Fünftes Buch Sozialgesetzbuch (SGB V) – Gesetzliche Krankenversicherung –
vom 20. Dezember 1988
(BGBl. I. I S. 2477)

Anlage 3 (zu § 307 Absatz 1 Satz 3 SGB V) - Datenschutz-Folgenabschätzung

zuletzt (inhaltlich) geändert durch die Artikel 1 des Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG)
vom 22. März 2024
(BGBl. I Nr. 101 vom 25. März 2024)

Inhaltsverzeichnis

1 Zusammenfassung

[1]Diese Anlage enthält die Datenschutz-Folgenabschätzung nach Artikel 35 Absatz 10 der Verordnung (EU) 2016/679 (DSGVO) gemäß § 307 Absatz 1 Satz 3 des Fünften Buches Sozialgesetzbuch (SGB V).

[2]Die Datenschutz-Folgenabschätzung dieser Anlage betrachtet ausschließlich die von der Gesellschaft für Telematik zugelassenen Komponenten der dezentralen Telematikinfrastruktur (TI) nach § 306 Absatz 2 Nummer 1 SGB V. [3]Da diese dezentralen Komponenten jedoch nur einen Teilbereich der gesamten IT-Unterstützung beim Leistungserbringer darstellen und der Leistungserbringer regelmäßig weitere Betriebsmittel nutzen wird, hat der Leistungserbringer zu prüfen, ob nach Artikel 35 DSGVO für diese weiteren Betriebsmittel eine ergänzende Datenschutz-Folgenabschätzung durchzuführen ist.

Ergebnis der Datenschutz-Folgenabschätzung (§ 307 Absatz 1 Satz 3 SGB V):

[1]Die korrekte Nutzung einer von der Gesellschaft für Telematik gemäß § 325 SGB V zugelassenen Komponente der dezentralen Infrastruktur der TI nach § 306 Absatz 2 Nummer 1 SGB V ist geeignet, ein Schutzniveau zu gewährleisten, das dem hohen Risiko entspricht, welches aus der Datenverarbeitung für die Rechte und Freiheiten der Betroffenen folgt, sofern die Komponenten vom Leistungserbringer gemäß Betriebshandbuch betrieben werden und der Leistungserbringer für seine Ablauforganisation sowie die weiteren genutzten dezentralen Betriebsmittel (z. B. IT-gestützter Arbeitsplatz, aktive Netzwerkkomponenten) die Vorschriften zum Schutz personenbezogener Daten einhält.

[2]Die technischen Maßnahmen der Komponenten der dezentralen Infrastruktur der TI zur Gewährleistung der Datensicherheit werden gemäß § 311 Absatz 2 SGB V im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) festgelegt und

---

wirken den Risiken für die Rechte und Freiheiten der Betroffenen angemessen entgegen. [3]Die korrekte Implementierung dieser Maßnahmen in den Komponenten der dezentralen Infrastruktur der Hersteller wird der Gesellschaft für Telematik im Rahmen des Zulassungsprozesses gemäß § 325 SGB V nachgewiesen.

[4]Die in dieser Anlage betrachteten Verarbeitungsvorgänge der dezentralen Komponenten der TI entsprechen den konkreten Verarbeitungsvorgängen in den Komponenten der dezentralen TI eines Leistungserbringers. [5]Die Komponenten der dezentralen TI stellen technisch sicher, dass Leistungserbringer mit diesen Komponenten ausschließlich die in dieser Anlage betrachteten Verarbeitungsvorgänge durchführen können. [6]Es ist mit diesen Komponenten nicht möglich, darüber hinausgehende oder abweichende Verarbeitungsvorgänge durchzuführen. [7]Zur Verhinderung einer negativen Beeinflussung der Verarbeitungen in den Komponenten besitzen die Komponenten geprüfte Schutzmaßnahmen. [8]Die konkrete Einsatzumgebung der Komponenten der dezentralen TI ist spezifisch für den jeweiligen Leistungserbringer; für diese hat der Leistungserbringer daher erforderlichenfalls eine eigene ergänzende Datenschutz-Folgenabschätzung durchzuführen.

Fünftes Buch Sozialgesetzbuch (SGB V) – Gesetzliche Krankenversicherung –
vom 20. Dezember 1988
(BGBl. I. I S. 2477)

Anlage 3 (zu § 307 Absatz 1 Satz 3 SGB V) - Datenschutz-Folgenabschätzung

zuletzt (inhaltlich) geändert durch die Artikel 1 des Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG)
vom 22. März 2024
(BGBl. I Nr. 101 vom 25. März 2024)

---

2 Datenschutz - Folgenabschätzung (§ 307 Absatz 1 Satz 3 SGB V)

Die Datenschutz-Folgenabschätzung für die Komponenten der dezentralen Infrastruktur der TI gemäß § 306 Absatz 2 Nummer 1 SGB V basiert auf den Kriterien der „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679, wahrscheinlich ein hohes Risiko mit sich bringt' (Artikel 29 WP 248 Rev. 1)" der Datenschutzgruppe nach Artikel 29 (nun Europäischer Datenschutzausschuss; der Europäische Datenschutzausschuss hat die mit der Datenschutz-Grundverordnung zusammenhängenden Leitlinien der Artikel-29-Datenschutzgruppe – darunter die soeben genannte – bei seiner ersten Plenarsitzung bestätigt, so dass diese fortgelten).

2.1 Systematische Beschreibung der Verarbeitungsvorgänge (Artikel 35 Absatz 7 Buchstabe a DSGVO)

[1]Mittels der Komponenten der dezentralen TI nutzen Leistungserbringer Anwendungen der TI, Dienste der zentralen TI oder der Anwendungsinfrastruktur der TI sowie über die TI erreichbare Anwendungen bzw. Dienste. [2]Die Komponenten bieten den Leistungserbringern zudem Funktionen zur Ver- bzw. Entschlüsselung und Signatur von Daten.

[3]Die Gesellschaft für Telematik und die Krankenkassen stellen Informationsmaterial öffentlich zur Verfügung, in dem die Funktionsweise der Anwendungen der TI erklärt wird. [4]Zudem veröffentlicht die Gesellschaft für Telematik auf ihrer Internetseite die Spezifikationen, auf deren Basis die Komponenten und Dienste der TI entwickelt und zugelassen werden müssen.

2.1.1 Kategorien von Verarbeitungsvorgängen

Die Verarbeitungsvorgänge in der dezentralen Infrastruktur lassen sich in drei Kategorien unterteilen:

Kategorie 1: (ausschließlich) Transport von Daten ohne weitere Verarbeitung

Kategorie 2: Weitere Verarbeitung (betrifft ausschließlich Verschlüsselung, Signatur, Authentifizierung)

Kategorie 3: Verarbeitungen, die über jene in den Kategorien 1 und 2 hinausgehen.

<u>Kategorie 1: (ausschließlich) Transport von Daten ohne weitere Verarbeitung</u>

[1]Diese Kategorie umfasst alle Verarbeitungsvorgänge, in denen einer Komponente der dezentralen Infrastruktur personenbezogene Daten übergeben werden (z. B. vom Primärsystem) und in denen die Komponente der dezentralen Infrastruktur die übergebenen Daten unverändert an die vorgesehene Empfängerkomponente weiterleitet.

[2]Empfängerkomponenten können Teil der zentralen TI, der Anwendungsinfrastruktur der TI oder eines an die TI angeschlossenen Netzes sein. [3]Empfängerkomponenten können selbst Teil der dezentralen Infrastruktur sein (z. B. Kartenterminals).

---

[4]Die Komponente der dezentralen Infrastruktur übernimmt für diese Verarbeitungsvorgänge lediglich eine Weiterleitungsfunktion. [5]Eine weitere Verarbeitung der transportierten Daten erfolgt nicht.

[6]Zu dieser Kategorie gehören insbesondere Verarbeitungsvorgänge

- der weiteren Anwendungen nach § 327 SGB V,
- der sicheren Übermittlungsverfahren nach § 311 Absatz 1 Nummer 5 SGB V sowie
- der Anwendungen nach § 334 Absatz 1 Satz 2 Nummer 2, 6 und 7 SGB V.

Kategorie 2: Weitere Verarbeitung (Verschlüsselung, Signatur, Authentifizierung)

[1]Zu dieser Kategorie gehören die Ver- und Entschlüsselungen sowie die Signaturoperationen, die mittels der Verschlüsselungs- und Signaturfunktionen der dezentralen Infrastruktur durchgeführt werden. [2]Hier werden die zu verschlüsselnden bzw. zu entschlüsselnden Daten sowie die zu signierenden Daten übergeben. [3]Es erfolgt keine über die Ver- bzw. Entschlüsselung bzw. Signatur hinausgehende Verarbeitung in den Komponenten der dezentralen Infrastruktur.

[4]Die Funktionen zur Ver- und Entschlüsselung sowie der Signatur können durch Anwendungen der Kategorie 1 und 3 genutzt werden.

Kategorie 3: Verarbeitungen, die über jene in den Kategorien 1 und 2 hinausgehen

[1]In diesen Verarbeitungsvorgängen werden die einer Komponente der dezentralen Infrastruktur übergebenen Daten in der dezentralen Infrastruktur anwendungsspezifisch verarbeitet, d. h. die Verarbeitung ist im Gegensatz zu den bisherigen Kategorien nicht auf den Transport, die Ver- und Entschlüsselung oder die Signatur beschränkt.

[2]Zu dieser Kategorie gehören die Verarbeitungsvorgänge

- des Versichertenstammdatenmanagements nach § 291b SGB V sowie
- der Anwendungen nach § 334 Absatz 1 Satz 2 Nummer 1 und 3 bis 5 SGB V.

2.1.2 Systematische Beschreibung

Die systematische Beschreibung hat nach Erwägungsgrund (ErwG) 90 sowie Artikel 35 Absatz 7 Buchstabe a und Absatz 8 DSGVO sowie nach den „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 ‚wahrscheinlich ein hohes Risiko mit sich bringt'" der Artikel-29-Datenschutzgruppe (WP 248) zu enthalten:

Kriterium	**Beschreibung**
Art der Verarbeitung: **(ErwG 90 DSGVO)**	siehe Abschnitt 2.1.1
Umfang der Verarbeitung: **(ErwG 90 DSGVO)**	[1]Die Komponenten der dezentralen Infrastruktur der TI verarbeiten insbesondere besondere Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 DSGVO, nämlich Gesundheitsdaten natürlicher Personen (Versicherter) i.S.v. Artikel 4 Nummer 15 DSGVO. [2]Dies sind beispielsweise elektronische Arztbriefe, medizinische Befunde und Diagnosen, der elektronische Medikationsplan nach § 31a SGB V, die elektronischen Notfalldaten, elektronische Impfdokumentation oder elektronische Verordnungen. [3]Es werden zudem insbesondere Daten gemäß § 291a Absatz 2 und 3 SGB V (Versichertenstammdaten) verarbeitet. [4]Zum ordnungsgemäßen Betrieb der Komponenten der dezentralen Infrastruktur der TI erfolgt eine Protokollierung innerhalb der Komponenten. [5]Diese Protokolle enthalten keine personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSGVO. [6]Sie können personenbezogene Daten des Leistungserbringers enthalten, bei denen es sich regelmäßig nicht um besondere Kategorien personenbezogener Daten handelt. [7]In den Komponenten werden die Benutzernamen der berechtigten Administratoren hinterlegt. [8]Die Benutzernamen werden vom Leistungserbringer oder vom beauftragten Dienstleister frei gewählt. [9]Die Benutzernamen der Administratoren können auch Pseudonyme sein, sofern die Administratoren eindeutig unterschieden werden können.

Kriterium	Beschreibung
	[10]Personenbezogene Daten von Versicherten können in Protokollen nur im Falle eines Fehlers zum Zwecke der Behebung des Fehlers temporär gespeichert werden. [11]Zum Zwecke der netztechnischen Adressierung besitzen Komponenten der dezentralen Infrastruktur IP-Adressen. [12]Von der Verarbeitung betroffene Personen sind: – Versicherte, – Leistungserbringer sowie – ggf. Administratoren der Komponenten.
Umstände bzw. Kontext der Verarbeitung: **(Artikel-29-Datenschutzgruppe, WP 248, 21)**	Kategorie 1: Die Verarbeitung erfolgt im Kontext einer Anwendung bzw. der Nutzung eines Dienstes durch den Leistungserbringer, die bzw. der über die dezentrale Infrastruktur der TI technisch erreichbar ist (z. B. Nutzung einer weiteren Anwendung nach § 327 SGB V). Kategorie 2: Die Verarbeitung erfolgt im Rahmen einer vom Leistungserbringer gewünschten Ver- bzw. Entschlüsselung oder Signatur von Daten, die der Leistungserbringer auswählt. Kategorie 3: Die Verarbeitung der personenbezogenen Daten in den dezentralen Komponenten der TI erfolgt im Rahmen der Versorgung von Versicherten gemäß den im SGB V festgelegten Zwecken.
Zweck der Verarbeitung: **(Artikel 35 Absatz 7 Buchstabe a DSGVO)**	Kategorie 1: Der Zweck beschränkt sich auf die Weiterleitung der Daten an den korrekten Empfänger. Es erfolgt keine darüber hinausgehende Verarbeitung der Daten in den Komponenten der dezentralen Infrastruktur der TI. Kategorie 2: Zweck ist die Ver- bzw. Entschlüsselung bzw. Signatur der übergebenen Daten. Kategorie 3:

Kriterium	Beschreibung
	Die Zwecke der Verarbeitungen sind gesetzlich im SGB V festgelegt. – Den Zweck des Versichertenstammdaten-managements legt § 291b Absatz 1 und 2 SGB V fest. – Die Anwendungen nach § 334 Absatz 1 Satz 2 SGB V dienen gemäß § 334 Absatz 1 Satz 1 SGB V der Verbesserung der Wirtschaftlichkeit, der Qualität und der Transparenz der Versorgung. Der Zweck der einzelnen Anwendungen ist in § 334 Absatz 1 Satz 2 SGB V festgelegt und wird für einzelne Anwendungen in weiteren Paragraphen des SGB V konkretisiert (z. B. für die elektronische Patientenakte in § 341 SGB V).
Empfängerinnen und Empfänger: **(Artikel-29-Datenschutzgruppe, WP 248, 21)**	Kategorie 1: Die der dezentralen Komponente übergebenen Daten werden an die gewählte Empfängerkomponente weitergeleitet. Die Empfänger der Daten in den Empfängerkomponenten sind abhängig von der Anwendung bzw. dem Dienst, zu der bzw. zu dem die Empfängerkomponente gehört. Kategorie 2: Empfänger der ver- bzw. entschlüsselten bzw. signierten Daten ist der Leistungserbringer, der die Daten der Komponenten zur Ver- bzw. Entschlüsselung bzw. Signatur übergeben hat. Kategorie 3: Die in der dezentralen Komponente verarbeiteten Daten einer Anwendung können an die berechtigten Empfänger dieser Anwendung weitergeleitet werden. Die für die Anwendungen dieser Kategorie berechtigten Empfänger sind im SGB V gesetzlich festgelegt; ihnen wird durch Gesetz eine Berechtigung zum Zugriff auf die Daten der Anwendungen erteilt.
Speicherdauer: **(Artikel-29-Datenschutzgruppe, WP 248, 21)**	[1]In den Komponenten der dezentralen Infrastruktur der TI werden keine personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSGVO persistent gespeichert. [2]Sie werden nur temporär für den erforderlichen Zweck verarbeitet und danach sofort gelöscht. [3]Eine persistente Speicherung von personenbezogenen Daten kann in den Protokollen der Komponenten erfolgen. [4]Die Protokolle mit Personenbezug werden dabei nach

Kriterium	Beschreibung
	einem festgelegten Turnus durch die Komponente automatisch gelöscht bzw. können aktiv vom Administrator der Komponente gelöscht werden. [5]Die nach außen sichtbaren IP-Adressen der Komponenten werden regelmäßig gewechselt.
Funktionelle Beschreibung der Verarbeitung: **(Artikel 35 Absatz 7 Buchstabe a DSGVO)**	Kategorie 1: Hier erfolgt nur eine Weiterleitung übergebener Daten. Es erfolgt keine weitere Verarbeitung der Daten. Kategorie 2: Es handelt sich ausschließlich um Funktionen zur Ver- und Entschlüsselung sowie Signatur. Kategorie 3: Die Funktionalität dieser Anwendungen ist gesetzlich festgelegt. Die Konkretisierung dieser Funktionen in den Komponenten erfolgt in den Spezifikationen der Gesellschaft für Telematik, die auf deren Internetseite veröffentlicht werden.
Beschreibung der Anlagen (Hard- und Software bzw. sonstige Infrastruktur): **(Artikel-29-Datenschutzgruppe, WP 248, 21)**	[1]Die Komponenten der dezentralen Infrastruktur werden von der Gesellschaft für Telematik spezifiziert. [2]Die Spezifikationen sind von der Gesellschaft für Telematik auf ihrer Internetseite veröffentlicht. [3]Bei der Spezifikation werden die technischen und organisatorischen Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten gemäß Artikel 25 und 32 DSGVO berücksichtigt.
Eingehaltene, gemäß Artikel 40 DSGVO genehmigte Verhaltensregeln: **(Artikel-29-Datenschutzgruppe, WP 248, 21)**	Es wurden keine Verhaltensregeln gemäß Artikel 40 DSGVO berücksichtigt.

2.2 Notwendigkeit und Verhältnismäßigkeit (Artikel 35 Absatz 7 Buchstabe b DSGVO)

Im Rahmen der Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge müssen nach den ErwGen 90 und 96, nach Artikel 35 Absatz 7 Buchstabe b und d DSGVO sowie nach den „Leitlinien zur Datenschutz-Folgenabschätzung

(DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679, wahrscheinlich ein hohes Risiko mit sich bringt'" der Artikel-29-Datenschutzgruppe (WP 248) Maßnahmen zur Einhaltung der Verordnung bestimmt werden, wobei Folgendes berücksichtigt werden muss:

- Maßnahmen im Sinne der Verhältnismäßigkeit und Notwendigkeit der Verarbeitung (Artikel 5 und 6 DSGVO) sowie
- Maßnahmen im Sinne der Rechte der Betroffenen (Artikel 12 bis 21, 28, 36 und Kapitel V DSGVO).

Kriterium	**Beschreibung**
Festgelegter Zweck: **(Artikel 5 Absatz 1 Buchstabe b DSGVO)**	Kategorie 1: Der Zweck ist die Weiterleitung der Daten ohne sonstige Verarbeitung der Daten. Kategorie 2: Der Zweck ist durch die Funktionen Ver- bzw. Entschlüsselung und Signatur festgelegt. Kategorie 3: Die Zwecke der Anwendungen dieser Kategorie sind gesetzlich im SGB V festgelegt.
Eindeutiger Zweck: **(Artikel 5 Absatz 1 Buchstabe b DSGVO)**	[1]Die Zwecke sind eindeutig. [2]Für die Anwendungen nach den §§ 291b, 334 und 311 SGB V sind die Zwecke im SGB V eindeutig festgelegt; eine zweckfremde Verarbeitung unterliegt den Straf- und Bußgeldvorschriften der §§ 397 und 399 SGB V.
Legitimer Zweck: **(Artikel 5 Absatz 1 Buchstabe b DSGVO)**	Kategorie 1: Die Verarbeitung in der dezentralen Infrastruktur der TI erfolgt im Rahmen einer Anwendung, die der Leistungserbringer über die dezentrale Infrastruktur technisch erreicht. Im Rahmen der Nutzung dieser Anwendung (die selbst einem legitimen Zweck unterliegen muss) ist die Weiterleitung der Daten durch die dezentrale Infrastruktur nur ein technisches Hilfsmittel zur Nutzung der vom Leistungserbringer gewählten Anwendung und für die Nutzung der Anwendung erforderlich. Kategorie 2: Der Leistungserbringer verarbeitet die Daten für seine eigenen Zwecke. Er bestimmt den Zeitpunkt der Ver- bzw. Entschlüsselung bzw. Signatur und die Daten, die ver- bzw. entschlüsselt bzw. signiert werden sollen.

Kriterium	Beschreibung
	Kategorie 3: Die Zwecke der Verarbeitung der Daten in den Anwendungen dieser Kategorie sind legitim, da sie der Verbesserung der Wirtschaftlichkeit, der Qualität und der Transparenz der Versorgung im deutschen Gesundheitswesen dienen.
Rechtmäßigkeit der Verarbeitung: **(Artikel-29-Datenschutzgruppe, WP 248, 21 i.V.m. Artikel 6 DSGVO**	Kategorie 1: Die Rechtmäßigkeit basiert auf der Rechtmäßigkeit der Verarbeitung der Daten in der Anwendung, die der Leistungserbringer nutzt und an die die dezentrale Infrastruktur der TI die Daten technisch weiterleitet. Kategorie 2: Der Leistungserbringer verarbeitet die Daten für seine eigenen Zwecke, wobei es sich regelmäßig um Behandlungszwecke handelt, deren gesetzliche Verarbeitungsgrundlagen sich in § 22 Absatz 1 BDSG bzw. – im Falle der Verarbeitung durch Krankenhäuser oder Landeseinrichtungen – in speziellen Rechtsgrundlagen finden. Der Leistungserbringer bestimmt den Zeitpunkt der Ver- bzw. Entschlüsselung bzw. Signatur und die Daten, die ver- bzw. entschlüsselt bzw. signiert werden sollen. Kategorie 3: Die Rechtmäßigkeit ergibt sich aus – Artikel 6 Absatz 1 Buchstabe c DSGVO i.V.m. § 291b SGB V beim Versichertenstammdatenmanagement bzw. – der gesetzlichen Befugnis zur Verarbeitung nach § 339 Absatz 1 für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich als Verarbeitungsgrundlage im Recht eines Mitgliedstaats im Sinne von Artikel 9 Absatz 2 Buchstabe h in Verbindung mit Artikel 9 Absatz 3 DSGVO bei Anwendungen nach § 334 SGB V vorbehaltlich eines Widerspruchs des Versicherten nach § 339 Absatz 1, nach § 353 Absatz 1 und 2 bzw.

Kriterium	Beschreibung
	– – einer Einwilligung des Versicherten nach Artikel 9 Absatz 2 Buchstabe a DSGVO und nach § 339 Absatz 1a, § 353 Absatz 3 bis 6 SGB V bei Anwendungen nach § 334 SGB V.
Angemessenheit und Erheblichkeit der Verarbeitung, Beschränktheit der Verarbeitung auf das notwendige Maß: **(Artikel-29-Datenschutzgruppe, WP 248, 21 i.V.m. Artikel 5 Absatz 1** **Buchstabe c DSGVO)**	Kategorie 1: Die Verarbeitung ist auf die Weiterleitung von Daten an die vom Leistungserbringer gewünschte Empfängerkomponente beschränkt. Eine weitere Verarbeitung der Daten erfolgt nicht. Die Weiterleitung der Daten ist notwendig, damit der Leistungserbringer die zur Empfängerkomponente gehörende Anwendung nutzen kann. Da neben der Weiterleitung keine weitere Verarbeitung der Daten in den Komponenten der dezentralen Infrastruktur erfolgt, ist die Verarbeitung mit Blick auf ihren Zweck minimal. Kategorie 2: Um Daten ver- bzw. entschlüsseln bzw. signieren zu können, müssen diese Daten verarbeitet werden. Eine darüber hinausgehende Verarbeitung der Daten erfolgt nicht, so dass die Datenverarbeitung mit Blick auf ihren Zweck minimal ist. Kategorie 3: Die Verarbeitung setzt die gesetzlichen Vorgaben des SGB V um. Es erfolgen keine Verarbeitungen, die über den gesetzlichen Zweck hinausgehen. – Der Umfang der Versichertenstammdaten ist in § 291a SGB V festgelegt. – Die in den Anwendungen nach § 334 SGB V verarbeiteten medizinischen Daten sind im SGB V abstrakt gesetzlich festgelegt. Die Konkretisierung dieser Daten erfolgt in den Spezifikationen der Gesellschaft für Telematik, die diese auf ihrer Internetseite veröffentlicht. Die Festlegungen in den Spezifikationen werden nach § 311 Absatz 2 SGB V im Benehmen mit dem BSI und dem BfDI getroffen. Die Protokolldaten in den Komponenten der dezentralen Infrastruktur dienen der Analyse von Fehlern und Sicherheitsvorfällen sowie der Analyse der Performanz. Die Protokolle sind für einen sicheren und ordnungsgemäßen Betrieb des Konnektors notwendig. In den Protokollen

Kriterium	Beschreibung
	werden keine personenbezogenen Daten gemäß Artikel 9 Absatz 1 DSGVO gespeichert. Die IP-Adresse des Konnektors ist für die Kommunikation mit der zentralen TI technisch notwendig. Es wird bei jedem Neuaufbau einer Verbindung zur zentralen TI zufällig eine IP-Adresse zugewiesen.
Speicherbegrenzung: **(Artikel-29-Datenschutzgruppe, WP 248, 21 i.V.m. Artikel 5 Absatz 1 Buchstabe e DSGVO)**	siehe Speicherdauer in Abschnitt 2.1.2
Informationspflicht **gegenüber Betroffenem:** **(Artikel-29-Datenschutzgruppe, WP 248, 21 i.V.m. Artikel 12, 13 und 14 DSGVO)**	Kategorie 1: Die Verarbeitung in der dezentralen Infrastruktur der TI erfolgt im Rahmen einer Anwendung, die der Leistungserbringer über die dezentrale Infrastruktur technisch erreicht. Der Verantwortliche für die Anwendung hat die Informationspflichten gemäß DSGVO zu erfüllen. Kategorie 2: Der Leistungserbringer verarbeitet seine eigenen Daten zu eigenen Zwecken. Eine Information von betroffenen Personen ist nicht erforderlich. Kategorie 3: Der Leistungserbringer ist gemäß § 307 Absatz 1 Satz 1 SGB V Verantwortlicher für die Verarbeitung personenbezogener Daten mittels der Komponenten der dezentralen Infrastruktur und hat somit die Informationspflichten gegenüber den Betroffenen zu erfüllen. Begleitend werden Versicherten generelle Informationen zur TI zur Verfügung gestellt. Diesbezügliche gesetzliche Informationspflichten ergeben sich insbesondere aus den folgenden Normen: – § 314 SGB V verpflichtet die Gesellschaft für Telematik, auf ihrer Internetseite Informationen für die Versicherten in präziser, transparenter, verständlicher, leicht zugänglicher und barrierefreier Form zur Verfügung zu stellen.

Kriterium	Beschreibung
	– Die §§ 291, 342, 343 und 358 SGB V verpflichten die Krankenkassen zur Information von Versicherten: Gemäß § 291 Absatz 5 SGB V informiert die Krankenkasse den Versicherten spätestens bei der Versendung der elektronischen Gesundheitskarte an diesen umfassend und in allgemein verständlicher, barrierefreier Form über die Funktionsweise der elektronischen Gesundheitskarte und über die Art der personenbezogenen Daten, die nach § 291a SGB V mittels der elektronischen Gesundheitskarte zu verarbeiten sind. Gemäß § 343 SGB V haben Krankenkassen umfassendes, geeignetes Informationsmaterial über die elektronische Patientenakte in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache und barrierefrei zur Verfügung zu stellen. Zur Unterstützung der Informationspflichten der Krankenkassen nach § 343 SGB V hat der Spitzenverband Bund der Krankenkassen im Benehmen mit dem BfDI geeignetes Informationsmaterial, auch in elektronischer Form, zu erstellen und den Krankenkassen zur verbindlichen Nutzung zur Verfügung zu stellen. Jede Krankenkasse richtet zudem nach § 342a Absatz 1 SGB V eine Ombudsstelle ein, an die sich Versicherte mit ihren Anliegen im Zusammenhang mit der elektronischen Patientenakte wenden können. Die Ombudsstellen nehmen insbesondere Widersprüche von Versicherten nach § 342a Absatz 2 bis 4 entgegen und stellen den Versicherten nach § 342a Absatz 5 auf Antrag die in § 309 Absatz 1 genannten Protokolldaten der elektronischen Patientenakte nach § 342 Absatz 1 Satz 2 zur Verfügung. Mit der Einführung der elektronischen Notfalldaten, der elektronischen Patientenkurzakte und des elektronischen Medikationsplans haben die Krankenkassen den Versicherten auch hierzu nach § 358 Absatz 9 SGB V geeignetes Informationsmaterial in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache barrierefrei zur Verfügung zu stellen. Auch dieses Informationsmaterial ist gemäß § 358 Absatz 10 SGB V im Einvernehmen mit dem BfDI zu erstellen.
Auskunftsrecht der	[1]Diese Anlage i.V.m. den Informationen gemäß den §§ 314 und 343 SGB V gibt den Versicherten Auskunft über die in

Kriterium	Beschreibung
betroffenen Personen: **(Artikel-29-Datenschutzgruppe, WP 248, 21 i.V.m. Artikel 15 DSGVO)**	Artikel 15 DSGVO geforderten Informationen. [2]Die Informationen nach § 314 Satz 1 Nummer 7 und 8 SGB V enthalten insbesondere die Benennung der Verantwortlichen für die Daten im Hinblick auf die verschiedenen Datenverarbeitungsvorgänge und die Pflichten der datenschutzrechtlich Verantwortlichen sowie die Rechte des Versicherten gegenüber den datenschutzrechtlich Verantwortlichen nach der DSGVO. [3]In den Komponenten der dezentralen Infrastruktur werden zudem keine Daten von Versicherten persistent gespeichert.
Recht auf Berichtigung und Löschung: **(Artikel-29-Datenschutzgruppe, WP 248, 21 i.V.m. Artikel 16, 17 und 19)**	In den Komponenten der dezentralen Infrastruktur werden Daten von Versicherten nur temporär verarbeitet und dann sofort gelöscht. Es erfolgt keine persistente Speicherung von Daten der Versicherten.
Recht auf Datenübertragbarkeit: **(Artikel 20 DSGVO)**	Es werden in den Komponenten der dezentralen Infrastruktur keine Daten von Versicherten persistent gespeichert, so dass keine Daten übertragen werden könnten.
Auftragsverarbeiterinnen und Auftragsverarbeiter: **(Artikel 28 DSGVO)**	Der Leistungserbringer ist nach § 307 Absatz 1 Satz 1 SGB V Verantwortlicher für die Verarbeitung personenbezogener Daten mittels der Komponenten der dezentralen Infrastruktur. Falls der Leistungserbringer einen Auftragsverarbeiter mit dem Betrieb der dezentralen Komponenten der TI beauftragt, hat der Leistungserbringer die Einhaltung der Vorgaben gemäß Artikel 28 DSGVO zu gewährleisten.
Schutzmaßnahmen bei der Übermittlung in Drittländer: **(Kapitel V DSGVO)**	Kategorie 1: Die Verarbeitung in der dezentralen Infrastruktur der TI erfolgt im Rahmen einer Anwendung, die der Leistungserbringer über die dezentrale Infrastruktur technisch erreicht. Der Verantwortliche für die Anwendung hat bei der Übermittlung in Drittländer die Schutzmaßnahmen gemäß DSGVO zu berücksichtigen. Kategorie 2:

Kriterium	Beschreibung
	Es erfolgt keine Übermittlung an Drittländer. Kategorie 3: Es erfolgt keine Übermittlung an Drittländer, da die Dienste innerhalb der EU bzw. des EWR betrieben werden müssen.
Vorherige Konsultation: **(Artikel 36 und ErwG 96 DSGVO)**	Gemäß § 311 Absatz 2 SGB V hat die Gesellschaft für Telematik die Festlegungen und Maßnahmen für die TI nach § 311 Absatz 1 Nummer 1 SGB V im Benehmen mit dem BSI und dem BfDI zu treffen. Dies umfasst insbesondere auch die Erstellung der funktionalen und technischen Vorgaben der Komponenten der dezentralen Infrastruktur der TI.

2.3 Risiken für die Rechte und Freiheiten der betroffenen Personen (Artikel 35 Absatz 7 Buchstabe c DSGVO)

Die Risiken für die Rechte und Freiheiten der betroffenen Personen sind nach ihrer Ursache, Art, Besonderheit, Schwere und Eintrittswahrscheinlichkeit zu bewerten (ErwGe 76, 77, 84 und 90 DSGVO). Nach den ErwGen 75 und 85 DSGVO sind unter anderem die potentiellen Risiken dieses Abschnitts genannt.

Risikoquellen sind

- beim Leistungserbringer tätige Personen inklusive des Leistungserbringers als Verantwortlicher, die unbeabsichtigt und unbewusst den zulässigen Rahmen der Verarbeitung überschreiten könnten,
- Angreifer, die bewusst aus der Umgebung des Leistungserbringers in die Verarbeitungsvorgänge der Komponenten der dezentralen TI eingreifen wollen,
- Angreifer, die bewusst von außerhalb der Leistungserbringerumgebung in die Verarbeitungsvorgänge der Komponenten der dezentralen TI eingreifen wollen,
- Hersteller der Komponenten der dezentralen TI sowie
- technische Fehlfunktionen der Komponenten der dezentralen TI.

Da in den Komponenten der dezentralen TI besondere Kategorien personenbezogener Daten verarbeitet werden, besteht ein hohes Ausgangsrisiko für die Rechte und Freiheiten natürlicher Personen. Das hohe Ausgangsrisiko wird durch die Abhilfemaßnahmen in Abschnitt 2.4 auf ein angemessenes Risiko gesenkt, falls die dezentralen Komponenten vom Leistungserbringer gemäß Betriebshandbuch betrieben werden. Durch die Anwendung der in § 75b SGB V geforderten Richtlinie zur IT-Sicherheit, die IT-Sicherheitsanforderungen an Krankenhäuser nach § 391 SGB V und die Anforderungen an die Wartung von Diensten gemäß § 332 SGB V werden Risiken im Betrieb der dezentralen Komponenten der TI wesentlich gesenkt.

Da die Maßnahmen der Komponenten der dezentralen TI zur Gewährleistung der Datensicherheit in gleicher Weise auf alle in den Komponenten verarbeiteten personenbezogenen Daten wirken und nicht spezifisch für einzelne Verarbeitungsvorgänge sind, erfolgt die Bewertung der Angemessenheit der Abhilfemaßnahmen der Komponenten hinsichtlich der Daten, deren Verarbeitung die höchsten Risiken für die Betroffenen bedeutet, nach dem Maximum-Prinzip. Es handelt sich hierbei um die personenbezogenen Daten nach Artikel 9 Absatz 1 DSGVO der Versicherten. Nach diesen Daten bestimmen sich die in den Komponenten zu treffenden Abhilfemaßnahmen. Die Abhilfemaßnahmen sind dann ebenfalls angemessen für die Verarbeitung der weniger sensiblen Daten.

Die Risikobewertung orientiert sich am Standard-Datenschutzmodell (SDM) der Aufsichtsbehörden für den Datenschutz und den dort definierten Gewährleistungszielen. Die Schadens- und Eintrittswahrscheinlichkeitsstufen sowie die Risikomatrix orientieren sich am DSK-Kurzpapier Nummer 18 „Risiko für die Rechte und Freiheiten natürlicher Personen“ i.V.m. der ISO/IEC 29134:2017 zum Privacy Impact Assessment. In der folgenden Tabelle werden die einzelnen Risiken identifiziert, inklusive Schadenshöhe, Schadensereignissen, betroffenen Gewährleistungszielen des Standard-Datenschutzmodells und Eintrittswahrscheinlichkeit. Die

Bewertung der Eintrittswahrscheinlichkeit erfolgt unter Berücksichtigung der referenzierten Abhilfemaßnahmen, die detailliert in Abschnitt 2.4 beschrieben sind.

Schaden	**Beschreibung der Schadensereignisse**	**Eintrittswahrscheinlichkeit (EWS) mit Abhilfemaßnahmen (Abschnitt 2.4)**
Physische, materielle oder immaterielle Schäden, finanzielle Verluste, erhebliche wirtschaftliche **Nachteile:** **(ErwG 90 i.V.m 85 DSGVO)** **Schadenshöhe: groß**	Durch die unbefugte, unrechtmäßige oder zweckfremde Verarbeitung sowie eine unbefugte Offenlegung oder Änderung der in den Komponenten der dezentralen TI verarbeiteten Gesundheitsdaten der Versicherten können Versicherte große immaterielle Schäden erleiden. Bei einer unbefugten Offenlegung der Gesundheitsdaten ihrer Patienten können Leistungserbringer materielle, immaterielle, finanzielle bzw. wirtschaftliche Schäden erleiden, da Leistungserbringer dem Berufsgeheimnis mit zugehörigen Straf- und Bußgeldvorschriften, insbesondere dem Straftatbestand des § 203 StGB, unterliegen. Zusätzlich können Geldbußen gemäß Artikel 83 DSGVO verhängt werden. Die Nutzung der Komponenten der dezentralen Infrastruktur der TI und die Anbindung an die TI dürfen nicht dazu führen, dass Leistungserbringer gegen das Berufsgeheimnis oder die Vorgaben der DSGVO verstoßen.	EWS: geringfügig – Minimierung der Verarbeitung personenbezogener Daten – Schnellstmögliche Pseudonymisierung – Datensicherheits-maßnahmen

Schaden	Beschreibung der Schadensereignisse	Eintrittswahrscheinlichkeit (EWS) mit Abhilfemaßnahmen (Abschnitt 2.4)
	Betroffene Gewährleistungsziele (SDM): Datenminimierung, Nichtverkettung, Vertraulichkeit, Integrität	
Verlust der Kontrolle über personenbezogene Daten: **(ErwG 90 i.V.m. 85 DSGVO)** **Schadenshöhe: groß**	Ein Angreifer (insbesondere auch der Hersteller) könnte die Komponenten der dezentralen TI manipulieren, was zu einer für den Versicherten oder den Leistungserbringer intransparenten Datenverarbeitung führen würde. Es könnte das Risiko bestehen, dass eine Verarbeitung von personenbezogenen Daten in den Komponenten der dezentralen Infrastruktur für die Versicherten im Nachhinein nicht erkannt werden kann und dass er nicht in diese Datenverarbeitung intervenieren (z. B. ihr widersprechen) kann. Betroffene Gewährleistungsziele (SDM): Transparenz, Intervenierbarkeit	EWS: geringfügig – Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten – Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen – Datensicherheits-maßnahmen
Diskriminierung, Rufschädigung, erhebliche	Die Verarbeitung von Daten besonderer Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1	EWS: geringfügig – Minimierung der Verarbeitung

Schaden	Beschreibung der Schadensereignisse	Eintrittswahrscheinlichkeit (EWS) mit Abhilfemaßnahmen (Abschnitt 2.4)
gesellschaftliche Nachteile: **(ErwG 90 i.V.m. 85 DSGVO)** **Schadenshöhe: groß**	DSGVO birgt Risiken einer Diskriminierung oder Rufschädigung für Versicherte, falls Gesundheitsdaten über den Versicherten offengelegt, unbefugt oder unrechtmäßig verarbeitet werden. Dies kann zu erheblichen gesellschaftlichen Nachteilen für den Versicherten führen. Falls Gesundheitsdaten, die ein Leistungserbringer verarbeitet, unberechtigt offengelegt werden und der Leistungserbringer somit sein Berufsgeheimnis verletzt, kann dies zu einer Rufschädigung des Leistungserbringers führen. Betroffene Gewährleistungsziele (SDM): Datenminimierung, Nichtverkettung, Vertraulichkeit, Integrität	personenbezogener Daten – Schnellstmögliche Pseudonymisierung – Datensicherheits-maßnahmen – Überwachung der Verarbeitung personenbezogener Daten durch die betroffenen Personen
Identitätsdiebstahl oder -betrug: **(ErwG 90 i.V.m. 85 DSGVO)** **Schadenshöhe: groß**	In den Komponenten der dezentralen Infrastruktur der TI werden kryptographische Identitäten von Versicherten und Leistungserbringern verarbeitet. Ein Missbrauch dieser Identitäten durch eine unbefugte oder unrechtmäßige Nutzung muss verhindert werden, um Schäden für den Versicherten oder Leistungserbringer abzuwehren. Hierdurch könnte z. B. unter der Identität des Versicherten oder Leistungserbringers	EWS: geringfügig – Minimierung der Verarbeitung personenbezogener Daten – Datensicherheits-maßnahmen

Schaden	**Beschreibung der Schadensereignisse**	**Eintrittswahrscheinlichkeit (EWS) mit Abhilfemaßnahmen (Abschnitt 2.4)**
	gehandelt werden, um medizinische Daten zu lesen, zu ändern oder weiterzugeben. Betroffene Gewährleistungsziele (SDM): Datenminimierung, Nichtverkettung, Vertraulichkeit, Integrität	
Verlust der Vertraulichkeit bei Berufsgeheimnissen: **(ErwG 90 i.V.m. 85 DSGVO)** **Schadenshöhe: groß**	In den Komponenten der dezentralen Infrastruktur der TI werden Daten verarbeitet, die unter das Berufsgeheimnis fallen. Der Verlust der Vertraulichkeit dieser Daten durch eine unbefugte Offenlegung muss verhindert werden, damit Leistungserbringer ihren Geheimhaltungspflichten nachkommen können. Neben einer Rufschädigung können den Leistungserbringer Straf- und Bußgeldvorschriften (insbesondere § 203 StGB) treffen. Betroffene Gewährleistungsziele (SDM): Datenminimierung, Vertraulichkeit, Integrität	EWS: geringfügig – Minimierung der Verarbeitung personenbezogener Daten – Schnellstmögliche Pseudonymisierung – Datensicherheits-maßnahmen
Beeinträchtigung/Verlust der Verfügbarkeit **Schadenshöhe: geringfügig**	Eine Beeinträchtigung bzw. der Verlust der Verfügbarkeit der Komponenten der dezentralen TI durch technische Fehlfunktionen könnte dazu führen, dass a) Dienste in der zentralen TI, der	EWS: überschaubar Ein Ausfall einer Komponente kann nicht ausgeschlossen werden. Zusätzliche Abhilfemaßnahmen zur Verfügbarkeit der

Schaden	Beschreibung der Schadensereignisse	Eintrittswahrscheinlichkeit (EWS) mit Abhilfemaßnahmen (Abschnitt 2.4)
	Anwendungsinfrastruktur der TI oder eines an die TI angeschlossenen Netzes oder b) lokale Funktionen (insbesondere Verschlüsselung, Signatur, Authentifizierung) Von Leistungserbringer nicht mehr genutzt werden können. Durch eine beeinträchtige Verfügbarkeit der Komponenten der dezentralen TI ergeben sich nur geringfügige Schäden für Versicherte oder Leistungserbringer, da die Verarbeitungen nicht zeitkritisch sind bzw. es Ersatzverfahren gibt. Es ist zudem nur eine Leistungserbringerumgebung betroffen. Betroffene Gewährleistungsziele (SDM): Verfügbarkeit	Komponenten der dezentralen TI sind aufgrund des geringen vom Leistungserbringer nicht mehr genutzt Risikos nicht erforderlich.

2.4 Abhilfemaßnahmen (Artikel 35 Absatz 7 Buchstabe d DSGVO)

Gemäß Artikel 35 Absatz 7 Buchstabe d DSGVO sind zur Bewältigung der Risiken Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, umzusetzen, durch die die Risiken für die Rechte der Betroffenen eingedämmt werden und der Schutz personenbezogener Daten sichergestellt wird.

Als Maßnahmen, Garantien und Verfahren zur Eindämmung von Risiken werden insbesondere in den ErwGen 28, 78 und 83 DSGVO genannt:

Kriterium	Beschreibung
Minimierung der Verarbeitung personenbezogener Daten: **(ErwG 78 DSGVO)**	Kategorie 1: Die Verarbeitung ist mit Blick auf den Zweck der Weiterleitung von Daten minimal. Eine über den Transport hinausgehende Verarbeitung erfolgt nicht. Der Umfang der transportierten Daten ist abhängig von der über die dezentrale Infrastruktur genutzten Anwendung. Der Verantwortliche dieser Anwendung hat entsprechende Maßnahmen zur Minimierung zu ergreifen. Dies liegt jedoch nicht in der Verantwortung des Leistungserbringers als Nutzer der Anwendung. Kategorie 2: Die Verarbeitung ist minimal, da sie nur die zum Zwecke der Ver- bzw. Entschlüsselung bzw. Signatur benötigten Daten verarbeitet. Kategorie 3: Die Verarbeitung ist minimal, da in den Anwendungen dieser Kategorie ausschließlich die Daten verarbeitet werden, die zur Erfüllung des gesetzlich vorgegebenen Zweckes erforderlich sind. Zudem werden Anwendungsdaten in den Komponenten der dezentralen Infrastruktur nach der Verarbeitung sofort gelöscht und nicht persistent gespeichert. Die Spezifikationen zu diesen Anwendungen sowie Art und Umfang der verarbeiteten Daten werden im Benehmen mit dem BfDI erstellt und sind öffentlich für eine Prüfung verfügbar.
Schnellstmögliche Pseudonymisierung personenbezogener Daten **(ErwG 28 und 78 DSGVO)**	Kategorie 1: Die Daten werden unverändert weitergeleitet. Es erfolgt keine weitere Verarbeitung in den Komponenten der dezentralen Infrastruktur, d. h. auch keine Pseudonymisierung. Der Verantwortliche der Anwendung, zu der die transportierten Daten gehören, hat entsprechende Maßnahmen zur Pseudonymisierung zu ergreifen. Dies liegt jedoch nicht in der Verantwortung des Leistungserbringers als Nutzer der Anwendung. Kategorie 2: Zweck ist die Ver- bzw. Entschlüsselung bzw. Signatur der übergebenen Daten. Eine Pseudonymisierung und damit Veränderung der Daten ist nicht gewünscht. Kategorie 3:

Kriterium	Beschreibung
	Eine Pseudonymisierung der personenbezogenen Daten in den Anwendungen dieser Kategorie erfolgt, sofern es für den gesetzlich vorgegebenen Zweck möglich ist. Bei der Gestaltung der Anwendungen werden die Artikel 25 und 32 DSGVO berücksichtigt. Die Spezifikationen zu diesen Anwendungen sowie Art und Umfang der verarbeiteten Daten werden im Benehmen mit dem BfDI erstellt und sind öffentlich für eine Prüfung verfügbar.
Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten **(ErwG 78 DSGVO):**	[1]Durch die Veröffentlichung der Spezifikationen der Komponenten der dezentralen Infrastruktur auf der Internetseite der Gesellschaft für Telematik können die Funktionen und die generelle Verarbeitung personenbezogener Daten in den Komponenten der dezentralen Infrastruktur der TI von der Öffentlichkeit kostenlos nachvollzogen werden. [2]Experten für Datenschutz und Sicherheit können die Spezifikationen auf die Einhaltung der Vorschriften des Datenschutzes prüfen. [3]Die Gesellschaft für Telematik und die Krankenkassen sind gemäß den §§ 314 und 343 SGB V verpflichtet, für die Versicherten in präziser, transparenter, verständlicher, leicht zugänglicher und barrierefreier Form Informationen zur TI zur Verfügung zu stellen. [4]Die Informationen müssen über alle relevanten Umstände der Datenverarbeitung für die Einrichtung der elektronischen Patientenakte, die Übermittlung von Daten in die elektronische Patientenakte und die Verarbeitung von Daten in der elektronischen Patientenakte durch Leistungserbringer einschließlich der damit verbundenen Datenverarbeitungsvorgänge in den verschiedenen Bestandteilen der Telematikinfrastruktur und die für die Datenverarbeitung datenschutzrechtlich Verantwortlichen informieren. [5]Zur Unterstützung der Informationspflichten der Krankenkassen nach § 343 SGB V hat der Spitzenverband Bund der Krankenkassen im Benehmen mit dem BfDI geeignetes Informationsmaterial, auch in elektronischer Form, zu erstellen und den Krankenkassen zur verbindlichen Nutzung zur Verfügung zu stellen.
Überwachung der Verarbeitung personenbezogener Daten	Kategorie 1: Von den Verantwortlichen der Anwendungen, die über die Komponenten der dezentralen Infrastruktur für den

Kriterium	Beschreibung
durch die betroffenen Personen **(ErwG 78 DSGVO)**	Leistungserbringer erreichbar sind, sind Maßnahmen nach ErwG 78 DSGVO zu treffen. Kategorie 2: In den Komponenten der dezentralen Infrastruktur erfolgt eine Protokollierung der Nutzung der Funktionen, die eine Überwachung der Verarbeitung ermöglicht. Kategorie 3: [1]Für die Anwendungen dieser Kategorie bestehen gesetzliche Protokollierungspflichten gemäß § 309 SGB V zum Zwecke der Datenschutzkontrolle für den Versicherten. [2]Die Protokollierungspflichten richten sich dabei an den Verantwortlichen der Anwendung und nicht an den Leistungserbringer. [3]Der Versicherte kann sich nach Einsicht der Protokolldaten nach § 309 SGB V, die gemäß § 342a Absatz 5 SGB V auch bei den Ombudsstellen der Krankenkassen nach § 342a Absatz 1 SGB V beantragt werden kann, im Rahmen von Artikel 15 DSGVO an den Leistungserbringer wenden, um nähere Auskünfte über die den Leistungserbringer betreffenden Protokolleinträge nach § 309 SGB V zu erhalten. [4]Für die Auskunft kann der Leistungserbringer auch die in den Komponenten der dezentralen Infrastruktur erfolgte Protokollierung nutzen.
Datensicherheitsmaßnahmen: **(ErwG 78 und 83 DSGVO)**	[1]Die an der vertragsärztlichen und vertragszahnärztlichen Versorgung teilnehmenden Leistungserbringer sind verpflichtet, die Vorgaben der Richtlinie zur IT-Sicherheit gemäß § 75b SGB V zu beachten; Krankenhäuser haben die IT-Sicherheitsanforderungen nach § 391 SGB V einzuhalten. [2]Diese Richtlinie umfasst auch Anforderungen an die sichere Installation und Wartung von Komponenten und Diensten der TI, die in der vertragsärztlichen und vertragszahnärztlichen Versorgung genutzt werden, d. h. insbesondere auch die Komponenten der dezentralen Infrastruktur der TI sowie Maßnahmen zur Sensibilisierung von Mitarbeiterinnen und Mitarbeitern zur Informationssicherheit (Steigerung der Security-Awareness). [3]Die Anforderungen in der Richtlinie werden u. a. im Benehmen mit dem BSI sowie im Benehmen mit dem BfDI festgelegt.

Kriterium	Beschreibung
	[4]Wenn ein Leistungserbringer einen Dienstleister mit der Herstellung und der Wartung des Anschlusses von informationstechnischen Systemen der Leistungserbringer an die TI einschließlich der Wartung hierfür benötigter Komponenten sowie der Anbindung an Dienste der TI beauftragt, muss dieser Dienstleister gemäß § 332 SGB V besondere Sorgfalt walten lassen und über die notwendige Fachkunde verfügen. [5]Die technischen Maßnahmen der Komponenten der dezentralen Infrastruktur der TI zur Gewährleistung der Datensicherheit hat die Gesellschaft für Telematik gemäß § 311 Absatz 2 SGB V im Benehmen mit dem BSI und dem BfDI zu treffen, so dass Fragen der Sicherheit und des Datenschutzes bei der Gestaltung der Komponenten berücksichtigt werden, insbesondere auch die Vorgaben der Artikel 25 und 32 DSGVO. [6]Darüber hinaus erfolgt der Nachweis der vollständigen Umsetzung der technischen Maßnahmen zur Gewährleistung der Datensicherheit in einer Komponente der dezentralen Infrastruktur eines Herstellers gemäß § 325 Absatz 3 SGB V im Rahmen der Zulassung der Komponente bei der Gesellschaft für Telematik durch eine Sicherheitszertifizierung nach den Vorgaben des BSI bzw. durch eine im Benehmen mit dem BSI festgelegte abweichende Form des Nachweises der Sicherheit. [7]Auch die Hersteller von Komponenten der dezentralen Infrastruktur können gemäß § 325 Absatz 5 SGB V von der Gesellschaft für Telematik zugelassen werden, um insbesondere eine ausreichende Qualität der Herstellerprozesse bei der Entwicklung, dem Betrieb, der Wartung und der Pflege der Komponenten zu gewährleisten. [8]Um die Wirksamkeit der technischen Maßnahmen der Komponenten der dezentralen Infrastruktur der TI zur Gewährleistung der Datensicherheit kontinuierlich aufrechtzuerhalten, werden diese Maßnahmen kontinuierlich von der Gesellschaft für Telematik und dem BSI bewertet. [9]Insbesondere ist die Gesellschaft für Telematik gemäß § 333 SGB V dazu verpflichtet, dem BSI auf Verlangen Unterlagen und Informationen u. a. zu den Zulassungen von Komponenten der dezentralen Infrastruktur einschließlich der zugrundeliegenden Dokumentation sowie festgestellten Sicherheitsmängeln vorzulegen. [10]Die Gesellschaft für Telematik kann zudem

Kriterium	Beschreibung
	für die Komponenten der dezentralen Infrastruktur gemäß § 331 Absatz 1 SGB V im Benehmen mit dem BSI solche Maßnahmen zur Überwachung des Betriebs treffen, die erforderlich sind, um die Sicherheit, Verfügbarkeit und Nutzbarkeit der TI zu gewährleisten. [11]Soweit von den Komponenten der dezentralen Infrastruktur der TI eine Gefahr für die Funktionsfähigkeit oder Sicherheit der TI ausgeht, kann die Gesellschaft für Telematik gemäß § 329 SGB V unverzüglich die erforderlichen technischen und organisatorischen Maßnahmen treffen. [12]Das BSI ist hierüber von der Gesellschaft für Telematik zu informieren.

Die Abhilfemaßnahmen sind für alle Risikoquellen anwendbar. Technischen Fehlfunktionen der Komponenten der dezentralen TI wird im Rahmen der Zulassung durch funktionale Tests und Sicherheitsüberprüfungen entgegengewirkt.

2.5 Einbeziehung betroffener Personen

Gemäß § 311 Absatz 2 SGB V hat die Gesellschaft für Telematik die Festlegungen und Maßnahmen nach § 311 Absatz 1 Nummer 1 SGB V im Benehmen mit dem BSI und dem BfDI zu treffen. Die Aufgaben der Gesellschaft für Telematik nach § 311 Absatz 1 Nummer 1 SGB V umfassen hierbei insbesondere auch die Erstellung der funktionalen und technischen Vorgaben und die Zulassung der Komponenten der dezentralen Infrastruktur der TI.

Vertreter der Leistungserbringer sind als Gesellschafter der Gesellschaft für Telematik ebenfalls in die Erstellung der Vorgaben der dezentralen Infrastruktur der TI einbezogen.

Die Spezifikationen der Komponenten der dezentralen Infrastruktur der TI werden auf der Internetseite der Gesellschaft für Telematik veröffentlicht. Dadurch wird auch die Öffentlichkeit (u. a. Experten für Sicherheit und Datenschutz sowie Landesdatenschutzbehörden) einbezogen, so dass jederzeit die Möglichkeit der Prüfung der festgelegten Maßnahmen besteht.