichen Datenschutzbeauftragten (bDSB) bescheinigt wird, gerade nicht um eine DSGVO-Zertifizierung.

Eine Zertifizierung nach Artikel 42 DSGVO wird durch hierfür akkreditierte Zertifizierungsstellen, die ihre Unabhängigkeit und ihr Fachwissen nachgewiesen haben, und auf der Grundlage eines durch die zuständigen Behörden genehmigten Zertifizierungsprogramms wie etwa des „DSGVO – information privacy standard“ erteilt. Bei Datenschutzsiegeln oder sonstigen Nachweisen, die diese Voraussetzungen nicht erfüllen, handelt es sich also ebenfalls nicht um eine DSGVO-Zertifizierung, auch wenn hier oftmals ein anderer Anschein erweckt wird.

Eine Zertifizierung wird nach erfolgreichem Abschluss eines transparenten Zertifizierungsverfahrens für eine Höchstdauer von drei Jahren erteilt und kann jeweils um drei weitere Jahre verlängert werden, sofern die einschlägigen Kriterien weiterhin erfüllt werden.



Zertifizierte Organisationen profitieren insbesondere von Wettbewerbsvorteilen und einer Haftungsreduktion:

Unternehmen können sich gegenüber ihren Mitbewerbern abheben, indem sie mit einem DSGVO-Zertifikat nachweisen, dass bestimmte Verarbeitungsvorgänge die gesetzlichen Anforderungen erfüllen. Gerade im Bereich der Auftragsverarbeitung ist davon auszugehen, dass sich solche Zertifikate in wenigen Jahren zum Must-Have entwickeln werden (vergleichbar mit ISO/IEC 27001 bei Rechenzentren). Aber auch Dienstleister, die als Verantwortliche im Sinne der DSGVO agieren, können sich durch ein Zertifikat nach Artikel 42 DSGVO vom Wettbewerb hervorheben. Ein Zertifikat kann nicht zuletzt auch im Rahmen von Ausschreibungen (RFP¹¹s) das entscheidende Alleinstellungsmerkmal (USP¹²) sein, das zum Zuschlag führt.

Über ein unabhängiges Zertifikat können zudem die in der DSGVO verankerten Nachweispflichten optimal erfüllt werden, was im Ergebnis auch zu einer Haftungsreduktion führt. So ist eine Zertifizierung bei der Entscheidung darüber, ob ein Bußgeld verhängt wird, von der zuständigen Aufsichtsbehörde gebührend zu berücksichtigen¹³ – sie kann sich also positiv auf eine solche Entscheidung auswirken. Gleiches gilt für die Entscheidung über die Höhe eines etwaigen Bußgeldes. Dies kann auch bilanziell

¹¹ Request for Proposal

¹² Unique Selling Proposition

¹³ Art. 83 Abs. 2 S. 2 lit. j DSGVO

interessant sein (Stichwort: Rücklagen, KonTraG¹⁴, aber auch Versicherungen – gegebenenfalls kann eine DSGVO-Zertifizierung die Höhe einer Versicherungsprämie reduzieren).

5. Best Practice-Ansatz: Der „DSGVO – information privacy standard“

„DSGVO – information privacy standard“ ist ein offiziell genehmigter¹⁵, generischer Zertifizierungsstandard für Artikel 42 DSGVO-Zertifikate, mit dem IT-gestützte Verarbeitungsvorgänge von Verantwortlichen und Auftragsverarbeitern auf DSGVO-Konformität geprüft werden können. Programmeignerin dieses Standards ist die datenschutz cert GmbH, die auch als Zertifizierungsstelle für „DSGVO – information privacy standard“ agiert. Sie ist hierfür von der Deutsche Akkreditierungsstelle GmbH (DAkkS) akkreditiert worden¹⁶ und hat vom Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) Bremen die Befugnis zur Tätigkeit als Zertifizierungsstelle erhalten.



Bei „DSGVO – information privacy standard“ ist ein qualitätsgesichertes, zweistufiges Verfahren etabliert, wonach ein Evaluationsteam – bestehend aus juristischen und technischen Experten*innen – den Verarbeitungsvorgang prüft, bevor die Zertifizierungsstelle die Ergebnisse der Evaluierung bewertet und im Erfolgsfall das Zertifikat erteilt.

Ein Zertifikat gemäß „DSGVO – information privacy standard“ ist drei Jahre gültig. Nach der Erst- und Re-Zertifizierung sind jeweils jährliche Überwachungen vorgesehen.

Ein zentrales Dokument des „DSGVO – information privacy standard“ ist der Kriterienkatalog: Dieser stellt die verbindlichen inhaltlichen Anforderungen für die Prüfung und Beurteilung einer IT-gestützten Verarbeitung personenbezogener Daten dar. Der Kriterienkatalog sieht 50 Kriterien vor, die in acht Bereiche gruppiert sind:

¹⁴ Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

¹⁵ https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks/dsgvo-information_de

¹⁶ <https://www.dakks.de/de/akkreditierte-stelle.html?id=D-ZE-16077-02-00>

- P.1 Zulässigkeit der Datenverarbeitung
- P.2 Grundsätze
- P.3 Pflichten des Kunden
- P.4 Auftragsverarbeitung
- P.5 Technisch-organisatorische Maßnahmen
- P.6 Datenschutz-Management
- P.7 Datenverarbeitung außerhalb der EU
- P.8 Betroffenenrechte

6. Anwendungsbeispiele: Typische Use Cases im eHealth-Kontext

Mit Blick auf eHealth-Anbieter lassen sich beispielsweise die folgenden Arten von Verarbeitungsvorgängen nennen, die nach „DSGVO – information privacy standard“ zertifiziert werden können:

- Verarbeitungsvorgänge beim Betrieb eines Portals zur Arztsuche und Terminvereinbarung;
- Verarbeitungsvorgänge beim Betrieb eines digitalen Patientenportals im Auftrag eines Leistungserbringers oder Netzwerks;
- Verarbeitungsvorgänge im Rahmen des Betriebs einer Videosprechstunden-Plattform;
- Verarbeitungsvorgänge im Zusammenhang mit Telemonitoring/Remote-Patient-Monitoring-Services (z. B. Verarbeitung von Sensor- und Wearable-Daten);
- Verarbeitungsvorgänge bei der Bereitstellung einer Gesundheits-App (SaaS/App-Backend);
- Verarbeitungsvorgänge beim Einsatz KI-gestützter Funktionen in eHealth-Diensten;
- Verarbeitungsvorgänge beim Betrieb einer medizinischen Hotline/eines webbasierten Support- und Meldesystems;
- Verarbeitungsvorgänge im Rahmen digitaler Abrechnungs-, Zahlungs- oder Kostenerstattungsservices;
- Verarbeitungsvorgänge im Zusammenhang mit Studien-/Forschungsrekrutierung über digitale Kanäle;
- Verarbeitungsvorgänge bei Betreibern von Biobanken.



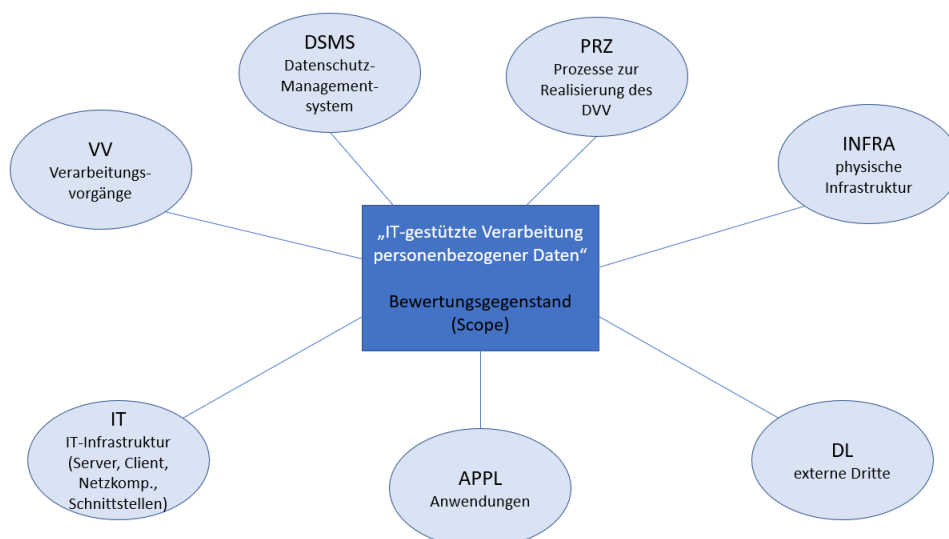
Hinweis:

Hierbei handelt es sich lediglich um eine beispielhafte Aufzählung. Nach „DSGVO – information privacy standard“ zertifiziert werden können jegliche Verarbeitungsvorgänge, die von eHealth-Providern als Verantwortliche oder Auftragsverarbeiter erbracht werden.

7. Expertentipp: Scope präzise definieren – der Schlüssel zum Erfolg

An dieser Stelle soll das Thema „Scoping“ näher beleuchtet werden, da es von fundamentaler Bedeutung für ein erfolgreiches Zertifizierungsverfahren ist. Scoping meint, den Geltungsbereich – also den Umfang der Zertifizierung – klar zu benennen, um zu definieren, was im Rahmen des Zertifizierungsverfahrens geprüft wird und was außerhalb der Betrachtungsgrenzen liegt. Dazu muss eindeutig beschrieben werden, welche Verarbeitungsvorgänge im Einzelnen zum Bewertungsgegenstand gehören, an welchen Standorten diese Tätigkeiten erbracht werden, welche externen Dritten (z. B. Dienstleister) ggf. einbezogen sind, welche IT-Komponenten erforderlich sind und auch welche Prozesse in einer Organisation etabliert sind, um die Datenverarbeitung insgesamt darstellen zu können. Konkret müssen also die folgenden Elemente (Zielobjektkategorien) charakterisiert werden:

- Verarbeitungsvorgänge (VV) zur Konkretisierung der zu zertifizierenden Datenverarbeitung (vgl. hierzu auch die exemplarische Auflistung in Anhang 2);
- Datenschutz-Managementsystem (DSMS) mit den internen Prozessen zur Steuerung der Datenschutz-Konformität;
- Prozesse (PRZ) mit den Tätigkeiten, die für die konkrete Datenverarbeitung benötigt werden;
- Physische Infrastruktur (INFRA) mit Standorten und Räumen;
- IT-Infrastruktur (IT) mit allen relevanten Komponenten (z. B. Servern, Clients, Netzkomponenten, Datenbanken, Speichersystemen und Schnittstellen);
- Applikationen (APPL), über die die Datenverarbeitung realisiert wird;
- Externe Dritte (DL), z. B. Dienstleister, Auftragsverarbeiter, Behörden oder Schwes-tergesellschaften, die für die Realisierung der Datenverarbeitung benötigt werden oder an die personenbezogene Daten übermittelt werden.





Empfehlung:

Es ist ratsam, mit einem kleinen Scope zu beginnen, also mit einer eher übersichtlichen Datenverarbeitung. Später den Scope zu erweitern, ist erfahrungsgemäß sehr viel einfacher, als gleich zu Beginn mit einem mächtigen und komplexen Scope loszulegen. So könnte man etwa in dem in Kapitel 4 genannten Beispiel „Verarbeitungsvorgänge beim Betrieb eines Portals zur Arztsuche und Terminvereinbarung“ zunächst nur die Datenverarbeitung bezüglich der Registrierung und Anmeldung am Portal zertifizieren lassen und den Bewertungsgegenstand dann zu einem späteren Zeitpunkt um zusätzliche Verarbeitungsvorgänge erweitern.



Achtung:

Unzulässig ist es hingegen, bewusst relevante, risikoreiche Bestandteile einer Datenverarbeitung auszusparen (Verbot des „Cherry Picking“).

8. Anleitung: In fünf Schritten zur Zertifizierung nach „DSGVO – information privacy standard“

Der Weg zum Zertifikat führt über die folgenden fünf Schritte:

8.1. Scoping

Im ersten Schritt ist die Datenverarbeitung, für die ein DSGVO-Zertifikat angestrebt wird, zu identifizieren und abzugrenzen, wie bereits im vorangegangenen Kapitel erläutert.

8.2. Vertraut werden mit „DSGVO – information privacy standard“

Wie der Zertifizierungsstandard „DSGVO – information privacy standard“ funktioniert, lässt sich auf der Website zum Zertifizierungsstandard¹⁷ oder direkt in dem dort verlinkten, öffentlich zugänglichen Kriterienkatalog nachlesen.

8.3. Angebot einholen

Die Kosten für ein DSGVO-Zertifikat orientieren sich an der Komplexität und dem Umfang der Datenverarbeitung, die im Scope ist. Deshalb werden einige Informationen benötigt, um den Aufwand zu kalkulieren. Nach dem bereits im ersten Schritt durchgeführten Scoping bedeutet die Zusammenstellung dieser Informationen allerdings nur noch einen verhältnismäßig geringen Aufwand.

8.4. Evaluierung

Von zentraler Bedeutung für die Evaluierung sind die folgenden Meilensteine:

- Übergabe der Referenzdokumentation (Scope-Beschreibung und weitere, vom Kunden zu erstellende Dokumente);

¹⁷ <https://www.ips-dsgvo-zertifikat.de/>

- Basisprüfung;
- Prüfung (rechtlich);
- Prüfung (technisch);
- Auditierung/Inspektion als Site Visit (Vor-Ort-Termin).

Wenn alle Evaluierungsschritte absolviert sind und die zu zertifizierende Datenverarbeitung sämtliche relevanten Anforderungen erfüllt, erstellen die Evaluatoren*innen ihre Berichte und reichen die gesamte Dokumentation in der Zertifizierungsstelle ein.

8.5. Zertifikat

Wenn auch die Zertifizierungsstelle zu dem Schluss kommt, dass alle einschlägigen Anforderungen des Kriterienkatalogs angemessen umgesetzt sind, wird eine positive Zertifizierungsentscheidung getroffen und das Zertifikat ausgestellt.



9. Fazit

Durch eine Zertifizierung nach dem „DSGVO – information privacy standard“ können eHealth-Anbieter Risiken minimieren, Compliance nachweisen, Wettbewerbsvorteile erlangen und Vertrauen und Reputation ausbauen sowie Due Diligence-Prozesse ihrer Kunden beschleunigen.

Wir freuen uns, wenn wir durch dieses dsc-Paper Ihr Interesse an einer Zertifizierung geweckt haben. Bei Fragen zögern Sie bitte nicht, uns anzusprechen. Als unabhängige Zertifizierungsstelle dürfen wir Sie zwar nicht beraten, wir dürfen aber selbstverständlich unsere Methodik erläutern und freuen uns, Ihre Fragen dazu zu beantworten.



Sie erreichen uns unter:

datenschutz cert GmbH
Konsul-Smidt-Straße 88a • 28217 Bremen
Tel.: +49 (0) 421 69 66 32 50
E-Mail: office@datenschutz-cert.de

A. Anhang 1: Kategorien von eHealth-Anbietern und ihre datenschutzrechtlichen Rollen (Verantwortlicher / Auftragsverarbeiter)

| ART DER E-HEALTH-DIENSTLEISTUNG | TYPISCHE DATENSCHUTZ-RECHTLICHE ROLLE |
|---|---|
| KIS/EHR-Software als SaaS / Hosting / Managed KIS | Auftragsverarbeiter |
| Patientenportal / Digital Front Door (Login, Dokumente, Formulare, eConsent) | Auftragsverarbeiter oder Verantwortlicher |
| Terminmanagement & Online-Buchung / Reminder-Services (SMS/E-Mail) | Auftragsverarbeiter |
| Telemedizin-Plattform (Video-Sprechstunde, Chat, Telekonsil) | Auftragsverarbeiter oder Verantwortlicher |
| KI-Triage / Symptom-Assessment / Care-Navigation (z. B. Routing, Priorisierung) | Auftragsverarbeiter |
| Risikoscoring / Frühwarnsysteme (z. B. Sepsis-Scores im stationären Setting) | Auftragsverarbeiter |
| Remote Patient Monitoring (RPM), Wearables-/IoMT-Plattformen | Auftragsverarbeiter oder Verantwortlicher |
| Medizinprodukte-/Gerätehersteller-Cloud (Fleet-/Performance-Monitoring, Serviceportal) | Auftragsverarbeiter |
| PACS/RIS/DICOM-Archiv (Bilddatenmanagement), Teleradiologie-Infrastruktur (ohne Diagnostik) | Auftragsverarbeitung |
| Abrechnung/Revenue Cycle/Factoring/Abrechnungsstellen | Auftragsverarbeiter oder Verantwortlicher |
| Plattformen/Marktplätze/Apps mit Direkt-Endkundenbeziehung (B2C-Gesundheitsapps) | Verantwortlicher |



Hinweis:

In dieser (nicht abschließenden) Übersicht werden die typischerweise einschlägigen datenschutzrechtlichen Rollen aufgelistet. Im konkreten Einzelfall muss aber stets unter Berücksichtigung aller relevanten Aspekte geprüft werden, ob eine Datenverarbeitung als Verantwortlicher oder als Auftragsverarbeiter durchgeführt wird.

B. Anhang 2: Relevante Verarbeitungsvorgänge am Beispiel einer Videosprechstunde

| VERARBEITUNGSVORGANG |
|---|
| Aufruf der Webseite(n)/Applikation |
| Videoverbindung der Individualsprechstunde |
| Videoverbindung der Gruppensprechstunde |
| Suchfunktion auf der Applikation |
| Terminbuchung auf der Applikation |
| Registrierung der Behandler*innen auf der Applikation |
| Registrierung der Patient*innen auf der Applikation |
| Verwaltung von Terminen auf der Applikation |
| Versendung der Zugangsdaten (z. B. TAN) auf der Applikation |
| Funktionen im Accountbereich der Applikation (Dokumentenablage, Chat, Notizen, usw.) |
| Funktionen der Videosprechstunde auf der Applikation (Aufnahme, Dokumententeilung, Chat, Notizen, Konsul, Einladung weiterer Teilnehmer*innen usw.) |
| Online-Kontaktformular auf der Applikation |
| Newsletter-Anmeldung auf der Applikation |
| Online-Support auf der Applikation |
| Bezahlungsfunktion auf der Applikation |



Hinweis:

In dieser Übersicht werden typische Verarbeitungsvorgänge, die für die Zertifizierung einer Videosprechstunde relevant sind bzw. sein können, aufgelistet. Diese Auflistung ist nicht abschließend, es können also im Einzelfall noch weitere Verarbeitungsvorgänge hinzukommen. Genauso gut ist es möglich, dass nicht alle dieser Verarbeitungsvorgänge für die Zertifizierung einer konkreten Videosprechstunde relevant sind.