Bundesinstitut
für Arzneimittel
und Medizinprodukte

Prüfkriterien für die von digitalen Gesundheitsanwendungen (DiGA) und digitalen Pflegeanwendungen (DiPA) nachzuweisenden Anforderungen an den Datenschutz

Version 1.0 vom 24.04.2024

››› WIR HABEN
DIE ANTWORTEN.

Inhaltsverzeichnis

Teil 1: Definitionen

Teil 2: Grundsätze

Teil 3: Verantwortlicher und Auftragsverarbeiter

Teil 4: Anlagen

Teil 1: Definitionen

1 Begriffsbestimmungen

GLSR_1 Schlüsselwörter

GLSR_1.1 Das Schlüsselwort "MUSS" entspricht dem Schlüsselwort "MUST" gemäß [RFC 2119] und zeichnet eine Anforderung als verpflichtend umzusetzen aus. Die Verpflichtung ist normativ, d. h. eine Nicht-Erfüllung kommt einer Nicht-Erfüllung des Kriteriums gleich.

GLSR_1.2 Die Schlüsselwörter "DARF NICHT" und "DARF KEIN" entsprechen dem Schlüsselwort "MUST NOT" gemäß [RFC 2119] und drücken ein Verbot aus. Das Verbot ist normativ, d. h. eine Nicht-Erfüllung kommt einer Nicht-Erfüllung des Kriteriums gleich.

GLSR_1.3 Das Schlüsselwort "SOLL" entspricht dem Schlüsselwort "SHOULD" gemäß [RFC 2119] und drückt eine starke Empfehlung aus, von der in Einzel- und Ausnahmefällen abgewichen werden kann. Eine Empfehlung ist nicht normativ, ein Abweichen MUSS aber durch den Hersteller der digitalen Anwendung nachvollziehbar begründet werden.

GLSR_1.4 Das Schlüsselwort "KANN" bezeichnet eine explizit zulässige Umsetzung einer MUSS-Anforderung bzw. eine anerkannte Abweichung von einer SOLL-Anforderung, die nicht speziell begründet werden muss.

GLSR_2 Begriffsdefinitionen

GLSR_2.1 Es gelten alle Definitionen aus Art. 4 DSGVO.

GLSR_2.2 **Digitale Anwendungen** sind Digitale Gesundheitsanwendungen (DiGA) nach § 33a SGB V und Digitale Pflegeanwendungen (DiPA) nach § 40a SGB XI.

GLSR_2.3 **Hersteller** einer digitalen Anwendung ist die natürliche oder juristische Person, die eine digitale Anwendung hergestellt und diese digitale Anwendung unter ihrem eigenen Namen oder ihrer eigenen Marke in Verkehr gebracht hat. Handelt es sich bei der digitalen Anwendung um ein Medizinprodukt, ist der Hersteller im Sinne dieses Dokuments der Hersteller des Medizinproduktes im Sinne der jeweils geltenden medizinprodukterechtlichen Vorschriften.

GLSR_2.4 Die **Etablierung** einer technisch-organisatorischen Maßnahme oder eines Prozesses umfasst alle Schritte der Verankerung in der gelebten Praxis. Hierzu zählen z. B. Konzeption, Dokumentation, Einführung, Anwendung und kontinuierlichen Verbesserung.

GLSR_2.5 **Zwecke des bestimmungsgemäßen Gebrauchs** einer digitalen Anwendung sind alle Zwecke, die in unmittelbarem Zusammenhang mit der Erreichung des medizinischen bzw. pflegerischen Nutzens oder von patientenrelevanten Struktur- und Verfahrensverbesserungen stehen. Für digitale Gesundheitsanwendungen nach § 33a SGB V sind alleinig Zwecke nach § 4 Absatz 2 Satz 1 Nummer 1 DiGAV Zwecke des bestimmungsgemäßen Gebrauchs.

GLSR_2.6 **Primärer Zweck** einer digitalen Anwendung sind Zwecke des bestimmungsgemäßen Gebrauchs sowie alle Zwecke, die unmittelbar auf die Verankerung der Anwendung im geltenden Rechtsrahmen abzielen (regulatorisch bedingte Zwecke). Für digitale Gesundheitsanwendungen nach § 33a SGB V bilden die Zwecke nach § 4 Absatz 2 Satz 1 Nummer 1 bis 3 zusammen mit den Verpflichtungen aus dem Medizinprodukterecht den primären Zweck der digitalen Gesundheitsanwendung.

GLSR_2.7 **Rechtmäßige Zwecke** einer digitalen Anwendung sind alle Zwecke, die durch die der Anwendung zugrunde liegenden Rechtsverordnung als Grundlage der Verarbeitung personenbezogener Daten zugelassen sind. Für digitale Gesundheitsanwendungen nach § 33a SGB V definieren § 4 Absatz 2 und Absatz 4 DiGAV abschließend die legitimen Zwecke.

GLSR_2.8 Unter dem Begriff der **Vertriebsplattformen** sind alle Quellen zusammengefasst, über die eine digitale Anwendung legal bezogen werden kann. Für mobile Anwendungen sind dies z. B. alle App-Stores, über die der Hersteller die digitale Anwendung zum Download anbietet.

GLSR_2.9 Als **auf die digitale Anwendung bezogene Verarbeitungstätigkeiten** gelten alle vollständig oder teilweise digital ausgeführten Verarbeitungstätigkeiten, die in unmittelbarem Zusammenhang mit der digitalen Anwendung einschließlich ihrer Bereitstellung und Erstattung stehen. Für digitale Gesundheitsanwendungen nach § 33a SGB V gelten alle aus der DiGAV begründeten Verarbeitungstätigkeiten als auf die digitale Anwendung bezogen.

GLSR_2.10 **Verantwortlicher** einer digitalen Anwendung ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet [Art. 4 Satz 1 Nr. 7 DSGVO]

GLSR_2.11 Eine **Zertifizierungsstelle** ist eine unabhängige private oder behördliche Konformitätsbewertungsstelle die Zertifizierungen gemäß ISO/IEC 17065 durchführt (Art. 2 Satz Nr. 13 VO (EG) 765/2008).

GLSR_2.12 In diesem Kriterienkatalog werden die folgenden **Gesetze und Verordnungen** referenziert:

- BDSG: Bundesdatenschutzgesetz (Neufassung von 2017)
- DSGVO: Datenschutz-Grundverordnung
- DiGAV: Digitale-Gesundheitsanwendungen-Verordnung
- DiPAV: Verordnung zur Erstattungsfähigkeit digitaler Pflegeanwendungen
- SGB V: Fünften Buch Sozialgesetzbuch
- DVG: Digitale-Versorgung-Gesetz

- PDSG: Patientendaten-Schutz-Gesetz
- DVPMG: Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz

GLSR_2.13 Eine **inhaltliche Verarbeitung** erfolgt, wenn hierbei die Semantik der Daten und nicht nur lediglich deren technische Repräsentation eine Rolle spielt. Ein Auftragsverarbeiter, der z. B. ein vorgeschaltetes Gateway zum Abfangen von DDoS-Angriffen betreibt, führt in der Regel keine inhaltliche Verarbeitung von Daten durch.

GLSR_2.14 **Daten mit Verarbeitungsrisiken** sind alle Daten, die durch inhaltliche Verfälschung, ungesicherte Herkunft, Unvollständigkeit oder nicht mehr gegebene Aktualität eine Nutzbarkeit der digitalen Anwendung zu ihren rechtmäßigen Zwecken erheblich in Frage stellen. Als erheblich gelten dabei alle Einschränkungen, aus denen sich Risiken für die Rechte und Freiheiten natürlicher Personen ergeben.

1.1 Allgemeine Erläuterungen

Dieses Glossar ist normativer Bestandteil des Kriterienkatalogs zum Datenschutz. Die Gültigkeit der Definitionen ist auf diesen Kriterienkatalog beschränkt.

1.2 Spezifische Erläuterungen

Zu Schlüsselwort GLSR_1.4: Die Definition des Schlüsselworts "KANN" stellt die Semantik des Schlüsselworts "MAY" gemäß [RFC 2119] in den Kontext von MUSS- und SOLL-Kriterien, um zulässige Interpretationen bzw. Umsetzungsmöglichkeiten solcher Anforderungen explizit hervorzuheben. Sofern eine gemäß [RFC 2119] als optional ("MAY") anzusehende Produkteigenschaft oder Maßnahme ohne Bezug zu anderen Anforderungen ist, wird die Formulierung "kann" ohne Hervorhebung durch Großschreibung verwendet.

Zu Definition GLSR_2.3: Die Definition des Begriffs "Hersteller" basiert auf § 1 Absatz 2 DiGAV.

Zur Abgrenzung der Definitionen GLSR_2.3 und GLSR_2.10: Der Begriff "Hersteller" wird verwendet, wenn sich die umzusetzende Anforderung aus der DiGAV oder DiPAV ableitet oder Prozesse betroffen sind, die aus DiGAV oder DiPAV begründet sind (z. B. Studiendurchführung oder Verordnungsprozess). Der Begriff "Verantwortlicher" wird verwendet, wenn sich die umzusetzende Anforderung aus der DSGVO ableitet oder Prozesse betroffen sind, die aus der DSGVO begründet sind (z. B. Durchführung einer Datenschutz-Folgenabschätzung).

Teil 2: Grundsätze

2 Rechtmäßigkeit

2.1 Regulatorische Grundlagen

- Art. 5 DSGVO
- Art. 6 DSGVO
- Art. 7 DSGVO
- Art. 8 DSGVO
- Art. 9 DSGVO
- § 24 BDSG
- § 4 Absatz 2 DiGAV

2.2 Gegenstandsbereich und Motivation

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten über eine DiGA oder DiPA leitet sich aus der DiGAV (§ 4 Absatz 2 Satz 1) bzw. der DiPAV ab, in denen die rechtmäßigen Verarbeitungszwecke festgeschrieben sind. Hier werden auch Regelungen getroffen, welche Einwilligungen der betroffenen Person abverlangt werden können und wie diese kombiniert werden dürfen.

Eine besondere Herausforderung besteht darin, dass Hersteller und Verantwortlicher bei der Verordnung bzw. Bewilligung einer digitalen Anwendung lediglich einen pseudonymen Freischaltcode erhalten und keine Maßnahmen für eine Identifizierung der betroffenen Person vorsehen dürfen, wenn dieses nicht zwingend erforderlich ist (siehe Kriterium "Technische und organisatorische Maßnahmen"). Hiermit können abgegebene Erklärungen zwar einem Nutzer-Account einer digitalen Anwendung zugeordnet werden, nicht aber einer natürlichen Person. Dies spielt insbesondere dadurch eine Rolle, dass so alternative, die betroffene Person potenziell identifizierende Kommunikationsformen wie z. B. E-Mail oder Telefon wegfallen.

In diesem Kriterium wird dargelegt, welche Anforderungen sich unter diesen Rahmenbedingungen und mit Blick auf die spezifischen Erfordernisse einer Integration von digitalen Anwendungen in den ersten Gesundheitsmarkt an eine rechtmäßige Verarbeitung stellen.

2.3 Kriterien

CNST_1 Rechtmäßigkeit durch Einwilligung

CNST_1.1 Jegliche mit der digitalen Anwendung verfolgten Zwecke einer Verarbeitung personenbezogener Daten MÜSSEN auf einer informierten Einwilligung der betroffenen Person nach Art. 9 Absatz 2 Buchstabe a DSGVO basieren oder durch eine Befugnis aus einer Rechtsvorschrift gedeckt sein.

a) Der Verantwortliche der digitalen Anwendung MUSS nachweisen können, dass alle in der digitalen Anwendung umgesetzten Verarbeitungstätigkeiten personenbezogener Daten rechtmäßig sind, da sie zur Erreichung der rechtmäßigen Zwecke der digitalen Anwendung erforderlich sind.

b) Der Verantwortliche der digitalen Anwendung MUSS nachweisen können, dass alle verarbeiteten personenbezogenen Daten rechtmäßig sind, da sie zur Erreichung der rechtmäßigen Zwecke der digitalen Anwendung bzw. zur Umsetzung der rechtmäßigen Verarbeitungstätigkeiten erforderlich sind.

CNST_1.2 Einwilligungen DÜRFEN NICHT zu anderen als den rechtmäßigen Zwecken der digitalen Anwendung eingefordert werden. Die mit den Einwilligungen verbundenen Erklärungen DÜRFEN KEINE über die zulässigen Zwecke hinausgehenden Sachverhalte enthalten.

CNST_1.3 Die Abgabe von Einwilligungen nach Art. 9 Absatz 2 Buchstabe a DSGVO MUSS ausschließlich elektronisch aus der digitalen Anwendung heraus erfolgen. Die Aufforderung zur Abgabe einer Einwilligung MUSS in klarer und knapper Form erfolgen. Die Abgabe der Einwilligung MUSS durch eine eindeutige, aktive und bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten zu den benannten Zwecken durch den benannten Verantwortlichen einverstanden ist.

a) Im Zusammenhang mit der Abgabe einer Einwilligung MUSS ein pseudonymer Benutzeraccount unter einer von der betroffenen Person frei gewählten oder von der Anwendung automatisch vergebenen pseudonymen Identität angelegt werden. Alle von der betroffenen Person abgegeben Einwilligungen MÜSSEN mit diesem Account verknüpft werden, um einen sicheren Widerruf abgegebener Einwilligungen zu ermöglichen.

CNST_1.4 Jede abgegebene Einwilligung MUSS durch die betroffene Person aus der digitalen Anwendung heraus widerrufen werden können. Die betroffene Person MUSS vor der Abgabe einer Einwilligung explizit auf dieses Recht hingewiesen werden.

a) Die betroffene Person DARF KEINE Einwilligungen widerrufen, die nicht mit dem aktuell genutzten Benutzeraccount verknüpft sind.

CNST_1.5 Die Einwilligungserklärung MUSS in verständlicher Form und in klarer, einfacher Sprache gehalten sein. Sie DARF KEINE widersprüchlichen oder potenziell missverständlichen Klauseln enthalten.

a) In der Einwilligungserklärung MÜSSEN zumindest Informationen zu den Zwecken der beabsichtigten Datenverarbeitung, den verarbeiteten Datenkategorien, der Identität des Verantwortlichen sowie ein Hinweis auf die Wahrnehmbarkeit des Widerspruchsrechts gegeben werden.

CNST_1.6 Sofern der Hersteller der digitalen Anwendung eine Verordnung oder Bewilligung der digitalen Anwendung für Kinder und/oder Jugendliche, die jünger als 16 Jahre sind, nicht explizit ausschließt, MUSS die digitale Anwendung alle möglichen Maßnahmen vorsehen, um eine Nutzung der digitalen Anwendung durch nicht einwilligungsfähige Kinder und Jugendliche nur mit dem Einverständnis eines Erziehungsberechtigten zu ermöglichen.

a) Aus der digitalen Anwendung heraus MUSS vor der Einholung der Einwilligung die Einwilligungsfähigkeit der betroffenen Person abgefragt werden. Sofern keine Einwilligungsfähigkeit besteht, MUSS auf das Erfordernis einer Einwilligung eines Erziehungsberechtigten verwiesen werden und dieses abgefragt werden.

b) Der Verantwortliche der digitalen Anwendung MUSS über die Hinweis- und Werbematerialen für verordnende Leistungserbringer darauf hinwirken, dass die Verordnung der digitalen Anwendung nur in Gegenwart eines Erziehungsberechtigten erfolgt und dass dieser explizit auf das Erfordernis der Einwilligung in Vertretung des Kindes/Jugendlichen hingewiesen wird.

CNST_1.7 Der Verantwortliche der digitalen Anwendung MUSS technische und organisatorische Maßnahmen umgesetzt haben, die sicherstellen, dass jegliche Verarbeitung personenbezogener Daten auf einer aktuellen und gültigen Einwilligung basiert.

CNST_2 Verarbeitung zu den primären Zwecken der digitalen Anwendung

CNST_2.1 Bevor eine über die Verarbeitung der übermittelten Verordnungs- bzw. Bewilligungsdaten hinausgehende Verarbeitung personenbezogener Daten in der digitalen Anwendung stattfindet, MUSS der Verantwortliche der digitalen Anwendung die Einwilligung der betroffenen Person für die primären Zwecke der Anwendung einholen.

CNST_2.2 Für eine endgültig in das DiGA- bzw. DiPA-Verzeichnis des BfArM aufgenommene digitale Anwendung DARF der Verantwortliche KEINE Einwilligung zu Verarbeitungen zum Zweck der Durchführung einer Erprobungsstudie abfragen.

CNST_2.3 [nur DiGA] Für eine vorläufig in das DiGA- Verzeichnis des BfArM aufgenommene digitale Anwendung DARF der Verantwortliche KEINE Einwilligung zur Verarbeitung zum Zweck der Durchführung einer Erprobungsstudie abfragen, nachdem die Datenerhebung zum Nachweis positiver Versorgungseffekte abgeschlossen ist.

CNST_2.4 [nur DiGA] Sofern der Hersteller mit dem Spitzenverband Bund der Krankenkassen erfolgsabhängige Preisbestandteile vereinbart hat, KANN der Verantwortliche der digitalen Anwendung eine Einwilligung nach § 4 Absatz 2 Satz 1 Nummer 3 DiGAV abfragen.

CNST_2.5 Der Verantwortliche der digitalen Anwendung MUSS die betroffene Person auf die Auswirkungen des Widerrufs der Einwilligung zu dem primären Zweck der digitalen Anwendung aufmerksam machen. Er DARF dieser aber den Widerruf selbst NICHT verweigern.

a) Der Verantwortliche der digitalen Anwendung MUSS ein Löschkonzept etabliert haben, das regelt, welche Daten beim Widerruf einer Einwilligung zum primären Zweck der digitalen Anwendung gelöscht bzw. gesperrt werden MÜSSEN.

CNST_3 Verarbeitung zu rechtmäßigen Zwecken des Herstellers

CNST_3.1 Die digitale Anwendung KANN über die zur Erzielung positiver Versorgungseffekte oder eines pflegerischen Nutzens erforderlichen Daten hinaus auch Daten zu der dauerhaften Gewährleistung der Sicherheit (bei DiPA), technischen Funktionsfähigkeit, der Nutzerfreundlichkeit, der altersgerechten Nutzbarkeit (bei DiPA) und der Weiterentwicklung der digitalen Anwendung verarbeiten:

a) Hierzu MUSS vor Beginn dieser Verarbeitungen eine explizit auf diese Zwecke abzielende, von allen anderen Einwilligungen unabhängige Einwilligung der betroffenen Person eingefordert werden.

b) Die betroffene Person MUSS diese Einwilligung ablehnen oder zu jedem Zeitpunkt widerrufen können, ohne dass dadurch der bestimmungsgemäße Gebrauch der digitalen Anwendung sowie die Nutzbarkeit eingeschränkt wäre.

CNST_3.2 Der Widerruf der Einwilligung zur Verarbeitung von Daten zu der dauerhaften Gewährleistung der Sicherheit (bei DiPA), technischen Funktionsfähigkeit, der Nutzerfreundlichkeit, der altersgerechten Nutzbarkeit (bei DiPA) und der Weiterentwicklung der digitalen Anwendung MUSS zu einem unmittelbaren Stopp der Verarbeitung von Daten ausschließlich zu Zwecken der dauerhaften Gewährleistung der Sicherheit (bei DiPA), technischen Funktionsfähigkeit, der Nutzerfreundlichkeit, der altersgerechten Nutzbarkeit (bei DiPA) und der Weiterentwicklung der digitalen Anwendung führen.

CNST_3.3 Der Verantwortliche der digitalen Anwendung MUSS ein Löschkonzept etablieren, das regelt, welche Daten beim Widerruf einer Einwilligung zu Zwecken der dauerhaften Gewährleistung der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit und der Weiterentwicklung der digitalen Anwendung gelöscht bzw. gesperrt werden.

2.4 Allgemeine Erläuterungen

Das Kriterium der Rechtmäßigkeit basiert auf den Vorgaben von § 4 DiGAV beziehungsweise § 5 DiPAV sowie den Artikeln 5 bis 9 der DSGVO mitsamt der zugehörigen Erwägungsgründe. Der Begriff der "Einwilligung" folgt der Definition aus Artikel 4 Nummer 11 DSGVO: *„Einwilligung" der betroffenen Person: jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist*.

Für DiGA leiten sich die Anforderungen an die zulässigen Verarbeitungszwecke unmittelbar aus der DiGAV ab:

- § 4 Absatz 2 Satz 1 Nummer 1 bis 3 DiGAV umfassen die für die Nutzung und Erstattung einer DiGA erforderlichen Zwecke einer Verarbeitung personenbezogener Daten durch den DiGA-Hersteller. Die betroffene Person muss in diese Zwecke und die damit verbundene, erforderliche Datenverarbeitung einwilligen, um die DiGA überhaupt nutzen zu können.
- § 4 Absatz 2 Satz 1 Nummer 4 DiGAV erlaubt dem DiGA-Hersteller grundsätzlich, Daten für eigene Zwecke der Verbesserung und Weiterentwicklung seines Produkts zu verarbeiten. Hierzu ist eine separate Einwilligung erforderlich. Eine bestimmungsgemäße

Nutzung der DiGA muss uneingeschränkt möglich sein, auch wenn die betroffene Person diese Einwilligung verweigert.

Für DiPA leiten sich die Anforderungen an die zulässigen Verarbeitungszwecke unmittelbar aus der DiPAV ab:

- § 5 Absatz 3 Satz 1 Nummer 1 der DiPAV umfasst die für die Nutzung einer DiPA erforderlichen Zwecke einer Verarbeitung personenbezogener Daten durch den DiPA-Hersteller. Die betroffene Person muss in diese Zwecke und die damit verbundene, erforderliche Datenverarbeitung einwilligen, um die DiPA überhaupt nutzen zu können.
- § 5 Absatz 3 Satz 1 Nummer 2 der DiPAV erlaubt dem DiPA-Hersteller grundsätzlich, Daten für eigene Zwecke der Verbesserung und Weiterentwicklung seines Produkts zu verarbeiten. Hierzu ist eine separate Einwilligung erforderlich. Eine bestimmungsgemäße Nutzung der DIPA muss uneingeschränkt möglich sein, auch wenn die betroffene Person diese Einwilligung verweigert.

Die Bedingungen zur Abgabe einer wirksamen Einwilligung sind in Art. 7 DSGVO beschrieben und werden insbesondere in den Erwägungsgründen 42 und 43 DSGVO näher erörtert. Etwas detailliertere Erläuterungen hierzu werden in [DSK-20] gegeben.

Die Anforderungen nach Art. 7 Absatz 1 zur Dokumentation von gegebenen Einwilligungen werden im Kriterium "Rechenschaftspflicht" aufgegriffen.

2.5 Spezifische Erläuterungen

Zu Anforderung CNST_1.3: Bei der Verordnung oder Bewilligung einer digitalen Anwendung erhalten Hersteller und Verantwortlicher der digitalen Anwendung lediglich einen für diese pseudonymen Freischaltcode, der die einlösende Person zur Nutzung der digitalen Anwendung berechtigt. Im Kontext der elektronischen Einlösung des Freischaltcodes erteilt die einlösende Person elektronisch ihre Einwilligung zu den Verarbeitungszwecken und Datenverarbeitungen der digitalen Anwendung. Die Einwilligung kann nur elektronisch gegeben werden, da eine Anforderung nach einer schriftlichen oder mündlichen Einwilligung die Pseudonymisierung durchbrechen würde. Da hierfür kein Erfordernis besteht und der Verantwortliche nach Artikel 11 Absatz 1 DSGVO und Erwägungsgrund 57 Satz 1 DSGVO auch nicht verpflichtet ist, hier eine De-Pseudonymisierung zu forcieren, wird die Abgabe der Einwilligung auf den elektronischen Weg beschränkt.

Zu Anforderung CNST_1.4: Da der Verantwortliche die betroffene Person nicht identifizieren kann (siehe Erläuterung Zu Anforderung CNST_1.3), kann eine Einwilligung nur von der Person widerrufen werden, die diese Einwilligung abgegeben hat. Als Bindeglied dient ein zwingend anzulegender Nutzeraccount, gegen den sich die nutzende Person authentisieren muss. Der Widerruf einer Einwilligung durch einen berechtigten Vertreter ist in diesem Fall technisch nicht umsetzbar.

Zu Anforderung CNST_1.5: Im Kurzpapier 20 zur Einwilligung nach DSGVO fordert die DSK, dass die betroffene Person zusätzlich über mögliche Risiken von Datenübermittlungen in Drittländer ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien nach Artikel 46 DSGVO zu informieren ist. Diese Forderung wurde nicht übernommen, da DiGA und DiPA ausschließlich eine Datenübermittlung in Drittländer auf Basis von Art. 45 DSGVO erlauben.

Zu Anforderung CNST_1.6: In Handreichungen der LfDI werden verschiedene Möglichkeiten zur Einwilligungsabfrage bei der Nutzung digitaler Dienste durch nicht einwilligungsfähige Personen vorgeschlagen (z. B. formularbasierte Papierverfahren). Diese erfordern alle eine sichere Identifizierung der betroffenen Person, was für digitale Anwendungen aktuell nicht möglich ist und dem Ziel widersprechen würde, dass Betroffene eine digitale Anwendung pseudonym nutzen können sollen (siehe TOM_2.1).

Zu Anforderung CNST_1.7: siehe hierzu auch Anforderungen TPZ_1.8 und TPZ_1.9 im Abschnitt „Transparenz“, in denen Vorgaben zu Änderungen von AGB und Datenschutzerklärung beschrieben werden.

3 Verarbeitung nach Treu und Glauben

3.1 Regulatorische Grundlagen

- Art. 5 DSGVO

3.2 Gegenstandsbereich und Motivation

Der in Art. 5 DSGVO benannte Grundsatz einer "Verarbeitung nach Treu und Glauben" wird in diesem Kriterium unter die Überschrift "Fairness" gestellt: Der Verantwortliche übervorteilt die betroffene Person nicht und nimmt keine Verarbeitungen von personenbezogenen Daten vor, die außerhalb dessen liegen, was die betroffene Person typischerweise als angemessen und erforderlich erachten würde.

3.3 Kriterien

TuG_1 Ausrichtung an den Erwartungen der betroffenen Person

TuG_1.1 Die digitale Anwendung MUSS die vernünftigen Erwartungen der betroffenen Personen an die Verarbeitung personenbezogener Daten berücksichtigen. Die digitale Anwendung DARF KEINE Datenverarbeitungen vornehmen, mit denen ein vernünftiger Betroffener nicht rechnen würde.

a) Aussagen des Herstellers oder Verantwortlichen zu Grundsätzen, Zielen und Maßnahmen des Datenschutzes in der digitalen Anwendung MÜSSEN präzise formuliert sein und MÜSSEN in der vollen Spannbreite ihrer vernünftigen Interpretationsspielräume durch geeignete technische und organisatorische Maßnahmen abgesichert sein.

b) Sofern der Hersteller oder Verantwortliche mit spezifischen Maßnahmen des Datenschutzes wirbt und damit den Eindruck erweckt, hier über die üblichen Maßnahmen des Wettbewerbs hinauszugehen, MUSS sich dieses auch in den gewählten technischen-organisatorischen Maßnahmen und deren konkreter Umsetzung widerspiegeln.

c) Sofern die Verarbeitung personenbezogener Daten durch die digitale Anwendung über den branchenüblichen Umfang oder die Datenverarbeitung bei Verfahren mit vergleichbaren medizinischen oder pflegerischen Zielen

hinausgeht, MUSS der Verantwortliche der digitalen Anwendung besondere Anstrengungen unternehmen, Erfordernis und Mehrwert dieser Verarbeitung gegenüber der betroffenen Person zu begründen.

TuG_1.2 Die Verarbeitung personenbezogener Daten in der digitalen Anwendung MUSS den Aussagen des Verantwortlichen in der Datenschutzerklärung und der DSFA zu der Anwendung entsprechen. Es DÜRFEN KEINE Kategorien von Daten verarbeitet werden, die nicht in der Datenschutzerklärung benannt sind, und die in der DSFA dargestellten Verarbeitungstätigkeiten MÜSSEN in ihrer Umsetzung den Angaben in der DSFA entsprechen.

TuG_1.3 Der Hersteller der digitalen Anwendung DARF sich in den AGB der digitalen Anwendung KEINE Möglichkeiten vorbehalten, die AGB der digitalen Anwendung ohne Information der betroffenen Person zu ändern. Die Kenntnisnahme der Information MUSS durch die betroffene Person über eine aktive Handlung bestätigt werden.

TuG_1.4 Der Hersteller der digitalen Anwendung DARF KEINE Verwendungsrechte an Inhalten beanspruchen, welche von der betroffenen Person generiert wurden (z. B. Texte, Bilder oder Videos). Ebenso DÜRFEN entsprechende Rechte auch NICHT bei der betroffenen Person angefragt werden.

3.4 Allgemeine Erläuterungen

Die Kriterien zur Verarbeitung nach Treu und Glauben orientieren sich in Bezug auf die für die Zertifizierung als relevant angesehenen Anforderungen an dem Grundgedanken einer "fairen" Verarbeitung personenbezogener Daten und sind damit an der englischen Sprachfassung der DSGVO ausgerichtet ("Personal data shall be processed fairly").

3.5 Spezifische Erläuterungen

Beispiel zu Anforderung TuG_1.1 b: Ein Hersteller, der für eine digitale Anwendung mit einer verschlüsselten Datenspeicherung wirbt, suggeriert damit, dass auch für ihn selbst eine Einsicht in die gespeicherten Daten technisch ausgeschlossen ist. Eine alleinige Festplatten-Verschlüsselung widerspricht zwar nicht der Aussage einer verschlüsselten Speicherung, ist aber nicht die Lösung, die eine betroffene Person vernünftigerweise auf Grundlage der gemachten Werbeaussagen erwarten würde.

Zu Anforderung TuG_1.1 c: Die vernünftigen Erwartungen der betroffenen Person richten sich an dem aus, was in der Branche im Allgemeinen und in vermeintlich ähnlichen Anwendungen üblich ist. Auch Werbeversprechen des Herstellers beeinflussen die Erwartungen der Nutzerinnen und Nutzer. Gleichwohl muss es für innovative Lösungen möglich sein, von den Branchenstandards abzuweichen und disruptive Ansätze zu verfolgen. Dieses wird durch die Anforderung TuG_1.1 c ermöglicht, gleichwohl werden dem Verantwortlichen in diesem Fall besondere Pflichten der Information und Erklärung auferlegt.

4 Transparenz

4.1 Regulatorische Grundlagen

- Art. 5 DSGVO
- Art. 12 DSGVO
- Art. 13 DSGVO
- Art. 14 DSGVO
- § 29 BDSG

4.2 Gegenstandsbereich und Motivation

Dieses Kriterium beinhaltet die Herstellung von Transparenz durch Information: "Die Grundsätze einer fairen und transparenten Verarbeitung machen es erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird. Der Verantwortliche sollte der betroffenen Person alle weiteren Informationen zur Verfügung stellen, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten." [Erwägungsgrund 60 DSGVO]

Annahme ist, dass die Umsetzung der Informationspflichten (insb. Art. 13-14 DSGVO) vorrangig über eine Datenschutzerklärung des Verantwortlichen der digitalen Anwendung erfolgt. Ein großer Teil der Anforderungen zu diesem Kriterium befasst sich entsprechend mit den Inhalten der Datenschutzerklärung, deren Lebenszyklus und der einfachen Zugänglichkeit zu datenschutzrelevanten Informationen.

In Bezug auf die Einwilligung fokussiert dieses Kriterium auf die Informiertheit der Einwilligung. Anforderungen an die Einwilligung selbst und von deren Abgabe durch den Betroffenen sind Gegenstand des Kriteriums "Rechtmäßigkeit". In unmittelbarem Zusammenhang mit den Betroffenenrechten (Art. 15-22 DSGVO) stehende Informationspflichten werden im Kriterium "Intervenierbarkeit" abgehandelt. Dies beinhaltet insbesondere Vorgaben aus Art. 12 Absätze 2 bis 6 DSGVO.

4.3 Kriterien

TPZ_1 Datenschutzerklärung

TPZ_1.1 Die Datenschutzerklärung der digitalen Anwendung MUSS alle relevanten Informationen zum Verantwortlichen und dessen Datenschutzbeauftragtem, zu dem Zweck der digitalen Anwendung, zu den dazu verarbeiteten Datenkategorien, zur Verarbeitung und Weitergabe dieser Daten, zum Recht auf Widerruf gegebener Einwilligungen und zu den Möglichkeiten zur Wahrnehmung der Betroffenenrechte umfassen.

a) Der Verantwortliche der digitalen Anwendung MUSS sich in der Datenschutzerklärung eindeutig und zweifelsfrei identifizieren.

b) Der Verantwortliche der digitalen Anwendung MUSS die nutzende Person in der Datenschutzerklärung zu der Anwendung explizit und in verständlicher Sprache darauf hingewiesen, dass ihre Gesundheitsdaten oder Kopien dieser Daten im Rahmen der Nutzung der Anwendung auch außerhalb ihres mobilen Endgeräts auf Systemen unter der Kontrolle des Verantwortlichen gespeichert werden.

c) Der Verantwortliche der digitalen Anwendung MUSS die nutzende Person in der Datenschutzerklärung zu der Anwendung darüber informieren, welche Daten wann gelöscht bzw. gesperrt werden und wie die nutzende Person von sich aus eine Löschung oder Sperrung auslösen kann.

d) Die Datenschutzerklärung zu der digitalen Anwendung MUSS in allen Sprachen zur Verfügung stehen, die auch von der digitalen Anwendung unterstützt werden. In jedem Fall MUSS eine deutsche Version für die Prüfung durch Aufsichtsbehörden bereitgestellt werden.

TPZ_1.2 Der Verantwortliche der digitalen Anwendung MUSS die nutzende Person in der Datenschutzerklärung zu der Anwendung darüber informieren, welche Daten zu welchen Zwecken im Kontext welcher Verarbeitungstätigkeiten an Dritte weitergegeben werden können. Diese Dritten MÜSSEN eindeutig identifiziert werden, sofern diese nicht erst zur Laufzeit der digitalen Anwendung durch die betroffene Person selbst bestimmt werden (z. B. im Fall einer Weitergabe von Daten an einen behandelnden Arzt).

a) Sofern die digitale Anwendung Funktionen beinhaltet, über die personenbezogene Daten der betroffenen Person an Leistungserbringer übermittelt werden können, bzw. die Leistungserbringern einen Zugriff auf diese Daten ermöglichen, MUSS der Verantwortliche der digitalen Anwendung die betroffene Person informieren, welche Datenkategorien hiervon betroffen sind und wie die betroffene Person steuern kann, welche Leistungserbringer Einsicht in welche Daten erhalten.

TPZ_1.3 Der Verantwortliche der digitalen Anwendung MUSS die nutzende Person in der Datenschutzerklärung zu der Anwendung darüber informieren, welche Daten zu welchen Zwecken ggf. von Dritten übernommen werden und für welche Verarbeitungstätigkeiten diese erforderlich sind. Diese Dritten MÜSSEN eindeutig identifiziert werden und der betroffenen Person müssen Hinweise gegeben werden, wie sie die Datenübernahme ggf. einschränken oder anderweitig steuern kann.

a) Sofern die digitale Anwendung Funktionen beinhaltet, über die personenbezogene Daten der betroffenen Person durch Leistungserbringer zur weiteren Verarbeitung in der digitalen Anwendung bereitgestellt werden können, MUSS der Verantwortliche der digitalen Anwendung die betroffene Person informieren, welche Datenkategorien hiervon betroffen sind, zu welchen Zwecken diese in der Anwendung erforderlich sind und wie die betroffene Person steuern kann, welche Leistungserbringer welche Daten zur Verarbeitung durch die digitale Anwendung einbringen können.

b) Sofern die digitale Anwendung Funktionen beinhaltet, über die personenbezogene Daten der betroffenen Person durch Angehörige oder andere mit der betroffenen Person in (professioneller) Beziehung stehende Personen zur weiteren Verarbeitung in der digitalen Anwendung bereitgestellt werden können, MUSS der Verantwortliche der digitalen Anwendung die betroffene Person informieren, welche Datenkategorien hiervon betroffen sind, zu welchen Zwecken diese in der Anwendung erforderlich sind und wie die betroffene Person steuern kann, welche Personen welche Daten zur Verarbeitung durch die digitale Anwendung einbringen können.

TPZ_1.4 Der Verantwortliche der digitalen Anwendung MUSS sowohl in der Datenschutzerklärung zu der digitalen Anwendung als auch auf der Anwendungswebseite und in der digitalen Anwendung selbst Kontaktdaten angegeben, unter denen die Anwendung nutzenden oder an der Nutzung der Anwendung interessierten Personen Fragen zu Datenschutz und Privatsphäre in deutscher und englischer Sprache beantwortet werden.

a) Der Verantwortliche MUSS in der Datenschutzerklärung zu der digitalen Anwendung und/oder auf der Anwendungswebseite eine konkrete, verbindliche Zusicherung geben, in welcher Frist schriftliche Anfragen zu Datenschutz und Privatsphäre beantwortet werden. Der Verantwortliche KANN dabei zwischen Kern- und Nebenzeiten differenzieren. Die Frist MUSS angemessen und aus typischen Nutzungsszenarien der digitalen Anwendung heraus nachvollziehbar sein.

b) Der Verantwortliche MUSS in der Datenschutzerklärung zu der digitalen Anwendung und/oder auf der Anwendungswebseite eine konkrete, verbindliche Zusicherung zu der Erreichbarkeit bei telefonischen Anfragen zu Datenschutz und Privatsphäre geben. Der Verantwortliche KANN dabei zwischen Kern- und Nebenzeiten differenzieren. Die telefonische Erreichbarkeit MUSS angemessen und aus typischen Nutzungsszenarien der digitalen Anwendung heraus nachvollziehbar sein.

c) Der Verantwortliche MUSS qualitätssichernde Prozesse für Anfragen zu Datenschutz und Privatsphäre etabliert haben. Diese MÜSSEN sowohl qualitative Qualitätsziele als auch die Optimierung von Antwortzeiten adressieren.

TPZ_1.5 Der Verantwortliche MUSS in der Datenschutzerklärung und bei Antworten zu schriftlichen Anfragen auf die Möglichkeit der Beschwerde gegenüber der zuständigen Datenschutzaufsicht hinweisen. Hierbei MÜSSEN zumindest Postadresse und E-Mail-Adresse der zuständigen Datenschutzaufsicht angegeben werden.

TPZ_1.6 Der Verantwortliche der digitalen Anwendung MUSS der betroffenen Person die Möglichkeit geben, die Datenschutzerklärung zu der digitalen Anwendung vor der

Installation der Anwendung frei einzusehen. Hierzu MUSS die betroffene Person die Datenschutzerklärung der digitalen Anwendung zumindest über die Anwendungswebseite und über die genutzten App-Stores einfach auffinden und barrierefrei abrufen können.

TPZ_1.7 Der Verantwortliche der digitalen Anwendung MUSS einen Prozess zur Fortschreibung der Datenschutzerklärung und der gegenüber der betroffenen Person über die Anwendung und die Anwendungswebseite gegebenen datenschutzrelevanten Informationen etablieren.

a) Der Verantwortliche der digitalen Anwendung MUSS bereits in den Design- und Entwicklungsprozessen der Anwendung Prüfungen verankern, über die möglicherweise erforderliche Änderungen der Datenschutzhinweise erfasst werden.

b) Der Verantwortliche der digitalen Anwendung MUSS klare Zuständigkeiten für die Prüfung, Durchführung, Freigabe und Veröffentlichung von Änderungen der Datenschutzhinweise definieren und dokumentieren. Zu jeder Änderung der Datenschutzhinweise MUSS nachvollziehbar sein, wer diese zur Veröffentlichung freigegeben hat.

TPZ_1.8 Durch den Hersteller der digitalen Anwendung einseitig vorgenommene Änderungen an den allgemeinen Geschäftsbedingungen (AGB) DÜRFEN ohne die informierte, explizit bestätigte Kenntnisnahme der betroffenen Person NICHT wirksam werden, sofern diese Änderungen die Rechte des Verantwortlichen ausweiten oder die Rechte der betroffenen Person einschränken.

a) Der Hersteller MUSS die betroffene Person spätestens 14 Tage vor dem Inkrafttreten von einseitig durch den Hersteller geänderten AGB über die vorgenommenen Änderungen und deren Auswirkungen auf die Verarbeitung personenbezogener Daten informieren.

b) Solange Anlass zur Vermutung besteht, dass die betroffene Person einseitig durch den Verantwortlichen geänderte AGB nicht zur Kenntnis genommen hat, MUSS die Verarbeitung auf Grundlage der Version der AGB erfolgen, die der betroffenen Person bekannt ist.

c) Der Hersteller der digitalen Anwendung KANN die Verarbeitung personenbezogener Daten aussetzen und diese Daten sperren, bis die betroffene Person die geänderten AGB zur Kenntnis genommen hat. In diesem Fall MUSS der Hersteller der digitalen Anwendung eine Frist definieren, innerhalb derer die betroffene Person die Kenntnisnahme der einseitig durch den Hersteller geänderten AGB bestätigen muss. Mit Ablauf der Frist – spätestens jedoch nach drei Monaten – MUSS der Hersteller der digitalen Anwendung so verfahren, als ob die betroffene Person alle gegebenen Einwilligungen widerrufen hätte.

TPZ_1.9 Die betroffene Person MUSS bei durch den Verantwortlichen der digitalen Anwendung einseitig vorgenommenen Änderungen an der Datenschutzerklärung mindestens 14 Tage vor Inkrafttreten der Änderungen vom dem Verantwortlichen in verständlicher Form über die Änderungen informiert werden. Insbesondere MUSS aus der Information erkennbar sein, welche Änderungen vorgenommen wurden und ob hiervon der Umfang der Datenverarbeitung oder die Rechte der betroffenen Person berührt sind. Sollte es bei einer wesentlichen Änderung der Datenverarbeitung der Fall

sein, dass sich die ursprünglich von der betroffenen Person erteilte Einwilligung nicht mehr auf die neu gestaltete Datenverarbeitung erstreckt, MUSS eine neue Einwilligung zur Datenverarbeitung von der betroffenen Person eingeholt werden.

TPZ_2 Nutzung durch Kinder und Jugendliche

TPZ_2.1 Sofern Kinder und Jugendliche von der Nutzung der digitalen Anwendung nicht explizit ausgeschlossen sind, MUSS der Verantwortliche der digitalen Anwendung frei zugängliche und über die Anwendungswebseite sowie die Anwendung einfach auffindbare Informationen für die Beurteilung der kind- und jugendspezifischen Eignung bereitstellen (z. B. verlässliche Altersklassifizierung, Käufe, Kommunikationsrisiken).

TPZ_2.2 Sofern Kinder und Jugendliche von der Nutzung der digitalen Anwendung nicht explizit ausgeschlossen sind, MUSS der Verantwortliche der digitalen Anwendung sicherstellen, dass in allen Informationsmaterialien und bei der Abfrage von Einwilligungen in besonderem Maße Rücksicht darauf genommen ist, dass sich Kinder der Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind.

a) Sofern sich die digitale Anwendung direkt an Kinder und Jugendliche wendet, MÜSSEN Informationen und Hinweise in einer klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann.

TPZ_3 Informiertheit der Einwilligung

TPZ_3.1 Der Verantwortliche der digitalen Anwendung MUSS die betroffene Person vor Abgabe einer Einwilligung in klarer, verständlicher, nutzerfreundlicher und der Zielgruppe angemessener Form darüber informieren, welche Kategorien von Daten zu welchen Zwecken durch die digitale Anwendung bzw. den Verantwortlichen der digitalen Anwendung verarbeitet werden. Dieses DARF NICHT allein über einen Verweis auf die Datenschutzerklärung erfolgen.

TPZ_3.2 Die betroffene Person MUSS über die digitale Anwendung einsehen können, welche Einwilligungen sie abgegeben hat. Zu jeder Einwilligung MÜSSEN über die Anwendung Informationen zu den Zwecken der damit verbundenen Verarbeitung und den verarbeiteten Datenkategorien abrufbar sein.

TPZ_4 Sonstige Informationspflichten

TPZ_4.1 Der Verantwortliche der digitalen Anwendung MUSS auf der Anwendungsseite und/oder über die genutzten Vertriebsplattformen Informationen geben, die an der Nutzung interessierten Personen einen zutreffenden Eindruck von der grundsätzlichen Funktionalität und Funktionsweise der Anwendung sowie den damit verfolgten positiven Versorgungseffekten oder pflegerischen Nutzen vermitteln.

a) Der Verantwortliche MUSS auf der Anwendungswebseite und in den genutzten Vertriebsplattformen auf ggf. bestehende Risiken in der Verwendung des Produkts hinweisen. Die Darstellung MUSS in klarere Sprache erfolgen und geeignet sein, dass die nutzende Person ggf. bestehende Risiken in ihrer Höhe (Eintrittswahrscheinlichkeit, Auswirkungen) richtig einschätzen kann.

b) Um eine Irreführung oder auch Missverständnisse zu vermeiden, MÜSSEN bei der Darstellung von Risiken oder Erfolgschancen der digitalen Anwendung

ausschließlich natürliche Häufigkeiten und absolute Wahrscheinlichkeiten angegeben werden. Soweit sinnvoll, SOLL ein Bezug zu den notwendigen Behandlungseinheiten hergestellt werden.

TPZ_4.2 Die digitale Anwendung MUSS die betroffene Person spätestens 14 Tage vor dem Ablauf der verordneten bzw. bewilligten Nutzungsdauer sowie bei einem Widerruf der Einwilligung zu Zwecken des bestimmungsgemäßen Gebrauchs auf möglicherweise verlorengehende Daten und auf das Recht auf Datenübertragung gemäß Artikel 20 DSGVO sowie die Möglichkeiten des Datenexports hinweisen.

TPZ_4.3 Sofern über die digitale Anwendung eine Profilbildung erfolgt, MUSS diese für die betroffene Person transparent sein und in unmittelbarem Bezug zu den Zwecken des bestimmungsgemäßen Gebrauchs oder regulatorisch bedingten Zwecken stehen.

a) Die Transparenz über eine durchgeführte Profilbildung MUSS Informationen darüber einschließen, warum die betroffene Person einem bestimmten Profil zugeordnet wurde und welche Folgen sich daraus für die weitere Verarbeitung der Daten der betroffenen Person ergeben.

b) Die Transparenz über eine durchgeführte Profilbildung KANN über die Datenschutzerklärung der digitalen Anwendung hergestellt werden.

c) Sofern bei der betroffenen Person direkt erhobene Daten unmittelbar in die Bildung von Profilen bzw. in die Zuordnung der betroffenen Person zu einem vorab definierten Profil einfließen, MUSS die betroffene Person in zeitlicher Nähe vor der Datenerhebung darauf hingewiesen werden, dass die erhobenen Daten zur Profilbildung bzw. Profilzuordnung verwendet werden.

TPZ_4.4 Der Verantwortliche der digitalen Anwendung MUSS sowohl auf der Anwendungswebseite als auch in der digitalen Anwendung auf die Darstellung der Anwendung im Verzeichnis nach § 139e Absatz 1 SGB V ("DiGA-Verzeichnis") bzw. § 78a Absatz 3 SGB XI ("DiPA-Verzeichnis") hinweisen und einen einfachen Zugriff auf diese Informationen aus der Anwendungswebseite und der Anwendung heraus ermöglichen.

4.4 Allgemeine Erläuterungen

Die Kriterien zur Transparenz basieren auf den Vorgaben von Artikel 5 sowie den Artikeln 12-14 DSGVO mitsamt der zugehörigen Erwägungsgründe (insb. EG 39, 58, 60).

Die gewählten Begrifflichkeiten für die verschiedenen Stellen, an denen Informationen zur digitalen Anwendung verfügbar sind, sind an die DiGAV angelehnt, wo über die digitale Anwendung und die daran gebundenen Erklärungen hinaus das DiGA-Verzeichnis, die Vertriebsplattform sowie eine Anwendungswebseite als weitere Informationsquellen für die betroffene Person genannt werden. Während die Inhalte des Verzeichnisses abschließend geregelt sind, gibt es aus der Verordnung heraus keine Vorgaben, welche auf den Datenschutz und insbesondere die datenschutzrechtlichen Informationspflichten abzielenden Inhalte der Hersteller einer digitalen Anwendung auf der Vertriebsplattform oder der Anwendungswebseite veröffentlichen soll. Da sowohl Vertriebsplattform als auch Anwendungswebseite primär der Kundenansprache und Kundenwerbung dienen, ist es jedoch wichtig, dass essentielle Informationen zum Datenschutz gerade auch auf diesen Seiten zugänglich sind, um an der Nutzung der Anwendung interessierten Personen auch darzustellen, welche Datenverarbeitungen mit den angepriesenen Leistungsmerkmalen der Anwendung einhergehen.

Nur so kann die betroffene Person noch vor der Installation der Anwendung abwägen, ob sie die Nutzung ihrer Daten durch den Verantwortlichen der digitalen Anwendung für angemessen und für sich akzeptabel hält.

4.5 Spezifische Erläuterungen

Zu Anforderung TPZ_1.2 a: § 29 Absatz 2 BDSG definiert Ausnahmen für die Informationspflichten bei mit der Weitergabe personenbezogener Daten an Berufsgeheimnisträger (z. B. Ärzte) einhergehenden Zweckerweiterungen. Diese Anforderung stellt klar, dass diese Ausnahmen für DiGA und DiPA nicht greifen, da hier per se ein überwiegendes Interesse der betroffenen Person an der Herstellung von Transparenz zumindest auf der Ebene der Datenkategorien und Verarbeitungszwecke besteht. Für eine Datenweitergabe, die auch über die ursprünglichen Zwecke der DiGA oder DiPA hinaus weitere Zwecke (z. B. in der Forschung) beinhalten kann, besteht das Instrument der elektronischen Patientenakte, die dahingegen gesetzlich geregelt ist und die betroffene Person – mit der ab Januar 2022 gültigen Version 2 – hierzu mit weitreichenden Steuerungsmöglichkeiten ausstattet.

Zu Anforderung TPZ_1.3: Diese Anforderung bildet die über Art. 13 DSGVO hinausgehenden, in Art. 14 DSGVO benannten Informationspflichten ab, die für DiGA und DiPA greifen, wenn Daten nicht bei der betroffenen Person selbst erhoben werden. Dieses ist für DiGA insbesondere in der Kommunikation mit Leistungserbringern und bei DiPA in der Einbeziehung von Angehörigen und Pflegediensten relevant. Die Anforderungen TPZ_1.3 a und TPZ_1.3 b gehen daher auf diese Szenarien genauer ein.

Zu Anforderung TPZ_1.4 a: Es soll bei der Prüfung dieses Kriteriums davon ausgegangen werden, dass nach unmittelbarer Rücksendung einer Eingangsbestätigung eine Antwortzeit von 2 Werktagen für alle Arten digitaler Anwendungen angemessen und für die betroffenen Personen akzeptabel ist.

Zu Anforderung TPZ_1.4 b: Es soll bei der Prüfung dieses Kriteriums davon ausgegangen werden, dass eine telefonische Erreichbarkeit von 8 Stunden an Werktagen für alle Arten digitaler Anwendungen angemessen ist und dass Wartezeiten von bis zu 10 Minuten für die betroffenen Personen akzeptabel sind.

Zu Anforderung TPZ_1.8 und TPZ_1.9: Diese Anforderungen bilden die aktuelle Rechtsprechung ab, nach der eine Änderung von AGB und Datenschutzerklärung nicht als angenommen angesehen werden kann, wenn die betroffene Person auf eine entsprechende Information nicht reagiert.

Zu Anforderung TPZ_2.1 und TPZ_2.2: Diese Anforderungen bilden die in den Erwägungsgründen 38 und 58 zur DSGVO benannten Anforderungen an die Informationspflichten für den Fall einer Nutzung der Anwendung durch Kinder und Jugendliche ab. Eine digitale Anwendung, die Kinder und/oder Jugendliche nicht explizit von der Nutzung ausschließt, schließt diese implizit ein. Ein expliziter Ausschluss erfordert nicht nur deutlich erkennbare, vor der Installation der Anwendung angezeigte Hinweise, sondern auch eine explizite Bestätigung der nutzenden Person, dass diese der vom Hersteller der Anwendung festgelegten Altersgruppe angehört (siehe auch Kriterium "Rechtmäßigkeit").

Zu Anforderung TPZ_3.2: Die Anforderung verlangt minimal eine Übersicht der aktiven Einwilligungen. Der Hersteller kann auch eine Aufstellung aller möglichen Einwilligungen

umsetzen, solange klar erkennbar ist, welche Einwilligungen aktiv sind und welche zusätzlich noch gegeben werden können.

Beispiel zu Anforderung TPZ_4.1 b: Ohne Durchführung eines jährlichen Mammographie-Screening sind 4 Todesfälle bei je 1.000 Frauen zu verzeichnen. Bei regelmäßiger Durchführung eines Mammographie-Screening sind es hingegen 3 Todesfälle bei je 1.000 Frauen (jeweils über 10 Jahre betrachtet). Eine Darstellung über relative Wahrscheinlichkeiten suggeriert eine sehr hohe Wirksamkeit: „Das Mammographie-Screening verringert das Risiko, an Brustkrebs zu sterben, um 25 Prozent“. Absolute Wahrscheinlichkeiten erlauben auch mathematisch und medizinisch "normal" gebildeten Personen eine deutlich realistischere Einschätzung der Wirksamkeit der Vorsorge: „Das Mammographie-Screening verringert die Anzahl der Frauen, die an Brustkrebs sterben, um 1 pro 1.000, also um 0,1 Prozent“. Durch die Herstellung eines Bezugs zu notwendigen Behandlungseinheiten wird dieses noch plastischer: "Pro 1000 Frauen, die zehn Jahre lang am Screening teilnehmen, wird ein Todesfall verhindert.“

Zu Anforderung TPZ_4.2: Die DiGAV verpflichtet den Hersteller einer DiGA zur Umsetzung verschiedener Export-Formate und -Schnittstellen. Betroffene Personen können diese alternativ oder ergänzend zur Datenübertragbarkeit nach Art. 20 DSGVO nutzen. Die Anzeige von Hinweisen auf die Möglichkeiten des Datenexports und der Datenportabilität bedingt die Nutzung der Anwendung, d. h. eine Verwendung von Push-Benachrichtigungen allein zur Erfüllung dieser Anforderung ist nicht zulässig.

5 Nichtverkettbarkeit

5.1 Regulatorische Grundlagen

- Art. 5 DSGVO
- § 24 BDSG
- § 27 BDSG
- § 4 Absatz 2 und Absatz 4 DiGAV

5.2 Gegenstandsbereich und Motivation

Dieses Kriterium bildet das Gewährleistungsziel der Nichtverkettbarkeit auf DiGA und DiPA ab. Basierend auf der Definition im Standard-Datenschutzmodell fallen unter das Gewährleistungsziel der Nichtverkettbarkeit insbesondere die Vorgaben der DSGVO zur Zweckbindung, wobei jedoch auch Fragen der Zusammenführung von zu unterschiedlichen Zwecken erhobenen Daten sowie die Weiterverarbeitung von Daten zu veränderten Zwecken berücksichtigt sind.

Dadurch, dass an Verantwortliche von DiGA und DiPA im Rahmen der Verordnung bzw. Bewilligung einer digitalen Anwendung keine personenidentifizierenden Merkmale der betroffenen Person übermittelt werden, erfolgt die Nutzung einer digitalen Anwendung aus Sicht des Verantwortlichen unter einem Pseudonym. Die hier gewählten technischen Verfahren (zufällige Vermittlungscodes) bilden für sich bereits eine technische Maßnahme, mit der eine Verkettung von Daten aus verschiedenen digitalen Anwendungen erschwert – wenn nicht gar verhindert – wird.

Mit dem Kriterium "Nichtverkettbarkeit" wird abgesichert, dass die initial gegebene pseudonyme Nutzung auch über den Lebenszyklus der digitalen Anwendung und für alle rechtmäßigen Zwecke der Datenverarbeitung über eine digitale Anwendung durchgehalten wird. Der Fokus liegt dabei auf der Umsetzung einer wirksamen Trennung der Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten.

5.3 Kriterien

NVK_1 Zweckbindung und zulässige Ausnahmen

NVK_1.1 Eine Durchbrechung oder Ausweitung der rechtmäßigen Verarbeitungszwecke DARF NICHT stattfinden.

NVK_1.2 Über die digitale Anwendung erhobene Daten KÖNNEN zu wissenschaftlichen Forschungszwecken weiterverarbeitet werden, sofern diese Daten für die Erreichung des Forschungsziels erforderlich sind, eine Interessenabwägung gemäß § 27 Absatz 1 BDSG stattgefunden hat und hierzu eine informierte Einwilligung der betroffenen Person vorliegt.

a) Alle für die wissenschaftlichen Forschungszwecke erforderlichen Daten MÜSSEN vor der Weiterverarbeitung anonymisiert oder – sofern der Forschungszweck mit anonymen Daten nicht erreicht werden kann - pseudonymisiert werden.

NVK_2 Zweck- und Speichertrennung

NVK_2.1 [nur DiGA] Die Speicherung und Verarbeitung von Daten zu Zwecken des Nachweises positiver Versorgungseffekte MUSS technisch getrennt von der Speicherung und Verarbeitung von Daten zu anderen Zwecken erfolgen.

a) Die Verarbeitung von Daten zu Zwecken des Nachweises positiver Versorgungseffekte SOLL anonymisiert erfolgen.

b) Sofern der Hersteller der digitalen Anwendung einen Auftragsverarbeiter in die Auswertung der Daten zum Nachweis positiver Versorgungseffekte einbezieht, DARF dieser KEINEN Zugang zu den durch den Hersteller der digitalen Anwendung gespeicherten Daten erhalten. Vielmehr MUSS der Hersteller die für die Auftragsverarbeitung erforderlichen Daten in anonymisierter oder pseudonymisierter Form an den Auftragsverarbeiter übermitteln.

c) Die Verarbeitung zu Zwecken des Nachweises positiver Versorgungseffekte MUSS mit der endgültigen Aufnahme der digitalen Anwendung in das DiGA-Verzeichnis beim BfArM bzw. dem Empfang eines ablehnenden Bescheids enden. Der Hersteller der digitalen Anwendung MUSS anschließend die zu diesem Zweck verarbeiteten Daten löschen.

d) Sofern der Hersteller der digitalen Anwendung einen Auftragsverarbeiter in die Auswertung der Daten zum Nachweis positiver Versorgungseffekte einbezieht, MUSS dieser die übernommenen Daten nach Abschluss der Auswertung löschen, sofern nicht die Überführung der Daten in ein Register gesetzlich verlangt wird. In diesem Fall MÜSSEN die Daten gesperrt werden.

NVK_2.2 [nur DIGA] Die Speicherung und Verarbeitung von Daten zu Zwecken der Ermittlung erfolgsabhängiger Preisbestandteile MUSS technisch getrennt von der Speicherung und Verarbeitung von Daten zu anderen Zwecken erfolgen.

a) Die Verarbeitung von Daten zu Zwecken der Ermittlung erfolgsabhängiger Preisbestandteile SOLL anonymisiert erfolgen.

b) Eine Übermittlung personenbeziehbarer Daten an den GKV-SV oder die Schiedsstelle im Kontext der Umsetzung der Ermittlung erfolgsabhängiger Preisbestandteile DARF NICHT erfolgen.

NVK_2.3 Die Speicherung und Verarbeitung von Daten zu Zwecken der dauerhaften Gewährleistung der Sicherheit (bei DiPA), technischen Funktionsfähigkeit, der Nutzerfreundlichkeit, der altersgerechten Nutzbarkeit (bei DiPA) und Weiterentwicklung der digitalen Anwendung MUSS technisch getrennt von der Speicherung und Verarbeitung von Daten zu anderen Zwecken erfolgen.

a) Die Verarbeitung von Daten zu Zwecken der Sicherheit (bei DiPA), dauerhaften Gewährleistung der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit, der altersgerechten Nutzbarkeit (bei DiPA) und Weiterentwicklung der digitalen Anwendung SOLL anonymisiert erfolgen.

5.4 Allgemeine Erläuterungen

Die Kriterien zur Zweckbindung und Nichtverkettbarkeit basieren auf den Vorgaben von Artikel 5 DSGVO mitsamt der zugehörigen Erwägungsgründe sowie der Darstellung des Gewährleistungsziels "Nichtverkettbarkeit" im Standard-Datenschutzmodell.

5.5 Spezifische Erläuterungen

Zu Anforderung NVK_1.2: Art. 5 Absatz 1 Satz 1 Buchstabe b DSGVO und § 27 Absatz 1 BDSG erkennen eine Weiterverarbeitung von personenbezogenen Daten für die wissenschaftliche Forschung als grundsätzlich vereinbar mit den ursprünglichen Verarbeitungszwecken an. Die in § 27 Absatz 1 BDSG geforderten *angemessenen und spezifischen Maßnahmen zur Wahrung der Interessen der betroffenen Person* müssen zumindest eine Pseudonymisierung umfassen. Auch wenn der Hersteller oder Verantwortliche der digitalen Anwendung die über die digitale Anwendung erhobenen Daten bereits für die rechtmäßigen Zwecke nur pseudonymisiert verarbeitet, muss vor der Weiterverarbeitung für Zwecke der wissenschaftlichen Forschung eine erneute Pseudonymisierung durchgeführt werden, wobei die Pseudonyme nicht aus personenidentifizierenden Merkmalen oder dem Freischaltcode abgeleitet werden dürfen. Abweichend von § 27 BDSG wird eine Einwilligung der betroffenen Person verlangt, da die Verordnungen zu den digitalen Anwendungen alle Verarbeitungen auf Einwilligungen stützen und Ausnahmen hiervon nur aus dem SGB V bzw. SGB XI heraus begründbar sind.

6 Datenminimierung und Speicherbegrenzung

6.1 Regulatorische Grundlagen

- Art. 5 DSGVO

6.2 Gegenstandsbereich und Motivation

Dieses Kriterium gilt gleichermaßen für DiGA und DiPA und steht in engem Bezug zu den Zwecken der Verarbeitung. Das Kriterium deckt das Gewährleistungsziel der Datenminimierung aus dem Standard-Datenschutzmodell ab, in dem die Grundsätze der Datenminimierung und der Speicherbegrenzung aus der DSGVO abgebildet sind.

Das Kriterium stellt sicher, dass digitale Anwendungen nur Daten verarbeiten, die für die Verarbeitungszwecke angemessen und erheblich sind. Die verarbeiteten Daten sollen auf das für ihre Verarbeitungszwecke notwendige Maß beschränkt sein und insbesondere sollten die Zwecke nicht auch auf datensparsamere Weise erreichbar sein.

6.3 Kriterien

DMN_1 Erfordernis und Angemessenheit

DMN_1.1 Die über die digitale Anwendung verarbeiteten personenbezogenen Daten MÜSSEN dem Zweck angemessen, für die Zweckerreichung erheblich und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Der Verantwortliche der digitalen Anwendung MUSS den Beitrag aller verarbeiteten Kategorien personenbezogener Daten zur Erreichung der rechtmäßigen Zwecke bzw. zur Umsetzung von Datenschutz-, Sicherheits- und Qualitätsanforderungen begründen können und MUSS darstellen können, dass diese Zwecke bzw. Anforderungen ohne diese Daten nicht umsetzbar wären.

a) Datenminimierung MUSS als Prinzip entlang des Lebenszyklus aller von der digitalen Anwendung verarbeiteten Daten durchgesetzt werden, indem zur Erreichung der Verarbeitungszwecke nicht mehr erhebliche oder benötigte Daten anonymisiert oder gelöscht werden. Die Darstellungen des Verantwortlichen zur Angemessenheit und dem Erfordernis der Verarbeitung

einzelner Datenkategorien MÜSSEN entsprechend den gesamten Lebenszyklus der Anwendung berücksichtigen.

b) Der Verantwortliche der digitalen Anwendung DARF über die Anwendung grundsätzlich KEINE Daten erheben, die für sich oder in ihrem Zusammenspiel die Identifizierung einer natürlichen Person erlauben. Ist die Verarbeitung solcher Daten für Zwecke des bestimmungsgemäßen Gebrauchs erforderlich, MUSS der Verantwortliche technische und organisatorische Maßnahmen vorsehen, die eine Verwendung dieser Daten zu einer nicht legitimierten Identifizierung der betroffenen Person ausschließen.

c) Sofern die digitale Anwendung von der betroffenen Person einen Namen abfragt (z. B. zum Zweck der persönlichen Ansprache in der Anwendung), MUSS diese Abfrage so gestaltet sein, dass unmissverständlich erkennbar ist, dass lediglich die Eingabe des Vornamens oder eines Pseudonyms gewünscht ist.

DMN_1.2 Der Verantwortliche der digitalen Anwendung MUSS darlegen können, dass die rechtmäßigen Zwecke der Verarbeitung personenbezogener Daten durch die digitale Anwendung nicht in zumutbarer Weise durch andere, datensparsamere Mittel in gleichem Maße erreicht werden können.

DMN_1.3 [nur DiGA] Im Fall einer vorläufigen Aufnahme der DiGA in das DiGA-Verzeichnis des BfArM MUSS der Verantwortliche im Rahmen der Erprobung nach § 139e Absatz 4 SGB V das Erfordernis der verarbeiteten Gesundheitsdaten zur Erzielung des positiven Versorgungseffekts nachweisen können. In dem vorgelegten Studiendesign MUSS erkennbar sein, dass dieser Nachweis Bestandteil der Erprobung ist.

DMN_1.4 Die digitale Anwendung DARF KEINE Zugriffe auf zugangsbeschränkte Ressourcen der genutzten Plattform (Kamera, GPS etc.) oder an die Plattform angebundene externe Geräte ausführen, die für die Erreichung der rechtmäßigen Zwecke nicht erforderlich sind.

a) In besonderem Maße MÜSSEN Zugriffe auf Ressourcen abgesichert werden, über die auch personenbezogene Daten identifizierbarer Dritter oder Beziehungen der betroffenen Person zu Dritten offenbart werden (z. B. Adressbuch, Terminkalender). Sofern Zugriffe auf diese Ressourcen erforderlich sind, MUSS der Verantwortliche der Anwendung mit technischen Maßnahmen sicherstellen, dass nur die für die rechtmäßigen Verarbeitungszwecke erforderlichen Ausschnitte der über die Ressource verwalteten Daten durch die digitale Anwendung abrufbar sind.

b) Der Verantwortliche der digitalen Anwendung MUSS Prozesse zur regelmäßigen Überprüfung des Erfordernisses und der datensparsamen Ausgestaltung des Zugriffs auf zugangsbeschränkte Ressourcen der genutzten Plattform oder an die Plattform angebundene externe Geräte etabliert haben.

c) Der Verantwortliche der digitalen Anwendung MUSS Kriterien definiert haben, anhand derer neue technologische Ausgestaltungen der genutzten Ressourcen und Geräte in Bezug auf ihre Tauglichkeit, Zweckmäßigkeit, Datensparsamkeit und zielgruppengerechte Bedienbarkeit bewertet und ggf. von der Nutzung ausgeschlossen werden.

DMN_2 Löschen

DMN_2.1 Der Verantwortliche der digitalen Anwendung MUSS für die Anwendung ein an den Vorgaben der [DIN 66398] ausgerichtetes Löschkonzept erstellen und MUSS nachweisen können, dass die im Löschkonzept festgeschriebenen Löschregeln und Umsetzungsregeln rechtmäßig und wirksam sind. Das Löschkonzept MUSS die Angaben zu Löschfristen im Verzeichnis von Verarbeitungstätigkeiten (siehe DSFA_2.2) dahingehend ergänzen, als dass es die Operationalisierung der Löschvorgänge festschreibt.

a) Sofern einzelne Daten oder Datenkategorien nicht einer Löschfrist unterliegen oder über üblicherweise geltende Löschfristen hinaus aufgehoben werden müssen, MUSS der Verantwortliche der digitalen Anwendung im Löschkonzept die entsprechenden Gründe aufführen und MUSS Prozesse etablieren, über die der Fortbestand dieser Gründe regelmäßig überprüft wird. Der Verantwortliche MUSS technische Maßnahmen zur Sperrung dieser Daten bzw. Datenkategorien umsetzen.

b) Der Verantwortliche der digitalen Anwendung MUSS Verantwortlichkeiten festlegen und Prozesse etablieren, über die die Umsetzung des Löschkonzepts überwacht und die kontinuierliche Fortschreibung abgesichert werden.

c) Die zum Löschen eingesetzten technischen Verfahren MÜSSEN sicherstellen, dass eine Rekonstruktion gelöschter Daten nicht mit vertretbarem Aufwand möglich ist.

DMN_2.2 Temporäre Dateien, die personenbezogene Daten enthalten können, MÜSSEN regelmäßig und regelhaft wirksam gelöscht werden. Eine Löschung im Frontend MUSS in jedem Fall beim Deinstallieren der digitalen Anwendung oder der Beendigung der Nutzung der Anwendung durch die betroffene Person erfolgen. Des Weiteren MUSS das Hintergrundsystem der betroffenen Person die Möglichkeit geben, dass bei Deinstallation der Anwendung alle sensiblen Daten und anwendungsspezifischen Anmeldeinformationen vollständig vom Hintergrundsystem gelöscht bzw. unzugänglich gemacht werden.

DMN_2.3 Zu Zwecken des sicheren Betriebs geschriebene Systemprotokolle, die personenbezogene Daten enthalten können, MÜSSEN regelmäßig und regelhaft – spätestens jedoch nach drei Monaten - wirksam gelöscht werden.

DMN_2.4 Sicherungskopien (z. B. Backups), die personenbezogene Daten enthalten können, MÜSSEN regelmäßig und regelhaft wirksam gelöscht bzw. vollständig überschrieben werden.

a) Der Verantwortliche der digitalen Anwendung hat Maßnahmen etabliert, die sicherstellen, dass nach dem Einspielen einer Sicherungskopie alle personenbezogenen Daten unmittelbar gelöscht werden, die seit der Anlage der Sicherungskopie aus Gründen des Datenschutzes im Original-Datenbestand gelöscht wurden.

DMN_3 Datensparsamkeit

DMN_3.1 Daten MÜSSEN in dem datensparsamsten Format verarbeitet und gespeichert werden, mit dem sich die zugesagten Funktionalitäten der digitalen Anwendung erbringen lassen (z. B. Altersgruppe anstelle des genauen Geburtsdatums).

a) Bei der Nutzung der digitalen Anwendung an Backend-Systeme des Verantwortlichen der digitalen Anwendung übertragene IP-Nummern und/oder Gerätenummern SOLLEN nicht gespeichert werden. Ist eine Speicherung erforderlich, MÜSSEN IP-Nummern und Gerätenummern so weit als möglich verkürzt oder maskiert werden.

DMN_3.2 Der Verantwortliche der digitalen Anwendung MUSS Kriterien für die Bestimmung der Nicht-Identifizierbarkeit der betroffenen Personen definieren und die Einhaltung dieser Kriterien sicherstellen.

DMN_4 Benutzer-Account und Grace-Periode

DMN_4.1 Die digitale Anwendung MUSS für die betroffene Person mit der Freischaltung der Anwendung einen Benutzer-Account (Benutzerkonto) anlegen. Alle zu der betroffenen Person verarbeiteten Daten MÜSSEN an den Benutzer-Account gebunden sein.

a) Nutzer-Accounts MÜSSEN pseudonym nutzbar sein; Angaben zur Identität der betroffenen Person (Krankenversichertennummer, realer Name, Adresse, unmittelbar identifizierende E-Mail-Adresse etc.) DÜRFEN KEINE Voraussetzung für die Nutzung sein.

b) Der Zugriff auf einen Nutzer-Account und die daran gebundenen Daten MUSS über eine sichere Authentisierung gegen die bei der Anlage des Benutzer-Accounts erfassten authentisierenden Faktoren erfolgen.

c) Der für die Freischaltung der digitalen Anwendung genutzte Freischaltcode MUSS separat vom Nutzer-Account gespeichert werden und MUSS nach Freischaltung der digitalen Anwendung gelöscht werden. Ein Hashwert des für die Freischaltung der digitalen Anwendung genutzten Freischaltcodes KANN Bestandteil des Nutzer-Accounts sein. Die digitale Anwendung KANN zum Nachweis des Besitzes eines bestimmten Nutzer-Accounts von der nutzenden Person die erneute Eingabe des Freischaltcodes verlangen und gegen den im Nutzer-Account abgelegten Hashwert abgleichen. Die Berechnung des Hashwerts MUSS gemäß den Vorgaben der [TR-02102-1] erfolgen.

DMN_4.2 Um die Versorgungskontinuität bei Folgeverordnungen abzusichern, KÖNNEN der Nutzer-Account und die für eine kontinuierliche Fortsetzung der durch die Anwendung gestützten Versorgung erforderliche Daten nach Abschluss der Nutzung der digitalen Anwendung eine begrenzte Zeit weiter bestehen bleiben. Diese Grace-Periode DARF NICHT länger als ein Drittel der Verordnungsdauer bzw. Bewilligungsdauer – maximal aber drei Monate – dauern.

a) Mit Ablauf der Verordnung bzw. Genehmigung der digitalen Anwendung MUSS der Verantwortliche der Anwendung die betroffene Person über die Grace-Periode informieren. Der Verantwortliche MUSS von der betroffenen Person eine gesonderte Einwilligung für die weitere Vorhaltung der Daten und das Fortbestehen des Nutzer-Accounts aus der Anwendung heraus einholen. Willigt die betroffene Person nicht ein, MÜSSEN mit Ablauf der Verordnung bzw. Genehmigung der Nutzer-Account und daran gebundenen Daten gemäß Löschkonzept gelöscht bzw. gesperrt werden.

b) Während der Grace-Periode MÜSSEN die gespeicherten Daten gesperrt sein. Zulässig sind ausschließlich die Authentisierung der betroffenen Person gegen den Benutzer-Account, um gegebene Einwilligungen zu widerrufen, Daten zu

exportieren, Kontakt zum Verantwortlichen aufzunehmen oder den Nutzer-Account und die daran gebundenen Daten durch Eingabe eines neuen Freischaltcodes zu entsperren. Erfolgt innerhalb der Grace-Periode keine weitere Freischaltung der Anwendung infolge einer Folgeverordnung oder weiteren Bewilligung, MÜSSEN der Nutzer-Account und alle daran gebundenen Daten gemäß Löschkonzept gelöscht bzw. gesperrt werden.

c) Bei einer Folgeverordnung bzw. weiteren Bewilligung der digitalen Anwendung MUSS die betroffene Person entscheiden können, ob sie einen bestehenden Account und die daran gebundenen Daten weiternutzen oder einen neuen Account anlegen möchte. Im zweiten Fall MÜSSEN der alte Account und alle zu dem betroffenen noch vorgehaltenen Daten aus der vorangegangenen Nutzung der digitalen Anwendung unmittelbar gelöscht werden.

6.4 Allgemeine Erläuterungen

Das Kriterium zur Datenminimierung fokussiert auf die rechtmäßigen Verarbeitungszwecke von DiGA bzw. DiPA. Eine Datenverarbeitung außerhalb dieser Zwecke ist bereits durch die Kriterien zur Rechtmäßigkeit und Zweckbindung ausgeschlossen und wird daher hier nicht weiter berücksichtigt. Alle Anforderungen an Datenminimierung und Speicherbegrenzung basieren auf den Vorgaben von Artikel 5 DSGVO, dem Erwägungsgrund 39 zu den Grundsätzen des Datenschutzes sowie dem Gewährleistungsziel "Datenminimierung" aus dem Standard-Datenschutzmodell. Als technische Maßnahme wird die durchgehend pseudonyme Nutzung vorgegeben, da die regulatorischen Rahmenbedingungen von DVG, DiGAV und DiPAV keine Identifizierung der betroffenen Person erfordern und durch die gewählten Verfahren zur Freischaltung der Anwendung mit dem Freischaltcode bereits ein Pseudonym positioniert ist. In diesem Sinne können viele der die Speicherbegrenzung betreffenden Vorgaben der DSK zu datenschutzrechtlichen Prüfprogrammen unmittelbar auf das Löschen und/oder Sperren personenbezogener Daten abgebildet werden – die Nicht-Identifizierbarkeit wird durch den Freischaltcode und das Verbot der Erhebung direkt identifizierender Daten bereits proaktiv abgesichert.

6.5 Spezifische Erläuterungen

Zu Anforderung DMN_1.1: Als Datenschutz-, Sicherheits- und Qualitätsanforderungen gelten für DiGA alle in §§ 4-6a DiGAV benannten Anforderungen sowie Anforderungen, die sich aus den in § 7 DiGAV benannten Zertifikaten ergeben.

Zu Anforderung DMN_1.1 b: Der Hersteller und der Verantwortliche der digitalen Anwendung erhalten bei der Verordnung oder Bewilligung der Anwendung lediglich einen pseudonymen Freischaltcode, der als Nachweis für die Kostenerstattung dient. Der Freischaltcode enthält keine personenidentifizierenden Daten und kann durch den Hersteller und den Verantwortlichen auch nicht de-pseudonymisiert werden. Diese Pseudonymisierung soll nicht durch die Verarbeitung von potenziell über das Internet einer Person unmittelbar zuordenbaren Kontaktdaten (z. B. E-Mail-Adressen, die den realen Namen enthalten oder Handynummern) durchbrochen werden. Auch die Abfrage von direkt an eine Person gebundenen Identifizierern wie z. B. der KVNR soll

unterbleiben, da diese Identifizierer üblicherweise nicht gesondert geschützt sind bzw. potenziell vielen Personen bekannt sind.

Zu Anforderung DMN_1.3: Medizinische und pflegerische Daten sollen nur erhoben werden, wenn die darauf aufsetzenden Algorithmen und Verarbeitungen medizinisch-fachlich nachgewiesenermaßen sinnvoll mit Blick auf die Erreichung positiver Versorgungseffekte sind. Aus Algorithmen und Verarbeitungen, die diese Anforderung nicht erfüllen, kann der Verantwortliche kein Erfordernis für die Erhebung der verarbeiteten Daten ableiten. Da bei nur vorläufig in das DiGA-Verzeichnis aufgenommenen DiGA potenziell kein aus der Literatur ableitbarer Maßstab für das Erfordernis der Verarbeitung bestimmter Daten existiert, muss dieser Nachweis im Rahmen der Erprobungsstudie erbracht werden.

Zu Anforderung DMN_2.1 c: Bei der Bewertung des Aufwands ist der Schutzbedarf der zu löschenden Daten zu berücksichtigen. Je höher dieser ist, desto stärker müssen die zur Löschung eingesetzten Maßnahmen sein. Eine ausführliche Diskussion hierzu findet sich im Baustein 60 "Löschen und Vernichten" zum Standard-Datenschutzmodell [DSK-60].

Zu Anforderung DMN_2.3: Diese Anforderung folgt den Darstellungen in Baustein 60 "Löschen und Vernichten" zum Standard-Datenschutzmodell [DSK-60]. Auf den Produktivdaten vollzogene Löschungen müssen nicht in bestehenden Sicherungskopien nachvollzogen werden, wenn diese regelmäßig gelöscht oder überschrieben werden.

Zu Anforderung DMN_4.1: Diese Anforderung soll über Anforderung DMN_1.1 hinaus die pseudonyme Nutzung der digitalen Anwendung bestärken, indem die in Anforderung DMN_1.1 eher abstrakt formulierten Anforderungen noch einmal auf konkrete Vorgaben für die Verwaltung der Nutzerinnen und Nutzer der Anwendung herunter gebrochen werden. Über den Freischaltcode wird die Möglichkeit der Authentisierung ohne Identifizierung eröffnet. Bei einer Anmeldung an der Anwendung mittels Passwort kann so z. B. über die Eingabe des Freischaltcodes das Passwort zurückgesetzt werden. Um den Freischaltcode zu schützen, darf dieser nach seiner originären Nutzung als Kostenübernahmenachweis nur noch als Hashwert gespeichert werden.

7 Intervenierbarkeit

7.1 Regulatorische Grundlagen

- Art. 12 DSGVO
- Art. 15 DSGVO
- Art. 16 DSGVO
- Art. 17 DSGVO
- Art. 18 DSGVO
- Art. 19 DSGVO
- Art. 20 DSGVO
- § 35 BDSG

7.2 Gegenstandsbereich und Motivation

Dieses Kriterium bildet das Gewährleistungsziel der Intervenierbarkeit auf DiGA und DiPA ab. Basierend auf der Definition im Standard-Datenschutzmodell sind unter dem Gewährleistungsziel der Intervenierbarkeit die Rechte der betroffenen Person auf Benachrichtigung, Auskunft, Berichtigung, Löschung, Vergessenwerden, Einschränkung der Verarbeitung und Datenübertragbarkeit zusammengefasst. Zusätzlich wurden in dieses Kriterium Anforderungen aus der bisherigen Anlage 1 der DiGAV aufgenommen, die Möglichkeiten der betroffenen Person zur Steuerung der sie betreffenden Datenverarbeitung beschreiben.

7.3 Kriterien

ITV_1 Recht auf Auskunft

ITV_1.1 Der Verantwortliche der digitalen Anwendung MUSS der betroffenen Person über die digitale Anwendung die Möglichkeit bieten, Auskunft zu den über sie gespeicherten personenbezogenen Daten in dem in Artikel 15 Absätze 1 und 2 DSGVO festgelegten Umfang zu erhalten.

a) Der Verantwortliche MUSS den Eingang sowie die Bearbeitung eines Auskunftsverlangens im AuditTrail (siehe Kriterium "Rechenschaftspflicht") protokollieren.

b) Die Auskunft zu gespeicherten Daten DARF KEINE für Zwecke der Authentisierung genutzten Daten offenbaren.

ITV_1.2 Der Verantwortliche SOLL die betroffene Person im Zuge einer Auskunftsanfrage auf die Möglichkeiten des Datenexports hinweisen.

ITV_2 Recht auf Löschung und Einschränkung der Verarbeitung

ITV_2.1 Der Verantwortliche der digitalen Anwendung MUSS der betroffenen Person über die digitale Anwendung die Möglichkeit bieten, die Löschung von Daten sowie die Einschränkung der Verarbeitung von Daten zu verlangen, sofern die Verarbeitung der Daten aus Sicht der betroffenen Person nicht mehr erforderlich ist oder sofern sie aus anderen Gründen unrechtmäßig verarbeitet werden.

a) Der Verantwortliche MUSS prüfen, ob Gründe für eine Löschung bzw. Sperrung gemäß Art. 17 Absatz 1 DSGVO vorliegen. Der Verantwortliche MUSS einen entsprechenden Prüfprozess etabliert haben.

b) Der Verantwortliche MUSS den Eingang eines Lösch- bzw. Sperrverlangens über die digitale Anwendung bestätigen, sofern die Löschung bzw. Sperrung nicht unmittelbar umgesetzt wird.

c) Der Verantwortliche MUSS die Umsetzung eines Lösch- bzw. Sperrverlangens über die digitale Anwendung bestätigen. Sofern keine Gründe für eine Löschung gemäß Art. 17 Absatz 1 DSGVO vorliegen, MUSS der Verantwortliche der digitalen Anwendung die betroffene Person darüber informieren und auf die Möglichkeit des Widerrufs gegebener Einwilligungen hinweisen.

d) Der Verantwortliche MUSS den Eingang sowie die Schritte zur Bearbeitung eines Lösch- bzw. Sperrverlangens im AuditTrail (siehe Kriterium "Rechenschaftspflicht") protokollieren.

e) Der Verantwortliche MUSS Prozesse etabliert haben, die eine Umsetzung eines Lösch- bzw. Sperrverlangens innerhalb der in Art. 12 Absätze 3 und 4 DSGVO benannten Fristen sicherstellen.

ITV_2.2 [nur DiGA] Sofern personenbezogene Daten durch die betroffene Person gelöscht oder gesperrt wurden, MUSS die digitale Anwendung die betroffene Person auf die Möglichkeit des Einstellens eines aktualisierten Datenauszugs in die elektronische Patientenakte hinweisen.

a) Die DiGA SOLL der betroffenen Person die Möglichkeit geben, in der DiGA zu konfigurieren, dass das Löschen und Sperren von Daten automatisch eine Aktualisierung der in die elektronische Patientenakte geschriebenen Datenauszüge auslöst.

ITV_2.3 Sofern die digitale Anwendung personenbezogene Daten an Leistungserbringer übermittelt hat bzw. Leistungserbringern personenbezogene Daten zum Abruf bereitgestellt hat und diese Daten anschließend durch die betroffene Person gelöscht oder gesperrt wurden, da die Daten unrichtig waren oder unrechterweise verarbeitet wurden, MUSS die digitale Anwendung die betroffenen Leistungserbringer auf die Löschung bzw. Sperrung der Daten hinweisen.

ITV_2.4 Sofern die digitale Anwendung Daten verarbeitet, die über ein externes Gerät oder andere digitale Anwendungen erhoben wurden, MUSS der Verantwortliche die betroffene Person im Kontext eines Lösch- oder Sperrverlangens darauf hinweisen,

dass die auf externen Geräten bzw. in anderen Anwendungen oder in Backend-Systemen der Hersteller dieser Geräte bzw. Anwendungen gespeicherten Daten nicht über die digitale Anwendung gelöscht oder gesperrt werden.

a) [nur DiGA] Der Verantwortliche SOLL technische Möglichkeiten vorsehen, über die die betroffene Person auch auf Basis von § 374a SGB V über Hilfsmittel und Implantate erhobene Daten im Rahmen eines Lösch- oder Sperrverlangens löschen bzw. sperren kann. Dieses DARF NICHT automatisch erfolgen, sondern MUSS durch eine separate, explizite Handlung der betroffenen Person ausgelöst werden.

ITV_3 Recht auf Berichtigung

ITV_3.1 Der Verantwortliche der digitalen Anwendung MUSS der betroffenen Person über die digitale Anwendung die Möglichkeit bieten, die Berichtigung von sie betreffenden unrichtigen personenbezogenen Daten und die Vervollständigung von sie betreffenden unvollständigen personenbezogenen Daten zu verlangen.

a) Der Verantwortliche SOLL der betroffenen Person die Möglichkeit bieten, sie betreffende personenbezogene Daten selbst über die digitale Anwendung zu korrigieren und zu ergänzen.

b) Sofern die betroffene Person personenbezogene Daten nicht selbst über die digitale Anwendung korrigieren oder ergänzen kann, MUSS der Verantwortliche der digitalen Anwendung

i. den Eingang eines Verlangens nach Korrektur oder Vervollständigung über die digitale Anwendung bestätigen.
ii. den Eingang sowie die Schritte zur Bearbeitung eines Verlangens nach Korrektur oder Vervollständigung im AuditTrail (siehe Kriterium "Rechenschaftspflicht") protokollieren.
iii. Prozesse etabliert haben, die eine Umsetzung eines Verlangens nach Korrektur oder Vervollständigung innerhalb der in Art. 12 Absätze 3 und 4 DSGVO benannten Fristen sicherstellen.

ITV_3.2 [nur DiGA] Sofern personenbezogene Daten durch die betroffene Person korrigiert oder ergänzt wurden, MUSS die digitale Anwendung die betroffene Person auf die Möglichkeit des Einstellens eines aktualisierten Datenauszugs in die elektronische Patientenakte hinweisen.

a) Die DiGA SOLL der betroffenen Person die Möglichkeit geben, in der DiGA zu konfigurieren, dass das Korrigieren und Ergänzen von Daten automatisch eine Aktualisierung der in die elektronische Patientenakte geschriebenen Datenauszüge auslöst.

ITV_3.3 Sofern die digitale Anwendung personenbezogene Daten an Leistungserbringer übermittelt hat bzw. diesen personenbezogene Daten zum Abruf bereitgestellt hat und diese Daten anschließend durch die betroffene Person - bzw. im Rahmen eines Korrektur- oder Löschverlangens durch den Verantwortlichen - korrigiert oder ergänzt wurden, SOLL die digitale Anwendung die betroffenen Leistungserbringer auf die Aktualisierung der Daten hinweisen.

ITV_4 Datenportabilität

ITV_4.1 Der Verantwortliche der digitalen Anwendung MUSS der betroffenen Person über die digitale Anwendung die Möglichkeit geben, die über die digitale Anwendung verarbeiteten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu exportieren.

a) [nur DiGA] Der Datenexport MUSS gemäß einer Festlegung für die semantische und syntaktische Interoperabilität von Daten der elektronischen Patientenakte nach § 355 Absatz 2a SGB V erfolgen. Solange eine solche Festlegung nicht vorliegt, MUSS der Export in einem offenen anerkannten internationalen Standard oder in einem vom Hersteller offen gelegten Profil über einem offenen anerkannten internationalen Standard erfolgen.

b) [nur DiPA] Die über die DiPA verarbeiteten Daten MÜSSEN in einem definierten Binding des HL7 FHIR Standards exportiert und für die weitere Nutzung bereitgestellt werden können. Der Export MUSS die Interoperabilitätsvorgaben der KBV bzw. die FHIR Basisprofile von HL7 Deutschland - sofern anwendbar - berücksichtigen.

c) Der Datenexport SOLL eine ggf. bestehende pseudonyme Nutzung NICHT durchbrechen und SOLL ausschließlich und unmittelbar über die digitale Anwendung erfolgen. Der Verantwortliche MUSS vor dem Export der über die betroffene Person gespeicherten Daten die Authentizität der betroffenen Person verifizieren.

d) Der Verantwortliche MUSS die Durchführung eines Datenexports im AuditTrail (siehe Kriterium "Rechenschaftspflicht") protokollieren.

e) Der Datenexport DARF KEINE für Zwecke der Authentisierung genutzten Daten enthalten.

f) Die digitale Anwendung MUSS der betroffenen Person im Zuge eines Aufrufs der Export-Funktion auf die Möglichkeit des Ausspielens versorgungsrelevanter Daten in einem menschenlesbaren Format hinweisen.

g) [nur DiGA] Die DiGA MUSS die betroffene Person auf die die Möglichkeit des direkten Einspielens der exportierten Daten in die elektronische Patientenakte (Anlage 2 Nummer 5 DiGAV) hinweisen.

ITV_5 Übergreifende Anforderungen an die Umsetzung der Betroffenenrechte

ITV_5.1 Die Umsetzung der Anforderungen ITV_1 bis ITV_4 dieses Kriteriums DARF eine ggf. bestehende pseudonyme Nutzung NICHT durchbrechen und SOLL ausschließlich über die digitale Anwendung erfolgen.

ITV_5.2 Der Verantwortliche der digitalen Anwendung MUSS vor der Auskunft zu über die betroffene Person gespeicherten Daten, der Annahme eines Lösch-, Sperr-, Korrekturverlangens sowie der Durchführung eines Datenexports die Authentizität der betroffenen Person verifizieren.

ITV_5.3 Sofern der Verantwortliche der digitalen Anwendung auch nach Beendigung der Verordnungs- bzw. Bewilligungsdauer der digitalen Anwendung personenbezogene Daten der betroffenen Person speichert, MUSS die betroffene Person auch nach Beendigung der Verordnungs- und Bewilligungsdauer ihre Betroffenenrechte nach Artikel 12 bis 23 DSGVO wahrnehmen können. Der Verantwortliche KANN hierzu von den Vorgaben aus Nummer ITV_1 bis ITV_4 abweichen und die Wahrnehmbarkeit

einzelner Betroffenenrechte nicht aus der digitalen Anwendung heraus unterstützen, sondern hierzu alternative Wege anbieten.

a) Der Verantwortliche der digitalen Anwendung MUSS die betroffene Person in diesem Fall in der Datenschutzerklärung zu der digitalen Anwendung auf das Fortbestehen der genannten Rechte hinweisen.

b) Sofern die Verarbeitung von personenbezogenen Daten nach Beendigung der Verordnungs- bzw. Bewilligungsdauer auf Grundlage einer informierten Einwilligung der betroffenen Person erfolgt, MUSS der Widerruf dieser Einwilligung auch nach Beendigung der Verordnungs- bzw. Bewilligungsdauer aus der digitalen Anwendung heraus möglich sein.

ITV_5.4 Der Verantwortliche der digitalen Anwendung MUSS die betroffene Person in der Datenschutzerklärung sowie in der digitalen Anwendung über das Recht auf Auskunft zu gespeicherten Daten, das Recht auf Löschung, Sperrung, Korrektur und Vervollständigung gespeicherter personenbezogener Daten sowie das Recht auf Datenportabilität hinweisen und leicht verständliche Hinweise zur Wahrnehmung dieser Rechte geben.

7.4 Allgemeine Erläuterungen zur Anwendung von DiGAV, DiPAV und DSGVO

Die Kriterien zur Intervenierbarkeit basieren auf den Vorgaben von Artikel 12 sowie 15 bis 20 der DSGVO (Die Artikel 13 und 14 zu den Informationspflichten werden über das Kriterium "Transparenz" abgedeckt).

In Bezug auf die Berücksichtigung von gesetzlichen Aufbewahrungspflichten (z. B. wenn in einer DiPA eine pflegerische Primärdokumentation vorgenommen wird) wurden die Ergänzungen von § 35 Absatz 3 BDSG zu Art. 17 DSGVO berücksichtigt.

7.5 Spezifische Erläuterungen

Zu Anforderung ITV_1.1.b: Passwörter, Freischaltcodes und von der digitalen Anwendung zur Nutzung durch die betroffene Person erzeugte Authentisierungscodes dürfen nicht im Rahmen der Auskunft offenbart werden.

Zu Anforderungen ITV_2.2 und ITV_3.2: Die Übertragung von Daten aus der DiGA in eine elektronische Patientenakte soll nach entsprechender Autorisierung und Konfiguration durch die betroffene Person auch automatisiert ausgelöst werden können. Diese Automatismen sollen auch greifen können, um durch die betroffene Person vorgenommene Löschungen und Änderungen zu propagieren. Da davon ausgegangen wird, dass spätestens mit der verpflichtenden Umsetzung der ePA-Schnittstelle für DiGA zum 1.1.2023 die Datenkommunikation aus der DiGA in Richtung von Leistungserbringern vorrangig über die ePA erfolgt, bilden die Anforderungen ITV_2.2 und ITV_3.2 das in den Artikeln 17 und 19 DSGVO verankerte Recht auf Vergessenwerden auf die in der TI gegebenen technischen Möglichkeiten der Kommunikation zwischen DiGA, ePA und Leistungserbringern ab.

Zu Anforderung ITV_2.4: Ein automatisches Löschen oder Sperren der Primärdaten anderer Anwendungen oder Geräte darf aus der digitalen Anwendung heraus nicht automatisch angestoßen werden, da die digitale Anwendung potenziell nicht die einzige Datensenke dieser

Daten ist und damit die Funktionsfähigkeit anderer Anwendungen der betroffenen Person gefährden würde.

Zu Anforderung ITV_2.4.a: Eine Umsetzung dieses Kriteriums ist erst gefordert, wenn technische Spezifikationen und Testmöglichkeiten für die Anbindung von Hilfsmitteln und Implantaten an digitale Anwendungen auf der Basis des § 374a SGB V vorliegen.

Zu Anforderung ITV_3.3: Dieses Kriterium betrifft nur Datenänderungen im Kontext von Art. 16 und 17 DSGVO, die eindeutig als Korrekturen anzusehen sind. Änderungen, die im Kontext der digitalen Anwendung Fortschreibungen von Daten darstellen (z. B. tägliches Ändern des gewogenen Körpergewichts) werden durch dieses Kriterium nicht berührt.

Zu Anforderung ITV_4: Die Vorgaben zum Datenexport für DiGA entsprechen den Anforderungen aus Anlage 2 zur DiGAV bzw. Anlage 2 zur DiPAV. Der Fokus liegt auf der Übermittlung der verarbeiteten Daten an die betroffene Person durch Nutzung einer Exportfunktion. Die in Artikel 20 DSGVO ebenfalls geforderte Möglichkeit der direkten Bereitstellung für einen anderen Verantwortlichen unterliegt dem Vorbehalt der technischen Machbarkeit.

Zu Anforderung ITV_4.1.a: Es gibt aktuell keinen gesetzlichen Auftrag an die KBV analog zu dem Verfahren bei DiGA auch für DiPA ein interoperables Exportformat in Form eines MIO (medizinisches Informationsobjekt) zu spezifizieren. Die Anforderungen an DiPA enthalten daher keine Vorgabe zu einem bestimmten Format oder Standard, sondern beschränken sich auf die in der DSGVO gewählte Formulierung "strukturiertes, gängiges und maschinenlesbares Format". Es obliegt dem BfArM ggf. weitere Festlegungen zu treffen, welche Formate es für welche Art von DiPA als "gängig" akzeptiert.

Zu Anforderung ITV_4.1 c: Ein Export der Daten einer DiGA in die ePA über ein Pseudonym der betroffenen Person ist in der aktuellen Spezifikation der ePA noch nicht beschrieben und entsprechend auch nicht umgesetzt. Somit ist aktuell für das Schreiben in die ePA mit der KVNR ein personenidentifizierendes Datum erforderlich. Die einschränkende Formulierung „SOLL NICHT“ in Bezug auf das Durchbrechen der Pseudonymisierung zum Zweck des Datenexports wurde gewählt, um diese Ausnahme zuzulassen.

Zu Anforderung ITV_5.1: Bei der Verordnung oder Bewilligung einer digitalen Anwendung erhalten der Hersteller und der Verantwortliche der digitalen Anwendung lediglich einen pseudonymen Freischaltcode, der die einlösende Person zur Nutzung der digitalen Anwendung berechtigt. Gemäß Art. 11 DSGVO besteht keine Verpflichtung, alleine für die vollständige Umsetzung der Betroffenenrechte nach Art. 15 bis 20 DSGVO diese Pseudonymisierung zu durchbrechen. Daher sollen Umsetzungen der Betroffenenrechte über die digitale Anwendung gewählt werden.

Zu Anforderung ITV_5.3: Diese Anforderung bezieht sich vorrangig auf die Umsetzung der Grace Periode gemäß DMN_4.2. Sofern der Verantwortliche von dieser Möglichkeit Gebrauch macht, müssen auch bis zur Eingabe des neuen Freischaltcodes alle Betroffenenrechte gelten. DMN_4.2 schränkt hier jedoch die in der Grace Periode zulässigen Verarbeitungen ein, wovon potenziell auch technische Verfahren zur Wahrnehmung der Betroffenenrechte direkt aus der Anwendung heraus betroffen sind. Der Verantwortliche kann daher während der Grace Periode auch alternative Wege zur Wahrnehmung der Betroffenenrechte anbieten, z. B. durch Nutzung eines zuvor authentisierten Kommunikationskanals für eine direkte Kommunikation zwischen betroffener Person und Verantwortlichem.

8 Integrität, Richtigkeit und Vertraulichkeit

8.1 Regulatorische Grundlagen

- Art. 5 DSGVO
- Art. 32 DSGVO
- Art. 19 DSGVO

8.2 Gegenstandsbereich und Motivation

Dieses Kriterium leitet sich unmittelbar aus Art. 5 Absatz 1 Buchstaben d und f DSGVO sowie Art. 32 Absatz 1 Buchstabe b DSGVO ab und ist für DiGA und DiPA gleichermaßen gültig. Der Systematisierung des Standard-Datenschutzmodells folgend, wird der Grundsatz der "Richtigkeit" als Teil des Gewährleistungsziels "Integrität" behandelt. Die Zusammenfassung von Integrität und Vertraulichkeit zu einem Kriterium leitet sich nicht nur aus der DSGVO ab (Art. 5. Absatz 1 Buchstabe f), sondern trägt auch dem Umstand Rechnung, dass beide Grundsätze in Bezug auf die Anforderungen im Kriterium "DSFA" verankert sind, während die Umsetzung über geeignete Maßnahmen sehr stark in den Bereich der Informationssicherheit hineinreicht.

Hiermit fokussiert das Kriterium "Richtigkeit, Integrität und Vertraulichkeit" sehr stark auf Prozesse und Maßnahmen der Auswahl angemessener TOMs sowie der Kommunikation mit den Betroffenen.

8.3 Kriterien

IRV_1 Festlegungen zur Qualität der verarbeiteten Daten

IRV_1.1 Der Verantwortliche der digitalen Anwendungen MUSS Maßnahmen etablieren, mit denen regelhaft geprüft werden kann, ob die verarbeiteten Daten mit Blick auf die Anforderungen der rechtmäßigen Verarbeitungszwecke sachlich richtig, authentisch, vollständig und aktuell sind.

a) Hierzu MUSS der Verantwortliche der digitalen Anwendung die Anforderungen der einzelnen Verarbeitungstätigkeiten an die sachliche Richtigkeit, Authentizität, Vollständigkeit und Aktualität der verarbeiteten Daten nachvollziehbar analysieren und dokumentieren. Diese Anforderungen

SOLLEN so formuliert sein, dass eine automatisierte Prüfung ihrer Einhaltung möglich ist.

b) Sofern Daten die für eine Verarbeitungstätigkeit formulierten Anforderungen nicht erfüllen, MÜSSEN die Daten für die weitere Verarbeitung zu den der Verarbeitungstätigkeit übergeordneten Zwecken gesperrt werden, bis die erforderliche Datenqualität wiederhergestellt ist. Unrichtige oder potenziell nicht authentische Daten MÜSSEN in den datenspeichernden Systemen als solche markiert werden und erkennbar sein.

c) Sofern Daten die für eine Verarbeitungstätigkeit formulierten Anforderungen nicht erfüllen, MÜSSEN diese gelöscht werden, sofern sich die erforderliche Datenqualität nicht innerhalb einer im Löschkonzept festgelegten Frist wiederherstellen lässt. Ausgenommen hiervon sind zur Erfüllung der rechtmäßigen Zwecke erforderliche Historisierungen, gesetzliche Aufbewahrungsfristen sowie im Einzelfall zu begründenden legitimen Interessen des Verantwortlichen. Die vom Hersteller geltend gemachten Ausnahmen MÜSSEN rechtmäßig und im Löschkonzept der digitalen Anwendung dokumentiert und nachvollziehbar begründet sein.

d) Der Verantwortliche der digitalen Anwendung MUSS darlegen können, welche Maßnahmen er etabliert hat, um bei unrichtigen, veralteten, unvollständigen oder potenziell nicht authentischen Daten die geforderte Datenqualität wiederherzustellen. Der Hersteller MUSS die Wirksamkeit dieser Maßnahmen geeignet überprüfen und absichern.

IRV_1.2 Der Verantwortliche der digitalen Anwendungen MUSS Maßnahmen etablieren, mit denen Verletzungen der Integrität der verarbeiteten Daten erkennbar sind. Die Stärke dieser Maßnahmen MUSS ausreichend sein und diese Maßnahmen MÜSSEN sowohl die eingesetzten TOMs zur Sicherung der Integrität als auch die in der DSFA erfassten Risiken berücksichtigen.

a) Der Verantwortliche MUSS Maßnahmen etablieren, die unmittelbar greifen, sobald Verletzungen der Integrität verarbeiteter Daten erkannt oder begründet vermutet werden. Diese Maßnahmen MÜSSEN eine Sperrung oder Löschung von Daten beinhalten, für die keine zur Erfüllung der Verarbeitungszwecke und/oder Einhaltung der Schutzbedarfe auseichende Integrität festgestellt werden kann.

b) Der Verantwortliche MUSS Prozesse für eine regelmäßige Überprüfung und ggf. Verbesserung der Maßnahmen zur Erkennung von Verletzungen der Integrität etablieren.

IRV_1.3 Der Verantwortliche der digitalen Anwendungen MUSS Maßnahmen etablieren, mit denen Verletzungen der Vertraulichkeit der verarbeiteten Daten erkennbar sind. Die Stärke dieser Maßnahmen MUSS ausreichend sein und diese Maßnahmen MÜSSEN sowohl die eingesetzten TOMs zur Sicherung der Vertraulichkeit als auch die in der DSFA erfassten Risiken berücksichtigen.

a) Der Verantwortliche MUSS Maßnahmen etablieren, die unmittelbar greifen, sobald Verletzungen der Vertraulichkeit verarbeiteter Daten erkannt wurden oder konkrete Anhaltspunkte für die Vermutung bestehen, dass Verletzungen der Vertraulichkeit verarbeiteter Daten erfolgt sein können. Diese Maßnahmen MÜSSEN eine Sperrung von Daten beinhalten, für die keine zur Erfüllung der

Verarbeitungszwecke und/oder Einhaltung der Schutzbedarfe auseichende Vertraulichkeit festgestellt werden kann.

b) Der Verantwortliche MUSS Prozesse für eine regelmäßige Überprüfung und ggf. Verbesserung der Maßnahmen zur Erkennung von Verletzungen der Vertraulichkeit etablieren.

IRV_1.4 Sofern sich der Verantwortliche der digitalen Anwendung eines Auftragsverarbeiters bedient, MÜSSEN alle zu den Anforderungen IRV_1.1 bis IRV_1.3 aufgesetzten Maßnahmen und Prozesse über die Schnittstellen zwischen Verantwortlichem und Auftragsverarbeiter hinweg vertraglich abgesichert und friktionsfrei implementiert sein. Dies MUSS insbesondere klare Verpflichtungen des Auftragsverarbeiters beinhalten, bei der Vermeidung unrichtiger, nicht authentischer, unvollständiger, veralteter oder nicht integrer Daten mitzuwirken, diese bei Erkennen unverzüglich an den Verantwortlichen zu melden und den Verantwortlichen bei der Korrektur, Sperrung und/oder Löschung zu unterstützen.

IRV_1.5 Der Verantwortliche der digitalen Anwendung MUSS eine stets aktuelle und vollständige Übersicht führen, welche Logdateien durch welche Komponenten der digitalen Anwendung zu Zwecken des sicheren Betriebs und der Supportunterstützung geschriebenen werden.

a) Er MUSS darlegen können, in welchen Logdateien personenbezogene Daten enthalten sind und zu welchen betrieblichen Zwecken diese erforderlich sind. Er MUSS wirksame Maßnahmen zur Datenminimierung sowie zum Schutz der Vertraulichkeit dieser Logdateien umsetzen.

b) Mit dem Wegfall der Zwecke einer Protokollierung oder dem Wegfall der Nutzbarkeit geschriebener Logdateien für die vorgesehenen Zwecke MÜSSEN diese Logdateien unmittelbar gelöscht oder überschrieben werden. Eine dauerhafte Verwahrung oder Archivierung von Logdateien DARF NICHT stattfinden.

IRV_1.6 Sofern über die digitale Anwendung eine medizinisch motivierte Profilbildung im Sinne einer nur auf automatischen Verfahren über Gesundheitsdaten basierenden Zuordnung der betroffenen Person zu einer Personengruppe erfolgt, MUSS diese Profilbildung für die betroffene Person transparent sein und in unmittelbarem Bezug zu den Zwecken des bestimmungsgemäßen Gebrauchs stehen. Die Profilbildung MUSS anerkannten medizinischen bzw. pflegerischen Standards folgen bzw. der Hersteller MUSS deren Richtigkeit und Nutzen nachweisen können.

IRV_2 Proaktive Absicherung der Qualität der verarbeiteten Daten

IRV_2.1 Der Verantwortliche der digitalen Anwendung MUSS technische und organisatorische Maßnahmen für einen proaktiven Schutz der Richtigkeit, Integrität und Vertraulichkeit der verarbeiteten personenbezogenen Daten etablieren. Der Verantwortliche MUSS nachweisen können, dass diese Maßnahmen dem Stand der Technik entsprechen und gemessen an den in der DSFA festgestellten Risiken ausreichend sind.

a) Die gewählten technischen und organisatorischen Maßnahmen zur Absicherung von Integrität und Vertraulichkeit MÜSSEN unabhängig von den in der DSFA festgestellten Risiken mindestens die Anforderungen des Vertrauensniveaus substanziell nach Definition der eIDAS-Verordnung

abdecken. Sie SOLLEN unabhängig von den in der DSFA festgestellten Risiken geeignet sein, auch die Anforderungen an ein hohes Vertrauensniveau nach Definition der eIDAS-Verordnung abzudecken.

b) Die gewählten Maßnahmen MÜSSEN unabhängig von den in der DSFA festgestellten Risiken eine Berechtigungsmatrix beinhalten, aus der erkennbar ist, welche Rollen zu welchen Zwecken Daten welcher Datenkategorien anlegen/einspielen, einsehen, verändern und/oder löschen dürfen. Die Einhaltung dieser Berechtigungsmatrix MUSS technisch durch proaktive und reaktive Maßnahmen abgesichert sein. Es MUSS ein Prozess etabliert sein, der eine kontinuierliche Anpassung der Berechtigungsmatrix an die aus den Verarbeitungszwecken abgeleiteten Erfordernisse unter Berücksichtigung der im Betrieb festgestellten Zugriffe sicherstellt.

c) Die Maßnahmen zur Absicherung der Richtigkeit, Integrität, Aktualität und Vollständigkeit MÜSSEN bereits bei der Erhebung und Berechnung von Daten ansetzen und MÜSSEN Prüfungen auf Auffälligkeiten, offensichtliche Fehler, Inkonsistenzen und im Kontext der Verarbeitung nicht plausible Daten umfassen.

d) Der Verantwortliche MUSS Prozesse für eine regelmäßige Überprüfung der Wirksamkeit und eine kontinuierliche Verbesserung der Maßnahmen zur Absicherung der Richtigkeit, Integrität und Vertraulichkeit der verarbeiteten personenbezogenen Daten etablieren.

IRV_2.2 Der Verantwortliche der digitalen Anwendung MUSS durch angemessene Maßnahmen sicherstellen, dass die erforderliche Vertraulichkeit, Vollständigkeit, Richtigkeit und Integrität personenbezogener Daten auch in Backups und anderen für Betriebs- und Supportprozesse ausgespielten Daten sichergestellt sind. Der Verantwortliche MUSS sicherstellen, dass beim (Wieder-)Einspielen solcher Daten in die digitale Anwendung keine Änderungen oder Manipulationen an den Daten vorgenommen wurden.

a) Der Verantwortliche MUSS personenbezogene Daten ausschließlich zu definierten, rechtmäßigen und für den sicheren Betrieb oder die Erfüllung regulatorischer Vorgaben erforderlichen Zwecken aus der digitalen Anwendung ausspielen. Mit dem Wegfall der Zwecke oder dem Wegfall der Nutzbarkeit der ausgespielten Daten für diese Zwecke MÜSSEN die ausgespielten Daten unmittelbar gelöscht werden.

b) Sofern damit keine erhebliche Einschränkung der Verarbeitungszwecke einhergeht, SOLLEN personenbezogene Daten im Rahmen von Support- und Betriebsprozessen nur in anonymisierter oder pseudonymisierter Form ausgespielt werden.

c) Daten für Backups und rechtmäßige Archivierungen MÜSSEN ausschließlich verschlüsselt aus der digitalen Anwendung bzw. deren datenhaltenden Systemen ausgespielt werden. Der Verantwortliche der digitalen Anwendung MUSS sicherstellen, dass die zur Entschlüsselung der Daten erforderlichen Schlüssel ausschließlich gegenüber Berechtigten offenbart werden. Abruf oder Übermittlung der Schlüssel MÜSSEN nur über sichere Verfahren erfolgen, die die Authentizität des Berechtigten absichern.

IRV_3 Reaktive Wiederherstellung der geforderten Qualität der verarbeiteten Daten

IRV_3.1 Der Verantwortliche der digitalen Anwendung MUSS Prozesse für den Umgang mit im Nachhinein als unrichtig, nicht authentisch, unvollständig, veraltet oder verfälscht erkannten personenbezogenen Daten etablieren. Diese MÜSSEN greifen, wenn solche Daten verarbeitet oder gegenüber Auftragsverarbeitern oder anderen Verantwortlichen offenbart wurden.

a) Sofern im Nachhinein als unrichtig, nicht authentisch, unvollständig, veraltet oder verfälscht erkannte personenbezogene Daten verarbeitet wurden und darüber in abgeleitete oder berechnete Daten eingeflossen sind, MÜSSEN diese Verarbeitungen – unter der Maßgabe der Verhältnismäßigkeit und unter Berücksichtigung der für den konkreten Fall erhobenen Risiken – zurückgerollt und die abgeleiteten bzw. berechneten Daten gelöscht bzw. bis zur Korrektur gesperrt werden.

b) Sofern im Nachhinein als unrichtig, nicht authentisch, unvollständig, veraltet oder verfälscht erkannte personenbezogene Daten gegenüber Auftragsverarbeitern oder anderen Verantwortlichen offenbart wurden, MÜSSEN die Empfänger dieser Daten – unter der Maßgabe der Verhältnismäßigkeit und unter Berücksichtigung der für den konkreten Fall erhobenen Risiken – informiert werden.

c) Auf Verlangen der betroffenen Person MUSS der Verantwortliche der digitalen Anwendung der betroffenen Person darlegen können, welche Verarbeitungen mit welchem Ergebnis zurückgerollt wurden und welche Empfänger informiert wurden.

8.4 Allgemeine Erläuterungen

Die Kriterien zur Richtigkeit basieren auf den Vorgaben von Artikel 5 DSGVO mitsamt der zugehörigen Erwägungsgründe (insb. EG 39). Der Grundgedanke einer Prüfung gegen formulierte Qualitätsanforderungen ist aus den Anforderungen der DSK an datenschutzrechtliche Zertifizierungsprogramme entnommen und wurde in diesem Kriterium so weit als möglich auch auf die Absicherung der Integrität und Vertraulichkeit personenbezogener Daten ausgeweitet.

8.5 Spezifische Erläuterungen

Zu Anforderung IRV_1.6: Bei einer nur vorläufig in das Verzeichnis des BfArM aufgenommenen DIGA muss aus dem Studiendesign ersichtlich sein, dass ein solcher Nachweis im Rahmen einer Erprobung geführt werden kann.

Zu Anforderung IRV_3.1: Diese Anforderung bildet die Vorgaben aus Art. 19 DSGVO auf Fälle der Berichtigung bzw. Sperrung von durch den Verantwortlichen selbst als unrichtig oder anderweitig nicht verarbeitungsgeeignet erkannten Daten ab.

Zu Anforderung IRV_2.1 a: Es wird davon ausgegangen, dass DiGA und DiPA immer auch Daten verarbeiten, die unter Art. 9 DSGVO fallen. Hieraus wird abgeleitet, dass die in der eIDAS-Verordnung festgeschriebenen Anforderungen an das Schutzniveau "substanziell" ungeachtet der

Spezifika der einzelnen Anwendung eine untere Schranke („baseline“) für die gewählten technischen und organisatorischen Maßnahmen darstellen. Maßnahmen, deren Schutzwirkung unterhalb dieser Schranke liegt sind – sofern diese nicht in Kombination mit anderen Maßnahmen wirken – per se als nicht angemessen zu werten. Soweit umsetzbar sollen Hersteller und Verantwortliche von digitalen Anwendungen ungeachtet der Spezifika der einzelnen Anwendung immer auf Maßnahmen abzielen, mit denen ein hohes Vertrauensniveau nach eIDAS erreicht werden kann. Für die Abbildung der in Anlage 1 DiGAV zugrunde gelegten Schutzbedarfe nach BSI-Standard 200-2 auf die hier verwendeten Vertrauensniveaus gelten die Definitionen aus Kapitel 2.3 und Anlage A der BSI TR-03107.

Zu Anforderung IRV_2.1 b: Die geforderten Prozesse müssen eine Analyse der real erfolgten Zugriffe einschließen. Vergebene, aber nicht oder nur sehr selten in Anspruch genommene Zugriffsrechte müssen hinterfragt und ggf. zurückgenommen werden.

9 Rechenschaftspflicht

9.1 Regulatorische Grundlagen

- Art. 5 DSGVO
- Art. 32 DSGVO

9.2 Gegenstandsbereich und Motivation

Dieses Kriterium leitet sich unmittelbar aus Art. 5 Absatz 2 DSGVO ab und ist für DiGA und DiPA gleichermaßen gültig. Art. 5 Absatz 2 DSGVO bezieht sich in Bezug auf die Rechenschaftspflicht auf alle in Art. 5 Absatz 1 benannten Grundsätze der Verarbeitung personenbezogener Daten. Dieses wird hier auf konkrete, auf DiGA und DiPA bezogene Kriterien, heruntergebrochen.

Die Protokollierung von Datenverarbeitungen ist eine wesentliche Maßnahme zur Erfüllung der Rechenschaftspflicht. Neben der reaktiven Protokollierung zu Nachweiszwecken werden in diesem Kriterium auch weitere Zwecke einer Protokollierung wie z. B. die Auswertung von Ereignissen zur *regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung* [Art. 32 Absatz 1 Satz 1 Buchstabe d DSGVO] betrachtet.

Analog zu den Vorgaben zur elektronischen Patientenakte wird auch für digitale Anwendungen zwischen einer Protokollierung zu Datenschutzzwecken des Verantwortlichen und einem Protokoll zur Datenschutzkontrolle durch den Betroffenen unterschieden.

9.3 Kriterien

ACC_1 Protokollierung zur Datenschutzkontrolle durch die betroffene Person

ACC_1.1 Die digitale Anwendung MUSS alle für den Datenschutz relevanten Aktivitäten der betroffenen Person in einem Protokoll erfassen, dessen Zweck die Datenschutzkontrolle durch die betroffene Person ist (Verwaltungsprotokoll).

a) Über das Verwaltungsprotokoll MUSS erkennbar sein, wann welche Einwilligungen in welcher Version durch die betroffene Person abgegeben bzw. widerrufen wurden. Hierzu MUSS jede Ausprägung einer

Einwilligungserklärung vom Verantwortlichen der digitalen Anwendung versioniert und historisiert werden.

b) Über das Verwaltungsprotokoll MÜSSEN alle durch die betroffene Person vorgenommenen Vergaben von Berechtigungen sowie Änderungen und Rücknahmen dieser Berechtigungen erkennbar sein.

c) Über das Verwaltungsprotokoll MÜSSEN alle durch die betroffene Person vorgenommenen Änderungen an für die Authentisierung genutzten Daten erkennbar sein.

d) Einträge in dem Verwaltungsprotokoll SOLLEN auch verfügbare Informationen zum Kontext der protokollierten Aktivität – insbesondere zu den verwendeten IT-Systemen - umfassen.

e) Einträge im Verwaltungsprotokoll MÜSSEN authentisch sein, in unmittelbarer zeitlicher Nähe zum Ereignis erstellt werden und mit geeigneten technischen Maßnahmen gegen jegliche Manipulation geschützt sein.

f) Die betroffene Person MUSS über die digitale Anwendung Einsicht in das Verwaltungsprotokoll nehmen können.

ACC_1.2 Der Verantwortliche der digitalen Anwendung MUSS der betroffenen Person vor Beendigung der Anwendungsnutzung den Download des Verwaltungsprotokolls aus der Anwendung heraus ermöglichen.

a) Sofern der Hersteller nach Abschluss der Anwendungsnutzung ein Grace-Periode gemäß Anforderung DMN_4 im Kriterium "Datenminimierung" zulässt, MUSS der Download des Verwaltungsprotokolls auch während der Grace-Periode möglich sein.

b) Mit Beendigung der Nutzung der digitalen Anwendung (einschließlich einer ggf. vorgesehenen Grace-Periode) MUSS das Verwaltungsprotokoll gelöscht werden.

ACC_2 Protokollierung zu Datenschutzzwecken des Verantwortlichen

ACC_2.1 Für die digitale Anwendung MUSS ein Protokoll zu Datenschutzzwecken des Verantwortlichen (Audit Trail) geschrieben werden.

a) Der Audit Trail MUSS die Dokumentation von Zugriffen, Datenweitergaben und Datenänderungen, den Nachweis der Quellen von über die Anwendung erhobenen Daten sowie die Protokollierung von (auch automatisiert durchgeführten) Sperrungen und Löschungen von Daten beinhalten.

b) Der Audit Trail MUSS alle Zugriffe von Administrations-, Betriebs- und Support-Personal auf personenbezogene Daten einschließlich des Audit Trails erfassen, um interne Datenschutzverletzungen aufdecken zu können. Alle potenziell auf Rollen, Rechte und Rechteinhaber wirkenden Systemänderungen MÜSSEN protokoliert werden.

c) Für alle protokollierten Ereignisse MUSS erfasst werden, welche Daten diese betreffen und wann diese von welchem Nutzer und – bei Nutzung mobiler Endgeräte - über welches Gerät diese durchgeführt wurden.

d) Der Audit Trail MUSS durch technische und organisatorische Maßnahmen gegen Verfälschung und Verlust geschützt sein. Übermittlung und Speicherung

von Protokolldaten MÜSSEN mit dem Schutzbedarf angemessener Verschlüsselung erfolgen.

e) Die Einsicht in den Audit Trail MUSS auf möglichst wenige Personen beschränkt und durch technische Maßnahmen abgesichert sein. In einem Rollen- und Rechtekonzept MÜSSEN die entsprechenden Regelungen konkret erfasst sein und es MUSS für jede berechtigte Rolle ausgeführt werden, zu welchen Zwecken und unter Einhaltung welcher technischen und organisatorischen Absicherungsmaßnahmen eine Einsicht in Protokolldaten möglich ist.

f) Der Verantwortliche der digitalen Anwendung MUSS Verfahren vorsehen, über die Protokolldaten regelhaft mit Blick auf mögliche Sicherheits- oder Datenschutzvorfälle ausgewertet werden. Diese Auswertungen SOLLEN automatisch erfolgen und MÜSSEN im Fall des Verdachts eines Vorfalls in einen definierten Eskalationsprozess münden. Hierbei erforderlich Zugriffe auf Protokolldaten durch natürliche Personen MÜSSEN den Einschränkungen aus Anforderung ACC_2.1 e unterliegen.

g) Der Audit Trail MUSS so geschrieben werden, dass er keine Verhaltens- und Leistungskontrolle von Mitarbeitern des Herstellers oder des Verantwortlichen der digitalen Anwendung erlaubt. Ist dies technisch nicht möglich, ohne die Umsetzung der Anforderungen ACC_2.1 a bis ACC_2.1 d zu gefährden, so MUSS durch organisatorische Maßnahmen eine zweckfremde Nutzung von Protokolldaten ausgeschlossen werden.

h) Bei mehrschrittigen oder kontinuierlichen Verarbeitungsvorgängen umfasst der Audit Trail lediglich Einträge über den Start oder den Abschluss der Verarbeitung. Eine Protokollierung granularer Aktivitäten findet aus Gründen der Datenminimierung nicht statt.

i) Die Protokolldaten MÜSSEN nach 3 Monaten sicher gelöscht werden, es sei denn, dass eine weitere Aufbewahrung für laufende Untersuchungen erforderlich ist.

ACC_2.2 Im Kontext der Umsetzung der Auswertung von Protokolldaten MUSS der Verantwortliche aufzeigen können, welche Soll-Zustände in den Protokollen bei den Verarbeitungen zu den rechtmäßigen Verarbeitungszwecken erwartet werden und gegen welche Abweichungen die Ist-Zustände mit automatischen Verfahren geprüft werden.

ACC_2.3 Der Verantwortliche der digitalen Anwendung MUSS anhand der Protokolle die ordnungsgemäße Umsetzung seines Löschkonzepts verifizieren können. Er MUSS Aufsichtsbehörden auf Verlangen Protokollauszüge vorlegen, aus denen nachvollziehbar ist, dass die gesetzlichen Vorgaben zur Sperrung und Löschung nicht mehr erforderlicher Daten vollständig umgesetzt sind.

ACC_3 Wirksamkeit der Protokollierung

ACC_3.1 Der Verantwortliche der digitalen Anwendung MUSS einen Prozess etablieren, über den die Auswirkungen von Änderungen in den Verarbeitungsvorgängen auf das Schreiben und Auswerten von Protokolldaten analysiert und ggf. Anpassungen an der Protokollierung vorgenommen werden.

ACC_3.2 Der Verantwortliche der digitalen Anwendung MUSS einen Prozess etablieren, über den die Auswirkungen von Änderungen in Administrations-, Betriebs- und Support-Prozessen auf das Schreiben und Auswerten von Protokolldaten analysiert und ggf. Anpassungen an der Protokollierung vorgenommen werden.

ACC_3.3 Der Verantwortliche der digitalen Anwendung MUSS – ggf. organisatorisch gestützte – technische Maßnahmen in der digitalen Anwendung und in den internen IT-Systemen implementieren, die sicherstellen, dass einer Protokollierung unterliegende Verarbeitungsvorgänge nur ausgeführt werden, wenn sichergestellt ist, dass die geforderten Protokolleinträge geschrieben werden können. Erfolgte Schreibzugriffe, die nicht protokolliert werden können, MÜSSEN zurückgerollt werden. Erfolgte Lesezugriffe, die nicht protokolliert werden können, MÜSSEN abgebrochen werden, bevor das gelesene Datum an das anfordernde System bzw. den anfordernden Nutzer übergeben wird.

ACC_3.4 Der Verantwortliche der digitalen Anwendung MUSS Prozesse zu einer regelmäßigen Überprüfung der Qualität der automatisierten Auswertung von Protokollen zur Erkennung von potenziellen Datenschutz- und/oder Sicherheitsvorfällen und zur Überwachung der Wirksamkeit der eingesetzten technischen und organisatorischen Maßnahmen etablieren. Der Prozess MUSS Vorgaben zur kontinuierlichen Verbesserung der genutzten Datengrundlagen und Algorithmen beinhalten. Der Prozess SOLL auch regelmäßige manuelle Prüfungen von Protokollen durch Personen mit entsprechenden Befugnissen umfassen.

9.4 Allgemeine Erläuterungen zur Anwendung von DiGAV, DiPAV und DSGVO

Die Kriterien zur Rechenschaftspflicht basieren auf den Vorgaben von Artikel 5 Absatz 2 DSGVO. Für die Rechenschaftspflicht im Zusammenhang mit Einwilligungen (Art. 7 Absatz 1 DSGVO) wurden zusätzlich die Erläuterungen aus dem *Kurzpapier Nr. 20 der Datenschutzkonferenz (Einwilligung nach der DSGVO)* berücksichtigt (abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf). Die Vorgaben zur technischen und organisatorischen Umsetzung einer Protokollierung zu Datenschutzzwecken wurden teilweise aus dem Baustein 43 "Protokollierung" des Standard-Datenschutzmodells übernommen.

Bei der Verordnung oder Bewilligung einer digitalen Anwendung erhalten der Hersteller und der Verantwortliche der digitalen Anwendung lediglich einen pseudonymen Freischaltcode, der die einlösende Person zur Nutzung der Anwendung berechtigt. Der Hersteller legt für jeden Nutzer der digitalen Anwendung einen Nutzer-Account mit einem vom Hersteller vergebenen Identifier an. Dieser soll im Rahmen der Protokollierung verwendet werden. Im Streitfall ist eine Auflösung des Freischaltcodes zu einer Personenidentität unter Zuhilfenahme von Daten der Krankenkasse der betroffenen Person möglich.

9.5 Spezifische Erläuterungen

Zu Anforderung ACC_1.1: Der Verantwortliche der digitalen Anwendung muss das Recht auf Auskunft insofern einschränken, als dass er aufgrund der pseudonymen Nutzung nur den Zugang zu Protokolldaten über die digitale Anwendung selbst ermöglicht.

Zu Anforderung ACC_1.1d: Die Angaben zum genutzten Gerät sollen ausreichend sein, damit die betroffene Person erkennen kann, ob/dass es das eigene Gerät ist. Beispielsweise können Hersteller, Produktname und Produktversion protokolliert werden.

Zu Anforderung ACC_2.1 h: Diese Einschränkung betrifft vor allem Datenverarbeitungen im Zusammenspiel mit an die digitale Anwendung angebundener Sensorik. Beispielsweise ist es wenig zielführend, wenn das Einspielen von Daten aus einem Blutzuckermessgerät in ein Diabetestagebuch darin mündet, dass für jedes abgespeicherte Einzeldatum ein Protokolleintrag geschrieben wird. Hier ist es ausreichend, wenn Angaben zum ersten und letzten importierten Datum in einer Form protokolliert werden, dass implizit erkennbar ist, welche weiteren Daten im Rahmen dieses Importvorgangs eingelesen wurden.

Zu Anforderung ACC_2.3: Grundlage dieser Anforderung ist, dass Maßnahmen zur Überprüfbarkeit des Löschkonzepts Bestandteil desselben sind (siehe Anforderung DMN_2.1 c).

Zu Anforderung ACC_3.3: Die beschriebenen Anforderungen an schreibende Zugriffe bauen aufeinander auf, d. h. die technische Möglichkeit eines Rollback sichert die Protokollierung ab und greift nur, wenn das System trotz einer theoretisch gegebenen Protokollierungsmöglichkeit kein Protokoll schreiben kann. Die Sicherstellung der Protokollierbarkeit muss nicht zwingend vor jedem schreibenden Verarbeitungsschritt erfolgen. Vielmehr reicht es aus, wenn – bei gegebener Rollback-Möglichkeit – das System regelmäßig oder bei Eintritt in definierte Systemzustände die Verfügbarkeit des Protokollierungsdienstes prüft.

Zu Anforderung ACC_3.4: Die manuellen Prüfungen von Protokollen sollen in Stichproben erfolgen und vorrangig absichern, dass die automatischen Prüfungen vollständig sind, d. h. keine erkennbaren, potenziell auf unzulässige Verarbeitungen hindeutende Muster übersehen werden.

Teil 3: Verantwortlicher und Auftragsverarbeiter

10 Wahrnehmung von Verantwortung

10.1 Regulatorische Grundlagen

- Art. 24 DSGVO
- Art. 26 DSGVO
- Art. 28 DSGVO
- Art. 33 DSGVO
- Art. 34 DSGVO
- Art. 37-39 DSGVO
- § 4 Absatz 5 DiGAV

10.2 Gegenstandsbereich und Motivation

Die gesamthafte und übergreifende Verantwortung für die Einhaltung des Datenschutzes bei einer digitalen Anwendung liegt beim Verantwortlichen der digitalen Anwendung:

- Er muss die Risiken seiner Anwendung kennen und entsprechend handeln (siehe Kriterium "Datenschutz-Folgenabschätzung und Verzeichnis von Verarbeitungstätigkeiten").
- Er muss ggf. einbezogene Auftragsverarbeiter sorgsam auswählen, steuern und überwachen (siehe Kriterium "Auftragsverarbeitung und Datenübermittlung").
- Er muss sicherstellen, dass die Grundprinzipien des Datenschutzes in der digitalen Anwendung selbst und über deren gesamten Lebenszyklus hinweg berücksichtigt sind (siehe Kriterien in Teil 1 dieses Katalogs).

Darüber hinaus muss der Verantwortliche der digitalen Anwendung sicherstellen, dass der Datenschutz über einzelne Maßnahmen und Prinzipien hinweg auch in der Struktur und den Prozessen der Organisation des Herstellers verankert ist. Dieses ist Gegenstand des Kriteriums "Wahrnehmung von Verantwortung".

10.3 Kriterien

CTRL_1 Interne Organisation

CTRL_1.1 Der Verantwortliche der digitalen Anwendung MUSS alle Personen, die aus ihrer Tätigkeit heraus Zugang zu personenbezogenen Daten haben, auf die Verschwiegenheit verpflichten.

CTRL_1.2 Der Verantwortliche der digitalen Anwendung MUSS einen Datenschutzbeauftragten ernennen. Der Datenschutzbeauftragte MUSS gegenüber den von Verarbeitungsprozessen der digitalen Anwendung Betroffenen als Ansprechpartner für alle Fragen zum Datenschutz benannt sein.

a) Der Verantwortliche der digitalen Anwendung MUSS die fachliche Eignung des ernannten Datenschutzbeauftragten belegen können. Er MUSS dem Datenschutzbeauftragten angemessene Möglichkeiten zum Erhalt seines Fachwissens bieten. Er MUSS sich vergewissern, dass diese Möglichkeiten wahrgenommen werden.

b) Der Datenschutzbeauftragte DARF KEINE Aufgaben im Rahmen der Entwicklung oder des Betriebs der digitalen Anwendung wahrnehmen, die zu einem Interessenskonflikt mit der Rolle des Datenschutzbeauftragten führen können.

c) Der Datenschutzbeauftragte MUSS Zugang zu allen Verarbeitungsvorgängen und den zugehörigen Dokumentationen haben. Er MUSS eigenaktiv Verbesserungen vorschlagen und anmahnen können. Eine Ablehnung von Einbringungen des Datenschutzbeauftragten MUSS begründet und dokumentiert werden.

d) Der Verantwortliche der digitalen Anwendung MUSS dem Datenschutzbeauftragten ausreichend Ressourcen für die Wahrnehmung seiner Aufgaben zur Verfügung stellen. Sofern es sich bei dem Datenschutzbeauftragten um einen Mitarbeiter des Verantwortlichen der digitalen Anwendung handelt, MUSS der Verantwortliche der digitalen Anwendung dem Datenschutzbeauftragten für einen angemessenen Anteil seiner Arbeitszeit von anderen Aufgaben freistellen.

CTRL_1.3 Der Verantwortliche der digitalen Anwendung MUSS sicherstellen, dass Personen, die von ihrer Rolle oder Stellung im Unternehmen her nicht in Prozesse zur rechtmäßigen Datenverarbeitung der digitalen Anwendung einbezogen sind, keinen Zugriff auf durch diese Anwendung verarbeitete personenbezogene Daten haben.

a) Der Verantwortliche der digitalen Anwendung MUSS die Rollen seiner Beschäftigten so definiert haben, dass aus der Stellenbeschreibung erkennbar ist, ob eine Befassung mit über die digitale Anwendung verarbeiteten personenbezogenen Daten erforderlich ist.

CTRL_1.4 Soweit es sich um einen nicht in der Europäischen Union niedergelassenen Verantwortlichen handelt, MÜSSEN die Vorgaben des Art. 27 DSGVO eingehalten werden. Der schriftlich durch den Verantwortlichen benannte Vertreter MUSS in Deutschland niedergelassen sein.

CTRL_2 Entwicklungs- und Betriebsprozesse ("Privacy by Design")

CTRL_2.1 Der Verantwortliche der digitalen Anwendung MUSS einen Prozess zur Erfassung und Überwachung von Risiken etabliert haben.

a) Der Verantwortliche der digitalen Anwendung MUSS in der Datenschutz-Folgenabschätzung verbliebene Restrisiken in seine regulären Prozesse der Risikoüberwachung überführen.

b) Der Verantwortliche der digitalen Anwendung MUSS alle neu erfassten Risiken in Bezug auf ihre Auswirkungen auf die Rechte und Freiheiten natürlicher Personen bewerten (siehe auch DSFA_1.8).

CTRL_2.2 Der Verantwortliche der digitalen Anwendung MUSS einen Prozess etabliert haben, über den Themen des Datenschutzes in der Planung, Umsetzung und dem Ausrollen von Produkt-Releases berücksichtigt werden.

a) Der Verantwortliche der digitalen Anwendung MUSS sicherstellen, dass neue Leistungsmerkmale der digitalen Anwendung erst nach einer Abschätzung der damit potenziell einhergehenden Risiken für die Rechte und Freiheiten natürlicher Personen einem konkreten Release zugeordnet werden.

b) Der Verantwortliche der digitalen Anwendung MUSS sicherstellen, dass alle für ein neues Leistungsmerkmal der digitalen Anwendung erforderlichen technisch-organisatorischen Maßnahmen vor Produktivsetzung des Releases aktiv sind oder zumindest zusammen mit dem Release aktiv werden.

c) Der Verantwortliche der digitalen Anwendung MUSS sicherstellen, dass kein Release der digitalen Anwendung produktiv gesetzt wird, in dem Leistungsmerkmale enthalten sind, für die nach einer Datenschutz-Folgenabschätzung und Umsetzung risikomindernder Maßnahmen ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht.

CTRL_2.3 Der Verantwortliche der digitalen Anwendung MUSS einen Prozess etabliert haben, über den Themen des Datenschutzes in der Planung, Umsetzung und dem Einspielen von Hotfixes berücksichtigt werden.

a) Der Verantwortliche der digitalen Anwendung MUSS grundsätzlich sicherstellen, dass kurzfristig vorgenommene Änderungen an der digitalen Anwendung die Wirksamkeit bestehender technisch-organisatorischer Maßnahmen nicht schwächen.

CTRL_2.4 Der Verantwortliche der digitalen Anwendung MUSS sicherstellen, dass für Analyse und Design der digitalen Anwendung verantwortliche Personen über aktuelles Wissen zu technischen Maßnahmen des Datenschutzes verfügen.

a) Der Hersteller und der Verantwortliche der digitalen Anwendung SOLLEN eine Unternehmenskultur fördern, in der für Analyse und Design der digitalen Anwendung verantwortliche Personen den Datenschutzbeauftragten proaktiv einbeziehen.

b) Der Hersteller und der Verantwortliche der digitalen Anwendung SOLLEN eine Unternehmenskultur fördern, in der Defizite und Versäumnisse im Datenschutz offen angesprochen werden und deren Behebung als gemeinsame Aufgabe begriffen wird.

CTRL_3 Umgang mit Datenschutzverletzungen

CTRL_3.1 Der Verantwortliche der digitalen Anwendungen MUSS Prozesse etabliert haben, mit denen die fristgerechte Information von Aufsichtsbehörden im Fall von Verletzung des Schutzes personenbezogener Daten abgesichert ist.

a) Der Verantwortliche der digitalen Anwendung MUSS bei jeder vermuteten oder festgestellten Verletzung des Schutzes personenbezogener Daten unverzüglich einen Prozess initiieren, in dem festgestellt wird,
    a. ob ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht,
    b. wie hoch dieses Risiko einzuschätzen ist,
    c. ob unmittelbare Maßnahmen erforderlich sind und
    d. welche Personen und Kompetenzen für die weitere Analyse des Risikos erforderlich sind.

b) Der Verantwortliche der digitalen Anwendung SOLL Strukturen und Prozesse etabliert haben, die sicherstellen, dass für jede vermutete oder festgestellte Verletzung des Schutzes personenbezogener Daten innerhalb von 72 Stunden eine fundierte Einschätzung vorliegt, ob diese Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

c) Der Verantwortliche der digitalen Anwendung MUSS einen definierten Ablaufplan für Meldungen einer Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde aufgestellt haben, der eine Meldung innerhalb von 72 Stunden sicherstellt. Teil dieses Plans MUSS eine klare Definition der Entscheidungsverantwortungen sein.

d) Alle nach Buchstabe a bis c dieser Anforderung getroffenen Abwägungen und durchgeführten Handlungen MÜSSEN in einer Form dokumentiert werden, die es der zuständigen Aufsichtsbehörde erlaubte, die Rechtmäßigkeit der letztendlich getroffenen Entscheidungen zu bewerten.

CTRL_3.2 Der Verantwortliche MUSS auch bei einer ausschließlichen Verarbeitung pseudonymer Daten die gegebenen Möglichkeiten der digitalen Anwendung ausschöpfen, um eine betroffene Person über eine mit hohen Risiken einhergehende Verletzung des Schutzes personenbezogener Daten zu informieren.

a) Die Information der betroffenen Person MUSS in klarer und verständlicher Sprache erfolgen und der betroffenen Person eine realistische Einschätzung der für sie konkret bestehenden Risiken erlauben.

b) Sofern die Verletzung des Schutzes personenbezogener Daten fortbesteht oder daraus weitere Risiken resultieren, MUSS der Verantwortliche der betroffenen Person konkrete Maßnahmen vorschlagen, wie diese die bestehenden Risiken eindämmen oder ausschließen kann.

c) Der Verantwortliche MUSS technisch-organisatorische Maßnahmen vorsehen, mit denen eine Änderung von Anmeldedaten durch eine von einer Verletzung des Schutzes personenbezogener Daten betroffene Person erzwungen werden kann.

d) Der Verantwortliche MUSS Verfahrensregeln und Prozesse etabliert haben, die absichern, dass die Information der betroffenen Person innerhalb einer angemessenen Frist erfolgt.

CTRL_4 Gemeinsame Verantwortung

CTRL_4.1 Eine gemeinsame Verantwortung (Art. 26 DSGVO) ist für digitale Gesundheitsanwendungen nach § 33a SGB V und für digitale Pflegeanwendungen nach § 40a SGB XI grundsätzlich zulässig. In diesem Fall MÜSSEN alle Verantwortlichen jeweils den Nachweis der Einhaltung der Anforderungen aus diesem Dokument führen.

a) Jeder Verantwortliche MUSS für die in seine Verantwortung fallenden Verarbeitungstätigkeiten sowie für die Schnittstellen zu den Verarbeitungstätigkeiten der anderen Verantwortlichen eine Datenschutz-Folgenabschätzung unter Berücksichtigung der im Kriterium DSFA_1 aufgeführten Anforderungen durchführen. Er MUSS bei der Bewertung der Rest-Risiken und Rest-Folgen die von den anderen Verantwortlichen erhobenen Risiken und definierten technisch-organisatorischen Maßnahmen berücksichtigen.

b) Jeder Verantwortliche MUSS für die in seine Verantwortung fallenden Verarbeitungstätigkeiten ein Verzeichnis von Verarbeitungstätigkeiten unter Berücksichtigung der im Kriterium DSFA_2 aufgeführten Anforderungen durchführen.

10.4 Allgemeine Erläuterungen

Dieses Kriterium greift die Teile der Anlage 1 zur DiGAV auf, die sich primär mit der Verankerung des Datenschutzes in der Struktur und den Prozessen des Herstellers befassen und die in Art. 24 DSGVO beschriebene Verantwortung des Verantwortlichen widerspiegeln. In Bezug auf die Verankerung des Datenschutzes in den internen Prozessen gibt es Überschneidungen mit dem Kriterium "Datenschutz-Folgenabschätzung". Diese sind gewollt, da in diesem Kriterium der Blick von den bestehenden ITSM-Prozessen des Unternehmens auf den Datenschutz geht, während das Kriterium "Datenschutz-Folgenabschätzung" genau umgekehrt von den datenschutzrechtlichen Anforderungen ausgehend die erforderlichen Prozesse definiert.

10.5 Spezifische Erläuterungen

Zu Anforderung CTRL_1.1: Diese Anforderung leitet sich für DiGA unmittelbar aus § 4 Absatz 5 DiGAV und für DiPA aus § 5 Absatz 6 DiPAV ab.

Zu Anforderung CTRL_2.1: Die Datenschutz-Folgenabschätzung darf nicht als isolierte "Pflichtübung" wahrgenommen werden, sondern muss Bestandteil des regulären Risikomanagements sein. Nur so ist sichergestellt, dass die in der Datenschutz-Folgenabschätzung erfassten Risiken die erforderliche Sichtbarkeit bekommen und in den ITSM-Prozessen rund um Entwicklung und Betrieb der digitalen Anwendung berücksichtigt werden.

Zu Anforderungen CTRL_2.2 und CTRL_2.3: Jedes Release der digitalen Anwendung muss im Rahmen der Überwachung an die Zertifizierungsstelle gemeldet werden. Dabei hat der Verantwortliche die Änderungsparameter zum Stand der Zertifizierung darzustellen und zu begründen, warum die Konformitätsaussage trotz der Weiterentwicklung des Produkts erhalten bleibt. Es obliegt der Verantwortung und Haftung der Zertifizierungsstelle anhand dieser Informationen über die Notwendigkeit von weiteren Prüfungen zu entscheiden. Bei agiler

Entwicklung wird die Zertifizierungsstelle in die Abstimmungsprozesse zum Product-Backlog einbezogen und es wird die Sprint Planung übermittelt. Die Zertifizierungsstelle muss dann spätestes im Rahmen des Sprint-Review über weitere Prüfungen entscheiden. Es ist die Verantwortung der Zertifizierungsstelle die Ergebnisse des Sprint-Review zu dokumentieren.

Zu Anforderung CTRL_3.2: Hersteller und Verantwortliche von DiGA und DiPA erhalten im Prozess der Verordnung bzw. Bewilligung lediglich einen Freischaltcode als Nachweis der Kostenübernahme. Die nutzende Person selbst wird nicht identifiziert und bleibt damit für den Hersteller und den Verantwortlichen der digitalen Anwendung pseudonym. Dieses schließt ein, dass der Hersteller und der Verantwortliche – von begründeten Ausnahmefällen abgesehen - über keine Kontaktdaten der betroffenen Person verfügt. Die einzige Möglichkeit der Information der betroffenen Person zu Datenschutzvorfällen besteht damit über die digitale Anwendung selbst, z. B. durch Push-Nachrichten oder Einblenden eines Warnhinweises auf dem Start-Bildschirm.

11 Auftragsverarbeitung und Datenübermittlung

11.1 Regulatorische Grundlagen

- Art. 28 DSGVO
- Art. 29 DSGVO
- Art. 45 DSGVO
- § 4 Absatz 5 DiGAV

11.2 Gegenstandsbereich und Motivation

Fokus der meisten Anbieter digitaler Anwendungen sind die Bereitstellung einer Software, die Erfüllung der regulatorischen Auflagen an die Aufnahme in das DiGA- bzw. DiPA-Verzeichnis und die Umsetzung kundennaher Prozesse vom Vertrieb bis zur Abrechnung. Das Hosting der Hintergrundsysteme der digitalen Anwendung und weite Teile des IT-Servicemanagements werden hingegen oft als Auftragsverarbeitung an Dienstleister übertragen. Weitere Auftragsverarbeitungen können sich z. B. aus der Inanspruchnahme von Abrechnungsdienstleistern oder durch Nutzung von Cloud-basierten as-a-service-Angeboten (z. B. Aussenden von Push-Nachrichten oder Chat-Bots im 1st-Level-Support) ergeben.

In diesem Kriterium werden auf Grundlage des Art. 28 DSGVO und der weiterführenden Hinweise im Kurzpapier 13 der DSK die an den Verantwortlichen der digitalen Anwendung gestellten Anforderungen an die Beauftragung und Absicherung einer Auftragsverarbeitung zusammengefasst. Durch den Auftragsverarbeiter umzusetzende technische und organisatorische Maßnahmen zur Sicherheit der Verarbeitung (Art. 32 DSGVO) werden im Kriterium "Technische und organisatorische Maßnahmen" behandelt.

11.3 Kriterien

AV_1 Übermittlung an Drittländer

AV_1.1 Jegliche Verarbeitung personenbeziehbarer Daten zu den rechtmäßigen Zwecken der digitalen Anwendung MUSS ausschließlich im Inland, in einem anderen Mitgliedstaat der Europäischen Union, in einem diesem nach § 35 Absatz 7 des SGB I gleichgestellten Staat, oder auf Grundlage eines Angemessenheitsbeschlusses gemäß

Artikel 45 DSGVO erfolgen. Dieses schließt personenbeziehbare Bestands-, Nutzungs- und Verkehrsdaten ein.

AV_1.2 Der Verantwortliche der digitalen Anwendung DARF KEINE Verträge mit Dienstleistern abschließen, die dem Dienstleister das Recht einräumen, ohne Zustimmung des Herstellers der digitalen Anwendung Verarbeitungen personenbeziehbarer Daten an anderen als den vereinbarten Orten durchzuführen.

AV_1.3 Sofern eine Verarbeitung personenbeziehbarer Daten zu den rechtmäßigen Zwecken der digitalen Anwendung durch einen Dienstleister erfolgt, dessen Mutterkonzern in einem Drittland ansässig ist, das die Anforderung nach AV_1.1 nicht erfüllt, MÜSSEN zusätzliche technisch-organisatorische Maßnahmen greifen, die eine Datenverarbeitung in diesem Drittland und einen Datentransfer in dieses Drittland verhindern.

a) Der Verantwortliche der digitalen Anwendung MUSS sicherstellen, dass in Hintergrundsystemen verarbeitete personenbezogenen Daten verschlüsselt gespeichert und ausgetauscht werden. Die Schlüssel zur Entschlüsselung der Daten MÜSSEN vom Hersteller in der EU selbst verwaltet oder gespeichert werden. Anstelle des Verantwortlichen KANN auch ein Treuhänder die Verwaltung der Schlüssel übernehmen; dieser MUSS die Anforderungen aus AV_1.1 erfüllen.

b) Der Verantwortliche der digitalen Anwendung und der betroffene Dienstleister MÜSSEN bestätigen, dass im Fall von Herausgabeverlangen von Behörden eines Drittlandes zunächst keine Daten zur Verfügung gestellt und auch nicht an das Mutterunternehmen des Dienstleisters herausgegeben werden.

c) Der betroffene Dienstleister MUSS dem Verantwortlichen der digitalen Anwendung zusichern, dass er in jedem Fall eines Herausgabeverlangens den Rechtsweg beschreiten und ausschöpfen wird.

AV_1.4 Der Verantwortliche der digitalen Anwendung MUSS für alle in der digitalen Anwendung genutzten Komponenten von Drittanbietern sicherstellen, dass diese keine Datenübermittlung in Drittländer durchführen, die gegen die Vorgaben der Anforderungen AV_1.1 oder AV_1.3 verstößt. Hierbei sind auch Datenweitergaben zu Zwecken des Supports oder der Fehleranalyse (z. B. als Teil des 3rd-Level-Supports) zu berücksichtigen.

a) Der Verantwortliche der digitalen Anwendung MUSS für alle in der digitalen Anwendung genutzten Komponenten von Drittanbietern aktuelle Dokumentationen und/oder Verträge entsprechend der eingesetzten Version der digitalen Anwendung vorweisen können, aus denen sämtliche Anlässe einer Datenübermittlung sowie die Orte der Datenverarbeitung ersichtlich sind bzw. aus denen erkennbar ist, dass keine Datenübermittlung erfolgt.

b) Der Verantwortliche der digitalen Anwendung MUSS nachweisen können, dass die auf solche Datenübermittlungen folgenden Verarbeitungen bei einem Dritten keine Auftragsverarbeitung im Sinne des Art. 28 DSGVO darstellen.

AV_2 Auftragsverarbeitung

AV_2.1 Jegliche Datenverarbeitung durch einen Auftragsverarbeiter MUSS auf Grundlage eines rechtsgültigen Vertrags mit dem Verantwortlichen der digitalen Anwendung oder auf Basis eines anderen, nach Art. 28 Absatz 3 DSGVO zulässigen Rechtsinstruments erfolgen. Der Vertrag MUSS

Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegen.

a) Der Vertrag MUSS den Auftragsverarbeiter an den Hersteller der digitalen Anwendung binden, insofern als dass jegliche Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ausschließlich auf Weisung des Herstellers der digitalen Anwendung erfolgt. Der Verantwortliche der digitalen Anwendung MUSS einen Prozess zur Dokumentation und Kontrolle aller erteilten Weisungen etabliert haben.

b) Der Auftragsverarbeiter MUSS zusichern, dass alle mit der Verarbeitung personenbezogener Daten befassten Personen der Verschwiegenheit unterliegen oder sich auf Vertraulichkeit verpflichtet haben.

c) Der Auftragsverarbeiter MUSS die Sicherheit der Verarbeitung garantieren und zusichern, dieses durch angemessene technisch-organisatorische Maßnahmen abzusichern.

d) Der Vertrag MUSS transparent machen, welche weiteren Auftragsverarbeiter der Auftragsverarbeiter ggf. nutzt und welche Absicherungen und Garantien sicherstellen, dass das vom Hersteller der digitalen Anwendung vorgegebene Datenschutzniveau über die gesamte Kette von Auftragsverarbeitern eingehalten werden kann.

e) Der Verantwortliche der digitalen Anwendung MUSS alle vorgenommenen Vertragsänderungen und alle Nebenabsprachen zum Vertrag geeignet dokumentieren.

AV_2.2 Der Verantwortliche der digitalen Anwendung MUSS vor Vertragsschuss mit einem Auftragsverarbeiter überprüft haben, dass aussagekräftige und aktuelle Beschreibungen der von dem Auftragsverarbeiter etablierten technisch-organisatorischen Maßnahmen vorliegen.

a) Aus den Informationen MUSS hervorgehen, auf welche im Auftrag des Verantwortlichen der digitalen Anwendung durchgeführten Verarbeitungstätigkeiten und auf welche Kategorien personenbezogener Daten diese Maßnahmen wirken.

AV_2.3 Der Verantwortliche der digitalen Anwendung MUSS die reibungslose Zusammenarbeit mit einbezogenen Dienstleistern in allen Fragen des Datenschutzes sicherstellen.

a) Der Verantwortliche MUSS sicherstellen, dass jeder Auftragsverarbeiter einen Datenschutzbeauftragten benannt hat und dass die aktuellen Kontaktdaten dieser Person vorliegen.

b) Der Verantwortliche MUSS sich vertraglich bei jedem Auftragsverarbeiter abgesichert haben, dass

    a. ggf. für die Umsetzung der Betroffenenrechte erforderliche Zuarbeiten oder Zulieferung durch die Dienstleister zugesagt werden,

    b. er durch den Dienstleister unmittelbar informiert wird, wenn Verletzungen des Schutzes personenbezogener Daten festgestellt werden,

c. der Dienstleister im Fall eines gegenüber der Datenschutzaufsicht meldepflichtigen Ereignisses alle für die Meldung erforderlichen, in seinen Zuständigkeitsbereich fallenden Informationen beibringt.

c) Jeder Auftragsverarbeiter SOLL zusichern, dass jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung nachgelagerter Auftragsverarbeiter erst nach Information des Verantwortlichen der digitalen Anwendung umgesetzt wird.

AV_2.4 Der Verantwortliche der digitalen Anwendung MUSS die Zulässigkeit aller beauftragten Auftragsverarbeitungen nachweisen können.

a) Der Verantwortliche der digitalen Anwendung MUSS für jede Auftragsverarbeitung nachweisen können, dass diese keine gemeinsame Verantwortung nach Art. 26 DSGVO darstellt.

b) Der Verantwortliche der digitalen Anwendung MUSS vor Vertragsschluss mit einem Auftragsverarbeiter sichergestellt haben, dass dieser durch sein Fachwissen, seine Zuverlässigkeit und die bereitgestellten Ressourcen hinreichende Garantien für die Sicherheit der Verarbeitung bietet. Er SOLL hierzu vom Auftragsverarbeiter Nachweise zu Zertifizierungen verlangen.

AV_2.5 Der Verantwortliche der digitalen Anwendung MUSS angemessene Möglichkeiten der Kontrolle einbezogener Auftragsverarbeiter besitzen.

a) Der Verantwortliche der digitalen Anwendung MUSS einen Prozess etabliert haben, mit dem er die Einhaltung der vertraglichen Vereinbarungen sowie die Wirksamkeit der beim Auftragnehmer umgesetzten technischen und organisatorischen Maßnahmen fortlaufend kontrollieren kann.

AV_2.6 Der Verantwortliche der digitalen Anwendung MUSS in seinem Löschkonzept auch alle Daten erfassen, die bei Auftragsverarbeitern zu den rechtmäßigen Zwecken der digitalen Anwendung verarbeitet werden.

a) Ausgenommen hiervon sind beim Auftragsverarbeiter anfallende Bestands-, Verkehrs- und Nutzungsdaten. Für diese Daten MUSS der Auftragsverarbeiter ein Löschkonzept besitzen und dem Verantwortlichen der digitalen Anwendung zusichern, dass diese Daten mit Beendigung des Auftragsverhältnisses gemäß Löschkonzept sicher gelöscht werden.

b) Der Verantwortliche der digitalen Anwendung MUSS sicher nachvollziehen können, welche Daten welcher betroffenen Personen zu welchem Zeitpunkt an welche Auftragsverarbeiter übermittelt wurden.

AV_2.7 Der Verantwortliche der digitalen Anwendung MUSS die betroffenen Personen in der Datenschutzerklärung der digitalen Anwendung über das Vorliegen von Auftragsverarbeitungen, die Verarbeitungszwecke, die Person des Auftragsverarbeiters und die Kategorien übermittelter Daten informieren.

AV_2.8 Soweit es sich um einen nicht in der Union niedergelassenen Auftragsverarbeiter handelt, MÜSSEN die Vorgaben des Art. 27 DSGVO eingehalten werden. Der schriftlich durch den Auftragsverarbeiter benannte Vertreter MUSS in Deutschland niedergelassen sein.

11.4 Allgemeine Erläuterungen

Der Fokus dieses Kriteriums liegt auf vertraglichen Aspekten der Auftragsverarbeitung sowie den Prozessen des Verantwortlichen zur Absicherung des Vertrags und zur Kontrolle seiner Einhaltung. Entsprechend bildet vorrangig Art. 28 DSGVO die Basis für dieses Kriterium. Anderen im Kontext der Auftragsverarbeitung relevante Vorgaben der DSGVO sind in den Kriterien "Technische und organisatorische Maßnahmen" (Sicherheit der Verarbeitung) und "Datenschutz-Folgenabschätzung" (Angemessenheit und Weiterentwicklung von Maßnahmen) dargestellt.

11.5 Spezifische Erläuterungen

Zu Anforderung AV_1.1: Diese Anforderung gibt für DiGA die Vorgaben aus § 4 Absatz 5 DiGAV und für DiPA Vorgaben aus § 5 Absatz 4 DiPAV wieder.

Zu Anforderung AV_1.3: Töchter US-amerikanischer Unternehmen sind faktisch nicht ohne Weiteres in der Lage, die gegebenen Zusagen zum Ausschluss einer Verarbeitung von Daten in einem nicht zulässigen Drittland einzuhalten (siehe Begründung zu Schrems-II-Urteil). Daher müssen technische und organisatorische Maßnahmen vereinbart werden, die eine Datenherausgabe an US-Behörden oder eine Datenüberragung an den Mutterkonzern signifikant erschweren oder gar unmöglich machen. Hierzu hatte das BfArM Anfang 2021 Vorgaben formuliert, die in Anforderung AV_1.3 enthalten sind.

Zu Anforderung AV_1.4: Es ist nicht auszuschließen, dass aus dem Betrieb einer digitalen Anwendung heraus Datenübermittlungen stattfinden, die auf den ersten Blick nicht als Auftragsverarbeitungen erkennbar sind bzw. aus den Prozessen des Verantwortlichen heraus motiviert sind.

Zu Anforderung AV_2.4: Diese Anforderung zielt auf die Rechtmäßigkeit einer Auftragsverarbeitung ab. Grundlage ist in AV_2.4 alleinig das Datenschutzecht, weitergehende Vorgaben für einzelne Akteure ergeben sich unmittelbar aus der DiGAV bzw. DiPAV und sind an anderer Stelle berücksichtigt (z. B. AV_1.1).

Zu Anforderung AV_2.5: Die Ausführungen in [AnfDsZert] sehen ergänzend/alternativ zu einem kontinuierlichen Kontrollprozess auch die Vor-Ort-Inspektion vor. Diese Option wurde hier nicht erwähnt, da davon ausgegangen wird, dass ein großer Teil der Auftragsverarbeitungen von DiGA und DiPA in Cloud-Rechenzentren großer Hosting-Anbieter stattfinden wird, bei denen aussagekräftige Vor-Ort-Inspektionen kaum möglich sind.

12 Datenschutz-Folgenabschätzung und Verzeichnis von Verarbeitungstätigkeiten

12.1 Regulatorische Grundlagen

- Art. 30 DSGVO
- Art. 35 DSGVO

12.2 Gegenstandsbereich und Motivation

Die Anforderungen an die Umsetzung des Verzeichnisses von Verarbeitungstätigkeiten wurden überwiegend aus [DSK VV1] übernommen und im Hinblick auf die Spezifika digitaler Gesundheits- und Pflegeanwendungen konkretisiert.

Die Anforderungen an die Durchführung einer Risikobeurteilung im Kontext einer Datenschutz-Folgenabschätzung wurden überwiegend aus [DSK P18] übernommen und im Hinblick auf die Spezifika digitaler Gesundheits- und Pflegeanwendungen konkretisiert.

Dem Kriterium zur Datenschutz-Folgenabschätzung (DSFA) liegt eine Durchführung der DSFA in den folgenden Schritten zugrunde:

1. Durchführung einer Schwellwert-Analyse
2. Erfassung von Risiken und Bewertung der Folgen für die Rechte und Freiheiten natürlicher Personen
3. Definition von technischen und organisatorischen Maßnahmen zur Minimierung der Risiken
4. Bewertung der verbleibenden Rest-Risiken und deren Rest-Folgen
5. Sofern hohe Risiken verbleiben: Abstimmung mit BfDI/LDA (Art. 36 DSGVO)

Die definierten Anforderungen an die Risikoanalyse gelten gleichermaßen für die Schritte 2 und 4.

12.3 Kriterien

DSFA_1 Datenschutz-Folgenabschätzung

DSFA_1.1 Der Verantwortliche SOLL eine Schwellwertanalyse durchführen, in der er das Erfordernis einer Datenschutz-Folgenabschätzung für die digitale Anwendung untersucht. Er MUSS hierzu die aktuelle Version der Blacklist der Datenschutzkonferenz zugrunde legen ("Liste der Verarbeitungstätigkeiten, für die eine Datenschutz-Folgenabschätzung erforderlich ist").

a) Stellt der Verantwortliche kein Erfordernis für die Durchführung einer Datenschutz-Folgenabschätzung fest, MUSS er dieses nachvollziehbar dokumentieren. Er KANN in diesem Fall auf die Erfüllung der Anforderungen DSFA_1.2 bis DSFA_1.8 verzichten.

b) Der Verantwortliche KANN auf die Durchführung einer Schwellwertanalyse verzichten. In diesem Fall MUSS er eine Datenschutz-Folgenabschätzung für die digitale Anwendung durchführen.

DSFA_1.2 Sofern die Schwellwertanalyse das Erfordernis einer Datenschutz-Folgenabschätzung anzeigt, MUSS der Verantwortliche der digitalen Anwendung eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO) durchführen, die alle auf die digitale Anwendung bezogenen Verarbeitungstätigkeiten umfasst.

a) Der Verantwortliche der digitalen Anwendung KANN separate Datenschutz-Folgenabschätzungen für Verarbeitungen zu Zwecken des bestimmungsgemäßen Gebrauchs und für Verarbeitungen zu anderen Zwecken durchführen.

b) Der Verantwortliche der digitalen Anwendung KANN einzelne Verarbeitungen zu regulatorisch bedingten Zwecken aus der Datenschutz-Folgenabschätzung der digitalen Anwendung ausklammern, sofern hierfür oder für einen ähnlichen Verarbeitungsvorgang mit ähnlich hohen Risiken bereits eine Datenschutz-Folgenabschätzung vorliegt.

c) Der Verantwortliche der digitalen Anwendung KANN einzelne Verarbeitungen zu regulatorisch bedingten Zwecken aus der Datenschutz-Folgenabschätzung der digitalen Anwendung ausklammern, wenn für diese Verarbeitungen eine Zulassung durch die gematik erforderlich ist.

d) Der Verantwortliche SOLL auch bei Ausklammerung einzelner Verarbeitungen in der Lage sein, eine alle Verarbeitungstätigkeiten umfassende Sicht auf Risiken und deren Folgen für die Rechte und Freiheiten natürlicher Personen herzustellen, um auf dieser Basis eine übergreifende Bewertung machen zu können und die Vollständigkeit der Analyse sicherzustellen.

DSFA_1.3 Sofern die Schwellwertanalyse das Erfordernis einer Datenschutz-Folgenabschätzung anzeigt, MUSS die Datenschutz-Folgenabschätzung zu den auf die digitale Anwendung bezogenen Verarbeitungstätigkeiten sämtliche der in Art. 35 Abs. 7 DSGVO genannten Inhalte enthalten.

a) Die geplanten Verarbeitungsvorgänge und Zwecke der Verarbeitung MÜSSEN strukturiert beschrieben sein. Die Zweckbeschreibung MUSS den Zweck so eng fassen, dass die Grenzen der den Zweck erfüllenden Verarbeitungsvorgänge sowie die dazu notwendigen und erforderlichen Daten im dafür angemessenen

Umfang technisch und datenschutzrechtlich bestimmbar und nachvollziehbar sind. Für DiGA SOLL die Strukturierung entlang der rechtmäßigen Zwecke gemäß § 4 Abs. 2 Satz 1 DiGAV erfolgen. Für DiPA SOLL die Strukturierung entlang der rechtmäßigen Zwecke gemäß § 4 Absatz 3 Satz 1 DiPAV erfolgen.

b) Die Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck MUSS durch den Verantwortlichen der digitalen Anwendung bewertet werden. Das Ergebnis der Bewertung MUSS als Teil der Datenschutz-Folgenabschätzung dokumentiert sein.

c) Der Verantwortliche der digitalen Anwendung MUSS die Risiken der digitalen Anwendung für die Rechte und Freiheiten natürlicher Personen bewerten (siehe auch DSFA_1.5). Das Ergebnis der Bewertung MUSS als Teil der Datenschutz-Folgenabschätzung dokumentiert sein.

d) Der Verantwortliche der digitalen Anwendung MUSS als Teil der Datenschutz-Folgenabschätzung aufzeigen, wie die erhobenen Risiken durch geeignete technisch-organisatorische Maßnahmen, Garantien und Sicherheitsvorkehrungen bewältigt werden.

DSFA_1.4 Sofern die Schwellwertanalyse das Erfordernis einer Datenschutz-Folgenabschätzung anzeigt, MUSS der Verantwortliche der digitalen Anwendung bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten – sofern benannt - einholen.

DSFA_1.5 Sofern die Schwellwertanalyse das Erfordernis einer Datenschutz-Folgenabschätzung anzeigt, MUSS der Verantwortliche der digitalen Anwendung durch eine Risikobewertung alle Möglichkeiten des Eintritts von Ereignissen identifizieren und beurteilen, die zu Schäden für eine natürliche Person führen können ("Risiken").

a) Der Verantwortliche der digitalen Anwendung SOLL ein dokumentiertes, durch Datenschutzbehörden des Bundes und/oder der Länder anerkanntes Verfahren zur Risikobewertung nutzen, das klare Definitionen für Eintrittswahrscheinlichkeiten und Schwere von Schäden sowie eine daraus abgeleitete Risikoklassifizierung vorgibt. Er KANN ein anderes Verfahren nutzen, MUSS dann jedoch

   a. eine Dokumentation des Vorgehens in deutscher Sprache vorlegen können und MUSS darlegen können, worin die besondere Eignung dieses Verfahrens für die Risikobeurteilung der betrachteten digitalen Anwendung liegt,

   b. nachvollziehbare, weitgehend objektivierbare, mindestens dreistufige Skalen für die Eintrittswahrscheinlichkeiten und Schwere von Schäden definieren,

   c. eine mindestens dreistufige Risikoklassifizierung definieren, die jedes Risiko in Bezug zu der Eintrittswahrscheinlichkeit und Schwere des dadurch potenziell bedingten Schadens setzt und in der klar erkennbar ist, wann ein hohes Risiko im Sinne der DSGVO vorliegt.

b) Der Verantwortliche der digitalen Anwendung MUSS als Ausgangspunkt der Risikobewertung nachvollziehbar dokumentieren, welche Schäden für natürliche Personen auf der Grundlage der zu verarbeitenden Daten bewirkt werden können. Er MUSS hierbei physische, materielle und insbesondere auch immaterielle Schäden betrachten. Er MUSS die unrechtmäßige Verkettung von

zu unterschiedlichen Zwecken erhobenen Daten sowohl beim Verantwortlichen als auch bei eventuell eingebundenen Auftragsverarbeitern als eigenständiges Risiko berücksichtigen.

c) Der Verantwortliche der digitalen Anwendung MUSS für jeden analysierten Schaden erheben und nachvollziehbar dokumentieren, welche Ereignisse zu einem Eintritt des Schadens führen können.

d) Der Verantwortliche der digitalen Anwendung MUSS nachvollziehbar analysieren und dokumentieren, durch welche Handlungen und Umstände es zum Eintritt der potenziell einen Schaden bedingenden Ereignisse kommen kann.

e) Der Verantwortliche der digitalen Anwendung MUSS für jeden Schaden die Eintrittswahrscheinlichkeit und Schwere festlegen. Er SOLL hierzu jeweils eine vierstufige Skala verwenden (geringfügig, überschaubar, substanziell, groß). Er MUSS objektivierbare Kriterien heranziehen, um die Einordnung eines Schadens in gewählte Skala zu begründen. Er MUSS bei der Einordnung Art, Umfang, Umstände und Zweck der Verarbeitung sowie Spezifika des bestimmungsgemäßen Einsatzes und der Zielgruppen der digitalen Anwendung berücksichtigen.

f) Der Verantwortliche der digitalen Anwendung MUSS die analysierte Eintrittswahrscheinlichkeit und Schwere von Schäden auf die diesen zugrunde liegenden Ereignisse abbilden und diese in einer Risikomatrix dokumentieren. Für Ereignisse, die an der Grenze zwischen zwei Risikobereichen liegen, MUSS aus einer Einzelbetrachtung heraus die endgültige Einordnung nachvollziehbar begründet sein.

DSFA_1.6 Sofern die Schwellwertanalyse das Erfordernis einer Datenschutz-Folgenabschätzung anzeigt, MUSS der Verantwortliche der digitalen Anwendung für jedes analysierte Risiko der Risikoklassifizierung angemessene technisch-organisatorische Maßnahmen vorsehen, mit denen die Eintrittswahrscheinlichkeit und/oder Schwere des potenziell ausgelösten Schadens reduziert und damit das Risiko eingedämmt wird. Er MUSS durch geeignete Dokumentation nachvollziehbar machen, welche Maßnahmen auf welche Risiken abzielen und wie sich die Wirksamkeit der Maßnahmen bezogen auf ein konkretes Risiko begründet.

a) Der Verantwortliche der digitalen Anwendung MUSS in der Dokumentation der gewählten risikoeindämmenden Maßnahmen feststellen, ob durch die Maßnahme selbst neue Risiken ausgelöst oder bestehende Risiken verstärkt werden können. Aus der Maßnahme selbst resultierende, deren Wirksamkeit bedrohende Risiken MÜSSEN den Prozess der Risikobewertung durchlaufen. Sofern erforderlich, MÜSSEN auch zu diesen Risiken Maßnahmen definiert werden.

DSFA_1.7 Sofern die Schwellwertanalyse das Erfordernis einer Datenschutz-Folgenabschätzung anzeigt, MUSS der Verantwortliche für die digitale Anwendung die nach Umsetzung der definierten technisch-organisatorischen Maßnahmen verbleibenden Rest-Risiken und deren Rest-Folgen erfassen und bewerten.

a) Sofern Restrisiken verbleiben, die auch nach Umsetzung von risikoeindämmenden Maßnahmen hohe Risiken für die Rechte und Freiheiten natürlicher Personen darstellen, MUSS der Verantwortliche der digitalen Anwendung diese der zuständigen Aufsichtsbehörde melden. Der

Verantwortliche MUSS einen entsprechenden Eskalationsprozess unter Einbeziehung des Datenschutzbeauftragten definiert haben.

DSFA_1.8 Der Verantwortliche der digitalen Anwendungen MUSS einen Prozess zur Nachverfolgung aller erhoben Risiken bzw. zur regelhaften Neubewertung des Erfordernisses einer Datenschutz-Folgenabschätzung etabliert haben.

a) Sofern eine Datenschutz-Folgenabschätzung durchgeführt wurde, MUSS dieser Prozess eine regelhafte und regelmäßige, mindestens jedoch jährliche Neubewertung der Schwere und der Eintrittswahrscheinlichkeit der erhobenen Schäden beinhalten. Hierbei MÜSSEN technologische Entwicklungen und ein ggf. verändertes Nutzerverhalten betrachtet werden.

b) Dieser Prozess MUSS eine regelmäßige, mindestens jedoch jährliche Neubewertung der Wirksamkeit aller Maßnahmen zur Risikoeindämmung beinhalten. Hierbei MUSS eine Prüfung aller Maßnahmen gegen den Stand der Technik stattfinden (siehe auch TOM_1.3 b).

c) Dieser Prozess MUSS - insbesondere bei Änderungen der digitalen Anwendung oder Weiterentwicklungen des Stands der Technik oder des medizinischen bzw. pflegerischen Wissens – eine Bewertung der Erforderlichkeit der verarbeiteten Daten sowie der Einhaltung der rechtmäßigen Verarbeitungszwecke beinhalten (siehe auch DMN_1.2 und DMN_1.2).

d) Sofern keine Datenschutz-Folgenabschätzung durchgeführt wurde, MUSS dieser Prozess eine regelhafte und regelmäßige, mindestens jedoch jährliche Neubewertung der durchgeführten Schwellwertanalyse beinhalten. Sofern sich Anzeichen für signifikante Änderungen in der Bewertung der zugrundeliegenden Kriterien zeigen, MUSS der Verantwortliche eine erneute Schwellwertanalyse (siehe DSFA_1.1) und ggf. eine Datenschutz-Folgenabschätzung (siehe DSFA_1_2 bis DSFA_1.7) durchführen.

DSFA_2 Verzeichnis der Verarbeitungstätigkeiten

DSFA_2.1 Der Verantwortliche der digitalen Anwendung MUSS alle auf die digitale Anwendung bezogenen Verarbeitungstätigkeiten in sein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO aufnehmen.

a) Bei Verarbeitungen personenbezogener Daten zu Zwecken des bestimmungsgemäßen Gebrauchs MUSS der Verantwortliche der digitalen Anwendung darlegen, welche Leistungsmerkmale (*Features*) der digitalen Anwendung welcher Verarbeitungstätigkeit zugeordnet wurden. Er MUSS begründen können, warum bestimmte Leistungsmerkmale keine eigenständigen Verarbeitungstätigkeiten darstellen. Er MUSS bei thematisch „benachbarten“ Verarbeitungstätigkeiten, Verarbeitungen oder auch Befugnissen bei Zugriffen auf Datenbestände klare Kriterien der Abgrenzung im Sinne einer Zwecktrennung vornehmen.

b) Verarbeitungen personenbezogener Daten zu regulatorisch bedingten Zwecken MÜSSEN als eigenständige Verarbeitungstätigkeiten im Verzeichnis der Verarbeitungstätigkeiten erfasst werden.

c) Verarbeitungen personenbezogener Daten zu Zwecken der dauerhaften Gewährleistung der Sicherheit (bei DiPA), technischen Funktionsfähigkeit, der Nutzerfreundlichkeit, der altersgerechten Nutzbarkeit (bei DiPA) und der

Weiterentwicklung der digitalen Gesundheitsanwendung MÜSSEN als eigenständige Verarbeitungstätigkeiten im Verzeichnis der Verarbeitungstätigkeiten erfasst werden.

DSFA_2.2 Die Darstellungen der auf die digitale Anwendung bezogenen Verarbeitungstätigkeiten MÜSSEN sämtliche der in Art. 30 Abs. 1 Satz 2 Buchstabe a bis g DSGVO abschließend genannten Angaben enthalten.

a) Zu jeder Verarbeitungstätigkeit MÜSSEN Name und Kontaktdaten des Verantwortlichen, eines ggf. gemeinsam mit ihm Verantwortlichen, eines evtl. Vertreters für in Drittstaaten ansässige Verantwortliche und des Datenschutzbeauftragten benannt werden. Es SOLL erkennbar sein, welche Person oder Rolle primärer Ansprechpartner für Fragen seitens der Aufsichtsbehörden ist.

b) Zu jeder Verarbeitungstätigkeit MUSS der Verarbeitungszweck angegeben sein. Es DARF KEINEN vom Verantwortlichen der digitalen Anwendung implementierten rechtmäßigen Zweck geben, der nicht durch eine im Verzeichnis von Verarbeitungstätigkeiten aufgeführte, auf die digitale Anwendung bezogene Verarbeitungstätigkeit abgedeckt ist. Jede im Verzeichnis von Verarbeitungstätigkeiten aufgeführte, auf die digitale Anwendung bezogene Verarbeitungstätigkeit MUSS einem rechtmäßigen Zweck der digitalen Anwendung dienen.

c) Zu jeder Verarbeitungstätigkeit MÜSSEN die Kategorien betroffener Personen und die Kategorien der verarbeiteten, personenbezogenen Daten angegeben sein. Besondere Kategorien personenbezogener Daten – insbesondere Gesundheitsdaten – MÜSSEN als solche gekennzeichnet sein.

d) Zu jeder Verarbeitungstätigkeit MÜSSEN die Kategorien (Rollen, Funktionen, etc.) von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, benannt werden. Zu jeder Verarbeitungstätigkeit MÜSSEN die Kategorien (Rollen, Funktionen, etc.) von Personen, die auf die Daten zugriffsberechtigt sind oder zum Zugriff berechtigt werden können, benannt werden. Hierbei MÜSSEN sowohl Dritte als auch Auftragsverarbeiter und interne Rollen berücksichtigt werden.

e) Zu jeder Verarbeitungstätigkeit MUSS angegeben sein, ob durch den Verantwortlichen selbst oder entlang einer von dem Verantwortlichen verantworteten Kette von Auftragsverarbeitern eine Übermittlung in Drittländer stattfindet oder stattfinden kann. Ist dies der Fall, MUSS der Empfänger konkret benannt sein. Es MUSS erkennbar sein, für welche Kategorien von Daten eine Übermittlung in Drittländer stattfindet oder stattfinden kann.

f) Zu jeder Verarbeitungstätigkeit MÜSSEN die Fristen für die Löschung von Daten der einzelnen Kategorien angegeben sein. Details – z. B. zu technischen Verfahren zur Löschung und zur Prüfung erfolgreicher Löschungen – SOLLEN in einem separaten Löschkonzept beschrieben werden (siehe DMN_2).

g) Zu jeder Verarbeitungstätigkeit MÜSSEN die für die Gewährleistung eines dem Risiko angemessenen Schutzniveaus umgesetzten technischen und organisatorischen Maßnahmen benannt sein. Aus der Beschreibung der Maßnahmen MUSS erkennbar sein, welche Kategorien personenbezogener Daten welcher Kategorien betroffener Personen durch diese Maßnahme

geschützt werden. Es MUSS dargestellt sein, welche Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser Maßnahmen vom Hersteller der digitalen Anwendung etabliert wurden. Der Verantwortliche der digitalen Anwendung SOLL im Verzeichnis der Verarbeitungstätigkeiten die bestimmten und umgesetzten Maßnahmen nur benennen und für eine weitergehende Beschreibung auf das Sicherheitskonzept der digitalen Anwendung referenzieren.

DSFA_2.3 Der Verantwortliche der digitalen Anwendung MUSS Prozesse etabliert haben, um die Aktualität und Vollständigkeit des Verzeichnisses von Verarbeitungstätigkeiten abzusichern.

a) Es MUSS ein Prozess etabliert sein, über den die Aktualisierung des Verzeichnisses bei Einführung neuer Verarbeitungstätigkeiten, Änderungen an verzeichneten Verarbeitungstätigkeiten oder Außerbetriebnahme von Verarbeitungstätigkeiten erfolgt.

b) Es MUSS ein Prozess etabliert sein, über den die Aktualisierung des Verzeichnisses bei neu hinzukommenden, sich ändernden oder wegfallenden Auftragsverarbeitungsverhältnissen oder Datenweitergaben an Dritte erfolgt.

c) Der Verantwortliche der digitalen Anwendung MUSS Strukturen und Prozesse etablieren, die die Zusammenarbeit aller in die Fortschreibung und Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten einzubeziehenden Interessengruppen (Fachexperten und andere verantwortliche Personen beim Hersteller, Verantwortlichen und bei Auftragsverarbeitern, Datenschutzbeauftragte, etc.) organisieren und absichern.

d) Als Teil aller Prozesses zur Fortschreibung und Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten MUSS eine Bewertung stattfinden, ob eine erneute Durchführung einer vollständigen oder auf einzelne Verarbeitungen fokussierten Datenschutz-Folgenabschätzung erforderlich ist.

DSFA_2.4 Der Verantwortliche der digitalen Anwendung MUSS Prozesse etabliert haben, welche die Verwendbarkeit des Verzeichnisses von Verarbeitungstätigkeiten für die intendierten Zwecke sicherstellt.

a) Der Verantwortliche der digitalen Anwendung MUSS Aufsichtsbehörden eine schriftliche Fassung des Verzeichnisses in deutscher Sprache oder Auskünfte zu einzelnen Einträgen im Verzeichnis zur Verfügung stellen können.

b) Alle für die aufgeführten Verarbeitungstätigkeiten Verantwortlichen, der Datenschutzbeauftragte und ein ggf. berufener Informationssicherheitsbeauftragter MÜSSEN jederzeit auf das Verzeichnis von Verarbeitungstätigkeiten zugreifen können und MÜSSEN die in ihre Verantwortung fallenden Prozesse zur Pflege des Verzeichnisses kennen.

c) Der Verantwortliche der digitalen Anwendung MUSS für das Verzeichnis von Verarbeitungstätigkeiten eine Versionshistorie führen, über die erkennbar ist, welche Version des Verzeichnisses zu einem gegebenen Datum gültig war und welche Änderungen gegenüber der Vorversion vorgenommen wurden.

12.4 Allgemeine Erläuterungen

Für die Zertifizierung einer digitalen Anwendung werden nur die Verarbeitungstätigkeiten betrachtet, die in unmittelbarem Zusammenhang mit der digitalen Anwendung einschließlich ihrer Bereitstellung und Erstattung stehen. Allgemeine, unternehmensinterne Prozesse des Herstellers und des Verantwortlichen der digitalen Anwendung wie z. B. die Lohnbuchhaltung oder von der digitalen Anwendung unabhängige Verarbeitungen wie z. B. die Herausgabe eines Newsletters mit der damit einhergehenden Verwaltung eines E-Mail-Verteilers sind nicht Gegenstand der Prüfung.

Art. 30 Absatz 2 DSGVO verlangt auch von einem Auftragsverarbeiter das Führen eines Verzeichnisses von Verarbeitungstätigkeiten. Entsprechende Anforderungen finden sich im Kriterium "Auftragsverarbeitung und Datenübermittlung".

12.5 Spezifische Erläuterungen

Zu Anforderung DSFA_1.2 b: Diese Anforderung trifft insbesondere auf Verantwortliche zu, die mehrere DiGA und/oder DiPA anbieten. Hier sollen für die Abrechnungsprozesse und für die Durchführung einer Evaluation bereits bestehende Datenschutz-Folgenabschätzungen grundsätzlich auf weitere Anwendungen übertragbar sein, sofern sich die dahinterstehenden Verfahren oder die verarbeiteten Daten nicht oder nur unwesentlich verändert haben.

Zu Anforderung DSFA_1.2 c: Diese Anforderung zielt auf Verfahren ab, die in die Telematikinfrastruktur hineinreichen und durch die gematik im Ergebnis einer von der gematik definierten und abgenommen Datenschutz- und Sicherheitsprüfung zugelassen werden müssen. Dieses kann z. B. für das Schreiben von Daten einer DiGA in die elektronische Patientenakte der Fall sein.

Zu Anforderung DSFA_1.3 c: Die Beurteilung von Risiken ist nicht auf Verletzungen der Rechte und Freiheiten der betroffenen Person beschränkt, sondern umfasst grundsätzlich alle potenziell durch die digitale Anwendung gefährdeten natürlichen Personen. Beispielsweise können in durch die betroffene Person erstellten Tagebucheinträgen identifizierbare Dritte erwähnt werden, denen durch eine Offenbarung des Tagebuchs Schäden entstehen können.

Zu Anforderung DSFA_1.4: Diese Anforderung bildet die Vorgaben und Empfehlungen aus [DSK P18] ab.

Zu Anforderung DSFA_1.5a: Ein Beispiel für ein solches Verfahren ist das Standard-Datenschutzmodell der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder [DSM].

Zu Anforderung DSFA_2.1: Es soll zumindest jeder der in § 4 Absatz 2 Satz 1 DiGAV oder § 5 Absatz 3 DiPAV benannten Zwecke (mindestens) eine eigene Verarbeitungstätigkeit darstellen. Hierdurch ist eine klare Zuordnung der rechtmäßigen Zwecke zu Verarbeitungstätigkeiten gegeben.

Zu Anforderung DSFA_2.2: Anforderungen an ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Absatz 2 DSGVO finden sich im Kriterium "Auftragsverarbeitung und Datenübermittlung"

Zu Anforderung DSFA_2.2 g: Diese Anforderung greift die Interpretation des Begriffs "Übermittlung" in Art. 30 Abs. 1 Satz 2 Buchstabe d DSGVO durch die Datenschutzkonferenz auf (siehe [DSK VV1]).

13 Technische und Organisatorische Maßnahmen

13.1 Regulatorische Grundlagen

- Art. 25 DSGVO
- Art. 32 DSGVO

13.2 Gegenstandsbereich und Motivation

In dem Kriterium "Technische und Organisatorische Maßnahmen" sind Anforderungen zusammengefasst, die auf die Umsetzung der DSGVO-Vorgaben zu "Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen" (Art. 25 DSGVO) und "Sicherheit der Verarbeitung" (Art. 32 DSGVO) abzielen.

13.3 Kriterien

TOM_1 Auswahl und Weiterentwicklung von Maßnahmen

TOM_1.1 Der Verantwortliche der digitalen Anwendung und die von ihm als Auftragsverarbeiter einbezogenen Dienstleister MÜSSEN angemessene technische und organisatorische Maßnahmen gemäß dem Stand der Technik zum Schutz der Rechte und Freiheiten natürlicher Personen etablieren.

a) Die Bewertung der Angemessenheit MUSS neben der erhobenen Schwere und Eintrittswahrscheinlichkeit von Risiken auch Anforderungen der Zielgruppe und typische Nutzungsmuster berücksichtigen. Die betroffene Person DARF NICHT durch nicht handhabbare Maßnahmen dazu verleitet werden, die digitale Anwendung in einer Form zu nutzen, die diese Maßnahmen unterläuft oder die Eintrittswahrscheinlichkeit anderer Risiken erhöht.

b) Der Verantwortliche der digitalen Anwendung MUSS die von ihm gewählten, sowie die per Weisung seinen Auftragsverarbeitern vorgegebenen, technischen und organisatorischen Maßnahmen in geeigneter Form dokumentieren. Er KANN dieses im Rahmen eines Datenschutzkonzepts tun. Er KANN bei der Beschreibung der Maßnahmen auf ein Sicherheitskonzept oder ein Betriebskonzept verweisen.

c) Der Verantwortliche MUSS darlegen, welche Referenzen (Normen, Standards, Richtlinien, etc.) er als Maßstab für den "Stand der Technik" verwendet hat.

d) Als Teil der Maßnahmen-Dokumentation MUSS der Verantwortliche die Wahl der Maßnahmen begründen. Er SOLL darlegen, welche Alternativen untersucht und aus welchen Gründen diese verworfen wurden.

TOM_1.2 Technische und organisatorische Maßnahmen MÜSSEN die Sicherheit der Verarbeitung über den gesamten Lebenszyklus der digitalen Anwendung hinweg abdecken.

a) Der Verantwortliche der digitalen Anwendung MUSS bereits mit der Inbetriebnahme der digitalen Anwendung Verfahren definieren, die greifen, wenn die Anwendung vom Hersteller nicht mehr unterstützt wird.

TOM_1.3 Der Verantwortliche der digitalen Anwendung MUSS ein Verfahren zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen etabliert haben.

a) Die Überprüfung MUSS regelhaft und regelmäßig stattfinden. Modus, Durchführung und Ergebnisse der Überprüfungen MÜSSEN geeignet dokumentiert werden.

b) Teil der Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen MUSS eine Betrachtung des zum Zeitpunkt der Bewertung aktuellen Stands der Technik sein.

c) Der Verantwortliche der digitalen Anwendung MUSS Prozesse etabliert haben, die regeln, wie mit nicht mehr dem Stand der Technik entsprechenden Maßnahmen umgegangen wird. Teil dieser Prozesse MUSS ein strukturiertes Verfahren zur Bewertung der Kritikalität der bestehenden Maßnahme sowie der Umsetzbarkeit, Beherrschbarkeit und Wirksamkeit von technisch-organisatorischen Alternativ-Maßnahmen sein. Der Verantwortliche MUSS auf Basis dieser Bewertung beurteilen, ob die Maßnahme angepasst, ausgetauscht oder aufgrund vernachlässigbarer Risiken beibehalten werden kann (siehe hierzu auch DSFA_1.8).

d) Der Verantwortliche MUSS technologische Weiterentwicklungen und aktuelle, Sicherheit und/oder Datenschutz verbessernde Produktversionen losgelöst von deren akuter Notwendigkeit und der in c) erhobenen Bewertung innerhalb eines angemessenen Zeitrahmens umsetzen. Er SOLL zur Beschleunigung der Aktualisierung der eingesetzten Komponenten auch eine parallele Nutzung verschiedener Versionen dieser Komponenten zulassen.

TOM_2 Integrität und Vertraulichkeit

TOM_2.1 Im Rahmen der Verordnung oder Bewilligung einer digitalen Anwendung erhalten der Hersteller und der Verantwortliche keine identifizierenden Daten der betroffenen Person. Diese initial gegebene pseudonyme Nutzung DARF grundsätzlich NICHT durchbrochen werden.

a) Ist die Verarbeitung solcher Daten für Zwecke des bestimmungsgemäßen Gebrauchs erforderlich, MUSS der Verantwortliche technische und organisatorische Maßnahmen vorsehen, die eine Verwendung dieser Daten zu einer nicht legitimierten Identifizierung der betroffenen Person ausschließen.

b) Die digitale Anwendung DARF über die Plattform oder die Vertriebsplattform bereitgestellte oder übermittelte personenidentifizierende Daten NICHT speichern oder für andere als zum sicheren Betrieb der Anwendung erforderliche Zwecke verarbeiten.

c) Das Ausspielen von Daten aus der digitalen Anwendung zur Herstellung von Datenportabilität oder zur Erfüllung von Interoperabilitätsanforderungen MUSS grundsätzlich ausschließlich über Mittel der digitalen Anwendung erfolgen, die auf der pseudonym durchgeführten Authentisierung aufbauen. Das Ausspielen identifizierender Daten ist nur zulässig, wenn dieses zur Erfüllung einer regulatorischen Verpflichtung erforderlich ist.

TOM_2.2 Der Verantwortliche der digitalen Anwendung MUSS alle verwendeten kryptografischen Dienste zusammen mit ihrem Einsatzzweck und den verwendeten Algorithmen und vorgegebenen Schlüssellängen in einem Kryptografiekonzept dokumentieren. Das Kryptografiekonzept MUSS Maßnahmen beschreiben, wie Schlüssel und Zertifikate ausgetauscht werden können.

a) Jegliche Kommunikation zwischen Komponenten der digitalen Anwendung, zu Komponenten der digitalen Anwendung und aus Komponenten der digitalen Anwendung heraus MUSS verschlüsselt erfolgen.

b) Jegliche Speicherung von personenbezogenen Daten auf dem Endgerät der betroffenen Person MUSS verschlüsselt erfolgen.

c) Jegliche Speicherung von personenbezogenen Daten auf Hintergrundsystemen der digitalen Anwendung MUSS verschlüsselt erfolgen.

d) Für die Authentisierung und Autorisierung genutzte Sicherheitstoken MÜSSEN digital signiert sein. Die digitale Anwendung MUSS die Integrität und Authentizität dieser Signaturen prüfen.

e) Auf Hintergrundsystemen angesiedelte Dienste MÜSSEN sich gegenüber anfragenden Systemen authentisieren. Anfragende Systeme DÜRFEN KEINE personenbezogenen Daten an Dienste auf Hintergrundsystemen übermitteln, deren Authentizität sie nicht zuvor geprüft haben.

f) Alle verwendeten Zertifikate und Schlüssel MÜSSEN dem Stand der Technik entsprechen.

TOM_2.3 Der Verantwortliche der digitalen Anwendung MUSS die Verfahren zur Vergabe, Prüfung und Durchsetzung von Berechtigungen in einem Berechtigungskonzept dokumentieren. In die Berechtigungsprüfung MÜSSEN ausschließlich Attribute einfließen, die bei der betroffenen Person erhoben wurden oder die aus einer anderen vertrauenswürdigen Quelle stammen.

a) Das Berechtigungskonzept MUSS alle Zugriffe auf Dienste und Systeme regulieren, die personenbezogene Daten verarbeiten. Dieses MUSS Zugriffe von Beschäftigten des Verantwortlichen und seiner Auftragsverarbeiter (z. B. zu Zwecken der Wartung und des Supports) einschließen.

b) Jeder Zugriff auf Dienste und Systeme, die personenbezogene Daten verarbeiten, MUSS eine Berechtigungsprüfung durchlaufen haben.

c) Der Verantwortliche der digitalen Anwendung MUSS Verfahren für die weitere Verarbeitung abgewiesener Authentisierungs- und Zugriffsversuche definiert

haben. Diese MÜSSEN geeignet sein, *brute force* Angriffen wirksam zu begegnen.

TOM_3 Interaktion und Integration

TOM_3.1 Die digitale Anwendung KANN der betroffenen Person auch bei deaktivierter oder im Hintergrund laufender Anwendung und/oder bei im Ruhemodus befindlicher Plattform aus der digitalen Anwendung heraus getriggerte Nachrichten ("Push-Mitteilungen") senden.

a) Push-Mitteilungen DÜRFEN KEINE Gesundheitsdaten enthalten.

b) Die digitale Anwendung DARF grundsätzlich KEINE Push-Mitteilungen nutzen, die nicht zu Zwecken des bestimmungsgemäßen Gebrauchs erforderlich sind.

c) Der Verantwortliche der digitalen Anwendung MUSS die betroffene Person über die mit dem Versand von Push-Benachrichtigungen einhergehende Datenverarbeitung informieren.

d) Push-Mitteilungen MÜSSEN initial deaktiviert sein. Sie MÜSSEN ausschließlich über eine informierte Einwilligung der betroffenen Person aktiviert werden können, die durch eine durch eine explizite, aktive Handlung bestätigt werden MUSS.

TOM _3.2 Sofern die digitale Anwendung Funktionalitäten zum Teilen von personenbezogenen Daten mit Dritten oder zur unverschlüsselten Ablage von in der Anwendung erzeugten Dateien im Dateisystem der Plattform vorsieht, MUSS die betroffene Person vor Nutzung dieser Funktionen über die damit verbundenen Risiken informiert werden und MUSS durch eine explizite, aktive Handlung die Ausführung der Funktionalität autorisieren. Ausgenommen hiervon ist die Übermittlung von personenbezogenen Daten an Leistungserbringer oder an Anwendungen der Telematikinfrastruktur, die auf Basis einer vorab erteilten Berechtigung erfolgen.

TOM_3.3 Sofern die digitale Anwendung die Kamera, das Mikrofon und/oder Ortungsdienste des genutzten Endgeräts zur Erhebung von Gesundheitsdaten verwendet, MUSS sichergestellt sein, dass diese Daten nicht in Speicherbereichen abgelegt werden, die auch für andere Anwendungen zugänglich sind.

a) Die digitale Anwendung DARF Kamera, Mikrofon und/oder Ortungsdienste NICHT nutzen, sofern dies nicht zu Zwecken des bestimmungsgemäßen Gebrauchs erforderlich ist.

b) Die Nutzung von Kamera, Mikrofon und Ortungsdiensten MUSS initial deaktiviert sein. Sie MUSS ausschließlich über eine informierte Einwilligung der betroffenen Person aktiviert werden können, die durch eine durch eine explizite, aktive Handlung bestätigt werden MUSS.

TOM_3.4 Die betroffene Person SOLL sich nach der Authentifizierung ausschließlich innerhalb der Vertrauensdomäne der digitalen Anwendung bewegen. Sofern eine Weiterleitung auf durch Dritte verantwortete Inhalte zu rechtmäßigen Zwecken der digitalen Anwendung erforderlich ist, MUSS der Hersteller die Vertrauenswürdigkeit der aufgerufenen Angebote absichern.

a) Der Verantwortliche der digitalen Anwendung MUSS einen Prozess etabliert haben, mit dem aus der digitalen Anwendung heraus aufgerufene Angebote

Dritter regelmäßig in Bezug auf Korrektheit, Aktualität und Vertrauenswürdigkeit geprüft werden.

b) Es MUSS für die betroffene Person erkennbar sein, wenn sie sich außerhalb der Vertrauensdomäne der digitalen Anwendung bewegt.

c) Vor der Weiterleitung zu einem von einem Dritten verantworteten Angebot MUSS die betroffene Person informiert werden, dass dieses Angebot außerhalb der Vertrauensdomäne der digitalen Anwendung angesiedelt ist.

TOM_4 Betrieb und Nutzung

TOM_4.1 Der Verantwortliche der digitalen Anwendung MUSS für die Bereitstellung einer auf mobile Plattformen abzielende Version der Anwendung alternative Vertriebswege zu den App-Stores der Plattformanbieter prüfen. Er MUSS diese Prüfung regelmäßig wiederholen. Er KANN diese Prüfung als Teil der Datenschutz-Folgenabschätzung durchführen.

a) Sofern alternative Vertriebswege verfügbar sind, SOLL die digitale Anwendung auch über diese bereitgestellt werden.

TOM_4.2 entfallen

TOM_4.3 Alle Hintergrundsysteme der digitalen Anwendung MÜSSEN aus Umgebungen heraus betrieben werden, die einen wirksamen Schutz gegen physische Zugriffe Unbefugter auf Datenverarbeitungsanlagen sicherstellen. Der Verantwortliche der digitalen Anwendung MUSS die Wirksamkeit der Maßnahmen zum Zugangs- und Zugriffsschutz regelmäßig überprüfen und beständig an den Stand der Technik anpassten. Im Fall eines Betriebs der Hintergrundsysteme über eine Auftragsverarbeitung MUSS der Auftragsverarbeiter dem Verantwortlichen gegenüber entsprechende Zusagen machen und eine Prüfung der Einhaltung dieser Zusagen ermöglichen.

TOM_4.4 Sofern die digitale Anwendung über mobile Endgeräte genutzt werden kann, MUSS der Verantwortliche der Anwendung Maßnahmen des Zugriffsschutzes auf über das Gerät zugängliche oder zugreifbare personenbezogene Daten umsetzen, die auch wirken, wenn das Endgerät verloren geht oder gestohlen wurde. Insbesondere DARF allein der Besitz des Geräts NICHT dazu führen, dass Unbefugte Zugang zu personenbezogenen Daten der betroffenen Person erlangen können.

TOM_5 Privacy by Default

TOM_5.1 Sofern von der betroffenen Person beeinflussbare Systemeinstellungen der digitalen Anwendung Einfluss auf die Umsetzung der Grundprinzipien des Datenschutzes, den Umfang der verarbeiteten personenbezogenen Daten oder die Wahrnehmung von Betroffenenrechten haben, MUSS in der digitalen Anwendung die datenschutzfreundlichste Systemeinstellung voreingestellt sein.

a) Die betroffene Person MUSS in der digitalen Anwendung einen Hinweis erhalten, sofern eine Änderung einer Systemeinstellung zu neuen oder erhöhten Risiken für die Rechte und Freiheit der betroffenen Person führt.

b) Der betroffenen Person MUSS in der digitalen Anwendung die Möglichkeit gegeben werden, einfach und intuitiv die datenschutzfreundlichste Systemeinstellung wiederherzustellen.

c) Der Verantwortliche der digitalen Anwendung DARF KEINE *deceptive design pattern* ("Dark Pattern") verwenden, die der betroffenen Person suggerieren, dass eine andere als die datenschutzfreundlichste Konfigurationseinstellung der Default oder die bevorzugte Standardeinstellung wäre.

TOM_5.2 Die digitale Anwendung MUSS durchgängig das Prinzip von "Fail-Safe Defaults" verfolgen, d. h. jeder nicht explizit autorisierte Zugriffsversuch MUSS abgewiesen werden.

TOM_6 Umgang mit Ausnahmesituationen

TOM_6.1 Der Verantwortliche der digitalen Anwendung MUSS ein Konzept zum Anlegen und Wiedereinspielen von Backups erstellt haben und MUSS dieses vor der Inbetriebnahme der digitalen Anwendung getestet haben.

a) Das Backup-Konzept MUSS das Szenario "Ransomware-Befall" berücksichtigen und geeignete Maßnahmen und Schutzvorgaben für das Backup-Medium und das Einspielen von Backups beinhalten.

TOM_6.2 Im Fall des Verlusts oder Diebstahls des genutzten Endgeräts, der vermuteten Offenbarung von Zugangsdaten oder beim Verdacht unbefugter Zugriffe auf Anwendungsdaten MUSS die betroffene Person die Möglichkeit haben, beim Verantwortlichen der digitalen Anwendung die Sperrung aller von der Anwendung verwalteten personenbezogenen Daten gegenüber externen Zugriffen zu verfügen.

a) Der Verantwortliche der digitalen Anwendung MUSS einen Prozess zur Sperrung aller an einen Benutzeraccount gebundenen Daten für externe Zugriffe etabliert haben.

b) Der Verantwortliche MUSS in der digitalen Anwendung bzw. den damit verbundenen Prozessen der Benutzerverwaltung Maßnahmen verankert haben, die ein sicheres Zurücksetzen von Zugangsdaten bzw. die Ausgabe neuer Zugangsdaten an die betroffene Person ermöglichen. Die Person MUSS dabei als rechtmäßiger Besitzer des Accounts authentisiert werden können.

13.4 Allgemeine Erläuterungen

In diesem Kriterium wird nur dann zwischen Verantwortlichem und Auftragsverarbeiter unterschieden, wenn die Umsetzung einer Maßnahme klar einer dieser Akteursrollen zugeordnet werden soll. Ansonsten zielen die gewählten Formulierungen auf Leistungsmerkmale der digitalen Anwendung ab, deren Vorhandensein im Rahmen der Zertifizierung zu prüfen ist – unabhängig davon, ob die Umsetzung der Anforderung durch den Verantwortlichen selbst oder einen Auftragsverarbeiter erfolgte.

13.5 Spezifische Erläuterungen

Zu Anforderung TOM_1.1 a: Digitale Anwendungen spannen ein sehr heterogenes Spektrum von Themen und Zielgruppen auf. Der Verantwortliche der Anwendung muss darlegen können, dass er sich mit der Frage auseinandergesetzt hat, welche Maßnahmen am besten zu seiner konkreten Anwendung passen, sich in die Nutzungsabläufe einpassen und für die Zielgruppe handhabbar sind.

Zu Anforderung TOM_1.1 b: Redundante Dokumentation soll vermieden werden. Dem Verantwortlichen wird daher freigestellt, ob er eine bestimmte technische bzw. organisatorische Maßnahme im Datenschutzkonzept, im Sicherheitskonzept oder im Betriebskonzept beschreibt.

Zu Anforderung TOM_1.3 c/d: Der Verantwortliche muss eine nicht mehr dem Stand der Technik entsprechende technische Komponente nicht zwingend ersetzen, z. B. weil die damit verbundenen Risiken gering sind oder weil keine praktikable Alternative zur Verfügung steht. Beispielsweise ist der Übergang zwischen verschiedenen Versionen von Netzwerkprotokollen zuweilen ein langwieriger Prozess, bei dem die alte Version erst abgelöst werden kann, wenn sichergestellt ist, dass eine ausreichend große Zahl von mobilen Endsystemen diese auch unterstützt. Gemäß Buchstabe b soll hier die Option einer parallelen Unterstützung verschiedener Versionen geprüft werden; beispielsweise Unterstützung von TLS 1.2 und TLS 1.3, so dass angebundene Systeme, die die aktuellere Protokollversion unterstützen, auch über diese kommunizieren können.

Zu Anforderung TOM_2.1: Der Hersteller und der Verantwortliche erhalten im Rahmen der Verordnung bzw. Bewilligung einer DiGA bzw. DiPA einen Freischaltcode, der als Nachweis der Kostenübernahme dient. Unmittelbar nach der Eingabe des Freischaltcodes in der DiGA/DiPA und der damit verbundenen Aktivierung der Anwendung kann der Hersteller die Abrechnung mit dem Kostenträger durchführen. Es besteht daher aus den regulatorischen Begleitprozessen heraus keine Anforderung der Identifizierung der betroffenen Person durch den Hersteller oder Verantwortlichen der digitalen Anwendung. Die so gegebene Möglichkeit einer pseudonymen Nutzung soll soweit als möglich über den gesamten Lebenszyklus der DiGA/DiPA-Nutzung durchgezogen werden. Die beschriebenen Anforderungen stellen dieses sicher. Weitere Implikationen aus der pseudonymen Nutzung werden vor allem im Kriterium "Datenminimierung" (z. B. Anforderung DMN_1.1) beschrieben.

Zu Anforderung TOM_2.1 a: Beispiele für zulässige Ausnahmen können DiGA sein, die Datenzugänge für Ärzte zur Betreuung ihrer Patienten vorsehen oder DiPA, die aus der App heraus Hilfsmittelbeantragungen oder -bestellungen auslösen.

Zu Anforderung TOM_2.1 c: Die benannte Ausnahme zielt insbesondere auf § 351 Absatz 2 SGB V ab, der DiGA-Hersteller verpflichtet, der betroffenen Person die Möglichkeit des Einspielens von DiGA-Daten in eine ePA zu ermöglichen. Dieses wird zum im Gesetz genannten Zeitpunkt potenziell nur nach vorheriger Identifizierung möglich sein, da die aktuelle Spezifikation der ePA-Schnittstelle die Übermittlung der KVNR der betroffenen Person erfordert.

Zu Anforderung TOM_2.2 f: Maßgeblich für den Stand der Technik ist hier BSI TR-02102.

Zu Anforderung TOM_2.3 c: Die Anwendung muss Szenarien für *brute force* Angriffe erkennen und unterbinden, in denen Passwörter ausprobiert oder Aufrufe gegen fremde Nutzer-Accounts durchgeführt werden.

Zu Anforderung TOM_3.1 b: Ausnahmen bestehen zur Information der betroffenen Person über unverzüglich einzuleitende Maßnahmen gegen neu erkannte Risiken oder zur Information der betroffenen Person über weitreichende Änderungen in der Bereitstellung der digitalen Anwendung. Beispiele hierfür sind z. B. die Aufforderung zum Wechsel des Passworts bei Verdacht einer Kompromittierung der Passwort-Datenbank oder die Ankündigung der Einstellung des Supports für die digitale Anwendung oder Teile derselben. Informationen zu "normalen" Updates fallen regelmäßig nicht unter die zulässigen Ausnahmen.

Zu Anforderung TOM_3.1 d: Die geforderte Einwilligung kann für DiGA Bestandteil der Einwilligung zu dem Zweck nach § 4 Absatz 2 Satz 1 Nummer 1 DiGAV und für DiPA Bestandteil der Einwilligung zu dem Zweck nach § 5 Absatz 3 Satz 1 Nummer 1 DiPAV sein. Der Hersteller der digitalen Anwendung darf – sofern zutreffend – beim initialen Einrichtungsprozess darüber informieren, dass ohne Push-Benachrichtigungen die Wirksamkeit der digitalen Anwendung möglicherweise eingeschränkt ist.

Zu Anforderung TOM_3.3 b: Die geforderte Einwilligung kann für DiGA Bestandteil der Einwilligung zu dem Zweck nach § 4 Absatz 2 Satz 1 Nummer 1 DiGAV und für DiPA Bestandteil der Einwilligung zu dem Zweck nach § 5 Absatz 3 Satz 1 Nummer 1 DiPAV sein.

Zu Anforderung TOM_4.1: Aktuell ist kein alterativer App-Store bekannt, der die Anforderungen aus dem für DiGA und DiPA ebenfalls beizubringenden Zertifikat des BSI zur Informationssicherheit erfüllen würde. Da jedoch nicht ausgeschlossen ist, dass sich dieses in Zukunft ändert, darf die Prüfung auf alternative Vertriebswege nicht nur ein pauschaler Hinweis auf das Fehlen von solchen Angeboten sein, sondern muss auch eine Recherche nach möglicherweise neu in den Markt eingetretenen Vertriebsplattformen umfassen.

Zu Anforderung TOM_6.1: Beispiele für geeignete Schutzmaßnahmen sind im Arbeitspapier "Maßnahmenkatalog Ransomware" des BSI beschrieben [BSI RW]. Das Kapitel 2 dieses Papiers behandelt explizit den Schutz von Backups.

Teil 4: Anlagen

14 Referenzen

[AnfDsZert] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz): *Anforderungen an datenschutzrechtliche Zertifizierungsprogramme*. Version 1.8 vom 16.04.2021. Online abgerufen unter https://datenschutzkonferenz-online.de/media/ah/DSK_Anwendungshinweis_Zertifizierungskriterien.pdf (letzter Abruf: 20-09-2021)

[BDSG] *Bundesdatenschutzgesetz* in der Fassung vom25. Mai 2018. Online abgerufen unter https://www.gesetze-im-internet.de/bdsg_2018/ (letzter Abruf: 20.09.2021)

[BSI 200-2] Bundesamt für Sicherheit in der Informationstechnik: *BSI-Standards 200-2: IT-Grundschutz-Methodik*. Version 1.0. Online abgerufen unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2 (letzter Abruf: 23.09.2021)

[BSI IT-GS] Bundesamt für Sicherheit in der Informationstechnik: *IT-Grundschutz-Bausteine*. Edition 2021. Online abgerufen unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html (letzter Abruf: 23.09.2021)

[BSI RW] Bundesamt für Sicherheit in der Informationstechnik: Maßnahmenkatalog Ransomware. Version 1.0 vom 23.02.2022. Online abgerufen unter https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/Ransomware/Ransomware_Massnahmenkatalog.html (letzter Abruf: 06.03.2023)

[DiGAV] *Digitale Gesundheitsanwendungen-Verordnung* vom 8. April 2020 (BGBl. I S. 768), die durch Artikel 1 der Verordnung vom 22. September 2021 (BGBl. I S. 4355) geändert worden ist. Online abgerufen unter https://www.gesetze-im-internet.de/digav/BJNR076800020.html (letzter Abruf: 20.11.2021)

[DIN 66398] Deutsches Institut für Normung (DIN): DIN 66398 - Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten. Ausgabe 2016-05.

[DSGVO] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Online abgerufen unter https://www.bmjv.de/DE/Themen/FokusThemen/DS-GVO/_documents/Amtsblatt_EU_DS-GVO.pdf;jsessionid=0AE318603B85C445B3C3380DEFB8F350.1_cid297?__blob=publicationFile&v=1 (letzter Abruf: 20.09.2021)

[DSK-5] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder: Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DSGVO. Dezember 2018. Online abgerufen unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf (letzter Abruf: 30.11.2021)

[DSK-13] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz): *Kurzpapier Nr.13: Auftragsverarbeitung, Art. 28 DSGVO*. Dezember 2018. Online abgerufen unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf (letzter Abruf: 06.21.2021)

[DSK-18] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder: Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen. April 2018. Online abgerufen unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf (letzter Abruf: 29.11.2021)

[DSK-19] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz): Kurzpapier Nr. 19: Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung. Mai 2018. Online abgerufen unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf (letzter Abruf: 03.12.2021)

[DSK-20] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz): *Kurzpapier Nr. 20 der Datenschutzkonferenz (Einwilligung nach der DSGVO).* Online abgerufen unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf (letzter Abruf: 20.09.2021)

[DSK VV1] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder: Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DSGVO. Februar 2018. Online abgerufen unter https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf (letzter Abruf: 27.11.2021)

[edpb0520] Europäischer Datenschutzausschuss: *Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679. Version 1.1vom 04.05.2020* Online abgerufen unter https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf (letzter Abruf: 20.09.2021)

[RFC 2219] S. Bradner: *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119. März 1997. Online abgerufen unter https://www.ietf.org/rfc/rfc2119.txt (letzter Abruf: 21.11.2021)

[SDM] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz): Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Version 2.0b vom 17.04.2020. Online abgerufen unter https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V20b.pdf (letzter Abruf: 20.09.2021)

[SDM-43] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz): Baustein 43 „Protokollierung“ zum SDM

2.0. Version 1.0a vom 20.09.2020. Online abgerufen unter https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Protokollieren_V1.0a.pdf (letzter Abruf: 21.09.2021)

[SDM-50] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz): Baustein 50 „Trennen“ zum SDM 2.0. Version 1.0 vom 06.10.2020. Online abgerufen unter https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Trennen_V1.0.pdf (letzter Abruf: 20.09.2021)

[SDM-60] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz): Baustein 60 „Löschen und Vernichten“ zum SDM 2.0. Version 1.0a vom 02.09.2020. Online abgerufen unter https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_L%C3%B6schen_und_Vernichten_V1.0a.pdf (letzter Abruf: 18.10.2021)

[SDM-61] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz): Baustein 61 „Berichtigen“ zum SDM 2.0. Version 1.0 vom 06.10.2020. Online abgerufen unter https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Berichtigen_V1.0.pdf (letzter Abruf: 18.10.2021)

[SDM-62] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz): Baustein 62 „Einschränken der Verarbeitung“ zum SDM 2.0. Version 1.0 vom 06.10.2020. Online abgerufen unter https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Einschr%C3%A4nken_V1.0.pdf (letzter Abruf: 18.10.2021)

[TR-02102-1] Bundesamt für Sicherheit in der Informationstechnik: *BSI TR-02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen*. Version 2021-01 vom 24.03.2021. Online abgerufen unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile (letzter Aufruf: 21.11.2021)

[DiPAV] Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Pflegeanwendungen in der Sozialen Pflegeversicherung (DiPAV). Referentenentwurf vom 01.06.2022. Online abgerufen unter https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/V/vdipa_refe_bf.pdf (letzter Abruf: 16.06.2022)

[WP243] Artikel-29-Datenschutzgruppe: *Working Paper 243 - Leitlinien in Bezug auf Datenschutzbeauftragte.* Dezember 2016. Online abgerufen unter https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2017/07/WP243de_Art._29-Gruppe-Datenschutzbeauftragte.pdf (letzter Abruf: 03.12.2021)

[WP250] Artikel-29-Datenschutzgruppe: *Working Paper 250rev01 - Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten*. Februar 2018. Online abgerufen unter https://lfd.niedersachsen.de/download/137952 (letzter Abruf: 03.12.2021)

www.bfarm.de/diga