Anlage 1 DiGAV — Fragebogen gemäß § 4 Absatz 6

Digitale Gesundheitsanwendungen-Verordnung
Stand: 14.03.2026 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

(Fundstelle: BGBl. I 2020, 779 - 792)

Im nachfolgend aufgeführten Fragenbogen ist durch den Hersteller die Erfüllung der Anforderungen nach § 4 zu erklären. Der Hersteller bestätigt die Erfüllung der Anforderungen durch Kennzeichnung in der Spalte „zutreffend“. Die Vorschriften des Datenschutzes und die Anforderungen an die Datensicherheit – Basisanforderungen sind von allen digitalen Gesundheitsanwendungen zu erfüllen. Die Anforderungen Datensicherheit – Zusatzanforderungen bei digitalen Gesundheitsanwendungen mit sehr hohem Schutzbedarf sind von digitalen Gesundheitsanwendungen zu erfüllen, für die im Rahmen der geforderten Schutzbedarfsanalyse ein sehr hoher Schutzbedarf festgestellt wurde.

Nr. Themenfeld Anforderung zutreffend nicht zutreffend zulässige Begründung für „nicht zutreffend“
Datenschutz
1. Datenschutz-Grundverordnung als anzuwendendes Recht Die Verarbeitung personenbezogener Daten durch die digitale Gesundheitsanwendung und deren Hersteller unterfällt der Verordnung (EU) 2016/679 sowie ggf. weiteren Datenschutzregelungen.
2. Einwilligung Wird vor der Verarbeitung von personenbezogenen und -beziehbaren Daten eine freiwillige, spezifische und informierte Einwilligung der betroffenen Person zu den in § 4 Absatz 2 benannten Zwecken der Verarbeitung dieser Daten eingeholt? Es wird keine Einwilligung eingeholt, da der Zweck der Verarbeitung aus einer rechtlichen Verpflichtung des Herstellers der digitalen Gesundheitsanwendung resultiert.
3. Einwilligung Erfolgt die Abgabe von Einwilligungen und Erklärungen der betroffenen Person durchgängig ausdrücklich, d. h. durch eine aktive, eindeutige Handlung der betroffenen Person? Es wird keine Einwilligung eingeholt, da der Zweck der Verarbeitung aus einer rechtlichen Verpflichtung des Herstellers der digitalen Gesundheitsanwendung resultiert.
4. Einwilligung Kann die betroffene Person erteilte Einwilligungen einfach, barrierefrei, jederzeit und auf einem einfach verständlichen Weg mit Wirkung für die Zukunft widerrufen? Es wird keine Einwilligung eingeholt, da der Zweck der Verarbeitung aus einer rechtlichen Verpflichtung des Herstellers der digitalen Gesundheitsanwendung resultiert.
5. Einwilligung Wird die betroffene Person vor Abgabe der Einwilligung auf das Recht und die Möglichkeiten zum Widerruf der Einwilligung hingewiesen? Es wird keine Einwilligung eingeholt, da der Zweck der Verarbeitung aus einer rechtlichen Verpflichtung des Herstellers der digitalen Gesundheitsanwendung resultiert.
6. Einwilligung Wurde die betroffene Person vor Abgabe einer Einwilligung in klarer, verständlicher, nutzerfreundlicher und der Zielgruppe angemessener Form darüber informiert, welche Kategorien von Daten zu welchen Zwecken durch die digitale Gesundheitsanwendung bzw. den Hersteller der digitalen Gesundheitsanwendung verarbeitet werden? Es wird keine Einwilligung eingeholt, da der Zweck der Verarbeitung aus einer rechtlichen Verpflichtung des Herstellers der digitalen Gesundheitsanwendung resultiert.
7. Einwilligung Kann die betroffene Person die Texte der abgegebenen Einwilligungen und Erklärungen jederzeit aus der digitalen Gesundheitsanwendung oder über eine aus der digitalen Gesundheitsanwendung referenzierten Quelle abrufen? Es wird keine Einwilligung eingeholt, da der Zweck der Verarbeitung aus einer rechtlichen Verpflichtung des Herstellers der digitalen Gesundheitsanwendung resultiert.
8. Zweckbindung Erfolgt die Verarbeitung von personenbezogenen Daten durch die digitale Gesundheitsanwendung ausschließlich zu in § 4 Absatz 2 Satz 1 genannten Zwecken oder auf Grundlage sonstiger gesetzlicher Datenverarbeitungsbefugnisse nach § 4 Absatz 2 Satz 3?
9. Datenminimierung und Angemessenheit Sind die über die digitale Gesundheitsanwendung verarbeiteten personenbezogenen Daten dem Zweck angemessen sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt?
10. Datenminimierung und Angemessenheit Hat der Hersteller der digitalen Gesundheitsanwendung sichergestellt, dass die Zwecke der Verarbeitung personenbezogener Daten durch die digitale Gesundheitsanwendung nicht in zumutbarer Weise durch andere, datensparsamere Mittel in gleichem Maße erreicht werden können?
11. Datenminimierung und Angemessenheit Werden gesundheitsbezogene Daten getrennt von ausschließlich für die Leistungsabrechnung erforderlichen Daten gespeichert?
12. Datenminimierung und Angemessenheit Stellt der Hersteller der digitalen Gesundheitsanwendung sicher, dass mit nicht-produktbezogenen Aufgaben betraute

Mitarbeiterinnen und Mitarbeiter keinen Zugriff auf gesundheitsbezogene Daten haben?
13. Datenminimierung und Angemessenheit Sofern die Nutzung der digitalen Gesundheitsanwendung nicht auf ein privates IT-System der nutzenden Person beschränkt ist: –wurden entsprechende Einsatzszenarien in der Datenschutzfolgenabschätzung explizit berücksichtigt?–wird der Versicherte ausdrücklich darauf hingewiesen, dass die Nutzung der digitalen Gesundheitsanwendung in einer potenziell unsicheren Umgebung mit Sicherheitsrisiken einhergeht, die durch den Hersteller der digitalen Gesundheitsanwendung nicht vollständig adressiert werden können? Die Nutzung der digitalen Gesundheitsanwendung ist auf ein privates IT-System der nutzenden Person beschränkt.
–wird bei Nutzung der digitalen Gesundheitsanwendung auf einem nicht nur von dem Versicherten verwendeten IT-System vollständig die – auch temporäre – Speicherung von gesundheitsbezogenen Daten auf diesem IT-System unterbunden?
14. Integrität und Vertraulichkeit Sieht die digitale Gesundheitsanwendung angemessene technische und organisatorische Maßnahmen vor, um personenbezogene Daten gegen unbeabsichtigte oder unzulässige Zerstörung, Löschung, Verfälschung, Offenbarung oder nicht legitimierte Verarbeitungsformen zu schützen?
15. Integrität und Vertraulichkeit Ist der durch die digitale Gesundheitsanwendung gesteuerte Austausch von Daten zwischen dem Endgerät der betroffenen Person und externen Systemen durchgängig gemäß dem Stand der Technik verschlüsselt? Es werden keine personenbezogenen Daten zwischen dem Endgerät der betroffenen Person und externen Systemen ausgetauscht.
16. Richtigkeit Sieht die digitale Gesundheitsanwendung technische und organisatorische Maßnahmen vor, die sicherstellen, dass die über die digitale Gesundheitsanwendung verarbeiteten personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind?
17. Richtigkeit Trifft der Hersteller alle angemessenen Maßnahmen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden?
18. Erforderlichkeit Werden über die digitale Gesundheitsanwendung erhobene personenbezogene Daten nur so lange gespeichert, wie sie für die Erbringung der zugesagten Funktionalitäten der digitalen Gesundheitsanwendung oder zu anderen, unmittelbar aus rechtlichen Verpflichtungen resultierenden Zwecken zwingend erforderlich sind?
19. Erforderlichkeit Werden personenbezogene Daten nach Erfüllung der Zwecke nach § 4 Absatz 2 Satz 1 Nummer 1 bis 4 nicht weiter gespeichert? Die Zwecke der Speicherung und die maximale Speicherdauer sind unter Angabe der Gründe, warum diese Zwecke eine Legitimation der weiteren Speicherung personenbezogener Daten darstellen, durch den Hersteller gesondert zu begründen.
20. Datenportabilität Stellt der Hersteller der digitalen Gesundheitsanwendung Mechanismen bereit, über die die betroffene Person aus der digitalen Gesundheitsanwendung heraus das Recht auf Datenportabilität wahrnehmen und die von ihr, der betroffenen Person, der digitalen Gesundheitsanwendung bereitgestellten, sie betreffenden personenbezogenen Daten in einem geeigneten Format abrufen bzw. in eine andere digitale Gesundheitsanwendung überführen kann?
21. Informationspflichten Ist die Datenschutzerklärung der digitalen Gesundheitsanwendung über die Anwendungswebseite einfach auffindbar, barrierefrei zugänglich und frei einsehbar?
22. Informationspflichten Enthält die Datenschutzerklärung der digitalen Gesundheitsanwendung alle relevanten Informationen zum Hersteller und dessen Datenschutzbeauftragtem, zu dem Zweck der digitalen Gesundheitsanwendung, zu den dazu verarbeiteten Datenkategorien, zum Umgang des Herstellers mit diesen Daten, zum Recht auf Widerruf gegebener Einwilligungen und zu den Möglichkeiten zur Wahrnehmung der Betroffenenrechte und setzt der Hersteller der digitalen Gesundheitsanwendung darüber hinausgehende Informationspflichten nach den Artikeln 13 und 14 der Verordnung (EU) 2016/679 angemessen um?
23. Informationspflichten Ist die Datenschutzerklärung der digitalen Gesundheitsanwendung auch nach der Installation der digitalen Gesundheitsanwendung aus der digitalen Gesundheitsanwendung heraus bzw. in der digitalen Gesundheitsanwendung einfach auffindbar?
24. Informationspflichten Kann die betroffene Person vom Hersteller der digitalen Gesundheitsanwendung Auskunft zu den über sie gespeicherten personenbezogenen Daten in dem in Artikel 15 der Verordnung (EU) 2016/679 festgelegten Umfang erhalten?
25. Informationspflichten Ist in der Datenschutzerklärung der digitalen Gesundheitsanwendung ein nachvollziehbares Löschkonzept enthalten, das das Vorgehen bei Widerruf der Einwilligung und Deinstallation der digitalen Gesundheitsanwendung sowie den Umgang mit Ansprüchen auf Löschung von Daten sowie auf Einschränkung ihrer Verarbeitung regelt und den Anforderungen nach den Artikeln 17 bis 19 der Verordnung (EU) 2016/679 entspricht?
26. Informationspflichten Kann die betroffene Person vom Hersteller der digitalen Gesundheitsanwendung die Berichtigung von sie betreffenden unrichtigen personenbezogenen Daten und die Vervollständigung von sie betreffenden unvollständigen personenbezogenen

Daten verlangen?
27. Informationspflichten Wird die betroffene Person vor der Löschung des Benutzerkontos auf damit möglicherweise verlorengehende Daten und auf das Recht auf Datenübertragung gemäß Artikel 20 der Verordnung (EU) 2016/679 hingewiesen?
28. Datenschutz-Management Hat der Hersteller der digitalen Gesundheitsanwendung ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung umgesetzt, mit dem alle im Zusammenhang mit der digitalen Gesundheitsanwendung eingesetzten Systeme und Prozesse erfasst sind?
29. Datenschutz-Management Hat der Hersteller der digitalen Gesundheitsanwendung alle Personen, die aus ihrer Tätigkeit heraus Zugang zu personenbezogenen Daten haben, auf die Verschwiegenheit verpflichtet?
30. Datenschutz-Folgenabschätzung und Risikomanagement Hat der Hersteller der digitalen Gesundheitsanwendung für die digitale Gesundheitsanwendung eine Datenschutz-Folgenabschätzung durchgeführt und die hierbei durchgeführte Risikoanalyse in die dokumentierten Prozesse eines Risikomanagements überführt, nachdem eine kontinuierliche Neubewertung von Bedrohungen und Risiken erfolgt?
31. Datenschutz-Folgenabschätzung und Risikomanagement Stellt der Hersteller der digitalen Gesundheitsanwendung sicher, dass die Meldung von Verletzungen des Schutzes personenbezogener Daten innerhalb von 72 Stunden nachdem ihm die Verletzung bekannt wurde, an die Aufsichtsbehörde erfolgt?
32. Datenschutz-Folgenabschätzung und Risikomanagement Setzt der Hersteller der digitalen Gesundheitsanwendung die Vorgaben nach Artikel 34 der Verordnung (EU) 2016/679 zur Information Betroffener bei Datenschutzvorfällen um?
33. Nachweispflicht Hat der Hersteller die für das Unternehmen geltenden Datenschutzleitlinien dokumentiert und seine Mitarbeiter in deren Umsetzung geschult?
34. Nachweispflicht Realisiert der Hersteller der digitalen Gesundheitsanwendung Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem bei dem Hersteller gespeicherte personenbezogene Daten eingegeben, verändert oder entfernt worden sind?
35. Nachweispflicht Kann der Hersteller der digitalen Gesundheitsanwendung jederzeit nachweisen, dass zu einer durchgeführten Verarbeitung personenbezogener Daten die erforderliche Einwilligung der betroffenen Person vorlag, soweit die Datenverarbeitung nicht auf anderer rechtlicher Grundlage erfolgt?
36. Verarbeitung im Auftrag Werden über die digitale Gesundheitsanwendung oder den Hersteller der digitalen Gesundheitsanwendung personenbezogene Daten gar nicht an Auftragsverarbeiter oder ausschließlich an Auftragsverarbeiter weitergegeben, die über eine ausreichende Vertrauenswürdigkeit und Haftbarkeit verfügen, angemessene Mechanismen zum Schutz übernommener Daten realisieren und mit dem Hersteller in einem verpflichtenden vertraglichen Verhältnis stehen, das eine Abschwächung der dem Versicherten gegenüber gemachten Zusagen ausschließt?
37. Datenweitergabe an Dritte Werden über die digitale Gesundheitsanwendung oder den Hersteller der digitalen Gesundheitsanwendung keine personenbezogenen Daten an Dritte weitergegeben, sofern dies nicht unmittelbar für die Erfüllung von Zwecken nach § 4 Absatz 2 Satz 1 Nummer 1 oder die Erfüllung gesetzlicher Vorschriften erforderlich und auf diese Zwecke beschränkt ist?
38. Verarbeitung im Ausland Erfolgt die Verarbeitung von Gesundheitsdaten sowie personenidentifizierbaren Bestands- und Verkehrsdaten ausschließlich im Inland, in einem anderen Mitgliedstaat der Europäischen Union, in einem diesem nach § 35 Absatz 7 des Ersten Buches Sozialgesetzbuch gleichgestellten Staat, oder auf Grundlage eines Angemessenheitsbeschlusses gemäß Artikel 45 der Verordnung (EU) 2016/679?
39. Weitere Gewährleistungsziele Ist die Verkettung von personenbezogenen Daten über zwei oder mehr digitale Gesundheitsanwendungen hinweg technisch ausgeschlossen oder muss die betroffene Person für eine Verkettung von Daten über zwei oder mehr digitale Gesundheitsanwendungen hinweg eine explizite, gesondert eingeholte, informierte Einwilligung abgeben? Die digitale Gesundheitsanwendung bietet keine technische Möglichkeit einer Verknüpfung oder eines Datenaustauschs mit anderen digitalen Gesundheitsanwendungen.
40. Weitere Gewährleistungsziele Ist sichergestellt, dass eine Offenbarung von Informationen der betroffenen Person oder über die betroffene Person für die Öffentlichkeit oder eine für die betroffene Person nicht eingrenzbare Personengruppe gar nicht oder immer nur infolge einer expliziten, aktiven Handlung der betroffenen Person erfolgt, der eine zielgruppengerechte Information über die Art der offenbarten Informationen und den möglichen Kreis der Empfänger zugrunde liegt? Die digitale Gesundheitsanwendung unterstützt keine Offenbarung von Informationen der betroffenen Person oder über die betroffene Person für die Öffentlichkeit oder eine für die betroffene Person nicht eingrenzbare Personengruppe.
Datensicherheit

Basisanforderungen, die für alle digitalen Gesundheitsanwendungen gelten
1. Informationssicherheits- und Servicemanagement Hat der Hersteller der digitalen Gesundheitsanwendung ein Informationssicherheitsmanagementsystem (ISMS) gemäß ISO 27001 oder gemäß ISO 27001 auf der Basis von IT-Grundschutz (BSI-Standard 200-2: IT-Grundschutz-Methodik) umgesetzt und kann auf Verlangen des Bundesinstituts für Arzneimittel und Medizinprodukte ein entsprechendes anerkanntes Zertifikat vorlegen?
2. Informationssicherheits- und Service-Management Hat der Hersteller der digitalen Gesundheitsanwendung eine strukturierte Schutzbedarfsanalyse unter Betrachtung der Schadensszenarien „Verstoß gegen Gesetze/Vorschriften/Verträge“, „Beeinträchtigung des informationellen Selbstbestimmungsrechts“, „Beeinträchtigung der persönlichen Unversehrtheit“, „Beeinträchtigung der Aufgabenerfüllung“ und „negative Innen- oder Außenwirkung“ durchgeführt und dokumentiert, in deren Ergebnis für die digitale Gesundheitsanwendung ein normaler, hoher oder sehr hoher Schutzbedarf gemäß der Definition des BSI-Standards 200-2 festgestellt wurde, und kann er die Dokumentation der Schutzbedarfsanalyse auf Verlangen des Bundesinstituts für Arzneimittel und Medizinprodukte vorlegen?
3. Informationssicherheits- und Service-Management Hat der Hersteller der digitalen Gesundheitsanwendung Prozesse eines Release-, Change- und Configuration-Managements unter Berücksichtigung der Vorgaben der Verordnung (EU) 2017/745 umgesetzt und dokumentiert, die sicherstellen, dass Erweiterungen und Anpassungen der digitalen Gesundheitsanwendung, die selbst oder im Auftrag entwickelt wurden, ausreichend getestet und explizit freigegeben wurden, bevor sie produktiv gestellt werden?
4. Verhinderung von Datenabfluss Hat der Hersteller der digitalen Gesundheitsanwendung sichergestellt, dass die Kommunikation der digitalen Gesundheitsanwendung mit anderen Diensten technisch soweit eingeschränkt ist, dass aus der digitalen Gesundheitsanwendung heraus keine ungewollte Datenkommunikation erfolgen kann, über die personenbezogene Daten versendet werden?
5. Verhinderung von Datenabfluss Wird bei jeder über offene Netze stattfindenden Datenkommunikation zwischen verschiedenen Systembestandteilen der digitalen Gesundheitsanwendung zumindest eine Transportverschlüsselung gemäß des Mindeststandards des BSI zur Verwendung von Transport Layer Security (TLS) nach § 44 Absatz 1 Satz 1 des BSI-Gesetzes eingesetzt? Die digitale Gesundheitsanwendung löst keine über offene Netze stattfindende Datenkommunikation aus.
6. Verhinderung von Datenabfluss Prüft die digitale Gesundheitsanwendung bei jedem Zugriff auf über das Internet aufrufbare Funktionalitäten der digitalen Gesundheitsanwendung die Authentizität der aufgerufenen Dienste, bevor personenbezogene Daten mit diesen Diensten ausgetauscht werden? Die digitale Gesundheitsanwendung umfasst keine über das Internet aufrufbare Funktionalität.
7. Verhinderung von Datenabfluss Hat der Hersteller der digitalen Gesundheitsanwendung sichergestellt, dass die digitale Gesundheitsanwendung keine ungewollten Log- oder Hilfsdateien schreibt?
8. Verhinderung von Datenabfluss Hat der Hersteller der digitalen Gesundheitsanwendung sichergestellt, dass die digitale Gesundheitsanwendung keine Fehlermeldungen ausgibt, die möglicherweise vertrauliche Informationen offenbaren?
9. Authentisierung Müssen sich alle die digitale Gesundheitsanwendung nutzenden Personen über eine dem Schutzbedarf der durch die digitale Gesundheitsanwendung verarbeiteten Daten angemessene Methode authentisieren, bevor Zugriffe auf über die digitale Gesundheitsanwendung zugängliche Daten erfolgen können?
10. Authentisierung Ist durch geeignete technische Maßnahmen sichergestellt, dass zur Authentisierung einer die digitale Gesundheitsanwendung nutzenden Person verwendete Daten niemals über ungesicherte Transportverbindungen ausgetauscht werden?
11. Authentisierung Verwendet bzw. beinhaltet die digitale Gesundheitsanwendung eine zentrale Authentisierungskomponente, die mit etablierten Standardkomponenten umgesetzt wurde, die alleinig für die initiale Authentisierung zulässig ist und deren Vertrauenswürdigkeit durch Dienste der digitalen Gesundheitsanwendung verifizierbar ist?
12. Authentisierung Erzwingt die digitale Gesundheitsanwendung, dass eine die digitale Gesundheitsanwendung nutzende Person die für ihre Authentisierung genutzten Daten nur ändern kann, wenn hierbei für die Prüfung der Authentizität dieser Person ausreichende Informationen beigegeben werden?
13. Authentisierung Sofern die Authentisierung unter Nutzung eines Passworts erfolgt:
–Zwingt die digitale Gesundheitsanwendung alle die digitale Gesundheitsanwendung nutzenden Personen, sichere Passwörter gemäß einer Passwort-Richtlinie zu benutzen, die u. a. eine Mindestlänge für Passwörter vorgibt und Grenzwerte für fehlgeschlagene Anmeldeversuche definiert?–Ist sichergestellt, dass Passwörter niemals im Klartext übertragen oder gespeichert werden?–Wird das Ändern oder Zurücksetzen von Passwörtern protokolliert und wird die betroffene Person – sofern geeignete Kontaktdaten vorliegen – sofort über das Zurücksetzen oder Ändern des Passworts informiert? Die Authentisierung erfolgt nicht unter

Nutzung eines Passworts
14. Authentisierung Sofern die digitale Gesundheitsanwendung Authentisierungsdaten auf einem Endgerät oder in einer darauf befindlichen Softwarekomponente speichert: Wird die explizite Zustimmung der die digitale Gesundheitsanwendung nutzenden Person abgefragt („Opt-In“) und wird diese auf die Risiken der Funktion hingewiesen? Die digitale Gesundheitsanwendung speichert keine Authentisierungsdaten auf einem Endgerät oder in einer darauf befindlichen Softwarekomponente
15. Authentisierung Sofern Informationen zur Identität oder Authentizität der die digitale Gesundheitsanwendung nutzenden Person oder zur Authentizität von Komponenten der digitalen Gesundheitsanwendung über dedizierte Sitzungen („Sessions“) zwischen Komponenten der digitalen Gesundheitsanwendung geteilt werden: Die digitale Gesundheitsanwendung nutzt keine Sessions.
–Werden alle Sitzungsdaten sowohl beim Austausch als auch bei der Speicherung mit technischen Maßnahmen, die dem Schutzbedarf der digitalen Gesundheitsanwendung angemessenen, sind geschützt und werden ggf. genutzte Session-IDs zufällig, mit ausreichender Entropie und über etablierte Verfahren erzeugt?–Werden alle in einer Instanz einer digitalen Gesundheitsanwendung aufgebauten Sitzungen mit dem Abbruch oder der Beendigung der Nutzung der digitalen Gesundheitsanwendung invalidiert?–Kann die die digitale Gesundheitsanwendung nutzende Person auch die explizite Invalidierung einer Sitzung erzwingen?–Besitzen Sitzungen eine maximale Gültigkeitsdauer und werden inaktive oder unterbrochene Sitzungen automatisch nach einer bestimmten Zeit invalidiert?–Resultiert die Invalidierung einer Sitzung im Löschen aller Sitzungsdaten und ist sichergestellt, dass eine einmal ungültig gewordene Sitzung auch bei Kenntnis einzelner Sitzungsdaten nicht wieder aktiviert werden kann?
16. Zugriffskontrolle Stellt die digitale Gesundheitsanwendung sicher, dass jeder Zugriff auf geschützte Daten und Funktionen eine Berechtigungsprüfung durchläuft („complete mediation“), für die bei Zugriffen durch Betriebspersonal des Herstellers einer digitalen Gesundheitsanwendung eine dedizierte, alle geschützten Daten einschließende Autorisierungskomponente zum Einsatz kommt („reference monitor“ bzw. „secure node/application“), die eine vorherige sichere Authentisierung der zugreifenden Person erfordert?
17. Zugriffskontrolle Werden alle Berechtigungen initial und per default restriktiv zugewiesen und können Berechtigungen ausschließlich über kontrollierte Verfahren ausgeweitet werden, die bei Änderungen der Berechtigungen für Betriebspersonal des Herstellers einer digitalen Gesundheitsanwendung wirksame Prüf- und Kontrollmechanismen nach einem Mehraugenprinzip beinhalten?
18. Zugriffskontrolle Sofern die digitale Gesundheitsanwendung verschiedene Nutzerrollen vorsieht: Kann jede Rolle nur mit den für die Ausführung der mit der Rolle verbundenen Funktionalitäten erforderlichen Rechten auf Funktionen der digitalen Gesundheitsanwendung zugreifen? Die digitale Gesundheitsanwendung sieht keine unterschiedlichen Nutzerrollen vor.
19. Zugriffskontrolle Stellt der Hersteller der digitalen Gesundheitsanwendung sicher, dass Zugriffe auf Funktionen und Daten der digitalen Gesundheitsanwendung durch Betriebspersonal des Herstellers nur über sichere Netze und Zugangspunkte möglich sind?
20. Zugriffskontrolle Resultieren alle Fehler und Fehlfunktionen der Zugriffskontrolle in einer Ablehnung von Zugriffen?
21. Einbinden von Daten und Funktionen Kann sich der Versicherte ausschließlich innerhalb der Vertrauensdomäne der digitalen Gesundheitsanwendung bewegen bzw. können aus der digitalen Gesundheitsanwendung heraus nur vertrauenswürdige, durch den Hersteller der digitalen Gesundheitsanwendung geprüfte externe Inhalte genutzt werden und wird der Versicherte in diesem Fall informiert, wenn die Vertrauensdomäne der digitalen Gesundheitsanwendung verlassen wird?
22. Einbinden von Daten und Funktionen Sofern die digitale Gesundheitsanwendung der nutzenden Person den Upload von Dateien erlaubt: Ist diese Funktion so weit wie möglich eingeschränkt (z. B. Ausschließen aktiver Inhalte), findet eine Sicherheitsprüfung der Inhalte statt und ist sichergestellt, dass Dateien nur im vorgegebenen Pfad gespeichert werden können? Die digitale Gesundheitsanwendung erlaubt keinen Upload von Dateien.
23. Protokollierung Führt die digitale Gesundheitsanwendung eine vollständige, nachvollziehbare, verfälschungssichere Protokollierung aller sicherheitsrelevanten – d. h. die sichere Identifizierung, Authentisierung und Autorisierung von Personen und Organisationen betreffenden – Ereignisse durch?
24. Protokollierung Werden Protokollierungsdaten automatisiert ausgewertet, um sicherheitsrelevante Ereignisse zu erkennen bzw. proaktiv zu verhindern?
25. Protokollierung Ist der Zugriff auf Protokollierungsdaten durch ein geeignetes Berechtigungsmanagement abgesichert und auf wenige befugte Personen und definierte Zwecke eingeschränkt?
26. Regelmäßige und sichere Aktualisierung Informiert der Hersteller die betroffene Person

(z. B. über Push-Mechanismen oder vor dem Start der digitalen Gesundheitsanwendung), wenn ein sicherheitsrelevantes Update der digitalen Gesundheitsanwendung zur Installation bereitgestellt oder durchgeführt wurde?
27. Sichere Deinstallation Werden bei Deinstallation der digitalen Gesundheitsanwendung alle auf IT-Systemen in der Verfügung der betroffenen Person gespeicherten, durch die digitale Gesundheitsanwendung angelegten Daten und Dateien – einschließlich Caches und temporärer Dateien – gelöscht? Bei der digitalen Gesundheitsanwendung handelt es sich um eine rein webbasierte Anwendung.
28. Härtung Sofern Dienste der digitalen Gesundheitsanwendung über Web-Protokolle aufrufbar sind: –Sind nicht benötigte Methoden der genutzten Protokolle bei allen über offene Netze aufrufbaren Diensten deaktiviert?–Sind die zulässigen Zeichenkodierungen so restriktiv wie möglich eingeschränkt? Die digitale Gesundheitsanwendung umfasst keine über Web-Protokolle aufrufbaren Dienste.
–Sind für alle über offene Netze aufrufbaren Dienste Grenzwerte für Zugriffsversuche festgelegt?–Ist sichergestellt, dass keine sicherheitsrelevanten Kommentare oder Produkt- und Versionsangaben preisgegeben werden?–Werden nicht benötigte Dateien regelmäßig gelöscht?–Ist sichergestellt, dass diese Dienste durch Suchmaschinen nicht erfasst werden?–Wird auf absolute lokale Pfadangaben verzichtet?–Wird ein Abruf von Quelltexten ausgeschlossen?
29. Härtung Sofern die digitale Gesundheitsanwendung Daten verarbeitet, die durch die nutzende Person oder durch nicht durch die digitale Gesundheitsanwendung kontrollierte Quellen bereitgestellt werden: –Werden diese Daten als potenziell gefährlich behandelt und entsprechend validiert und gefiltert?–Erfolgt die Prüfung dieser Daten auf einem vertrauenswürdigen IT-System?–Werden Fehleingaben möglichst nicht automatisch behandelt bzw. werden entsprechende Funktionalitäten sicher umgesetzt, damit ein Missbrauch ausgeschlossen ist?–Werden diese Daten in einer Form kodiert, die sicherstellt, dass ein schadhafter Code nicht interpretiert oder ausgeführt wird?Erfolgt eine Trennung dieser Daten von konkreten Anfragen an datenhaltende Systeme (z. B. über Stored Procedures) bzw. werden Datenanfragen explizit gegen aus solchen Daten begünstigte Angriffsvektoren gesichert? Die digitale Gesundheitsanwendung verarbeitet keine Daten, die durch die nutzende Person oder durch nicht durch die digitale Gesundheitsanwendung kontrollierte Quellen bereitgestellt werden.
30. Härtung Ist durchgängig sichergestellt, dass Fehlerfälle in der digitalen Gesundheitsanwendung behandelt werden und zum Abbruch und ggf. Zurückrollen der angestoßenen Funktionen führen?
31. Härtung Ist die digitale Gesundheitsanwendung durch geeignete Schutzmechanismen vor automatisierten Zugriffen geschützt, sofern diese nicht gewollte Nutzungsmöglichkeiten der digitalen Gesundheitsanwendung realisieren?
32. Härtung Werden für den sicheren Betrieb der digitalen Gesundheitsanwendung relevante Konfigurationsdateien durch geeignete technische Maßnahmen vor Verlust und Verfälschung geschützt? Die digitale Gesundheitsanwendung nutzt keine Konfigurationsdateien bzw. diese sind für den sicheren Betrieb der digitalen Gesundheitsanwendung nicht relevant.
32a. Penetrationstests Hat der Hersteller der digitalen Gesundheitsanwendung für die im Verzeichnis nach § 139e Absatz 1 des Fünften Buches Sozialgesetzbuch aufzunehmende Version der digitalen Gesundheitsanwendung – einschließlich aller Backend-Komponenten – einen Penetrationstest durchgeführt, der dem vom Bundesamt für Sicherheit in der Informationstechnik empfohlenen Durchführungskonzept für Penetrationstests folgt, und – soweit die Anwendbarkeit gegeben ist – auch die jeweils aktuellen OWASP Top-10 Sicherheitsrisiken berücksichtigt, und kann er auf Nachfrage entsprechende Nachweise für die Durchführung der Penetrationstests und die Behebung der dabei gefundenen Schwachstellen vorlegen?
33. Nutzung von Sensoren und externen Geräten Sofern die digitale Gesundheitsanwendung direkt auf Sensoren eines mobilen Endgeräts und/oder externe Hardware (z. B. körpernahe Sensorik) zugreift: –Hat der Hersteller der digitalen Gesundheitsanwendung festgelegt, unter welchen Rahmenbedingungen Sensoren oder angebundene Geräte installiert, aktiviert, konfiguriert und verwendet werden können und wird das Bestehen dieser Rahmenbedingungen vor der Ausführung entsprechender Funktionalitäten soweit als möglich sichergestellt?–Stellt die digitale Gesundheitsanwendung sicher, dass Sensoren und angebundene Geräte bei der Installation bzw. erstmaligen Aktivierung für die digitale Gesundheitsanwendung in eine Grundeinstellung versetzt werden, die einer dokumentierten Sicherheitsrichtlinie entspricht?–Kann der Versicherte von der digitalen Gesundheitsanwendung direkt angesteuerte Sensoren und Geräte in eine Grundeinstellung zurücksetzen, die einer dokumentierten Sicherheitsrichtlinie entspricht?Ist ein Datenaustausch zwischen der digitalen Gesundheitsanwendung und direkt angesteuerten Sensoren oder Geräten erst dann möglich, wenn die Installation und Konfiguration der Sensoren bzw. Geräte vollständig abgeschlossen ist? Die digitale Gesundheitsanwendung greift weder auf Sensoren eines mobilen Endgeräts noch auf externe Hardware zu.

34. Nutzung von Sensoren und externen Geräten Sofern die digitale Gesundheitsanwendung Daten mit externer Hardware (z. B. körpernahe Sensorik) austauscht: –Sind die Abläufe zur Installation, Konfiguration, Aktivierung und Deaktivierung dieser Hardware zielgruppengerecht beschrieben und soweit als möglich gegen Fehlbedienungen gesichert?–Erfolgt eine wechselseitige Authentisierung zwischen der digitalen Gesundheitsanwendung und externer Hardware?–Werden Daten zwischen der digitalen Gesundheitsanwendung und externer Hardware nach einem initialen Handshake nur noch verschlüsselt ausgetauscht?–Ist sichergestellt, dass bei einer Deinstallation der digitalen Gesundheitsanwendung oder bei einer Beendigung von deren Nutzung alle auf externer Hardware gespeicherten Daten gelöscht werden?–Hat der Hersteller der digitalen Gesundheitsanwendung dokumentiert, wie eine angebundene Hardware sicher deaktiviert werden kann, so dass keine Daten verloren gehen und keine sensiblen Daten auf dem Gerät verbleiben? Die digitale Gesundheitsanwendung tauscht keine Daten mit externer Hardware aus.
35. Nutzung von Fremdsoftware Führt der Hersteller eine vollständige Aufstellung aller in der digitalen Gesundheitsanwendung verwendeten Bibliotheken und anderen Software-Produkte, die nicht durch den Hersteller der digitalen Gesundheitsanwendung selbst entwickelt wurden?
36. Nutzung von Fremdsoftware Stellt der Hersteller durch geeignete Verfahren der Marktbeobachtung sicher, dass von diesen Bibliotheken bzw. Produkten ausgehende, bislang nicht bekannte Risiken für den Datenschutz, die Datensicherheit oder die Patientensicherheit zeitnah erkannt werden?
37. Nutzung von Fremdsoftware Hat der Hersteller Verfahren etabliert, um im Fall solcher erkannten Risiken geeignete Maßnahmen wie z. B. eine Sperrung der App und Benachrichtigungen der Nutzer unmittelbar umsetzen zu können?
Zusatzanforderungen bei digitalen Gesundheitsanwendungen mit sehr hohem Schutzbedarf
1. Verschlüsselung gespeicherter Daten Werden auf nicht in der persönlichen Verfügung der nutzenden Person stehenden IT-Systemen verarbeitete personenbezogene Daten auf diesen Systemen nur verschlüsselt gespeichert?
2. (weggefallen)
3. (weggefallen)
4. Authentisierung Wird zumindest für die initiale Authentisierung aller die digitale Gesundheitsanwendung nutzenden Personen eine Zwei-Faktor-Authentisierung erzwungen?
5. Authentisierung Sofern die digitale Gesundheitsanwendung eine Rückfalloption auf eine Ein-Faktor-Authentisierung erlaubt: –Wird die die digitale Gesundheitsanwendung nutzende Person auf die damit verbundenen Risiken hingewiesen und wird ein solcher Rückfall erst nach einer, über eine aktive Handlung bestätigten, Zustimmung der nutzenden Person aktiviert?–Kann die die digitale Gesundheitsanwendung nutzende Person diese Rückfall-Option jederzeit aus der digitalen Gesundheitsanwendung heraus wieder deaktivieren? Die digitale Gesundheitsanwendung erlaubt keine Rückfalloption auf eine Ein-Faktor-Authentisierung.
6. (weggefallen)
7. Authentisierung Sofern die digitale Gesundheitsanwendung eine Nutzerrolle für Leistungserbringer vorsieht:Kann die digitale Gesundheitsanwendung bis spätestens zum 31. Dezember 2020 eine Authentisierung von Leistungserbringern als die die digitale Gesundheitsanwendung nutzende Personen über einen elektronischen Heilberufsausweis mit kontaktloser Schnittstelle unterstützen? Die digitale Gesundheitsanwendung sieht keine Nutzung durch Leistungserbringer vor.
8. Maßnahmen gegen DoS und DDoS Werden an über offene Netze zugängliche Dienste der digitalen Gesundheitsanwendung gesandte Nachrichten (XML, JSON, etc.) und Daten gegen definierte Schemata geprüft? Die digitale Gesundheitsanwendung tauscht keine Daten mit bzw. zwischen über offene Netze zugänglichen Diensten aus.
9. Eingebettete Webserver Sofern zu der digitalen Gesundheitsanwendung gehörende Komponenten Webserver – z. B. zur Administration oder Konfiguration – nutzen: –Ist der Webserver möglichst restriktiv konfiguriert?–Sind nur die benötigten Komponenten und Funktionen des Webservers installiert bzw. aktiviert?–Wird der Webserver soweit möglich nicht unter einem privilegierten Konto betrieben?–Werden sicherheitsrelevante Ereignisse protokolliert?–Ist der Zugang nur nach Authentisierung möglich?–Ist jegliche Kommunikation mit dem Webserver verschlüsselt? Die digitale Gesundheitsanwendung nutzt keinen Webserver.