gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Spezifikation Datenschutz- und Sicherheitsanforderungen

Version:	1.4.1
Revision:	\main\rel_online\rel_opb1\21
Stand:	23.11.2016
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemSpec_Sich_DS]

Dokumentinformationen

Änderungen zur Vorversion

Überarbeitung der Dokumente für den Online-Produktivbetrieb (Stufe 1), als Grundlage für Produktivzulassungen und den bundesweiten Rollout.

Dokumentenhistorie

Version	Datum	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.5.0	13.07.12		zur Abstimmung freigegeben	PL P77
			Einarbeitung Kommentare	P77
0.6.0	06.09.12		zur Abstimmung freigegeben	PL P77
			Ergänzungen und Aktualisierungen	P77
1.0.0	15.10.12		freigegeben	gematik
			Einarbeitung Kommentare aus der übergreifenden Konsistenzprüfung	P77
1.1.0	12.11.12		freigegeben	gematik
			Korrekturen	P77
1.1.9	22.04.13		zur Abstimmung freigegeben	PL P77
			Einarbeitung Kommentare LA	P77
1.2.0 RC	30.05.13		zur Freigabe empfohlen	PL P77
1.2.0	06.06.13		freigegeben	gematik
1.3.0	24.08.16		Anpassungen zum Online-Produktivbetrieb (Stufe 1)	gematik
			Anpassungen gemäß Änderungsliste	
1.4.0	16.10.16		freigegeben	gematik
1.4.1	23.11.16	5	Ausnahmeregelung aufgrund § 274 Abs. 1 SGB V ergänzt	gematik

Inhaltsverzeichnis

1 Einführung

1.1 Zielsetzung und Einordnung des Dokuments

Das Dokument definiert übergreifende Sicherheits- und Datenschutzanforderungen für den Aufbau und den Betrieb der Telematikinfrastruktur.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter von Produkten der TI.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des Deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Für Zertifizierungsdiensteanbieter (ZDAs) gelten die hier gestellten Anforderungen nur, sofern sie Dienstleistungen für die TI erbringen, die nicht unter das deutsche Signaturgesetz fallen. Das gilt auch, wenn sich aus der Schnittstelle zur TI besondere Anforderungen an die Sicherheit ergeben, die von den Aufsichtsmaßnahmen der Bundesnetzagentur nicht erfasst sind.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzung des Dokuments

Das Dokument enthält übergreifende Festlegungen für Herstellung und Betrieb von Produkttypen der TI. Spezifische Anforderungen für einzelne Produkttypen sind in den jeweiligen Spezifikationen sowie in Konzepten und Richtlinien zu Betrieb und Test der TI festgelegt.

1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

⌦ **GS-A_xxxx <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

2 Datenschutzanforderungen

Bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten im Gesundheitswesen sind die Rechte von Patientinnen und Patienten sowie die Vorschriften zum Schutz personenbezogener Daten der Betroffenen (u.a. Versicherte, Leistungserbringer) sicherzustellen. Nachfolgend werden für die TI Rahmenbedingungen sowie architektur- und lösungsneutrale Anforderungen des Datenschutzes für Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten festgelegt.

2.1 Sicherstellen des gesetzlichen Datenschutzniveaus

In der TI sind die notwendigen gesetzlichen Vorgaben des Datenschutzes sicherzustellen. Insbesondere sind die Anforderungen des § 11 BDSG bzw. § 80 SGB X (Auftragsverarbeitung) und der Datentrennung entsprechend Anlage zu §9 BDSG zu erfüllen.

⌦ **GS-A_2214 Anbieter müssen jährlich die Betreiber kontrollieren.**

Der Anbieter MUSS sich jährlich bei den von ihm nach §11 BDSG oder § 80 SGB X beauftragten Betreibern von der Einhaltung der von den Betreibern getroffenen Maßnahmen überzeugen. ⌫

⌦ **GS-A_2065 Beschlagnahmeschutz bei Anbietern und Betreibern**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN sicherstellen, dass der Beschlagnahmeschutz für die Daten der TI, die in ihren Systemen verarbeitet oder gespeichert werden, gewährleistet ist. ⌫

Für die Betroffenen und zuständigen datenschutzrechtlich zuständigen Aufsichtsbehörden soll eine möglichst hohe Transparenz über die in der TI erhobenen, verarbeiteten und genutzten personenbezogenen Daten erreicht werden. Dies ist zwingende Voraussetzung dafür, dass der Betroffene sein Recht auf informationelle Selbstbestimmung wahrnehmen kann. Anbieter müssen daher Betroffene informieren und die Gewährleistung der Betroffenenrechte nach § 6 BDSG gewährleisten.

⌦ **GS-A_2087 Information für Betroffene über Produkte durch Anbieter und Betreiber**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN Betroffene auf deren Anfrage in allgemein verständlicher Form über das Produkt, in denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, sowie über die Datenschutz- und Sicherheitsmaßnahmen informieren können. ⌫

⌦ **GS-A_2213 Wahrnehmung der Betroffenenrechte beim Anbieter**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN den Betroffenen ermöglichen, ihre datenschutzrechtlichen Betroffenenrechte nach § 6 BDSG bzgl. aller vom Anbieter

angebotenen Produkte in einer für den Betroffenen praktikablen Weise vollständig beim Anbieter wahrzunehmen. ⌫

2.2 Zulassungskriterien für Anbieter

Die Einhaltung der Vorschriften zum Datenschutz in der TI ist im Wirkbetrieb aufrecht zu erhalten und zu kontrollieren. Da die gematik nach § 291b Abs. 1 Satz 2 SGB V den gesetzlichen Auftrag hat, die Einhaltung der Vorschriften zum Schutz personenbezogener Daten in der TI sicherzustellen, hat sie ein Datenschutzkontrollrecht für die Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten.

Die Einhaltung der Kriterien des Datenschutzes ist im Zulassungsverfahren von Produkten für die TI zu berücksichtigen und vom Zulassungsnehmer nachzuweisen.

⌦ **GS-A_2070 Datenschutzkontrolle durch BfDI und gematik**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN im Rahmen ihrer Zulassung der gematik zusichern, dass der BfDI, und die Landesbeauftragten für den Datenschutz in ihrem jeweiligen Zuständigkeitsbereich und die gematik sie sowie die von ihnen betriebenen Produkte jederzeit in Bezug auf die Einhaltung des Datenschutzes kontrollieren können. ⌫

⌦ **GS-A_2071 Unterstützung bei der Datenschutzkontrolle durch BfDI und gematik**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN im Rahmen ihrer Zulassung der gematik zusichern, dass sie den BfDI und die gematik bei der Datenschutzkontrolle unterstützen sowie die für die Erfüllung der Datenschutzkontrolle erforderlichen Auskünfte unverzüglich und in einer Form erteilen, anhand derer die datenschutzgerechte Gestaltung mit angemessenen Aufwand geprüft werden kann. ⌫

⌦ **GS-A_2072 Bereitstellung von Datenschutz-Audits zur Datenschutzkontrolle durch BfDI und gematik**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN im Rahmen ihrer Zulassung der gematik zusichern, dass sie die Ergebnisse durchgeführter Datenschutz-Audits dem BfDI oder der gematik auf Verlangen bereitstellen. ⌫

⌦ **GS-A_2073 Anordnung von Maßnahmen des Datenschutzes durch BfDI und gematik**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN im Rahmen ihrer Zulassung der gematik zusichern, dass die gematik oder der BfDI Maßnahmen anordnen können, um insbesondere vom BfDI oder der gematik festgestellte technische oder organisatorische Mängel bzgl. des Datenschutzes zu beseitigen. ⌫

GS-A_2074 Umsetzung der durch BfDI und gematik angeordneten Maßnahmen

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN im Rahmen ihrer Zulassung der gematik zusichern, dass die vom BfDI oder der gematik angeordneten Maßnahmen zum Datenschutz unverzüglich umgesetzt werden. ⌫

GS-A_2075 Untersagen von Verfahren durch BfDI und gematik

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN im Rahmen ihrer Zulassung der gematik zusichern, dass die gematik oder der BfDI den Einsatz einzelner Verfahren bei Mängeln, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind und nicht in angemessener Zeit beseitigt wurden, untersagen können. ⌫

GS-A_2076 Datenschutzmanagement nach BSI für Betreiber

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN ein Datenschutzmanagement nach BSI Grundschutz-Baustein B1.5 umsetzen. ⌫

GS-A_2174 Inhalte des Sicherheitsgutachtens aus Sicht des Datenschutzes

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN im Sicherheitsgutachten nachvollziehbar darstellen, wie

- die BSI-Grundschutzmaßnahmen des ergänzenden Maßnahmenbündels für den Bereich Datenschutz (Baustein B1.5) umgesetzt sind und
- die Anforderungen des Datenschutzes der TI an die betriebenen Produkte umgesetzt sind. ⌫

GS-A_2176 Anbieter müssen Kontaktinformationen zum Datenschutz liefern

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN der Zulassungsstelle der gematik die Kontaktinformationen des Datenschutzes des Anbieters übermitteln, insbesondere die der verantwortlichen Stelle und die des betrieblichen Datenschutzbeauftragten. ⌫

GS-A_2177 Anbieter müssen Pflichten der Auftragsdatenverarbeitung erfüllen

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN nachweisen, dass die vertraglichen Regelungen zur Auftragsdatenverarbeitung für die von ihnen beauftragten Auftragnehmer entsprechend § 11 BDSG bzw. § 80 SGB X getroffen wurden. ⌫

3 Sicherheitsanforderungen

In der Telematikinfrastruktur sind Rahmenbedingungen und Anforderungen der Informationssicherheit einzuhalten, um die Interessen aller an der Telematikinfrastruktur Beteiligten zu wahren und die Erreichung und Einhaltung eines angemessenen Sicherheitsniveaus sicherzustellen. Nachfolgend sind Festlegungen zur Informationssicherheit beschrieben, die für die gesamte Telematikinfrastruktur unabhängig von der gewählten Architektur oder Technologie gelten.

Der Inhalt dieses Abschnittes wurde nach Kapitel 4 verschoben.

3.1 Einbindung in die Verantwortung für Informationssicherheit

Die Verantwortung für die Definition, die Erreichung und Aufrechterhaltung des notwendigen Datenschutz- und angemessenen Sicherheitsniveaus in der TI muss für alle Fachanwendungen und die TI-Plattform eindeutig, vollständig und nachvollziehbar festgelegt sein. Anbieter sind in die Verantwortung wie folgt eingebunden:

⌦ **GS-A_2012 Verantwortung der Anbieter und Betreiber für Einhaltung der Anforderungen Datenschutz und Informationssicherheit**

Anbieter in der TI MÜSSEN die Verantwortung für die Einhaltung der Anforderungen des Datenschutzes und der Informationssicherheit, die sich an den Betrieb des von ihnen betriebenen Produktes der TI ergeben, wahrnehmen. ⌫

⌦ **GS-A_5324 Teilnahme des Anbieters an Sitzungen des kDSMS/kISMS**

Anbieter in der TI MÜSSEN das koordinierende Datenschutz- und Informationssicherheitsmanagementsystem (kDSMS/kISMS) der gematik unterstützen, indem an den i.d.R. quartalsweise stattfindenden Sitzungen des Arbeitskreises Datenschutz und Informationssicherheit (AK DIS) ein Sicherheits- und ein Datenschutzbeauftragter teilnehmen, die sich im Rahmen ihrer beruflichen Tätigkeit mit dem operativen Betrieb der vom Anbieter betriebenen Dienste der TI befassen. ⌫

Anforderungen an die Betreiberumgebungen der Anbieter sind in [gemSpec_SiBetrUmg] festgelegt, insbesondere die Umsetzung eines Informationssicherheitsmanagements auf Basis des Standards ISO27001 und die Erreichung der Ziele des Standards ISO27002.

⌦ **GS-A_2021 Anwendung der einheitlichen Methoden der Informationssicherheit durch Betreiber und Anbieter**

Falls ein Anbieter die Einhaltung der Anforderungen des Datenschutzes und der Informationssicherheit, die sich an den Betrieb des von ihm betriebenen Produktes der TI ergeben, nicht bereits in einem durch einen unabhängigen Sachverständigen bestätigten Sicherheitskonzept gemäß Übergreifendem Sicherheitskonzept der Telematikinfrastruktur, Anhang G, Version 2.2.0, Release 0.5.3 nachgewiesen hat, MUSS der Anbieter die einheitlichen Methoden zu Datenschutz und Informa-

tionssicherheit anwenden, um Datenschutz- und Sicherheitskonzepte zu erstellen und zu pflegen oder die Anwendung äquivalenter Methoden nachweisen.⌫

Die Detailanforderungen ergeben sich aus den nachfolgenden Festlegungen dieses Dokumentes sowie aus den Sicherheitsanforderungen in den weiteren Konzept- und Spezifikationsdokumenten.

3.2 Überwachung des Sicherheitsniveaus durch Zulassungsverfahren

Die Erreichung des notwendigen Sicherheitsniveaus wird durch die gematik über ein Zulassungsverfahren gemäß §291b SGB V überwacht.

⌦ **GS-A_2019 Zulassung der Anbieter und Produkte**

Anbieter und Hersteller MÜSSEN für den Betrieb und den Einsatz von Produkten in der TI von der gematik zugelassen oder abgenommen sein. ⌫

⌦ **GS-A_2148 Zulassungsnachweis der sicherheitstechnischen Eignung bei dezentralen Produkttypen**

Im Rahmen von Zulassungen nach § 291b Abs. 1a SGB V MÜSSEN Hersteller (Zulassungsnehmer) die sicherheitstechnische Eignung ihrer Produkte für den dezentralen Einsatz (dezentrale Produkttypen, z.B. Karten, Kartenterminals, Konnektoren und Fachmodule) durch ein gültiges IT-Sicherheitszertifikat des BSI (nach Common Criteria und zugehörigem Protection Profile) nachweisen. ⌫

⌦ **GS-A_2150 Zulassungsnachweis der Sicherheit der Betriebsleistung bei Anbieterzulassung**

Im Rahmen der Zulassung nach § 291b Abs. 1b SGB V MÜSSEN Anbieter (Zulassungsnehmer) den Nachweis, dass die Sicherheit ihrer Produkte der TI gewährleistet ist, durch ein von einem unabhängigen Sachverständigen nach den Vorgaben der gematik erstelltes Sicherheitsgutachten erbringen. ⌫

⌦ **GS-A_2151 Erstellung von Sicherheitsgutachten im Rahmen der Zulassung nach gematik-Richtlinie**

Im Rahmen der Zulassung nach § 291b Abs. 1a SGB V sowie der Zulassung nach § 291b Abs. 1b SGB V MÜSSEN Zulassungsnehmer (Hersteller und Anbieter) sicherstellen, dass unabhängige Sachverständige (Sicherheitsgutachter) Sicherheitsgutachten gemäß der gematik-Richtlinie [gemRL_PruefSichEig_DS] erstellen. ⌫

⌦ **GS-A_2153 Sicherheitsgutachten verliert Gültigkeit bei wesentlichen Änderungen am Zulassungsobjekt**

Zulassungsnehmer (Hersteller und Anbieter) MÜSSEN der Zulassungsstelle bei Änderungen am Objekt der Zulassung nach § 291b Abs. 1a SGB V bzw. nach § 291b Abs. 1b SGB V, die die ursprüngliche Aussage des vorgelegten Sicherheitsgutachtens in Frage stellen, unverzüglich ein neues Sicherheitsgutachten vorlegen.⌫

⌦ **GS-A_2154 Vorlage eines neuen Sicherheitsgutachtens nach Gültigkeitsablauf (im Rahmen der Zulassung)**

Verliert ein im Rahmen der Zulassung nach § 291b Abs. 1a SGB V bzw. nach § 291b Abs. 1b SGB V vorgelegtes Sicherheitsgutachten seine Gültigkeit, MUSS der Zulassungsnehmer (Hersteller oder Anbieter) unverzüglich ein neues Sicherheitsgutachten vorlegen, um einen Widerruf der Zulassung zu vermeiden. ⌫

Für die Zulassung sind Nachweise zu erbringen, dass die von der gematik für den Erhalt der Sicherheit festgelegten Anforderungen erfüllt werden. Übergreifend sind dies:

⌦ **GS-A_2046 Umsetzung der Anforderungen aus [gemSpec_SiBetrUmg] durch Anbieter von zentralen Produkten**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN für ihre Betriebsumgebungen im Wirkbetrieb die Anforderungen aus dem Dokument [gemSpec_SiBetrUmg] nachweislich vollständig umsetzen oder im Falle einer SOLL-Maßnahme die Gleichwertigkeit seiner getroffenen Alternativmaßnahmen nachweisen. Der Nachweis kann im Rahmen des Sicherheitsgutachtens erbracht werden. ⌫

⌦ **GS-A_2155 Zulassungsnachweis der Qualifikation des unabhängigen Sachverständigen (Sicherheitsgutachter)**

Im Rahmen der Zulassung nach § 291b Abs. 1a SGB V, der Zulassung nach § 291b Abs. 1b SGB V oder bei Vorlage eines Sicherheitsgutachtens MÜSSEN Zulassungsnehmer (Hersteller oder Anbieter) gegenüber der gematik den Nachweis der Qualifikation des tätig gewordenen unabhängigen Sachverständigen (Sicherheitsgutachter) durch Vorlage der entsprechenden Zertifikate gemäß gematik-Richtlinie [gemRL_PruefSichEig_DS] erbringen. ⌫

⌦ **GS-A_2156 Auditierungen der Zulassungsnehmer**

Hersteller (Zulassungsnehmer nach § 291b Abs. 1a SGB V) sowie Anbieter (Zulassungsnehmer nach § 291b Abs. 1b SGB V) MÜSSEN Auditierungen (zwecks Feststellung ggf. vorhandener technischer oder organisatorischer Mängel) ermöglichen und angemessen unterstützen (bspw. erforderliche Auskünfte unverzüglich erteilen). ⌫

⌦ **GS-A_5087 Nachweis der Datenschutz- und Sicherheitsanforderungen der gematik durch eine Akkreditierung nach Signaturgesetz**

Falls ein Trust Service Provider (TSP) ein akkreditierter Zertifizierungsdiensteanbieter nach Signaturgesetz (SigG) ist und das Sicherheitskonzept nach § 4 Abs. 2 SigG auch die Verarbeitung der Informationsobjekte der TI abdeckt, KANN der TSP die Einhaltung der Datenschutz- und Sicherheitsanforderungen der gematik durch ein gültiges Gütezeichen nachweisen, dass er von der nach SigG zuständigen Behörde erhalten hat.⌫

3.3 Anforderungen an Entwicklungsumgebungen

Seitens der Herstellung der dezentralen Produkte der TI wird die Qualität der Entwicklung durch die CC-Evaluierung sichergestellt. Die folgenden Anforderungen sollen dies für die zentralen Produkte der TI sicherstellen.

⌦ **GS-A_4944 Produktentwicklung: Behebung von Sicherheitsmängeln**

Der Anbieter MUSS für die von ihm angebotenen Produkte der TI gewährleisten, dass technisch-organisatorische Verfahren zur Behebung von Sicherheitsmängeln in den Produkten während der Zeit des Einsatzes in der TI vorgehalten werden. Dies beinhaltet das kontinuierliche Aufspüren (bug tracking) und Nachbessern (bug fixing) von Sicherheitsmängeln (security bugs) und das zur Verfügung stellen von Updates (security updates). ⌫

⌦ **GS-A_4945 Produktentwicklung: Qualitätssicherung**

Der Anbieter MUSS für die von ihm angebotenen Produkte der TI gewährleisten, dass bei der Entwicklung der Produkte technisch-organisatorische Verfahren der Qualitätssicherung angewendet werden (bspw. fuzz (robustness) testing bzw. penetration testing und source code review). ⌫

⌦ **GS-A_4946 Produktentwicklung: sichere Programmierung**

Der Anbieter MUSS für die von ihm angebotenen Produkte der TI gewährleisten, dass bei der Entwicklung der Produkte Secure Coding Guidelines angewendet werden; d.h. in einschlägigen Fachkreisen anerkannte, erprobte und bewährte Regeln sicherer Programmierung befolgt werden. ⌫

⌦ **GS-A_4947 Produktentwicklung: Schutz der Vertraulichkeit und Integrität**

Der Anbieter MUSS für die von ihm angebotenen Produkte der TI gewährleisten, dass sie in einer Entwicklungsumgebung entwickelt werden, für die technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit und Integrität der Produkte getroffen werden. ⌫

3.4 Anforderungen an die Systemumgebungen

Spezifische Anforderungen zur Gewährleistung von Datenschutz und Sicherheit betreffen die Umgebung der Anbieter und Hersteller. Durch die Festlegung eines Mindestniveaus wird dabei die Wirtschaftlichkeit der technischen Sicherheitsmaßnahmen (Verschlüsselung, Anonymisierung) fokussiert. Insbesondere ist dabei auf die informationstechnische Trennung von Test- und Produktivumgebungen zu achten.

3.4.1 Systemumgebungen der Anbieter

⌦ **GS-A_2047 Gestaltung der Umgebung von zentralen Produkten durch Betreiber für Schutzbedarf "mittel"**

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten MÜSSEN die Umgebungen, in denen diese Produkte betrieben werden, so ausgestalten, dass Informationsobjekte und Anwendungsprozesse mit einem Schutzbedarf von „mittel" ohne weitere durch die gematik spezifizierte Sicherheitsmaßnahmen verarbeitet werden können.⌫

3.5 Anforderungen an das Informationssicherheitsmanagement (ISM)

Um das erforderliche Sicherheitsniveau in der TI zu kontrollieren und zu verwalten, interagieren die Betriebsverantwortlichen im Rahmen ihrer Aufgaben mit der gematik, welche

die Aufrecherhaltung des notwendigen Sicherheitsniveaus gewährleisten muss (§291b, Absatz 1, Satz 4, 2. Halbsatz). Dazu etabliert die gematik als Gesamtverantwortliche für den Betrieb der TI ein **koordinierendes ISM** für die TI, welches mit den **ISM der Beteiligten** der Betriebsverantwortlichen in ihrem jeweiligen Verantwortungsbereich zusammenarbeitet.

3.5.1 ISM der Anbieter

Im Folgenden sind übergreifende Anforderungen an das ISM der Anbieter von zentralen Produkten der TI beschrieben. Näheres zum ISM der Beteiligten regelt [gemSpec_ISM].

⌦ **GS-A_2309 ISM der Beteiligten: Rollen und Verantwortlichkeiten**

Anbieter von Produkten der TI MÜSSEN für ihr ISM Rollen und Verantwortlichkeiten innerhalb ihrer Organisation festlegen. ⌫

⌦ **GS-A_2326 ISM der Beteiligten: Etablierung**

Anbieter MÜSSEN in der initialen Planungsphase (vor Zulassung in den Wirkbetrieb) ein ISM etablieren, in dem

- das Management-Framework zum Aufbau und Management der Informationssicherheit durch den Anbieter festgelegt wird;
- die Organisationsstruktur (des ISM) aufgebaut wird;
- die Verantwortlichkeiten innerhalb des Anbieters verteilt werden;
- die notwendige Dokumentation erstellt und für die Zulassung zur Verfügung gestellt wird. ⌫

⌦ **GS-A_2328 ISM der Beteiligten: Pflege und Fortschreibung der Sicherheitskonzepte**

Anbieter MÜSSEN im Rahmen ihres ISM während des Wirkbetriebs die weitere Pflege und Fortschreibung der Sicherheitskonzepte für ihre Produkte der TI durchführen. ⌫

⌦ **GS-A_2329 ISM der Beteiligten: Umsetzung der Sicherheitskonzepte**

Anbieter MÜSSEN im Rahmen ihres ISM die Maßnahmen zur Sicherheit des Personals, der Organisation, der Infrastruktur und der eingesetzten Technologien, entsprechend der in der Planungsphase erstellten Sicherheitskonzepte, umsetzen; wozu insbesondere die Kommunikation, Implementierung und Einhalten der Sicherheitsrichtlinien und die Durchführung von Sensibilisierungen und Schulungen gehören. ⌫

⌦ **GS-A_2330 ISM der Beteiligten: Schwachstellen-Management**

Anbieter MÜSSEN im Rahmen ihres ISM zur Reduzierung bekannter und neuer Bedrohungen präventive Maßnahmen zur Erkennung und Analyse von technischen Schwachstellen („vulnerabilities“) wie auch zur Bewertung und Implementierung von Sicherheitsupdates durchführen. ⌫

⌦ **GS-A_5017 ISM der Beteiligten: Schließen von Schwachstellen**

Anbieter MÜSSEN die gematik unverzüglich über neu gemeldete Schwachstellen in ihren Produkten informieren und sich mit der gematik anhand einer Einzelfallbetrachtung und -bewertung der Schwachstelle hinsichtlich der einzuleitenden Maßnahmen und der Behebungszeit abstimmen.⌫

⌦ **GS-A_2331 ISM der Beteiligten: Sicherheitsvorfalls-Management**

Anbieter MÜSSEN im Rahmen ihres ISM Sicherheitsvorfälle („security incidents“) wirksam vorbeugen, aufdecken, und unterbinden. ⌫

⌦ **GS-A_2332 ISM der Beteiligten: Notfallmanagement**

Anbieter MÜSSEN im Rahmen ihres ISM die durch Sicherheitsnotfälle aufgetretenen Schäden zeitnah durch ein entsprechendes Notfallmanagement korrigieren. ⌫

⌦ **GS-A_2333 ISM der Beteiligten: Meldung an das koordinierende ISM**

Anbieter MÜSSEN im Rahmen ihres ISM das koordinierende ISM der TI zur Steuerung und Bewertung der notwendigen Maßnahmen hinzuzuziehen, wenn schwerwiegende oder über den Verantwortungsbereich von Betriebsverantwortlichen hinwegreichende Schwachstellen, Sicherheitsvorfälle oder Schäden auftreten. ⌫

⌦ **GS-A_2339 ISM der Beteiligten: regelmäßige Reviews**

Anbieter MÜSSEN im Rahmen ihres ISM regelmäßige Reviews der umgesetzten Maßnahmen und Bewertungen der in ihrem jeweiligen Betriebsverantwortungsbereich aufgetretenen und behobenen Schwachstellen, Sicherheitsvorfälle oder Schäden durchführen und diese Bewertungen regelmäßig dem koordinierenden ISM bereitstellen. ⌫

⌦ **GS-A_2343 ISM der Beteiligten: eigene Audits**

Anbieter MÜSSEN im Rahmen ihres ISM zur Überprüfung der Effektivität der ISM regelmäßige und ggf. anlassbezogene Audits planen und durchführen sowie die Ergebnisse dieser Audits dem koordinierenden ISM bereitstellen. ⌫

⌦ **GS-A_2345 ISM der Beteiligten: Reviews und Trendanalysen**

Anbieter MÜSSEN im Rahmen ihres ISM zur Verbesserung der in den Sicherheitsrichtlinien und Sicherheitskonzepten getroffenen Steuerungsmechanismen, Risikobewertungen und Reaktionen Reviews der Risikosteuerung und Trendanalysen von Schwachstellen, Sicherheitsvorfällen und aufgetretenen Schäden durchführen. ⌫

⌦ **GS-A_2347 ISM der Beteiligten: Grundlagen neuer Planungsphasen**

Anbieter MÜSSEN im Rahmen ihres ISM die Ergebnisse von Reviews und Trendanalysen als Grundlage für Verbesserungen der Sicherheitsmaßnahmen und gezielte Risikoabschwächungen verwenden, welche in eine neue Planungsphase einfließen. ⌫

⌦ **GS-A_2355 ISM der Beteiligten: Nutzung des Problem-Management-Prozesses**

Anbieter MÜSSEN im Rahmen ihres ISM den in den „Übergreifenden Richtlinien zum Betrieb der TI“ [gemRL_Betr_TI] festgelegten Problem-Management-Prozess nutzen, um Schwachstellen und Bedrohungen an das koordinierende ISM zu melden. ⌫

⌦ **GS-A_2356 ISM der Beteiligten: Nutzung des Incident-Management-Prozesses**

Anbieter MÜSSEN im Rahmen ihres ISM den in den „Übergreifenden Richtlinien zum Betrieb der TI“ [gemRL_Betr_TI] festgelegten Incident-Management-Prozess nutzen, um zeitkritische Sicherheitsvorfälle an das koordinierende ISM zu melden. ⌫

⌦ **GS-A_2357 ISM der Beteiligten: Nutzung der Prozesse und Reports des Betriebs**

Anbieter MÜSSEN im Rahmen ihres ISM die in den „Übergreifenden Richtlinien zum Betrieb der TI“ [gemRL_Betr_TI] festgelegten Prozesse und Reports nutzen, um die zu erstellenden Kennzahlenberichte, Reviews der Risikosteuerung und Trendanalysen von Schwachstellen, Sicherheitsvorfällen und aufgetretenen Schäden an das koordinierende ISM zu berichten. ⌫

⌦ **GS-A_2359 ISM der Beteiligten: Nutzung der Sicherheits-Technologien des koordinierenden ISM**

Anbieter MÜSSEN im Rahmen ihres ISM die vom koordinierenden ISM angebotenen Technologien zur Wahrung der Integrität, Authentizität und Vertraulichkeit der übermittelten Nachrichten einsetzen. ⌫

⌦ **GS-A_2360 ISM der Beteiligten: Meldung von Restrisiken**

Anbieter MÜSSEN Schwachstellen, die durch die jeweiligen Anbieter nicht behoben werden, innerhalb ihres Risikomanagements bewerten und behandeln sowie Restrisiken entsprechend der Risikopolicy der TI [gemRL_RiPo_TI] an das koordinierende ISM melden. ⌫

⌦ **GS-A_2361 ISM der Beteiligten: Vorfallsmanagement**

Anbieter MÜSSEN im Rahmen ihres ISM Prozesse zum Management von Sicherheitsvorfällen etablieren und sicherstellen, dass eine Bewertung und Behandlung von Sicherheitsvorfällen in festgelegten maximalen Reaktionszeiten stattfindet. ⌫

⌦ **GS-A_2362 ISM der Beteiligten: Bericht lokaler Sicherheitsvorfälle**

Anbieter MÜSSEN im Rahmen ihres ISM Informationen zu lokale Sicherheitsvorfällen regelmäßig an das koordinierende ISM berichten. ⌫

⌦ **GS-A_2363 ISM der Beteiligten: Meldung schwerwiegender Sicherheitsvorfälle**

Anbieter MÜSSEN im Rahmen ihres ISM schwerwiegende Sicherheitsvorfälle unverzüglich über das Incident Management dem koordinierenden ISM melden. ⌫

⌦ **GS-A_2366 ISM der Beteiligten: Notfallbewältigung**

Anbieter MÜSSEN Sicherheitsnotfälle im Rahmen der Notfallbewältigung unter Einbeziehung ihres ISM behandeln. ⌫

3.5.2 Einbindung der Hersteller

Von Herstellern wird kein ISM nach den vorangehenden Anforderungen dieses Kapitels gefordert. Sie sind jedoch in begrenztem Umfang ebenfalls in das ISM der TI involviert:

⌦ **GS-A_2524 Produktunterstützung: Nutzung des Problem-Management-Prozesses**

Hersteller von Produkten der TI MÜSSEN im Rahmen der Produktunterstützung den in den „Übergreifenden Richtlinien zum Betrieb der TI“ [gemRL_Betr_TI] festgelegten Problem-Management-Prozess nutzen, um Schwachstellen an das koordinierende ISM zu melden. ⌫

⌦ **GS-A_2525 Hersteller: Schließen von Schwachstellen**

Hersteller von Produkten der TI MÜSSEN die gematik unverzüglich über neu gemeldete Schwachstellen in Ihren Produkten informieren und innerhalb von 45 Tagen nach der initialen Meldung einen Antrag auf Zulassung unter Beistellung der neuen Version der Software bei der Zulassungsstelle der gematik einreichen. ⌫

⌦ **GS-A_2354 Produktunterstützung mit geeigneten Sicherheits-Technologien**

Hersteller von Produkten der TI MÜSSEN eine vom koordinierenden ISM freigegebene Technologie zur Wahrung der Integrität, Authentizität und (wo nötig) Vertraulichkeit der Informationen zur Produktunterstützung und Schwachstellenmeldung einsetzen. ⌫

⌦ **GS-A_2350 Produktunterstützung der Hersteller**

Hersteller von Produkten der TI MÜSSEN dem koordinierenden ISM Supportinformationen, Sicherheitswarnungen sowie Informationen zu Softwareupdates als Produktunterstützung für von ihnen entwickelte Produkte der TI zur Konsolidierung und Weiterleitung an die ISM der Beteiligten zur Verfügung stellen. ⌫

3.6 Anforderungen an Testumgebungen

⌦ **GS-A_2157 Keine Echtdaten in Referenz- und Testumgebungen**

Der Verantwortliche für die Testumgebung bzw. Referenzumgebung MUSS sicherstellen, dass in diesen Umgebungen keine Echtdaten verarbeitet werden. ⌫

⌦ **GS-A_2158 Informationstechnische Trennung von Umgebungen mit Echtdaten**

Der Verantwortliche für die Referenz- bzw. Testumgebung (Umgebungen ohne Echtdaten) MUSS sicherstellen, dass diese Umgebungen informationstechnisch von Produktivumgebungen (Umgebungen mit Echtdaten) der TI getrennt sind. ⌫

⌦ **GS-A_2160 Nachweispflicht bei rein logischer Separierung von Umgebungen mit Echtdaten**

Der Verantwortliche für die Referenz- bzw. Testumgebung (Umgebungen ohne Echtdaten) MUSS, falls er seine Referenz- und Testumgebungen von Produktivumgebungen logisch separiert, die Wirksamkeit der logischen Separierung nachweisen können.⌫

⌦ **GS-A_2161 Physische Separierung von Umgebungen mit Echtdaten**

Der Verantwortliche für die Referenz- bzw. Testumgebung (Umgebungen ohne Echtdaten) SOLL sicherstellen, dass die informationstechnische Trennung dieser Umgebungen von Produktivumgebungen der TI mittels physischer Separierung realisiert wird. ⌫

⌦ **GS-A_2162 Kryptographisches Material in Entwicklungs- und Testumgebungen**

Der Verantwortliche für die Referenz- bzw. Testumgebung (Umgebungen ohne Echtdaten) MUSS sicherstellen, dass in diesen Umgebungen keine kryptographischen Identitäten bzw. Schlüssel der Produktivumgebungen der TI (Umgebungen mit Echtdaten) genutzt werden.⌫

⌦ **GS-A_2163 Kryptographisches Material in Produktivumgebungen**

Der Verantwortliche für die Referenz- bzw. Testumgebung (Umgebungen ohne Echtdaten) MUSS sicherstellen, dass keine kryptographischen Identitäten bzw. Schlüssel der jeweils von ihnen verantworteten Entwicklungs-, Referenz- und Testumgebungen in Produktivumgebungen (Umgebungen mit Echtdaten) genutzt werden.⌫

3.7 Anforderungen an Schlüsselverwaltungen

Die Sicherheit der TI beruht auf der korrekten Verwendung kryptographischer Mechanismen und der dafür notwendigen kryptographischen Schlüssel. Aufgrund dieser zentralen Funktion der Kryptographie in der TI sind die folgenden Anforderungen an die Schlüsselverwaltung (vgl. [ISO11770]) zu erfüllen.

⌦ **GS-A_3078 Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive**

Der Anbieter einer Schlüsselverwaltung innerhalb der TI MUSS in seinem Sicherheitskonzept notwendige Umstellungsprozesse bei Schwächung von kryptographischen Primitiven beschreiben und die Wirksamkeit der getroffenen Maßnahmen ist nachzuweisen (z.B. durch dokumentierte Notfallübungen, Ablaufprotokolle von abgewickelten Vorfällen). ⌫

⌦ **GS-A_3125 Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip**

Der Anbieter einer Schlüsselverwaltung MUSS in seinem Sicherheitskonzept dokumentieren, welcher Schlüssel in welcher Phase seines Lebenszyklus in welcher Systemkomponente transportiert wird. Es MUSS dabei sichergestellt werden, dass die Schlüssel nur an diejenigen Systemkomponenten verteilt werden, in denen ihr Aufenthalt vorgesehen ist und wo sie hinreichend geschützt sind.⌫

⌦ **GS-A_3130 Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip**

Der Anbieter einer Schlüsselverwaltung MUSS in seinem Sicherheitskonzept dokumentieren, welcher Schlüssel in welcher Systemkomponente installiert wird. Es MUSS dabei sichergestellt werden, dass die Schlüssel in Systemkomponenten installiert werden, in denen ihr Aufenthalt vorgesehen ist und wo sie hinreichend geschützt sind.⌫

Der Dienst Schlüsselableitung (im Sinne von [ISO11770]) erstellt eine potentiell große Anzahl von Schlüsseln unter Benutzung eines geheimen Originalschlüssels, genannt Ableitungsschlüssel, nicht geheimen veränderlichen Daten und einem Transformationsprozess (der nicht immer geheim sein muss). Das Ergebnis dieses Prozesses ist der abgeleitete Schlüssel. Der Ableitungsschlüssel erfordert besonderen Schutz.

⌦ **GS-A_3139 Krypto_Schlüssel: Dienst Schlüsselableitung**

Der Anbieter einer Schlüsselverwaltung MUSS sicherstellen, dass der Ableitungsprozess unumkehrbar und nicht vorhersehbar ist (die Kompromittierung eines abgeleiteten Schlüssels darf nicht den Ableitungsschlüssel oder andere abgeleitete Schlüssel kompromittieren).⌫

⌦ **GS-A_3141 Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion**

Der Anbieter einer Schlüsselverwaltung MUSS im Falle des Einsatzes einer Schlüsselableitung (nach [ISO11770]) in seinem Sicherheitskonzept Maßnahmen für das Bekanntwerden von Schwächen des kryptographischen Verfahrens, welche die Grundlage der Schlüsselableitung ist, darlegen.⌫

⌦ **GS-A_3149 Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip**

Der Anbieter einer Schlüsselverwaltung MUSS, falls er kryptographische Schlüssel archiviert, in seinem spezifischen Sicherheitskonzept beschreiben, welcher Schlüssel in welcher Phase in welcher Systemkomponente archiviert wird. Er MUSS sicherstellen, dass die Schlüssel nur an diejenigen Systemkomponenten verteilt werden, in denen ihr Aufenthalt vorgesehen ist und wo sie hinreichend geschützt sind.⌫

3.8 Anforderungen an die Kartenpersonalisierung

Das Erstellen von Karten erfordert verschiedene Produktionsschritte. Dieser Abschnitt enthält Anforderungen an den Produktionsschritt der Kartenpersonalisierung.

⌦ **GS-A_5387 Beachten von Vorgaben bei der Kartenpersonalisierung**

Kartenpersonalisierer MÜSSEN die Vorgaben und Empfehlungen von Kartenherstellern (bspw. Personalisierungsguides) beachten und umsetzen.⌫

4 Anforderungen für die Erstellung für Spezifikationen

Die Anforderungen dieses Abschnittes richten sich an Anbieter bzw. Hersteller, die eine Spezifikation eines Produkttypen der TI erstellen.

Es ist vom Anbieter bzw. Hersteller bei der Erstellung der Spezifikation zu prüfen, ob die Anforderungen dieses Abschnittes für den Produkttyp umsetzbar sind. Falls die Anforderung bzgl. des Produkttyps nicht umsetzbar ist, ist dies nachvollziehbar in einem Anhang zur Spezifikation zu begründen. Falls eine Umsetzung möglich ist, sind die getroffenen Umsetzungsmaßnahmen innerhalb der Spezifikation zum Produkttyp zu dokumentieren.

⌦ **GS-A_2063 Schutz Arzt-Patient-Vertrauensverhältnis**

Die TI MUSS gewährleisten, dass durch ihren Einsatz das Vertrauensverhältnis zwischen Arzt und Patienten in der TI gewährleistet werden kann. ⌫

⌦ **GS-A_2084 Freie Wahl des Leistungserbringers**

Die TI MUSS sicherstellen, dass für den Versicherten unter den in der TI beteiligten Leistungserbringern und Leistungserbringerinstitutionen die freie Wahl besteht. ⌫

⌦ **GS-A_2085 Keine Diskriminierung von Leistungserbringern**

Die TI MUSS sicherstellen, dass keine Leistungserbringer oder medizinischen Institutionen in der TI diskriminiert werden.⌫

⌦ **GS-A_2102 Datenhoheit des Versicherten in der TI**

Die TI MUSS sicherstellen, dass der Versicherte die Datenhoheit über seine personenbezogenen Daten in der TI hat, wobei die konkrete Ausgestaltung der Datenhoheit bzgl. einer Fachanwendung von den rechtlichen Rahmenbedingungen abhängt. ⌫

⌦ **GS-A_2125 Einsatz technischer Maßnahmen zur Umsetzung des Datenschutzes**

Die TI MUSS zur Gewährleistung der Anforderungen des Datenschutzes technische Maßnahmen umsetzen, wenn deren Aufwand gegenüber organisatorischen Maßnahmen in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.⌫

⌦ **GS-A_2128 Verhinderung von Profilbildungen in der TI**

Die TI MUSS durch technische Maßnahmen eine unerlaubte Profilbildung in der TI erschweren bzw. verhindern.⌫

⌦ **GS-A_2130 Einhalten des Erforderlichkeitsprinzips in der TI**

Die TI MUSS sicherstellen, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten in der TI nur entsprechend ihrer Erforderlichkeit erfolgt.⌫

⌦ **GS-A_2136 Datensparsamkeit ist bei der Protokollierung zu beachten**

Die TI MUSS sicherstellen, dass bei der Erzeugung von Protokolldaten das Ziel der Datensparsamkeit berücksichtigt wird.⌫

⌦ **GS-A_2137 Zweckbindung der Protokolldaten**

Die TI MUSS sicherstellen, dass die in der TI erzeugten Protokolldaten nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes in einem datenschutzgerechten Verfahren verwendet werden.⌫

⌦ **GS-A_2140 Produkte der TI müssen praktikabel sein**

Die TI MUSS sicherstellen, dass die Maßnahmen des Datenschutzes der Produkte der TI für deren Nutzer praktikabel sind.⌫

⌦ **GS-A_2141 Maßnahmen zur Wahrnehmung der Betroffenenrechte müssen praktikabel sein**

Die TI MUSS sicherstellen, dass die organisatorischen und technischen Maßnahmen der TI zur Gewährleistung der datenschutzrechtlichen Betroffenenrechte für die Betroffenen praktikabel sind.⌫

⌦ **GS-A_2223 Berücksichtigung des Datenschutz-Schutzzieles der Zweckbindung**

Die TI MUSS sicherstellen, dass das Datenschutz-Schutzziel der Zweckbindung in der gesamten TI im gesamten Lebenszyklus berücksichtigt wird.⌫

⌦ **GS-A_2224 Berücksichtigung des Datenschutz-Schutzzieles der Transparenz**

Die TI MUSS sicherstellen, dass das Datenschutz-Schutzziel der Transparenz in der gesamten TI im gesamten Lebenszyklus berücksichtigt wird.⌫

⌦ **GS-A_2225 Berücksichtigung des Datenschutz-Schutzzieles der Intervenierbarkeit**

Die TI MUSS sicherstellen, dass das Datenschutz-Schutzziel der Intervenierbarkeit in der gesamten TI im gesamten Lebenszyklus berücksichtigt wird.⌫

⌦ **GS-A_2306 Sicherheitsfunktionen (Sicherheitsmaßnahmen) der in der TI eingesetzten Produkte (Produkttypen)**

In der TI eingesetzte Produkte (Produkttypen) MÜSSEN Sicherheitsfunktionen (Sicherheitsmaßnahmen) aufweisen, welche die in ihnen verarbeiteten Informationswerte (Informationsobjekte und Anwendungsprozesse) derart schützen (entlang der Schutzziele), dass höchstens akzeptable Restrisiken (gemäß Risikopolicy der TI) verbleiben.⌫

⌦ **GS-A_2023 Vorrang der Informationssicherheit des Gesamtsystems**

In der TI MUSS bei der Auswahl und Implementierung von Sicherheitsmaßnahmen vorrangig die Informationssicherheit des Gesamtsystems der TI als Zusammenspiel seiner Bestandteile (verschiedener Fachanwendungen und TI-Plattform) gewährleistet werden. ⌫

GS-A_2024 Verhinderung ungewollter Wechselwirkungen zwischen den verschiedenen Fachanwendungen

Die TI MUSS sicherstellen, dass keine Beeinträchtigung der TI durch ungewollte Wechselwirkungen zwischen den verschiedenen Fachanwendungen im Hinblick auf die Sicherheit in der TI erfolgen. ⌫

GS-A_2025 Anwendung des Maximumprinzips bei der Auswahl und Implementierung von Sicherheitsmaßnahmen

In der TI MUSS bei der Auswahl und Implementierung von Sicherheitsmaßnahmen das Maximumprinzip angewendet werden, d.h. die Resistenz (Widerstandsfähigkeit gegen Angriffe) dieser Sicherheitsmaßnahmen in der TI ist an dem jeweils höchsten Sicherheitsniveau (Maximumprinzip) auszurichten. ⌫

Das Maximumprinzip wird in [gemMeth_Schutzbed] erläutert.

GS-A_2026 Zugriffe auf die TI nur von zugelassenen Beteiligten des Gesundheitswesens mittels zugelassener Produkte

Die TI MUSS gewährleisten, dass Zugriffe auf die TI nur von zugelassenen Beteiligten des Gesundheitswesens mittels zugelassener Produkte erfolgen. ⌫

GS-A_2027 Ausschließliche Verwendung zugelassener Produkte

Die TI MUSS sicherstellen, dass in der TI nur zugelassene Produkte verwendet werden können. ⌫

GS-A_2028 Berücksichtigung der Interessen aller an der TI Beteiligten (Mehrseitige Sicherheit)

In der TI MÜSSEN bei der Auswahl und Implementierung von Sicherheitsmaßnahmen die Interessen aller an der TI Beteiligten berücksichtigt und gegeneinander abgewogen werden. ⌫

GS-A_2029 Risikobasierte Sicherheitsbetrachtung für alle Sicherheitsmaßnahmen

In der TI MUSS für alle Sicherheitsmaßnahmen eine risikobasierte Sicherheitsbetrachtung durchgeführt werden. ⌫

GS-A_2030 Akzeptanz von Restrisiken

In der TI KÖNNEN Restrisiken akzeptiert werden, wenn es einen Verantwortlichen gibt, der das Risiko trägt. ⌫

GS-A_2031 Verwendung von Standards und „Best Practices“ bei Sicherheitsmaßnahmen

In der TI MÜSSEN bei der Auswahl und Implementierung von Sicherheitsmaßnahmen vordringlich bereits erprobte und handhabbare Standards und „Best Practices" berücksichtigt werden. ⌫

GS-A_2033 Sicherheitsgutachten vor Aufnahme des Wirkbetriebs

In der TI MÜSSEN alle implementierten Sicherheitsmaßnahmen spätestens vor Aufnahme des Wirkbetriebes (vorzugsweise im Rahmen von Zulassungen) durch unabhängige Sachverständige begutachtet werden. ⌫

GS-A_2034 Meldung von Risiken durch Verursacher an gematik

Der Verursacher einer Abweichung von den Eckpunkten der Informationssicherheit MUSS das daraus resultierende Risiko bewerten und unverzüglich an die gematik melden. ⌫

GS-A_2035 Verantwortung des Verursachers für Risiken und Schäden

Der Verursacher einer Abweichung von den Eckpunkten der Informationssicherheit MUSS die Verantwortung für alle daraus resultierenden Risiken bzw. Schäden tragen. ⌫

5 Organisationen in § 274 Abs. 1 SGB V in der Rolle eines Anbieters

Sofern eine im § 274 Abs. 1 SGB V genannte Organisation, die gemäß § 274 Abs. 1 SGB V regelmäßig durch eine im § 274 Abs. 1 SGB V benannte Stelle geprüft wird, in der Rolle eines Anbieters auftritt, muss sie - unabhängig vom angebotenen Produkt bzw. der angebotenen Anwendung – die Anforderungen aus Tabelle 1 nicht nachweisen.

Tabelle 1 - Anforderungen, die bei einer Prüfung nach § 274 Abs. 1 SGB V, der gematik nicht nachgewiesen werden müssen

GS-A_2065	GS-A_2070	GS-A_2071	GS-A_2072	GS-A_2073	GS-A_2074
GS-A_2075	GS-A_2156	GS-A_2214	GS-A_2333	GS-A_2339	GS-A_2343
GS-A_2355	GS-A_2357	GS-A_2359	GS-A_2360	GS-A_2362	GS-A_5017

Anhang A - Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte(r) für Datenschutz und die Informationsfreiheit
BSI	Bundesamt für Sicherheit in der Informationstechnik
DSM	Datenschutzmanagement
ISM	Informationssicherheitsmanagement
SGB	Sozialgesetzbuch

A2 – Glossar

Das Glossar wird als eigenständiges Dokument, vgl [gemGlossar] zur Verfügung gestellt.

A3 – Tabellenverzeichnis

A4 - Referenzierte Dokumente

A4.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemRL_Betr_TI]	gematik: Übergreifende Richtlinien zum Betrieb der TI
[gemRL_PruefSichEig_DS]	gematik: Richtlinie zur Prüfung der Sicherheitseignung
[gemRL_RiPo_TI]	gematik: Risikopolicy für Informationssicherheitsrisiken in der TI
[gemSpec_ISM]	gematik: Koordinierendes Informationssicherheitsmanagement in der Telematikinfrastruktur
[gemSpec_SiBetrUmg]	gematik: Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Produkte der TI

A4.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ISO/IEC27001]	ISO/IEC 27001:2005 Specification for an Information Security Management System, ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques
[ISO/IEC27002]	ISO/IEC 27002:2005 Code of Practice for Information Security Management ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques
[ISO11770]	ISO/IEC 11770: 1996 Information technology – Security techniques – Key management Part 3: Mechanisms using asymmetric techniques
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2109

Anhang B – Beispiel für die Dokumentation der Äquivalenz bei Verwendung eigener Methoden (informativ)

Entsprechend Anforderung [GS-A_2021] sind vom Anbieter die einheitlichen Methoden zu Datenschutz und Informationssicherheit anzuwenden, um Datenschutz- und Sicherheitskonzepte zu erstellen und zu pflegen oder es ist die Anwendung äquivalenter Methoden nachzuweisen.

Falls der Anbieter äquivalente Methoden nutzt, obliegt es dem Sicherheitsgutachter im Sicherheitsgutachten (vgl. [GS-A_2153]) nachvollziehbar zu dokumentieren, wie die in den einheitlichen Methoden geforderten Inhalte umgesetzt sind.

Im Folgenden erfolgt exemplarisch ein informatives Beispiel, wie die Dokumentation zum Nachweis der Konsistenz erfolgen könnte.

Tabelle 2 - Dokumentation der Äquivalenz der eingesetzten Methoden (INFORMATIV)

einheitliche Methode der gematik	vom Anbieter genutzte äquivalente Methode
Datenschutzkonzeption in der TI [gemMeth_DSKonz]	Der Anbieter hat die gesetzlichen Rahmenbedingungen des Datenschutzes für das von ihm betriebene TI-Produkt in seinem Datenschutzkonzept in *<Abschnitt D.A>* vollständig beschrieben. Im Datenschutzkonzept in *<Abschnitt D.P>* sind alle Anwendungsprozesse inkl. ihrer Zweckbindung dokumentiert, in denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden. In *<Abschnitt D.IO>* erfolgt die vollständige Dokumentation der personenbezogenen Informationsobjekte. Die in der einheitlichen Methode der gematik definierten Datenschutzschutzziele Zweckbindung, Transparenz sowie Intervenierbarkeit sind im Datenschutzkonzept des Anbieters in den Abschnitten *<Abschnitten D.Z, D.T, D.I>* berücksichtigt. In diesen Abschnitten sind die organisatorischen und/oder technischen Maßnahmen zur Gewährleistung dieser Schutzziele beschrieben. Die in den *<Abschnitten D.X, D.Y>* des Datenschutzkonzeptes des Anbieters beschriebenen organisatorischen und/oder technischen Maßnahmen berücksichtigen die in der einheitlichen Methode der gematik definierten Eckpunkte des Datenschutzes.
Schutzbedarfsfeststellung in der TI [gemMeth_Schutzbed]	Der Anbieter nutzte zur Schutzbedarfsfeststellung die *<Methode XY>*. Der Schutzbedarf der Informationsobjekte und Prozesse ist im Sicherheitskonzept des Anbieters im *<Abschnitt X.Y>* durch eine Schadensbetrachtung begründet und dokumentiert. Es wurden dabei alle in den einheitlichen Methoden geforderten Schutzziele der Sicherheit (Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit und Nichtabstreitbarkeit) berücksichtigt. Die in der einheitlichen Methode zur Schutzbedarfsfeststellung definierten Klassifizierungen niedrig, mittel, hoch und sehr hoch entsprechen den Klassifizierungen *<K1, …, Kn>*.

einheitliche Methode der gematik	vom Anbieter genutzte äquivalente Methode
Bedrohungs- und Schwachstellenanalyse in der TI [gemMeth_Bedr]	Der Anbieter nutzte zur Bedrohungs- und Schwachstellenanalyse die <*Methode YZ*>. Eine Analyse der Bedrohungen und Schwachstellen ist im Sicherheitskonzept des Anbieters im <*Abschnitt Y.Z*> dokumentiert. Die Begriffe der Bedrohung und Schwachstelle stimmen in beiden Methoden überein. Die Angriffsszenarien sind im Sicherheitskonzept des Anbieters im <*Abschnitt Y.W*> dokumentiert
Sicherheitsanalyse in der TI [gemMeth_SichAnalyse]	Der Anbieter nutzte zur Sicherheitsanalyse die <*Methode W.Z*>. Eine Dokumentation der Umgebungsannahmen, die der Sicherheitsanalyse zugrunde liegen, ist im Sicherheitskonzept des Anbieters im <*Abschnitt A.B*> dokumentiert. Als Sicherheitsanalysegegenstände nach Definition der einheitlichen Methode werden folgende Systeme des Anbieters betrachtet: <*S1, …, Sn*>. Die Sicherheitsfunktionen und Umgebungsannahmen zum Schutz der Systeme <*S1, …, Sn*> bzgl. der identifizierten Angriffsszenarien sind im Sicherheitskonzept des Anbieters in den <*Abschnitten A, B, C, …*> dokumentiert. Das Ergebnis der Sicherheitsanalyse (d.h. ob die Sicherheitsfunktionen und Umgebungsannahmen ausreichend sind, um alle Angriffe abzuwehren oder ob ein Restrisiko besteht) ist in <*Abschnitt E*> beschrieben.
Risikoanalyse der Sicherheitskonzeption in der TI [gemMeth_Risk]	Der Anbieter nutzte zur Risikoanalyse die <*Methode RM*>. Die identifizierten Risiken, ihre Bewertung und Behandlung sind im Sicherheitskonzept des Anbieters im *{Abschnitt R.I.S}* dokumentiert. Hier ist ebenfalls die Restrisikoakzeptanz dokumentiert. Die in der einheitlichen Methode zur Risikoanalyse definierten Risikobereiche entsprechen im Sicherheitskonzept des Anbieters den folgenden Risikobereichen: <*Abbildung der ggf. unterschiedlichen Risikobereiche*>.
Dokumentation der Berechtigungen in der TI [gemMeth_Berechtig]	Das vom Anbieter verwendete Berechtigungsmodell ist im Sicherheitskonzept des Anbieters im <*Abschnitt B.R*> dokumentiert. Die Akteure und ihre Berechtigungen in den Systemen des Anbieters sind in <*Abschnitt B.B*> beschrieben.
Dokumentation von Schlüsselmaterial in der TI [gemMeth_Schluessel]	Das vom Anbieter verwendete Schlüsselmaterial ist im Sicherheitskonzept des Anbieters im <*Abschnitt S.Y*> dokumentiert. Die in der einheitlichen Methode geforderten Angaben zur Schlüsseldokumentation sind hierbei vollständig beschrieben.