gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

ENTWURF

Version:	1.0.0 CC 2
Revision:	\main\rel_opb1\rel_ors2\7
Stand:	07.12.2017
Status:	Entwurf
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_DS_Anbieter

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um die Erstversion des Dokumentes.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.9.0	18.09.17		Initiale Erstellung	gematik
1.0.0 CC	25.10.17		Kommentierung	
1.0.0 CC 2	07.12.17		zur Abstimmung freigegeben	gematik

ENTWURF

Inhaltsverzeichnis

Dokumentinformationen 2

Inhaltsverzeichnis 3

1 Einordnung des Dokuments 5
1.1 Zielsetzung 5
1.2 Zielgruppe 5
1.3 Geltungsbereich 5
1.4 Abgrenzungen 5
1.5 Methodik 6

2 Modularisierung 7
2.1 Zuordnung der Module zur Informationssicherheit 8
2.2 Zuordnung der Module zum Datenschutz 9
2.3 Regelungen im Anbietervertrag und Steckbriefen 10

3 Module der Informationssicherheit 11
3.1 Modul „Basis-IS“ 11
3.2 Modul „Basis-ISMS“ 12
3.3 Modul „Erweitertes ISMS“ 15
3.4 Modul „TI-Sicherheitsbericht“ 17
3.5 Modul „Erweiterter TI-Sicherheitsbericht“ 18

4 Module des Datenschutzes 21
4.1 Modul „Basis-DS“ 21
4.2 Modul „TI-Datenschutzbericht“ 22
4.3 Modul „Erweiterter TI-Datenschutzbericht“ 23

5 Spezifische Module 26
5.1 Module für weitere Anwendungen 26
5.1.1 Modul „Weitere Anwendungen (mit TI-Beeinträchtigung)“ 27
5.1.2 Modul „Weitere Anwendungen (ohne TI-Beeinträchtigung)“ 29
5.2 Modul „Schlüsselverwaltung“ 29
5.3 Modul „Kartenherausgabe“ 30

ENTWURF

Anhang A – Verzeichnisse 31

A1 – Abkürzungen 31

A2 – Abbildungsverzeichnis 31

A3 – Tabellenverzeichnis 32

A4 – Referenzierte Dokumente 32

A4.1 – Dokumente der gematik 32

A4.2 – Weitere Dokumente 33

Anhang B – Modularisierungskonzept 34

B1 – Anordnung der Module 34

B2 – Kriterien der Modulzuordnung 35

B2.1 – Kriterium: Spezifikationshoheit der gematik 35

B2.2 – Kriterium: Beeinträchtigung der TI 37

Anhang C – Modulzuordnung bei Anwendbarkeit des § 274 Abs. 1 SGB V .. 40

ENTWURF

1 Einordnung des Dokuments

1.1 Zielsetzung

Das Dokument definiert übergreifende Sicherheits- und Datenschutzanforderungen für Anbieter von Diensten der Telematikinfrastruktur (TI), Anbieter von Fachdiensten VSDM gemäß § 291 Abs. 2b SGB V sowie Anbieter weiterer Anwendungen gemäß § 291a Abs. 7 Satz 3 SGB V.

1.2 Zielgruppe

Das Dokument richtet sich an Anbieter von Diensten der Telematikinfrastruktur, Anbieter von Fachdiensten VSDM gemäß § 291 Abs. 2b SGB V sowie Anbieter weiterer Anwendungen gemäß § 291a Abs. 7 Satz 3 SGB V.

1.3 Geltungsbereich

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

Wichtiger 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 Abgrenzungen

Spezifische Datenschutz- und Sicherheitsanforderungen für einzelne Produkttypen sind in den jeweiligen Spezifikationen und Konzepten des Produkttyps festgelegt.

Übergreifende Anforderungen an die Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur sind in [gemSpec_Krypt] festgelegt.

Dieses Dokument enthält keine Anforderungen an Hersteller von Produkten der Telematikinfrastruktur. Diese sind in [gemSpec_Hersteller_SI] festgelegt.

ENTWURF

Dieses Dokument enthält keine Anforderungen an Anbieter von Rechenzentrums-Consumern (vgl. [gemKPT_Arch_TIP]).

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:

⌦ **gemxxxxxx_AFO_0000 <Titel der Afo>**

Text/Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

ENTWURF

2 Modularisierung

Dieses Dokument enthält übergreifende Datenschutz- und Sicherheitsanforderungen an Anbieter von Diensten der TI, Anbieter von Fachdiensten VSDM gemäß § 291 Abs. 2b SGB V sowie an Anbieter weiterer Anwendungen gemäß § 291a Abs. 7 S. 3 SGB V. Der Begriff „Dienste der TI“ umfasst dabei Dienste der TI-Plattform, Dienste der gesetzlichen Anwendungen der eGK nach § 291a Abs. 2 und Abs. 3 SGB V sowie Dienste der sicheren Übermittlungsverfahren nach § 291b Abs. 1e SGB V.

Alle Anforderungen sind in Module unterteilt. Jede Anforderung ist dabei genau einem Modul zugeteilt. Diese Module werden anschließend Anbietern zugeordnet (siehe Abbildung 1). Ist ein Modul einem Anbieter zugeordnet, muss dieser alle Anforderungen des Moduls umsetzen.

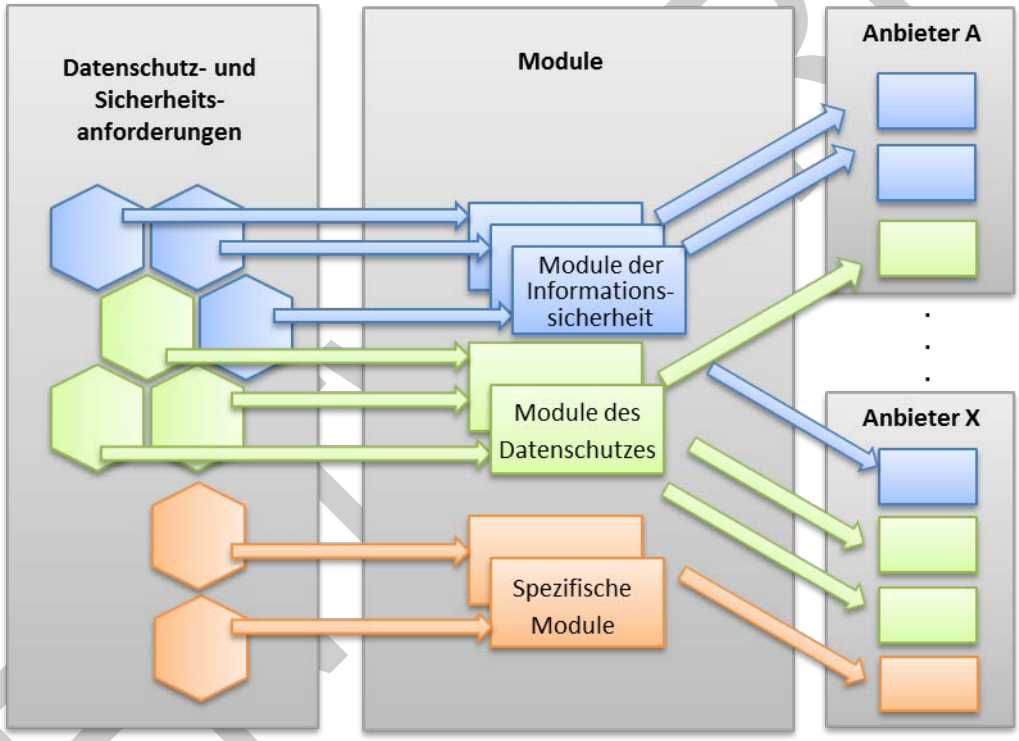

Abbildung 1 – Anforderungen, Module und Anbieter

Abbildung 2 zeigt die Module im Überblick; unterteilt in Module zur Informationssicherheit (blau), zum Datenschutz (grün) sowie spezifische Module (rot). Die Anforderungen der Module sind in den Kapiteln 3, 4 und 5 beschrieben.

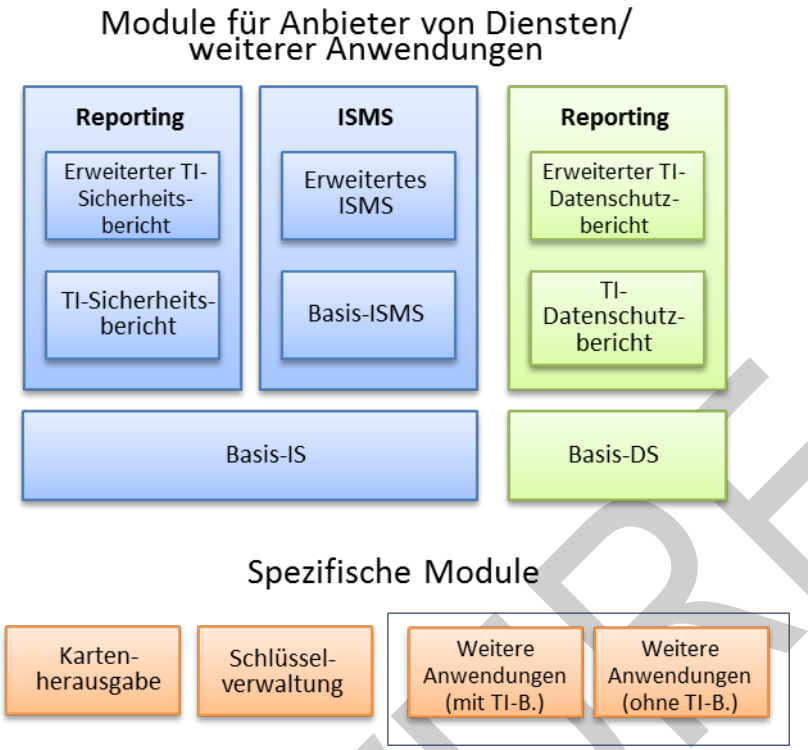

Abbildung 2 – Modulübersicht für Anbietermodule

Die Module zur Informationssicherheit (blau) und zum Datenschutz (grün) sind anbieter-übergreifend, d. h. unabhängig von einer speziellen Rolle des Anbieters.

Darüber hinaus gibt es spezifische Module für Kartenherausgeber, Anbieter von Schlüsselverwaltungen sowie Anbieter weiterer Anwendungen nach § 291a Abs. 7 S. 3 SGB V. Diese Module enthalten Sicherheitsanforderungen, die nur von Anbietern in diesen Rollen zu erfüllen sind.

Im Folgenden bezeichnet der Begriff „weitere Anwendungen“ immer weitere Anwendungen nach § 291a Abs. 7 S. 3 SGB V.

2.1 Zuordnung der Module zur Informationssicherheit

In diesem Abschnitt werden die anbieterübergreifenden Module zur Informationssicherheit Anbietern von Diensten der TI, Anbietern der Fachdienste VSDM und Anbietern weiterer Anwendungen zugeordnet (Abbildung 3).

Bei den Fachdiensten VSDM und weiteren Anwendungen wird unterschieden, ob der Verlust der Sicherheit des Dienstes die Sicherheit oder den Datenschutz der TI beeinträchtigen könnte oder ob dies technisch ausgeschlossen ist. Dies ist abhängig vom technischen Anschlusstyp des Dienstes an die TI.

Die aktuell verfügbaren Anschlusstypen sind der Sichere Zentrale Zugangspunkt (SZZP) und das Sicherheitsgateway Bestandsnetze (SG-BNet). Beim Sicherheitsgateway Bestandsnetze kann eine Beeinträchtigung der TI technisch ausgeschlossen werden, da darüber keine Dienste der TI erreichbar sind. Beim Verlust der Sicherheit eines über einen SZZP an die TI angeschlossenen Dienstes hingegen ist eine Beeinträchtigung der TI technisch nicht ausgeschlossen.

ENTWURF

Derzeit werden die Fachdienste VSDM mittels SZZP an die TI angeschlossen. Daher werden den Fachdiensten VSDM die Module der Zeile „Beeinträchtigt TI“ zugeordnet. Die Zuordnung der Module zu den Fachdiensten VSDM berücksichtigt die Anwendbarkeit des § 274 Abs. 1 SGB V (vgl. Anhang C).

Die gematik prüft, ob ein technischer Anschlusstyp zur Verfügung gestellt werden kann, über den ein Zugriff auf Dienste der TI ermöglicht wird und der gleichzeitig die TI vor Angriffen schützt, um so Sicherheitsanforderungen auf Seiten des Anbieters derart entbehrlich zu machen, dass bestimmte Module zur Sicherheit für den Anbieter entfallen. In den Abbildungen ist dieser intendierte technische Anschlusstyp als „Dienstegateway“ aufgenommen, um das Ziel zu verdeutlichen, welche Module mit dem Dienstegateway im Gegensatz zum Anschluss mittels SZZP entfallen sollen.

Der Verlust der Sicherheit eines Dienstes der TI beeinträchtigt die TI per Definition (daher „nicht anwendbar“ in der Abbildung für Dienste der TI-Plattform, der § 291a-eGK-Anwendungen und der sicheren Übermittlungsverfahren).

Die Produkttypen der TI-Plattform sind in [gemKPT_Arch_TIP] festgelegt.

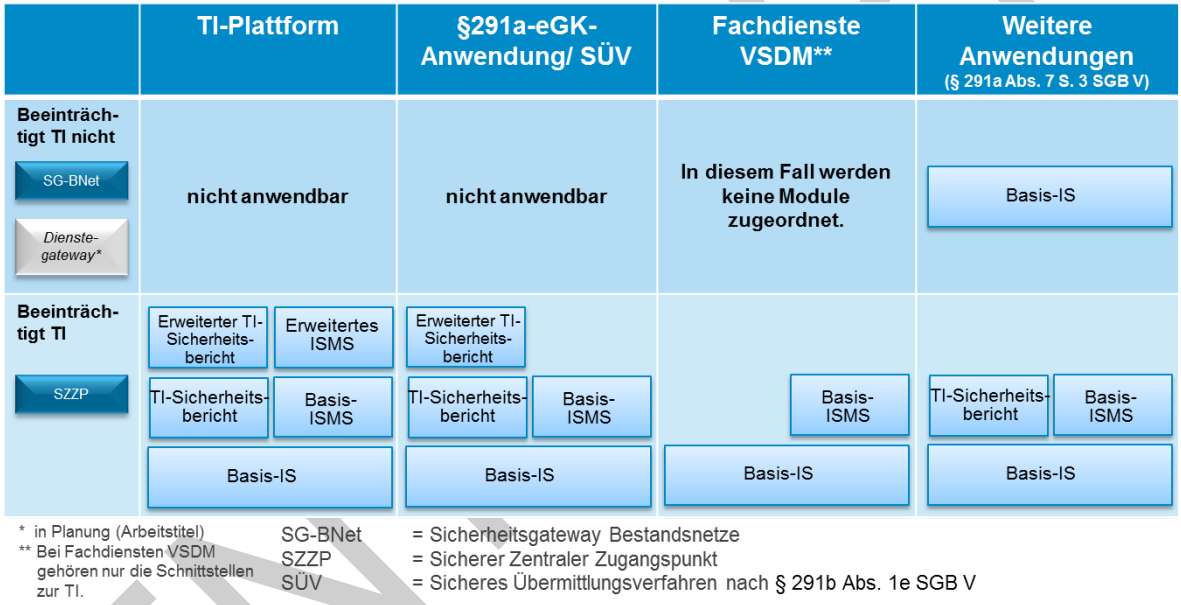

Abbildung 3 – Zuordnung der Module der Informationssicherheit

2.2 Zuordnung der Module zum Datenschutz

Abbildung 4 zeigt die Zuordnung der anbieterübergreifenden Module zum Datenschutz.

Anbietern werden Module zum Datenschutz nur zugeordnet, falls personenbezogene Daten in ihren Diensten verarbeitet werden.

Die Anforderungen der gematik zum Datenschutz konkretisieren die bestehenden Vorschriften zum Datenschutz um TI-spezifische Vorgaben, die aus Sicht der gematik notwendig sind, ihren gesetzlichen Auftrag nach § 291b Abs. 1 SGB V zu erfüllen. Die Anforderungen der gematik ersetzen die bestehenden Vorschriften zum Datenschutz nicht. Diese sind weiterhin von den Anbietern in ihrer eigenen Verantwortung einzuhalten.

EN PDF

	TI-Plattform	§291a-eGK-Anwendung/SÜV	Fachdienste VSDM**	Weitere Anwendungen (§ 291a Abs. 7 S. 3 SGB V)
Beeinträch-tigt TI nicht Sicherheits-gateway *Dienste-gateway**	**nicht anwendbar**	**nicht anwendbar**	**In diesem Fall werden keine Module zugeordnet.**	Basis-DS
Beeinträch-tigt TI SZZP	Erweiterter TI-Datenschutz-bericht TI-Datenschutz-bericht Basis-DS	Erweiterter TI-Datenschutz-bericht TI-Datenschutz-bericht Basis-DS	Basis-DS	TI-Datenschutz-bericht Basis-DS

* in Planung (Arbeitstitel)
** Bei Fachdiensten VSDM gehören nur die Schnittstellen zur TI.

SG-BNet = Sicherheitsgateway Bestandsnetze
SZZP = Sicherer Zentraler Zugangspunkt
SÜV = Sicheres Übermittlungsverfahren nach § 291b Abs. 1e SGB V

Abbildung 4 – Zuordnung der Module zum Datenschutz

2.3 Regelungen im Anbietervertrag und Steckbriefen

Neben den Anforderungen des Datenschutzes und der Informationssicherheit dieses Dokumentes können sich für Anbieter weitere vertragliche Pflichten bzgl. Datenschutz und Informationssicherheit ergeben.

Hierzu gehören insbesondere

- Festlegungen, ob bei Zuordnung des Moduls „Erweitertes ISMS“ zusätzlich eine ISO27001-Zertifizierung gefordert wird und
- Festlegungen zu durch die gematik veranlassten Audits.

Die Art des Nachweises der Anforderungen (Sicherheitsgutachten, Anbietererklärungen) ergibt sich aus dem Steckbrief des Dienstes bzw. der weiteren Anwendung.

ENTWURF

3 Module der Informationssicherheit

Dieses Kapitel beschreibt die Anforderungen der Module zur Informationssicherheit.

3.1 Modul „Basis-IS“

Die Anforderungen dieses Moduls fordern ein grundlegendes Informationssicherheitsmanagement. Vorgaben zu dessen konkreter Ausgestaltung erfolgen jedoch nicht.

⌦ **GS-A_5551 Betriebsumgebung in einem Mitgliedstaat der EU bzw. des EWR**

Der Anbieter MUSS sicherstellen, dass sich die Betriebsumgebung/en der mittels der TI erreichbaren Dienste auf dem Gebiet eines Mitgliedstaates der EU bzw. des EWR befindet/befinden. ⌫

Hinweis: Anbietern von Fachdiensten VSDM wird die Anforderung GS-A_5551 aufgrund gesetzlicher Regelungen im SGB X nicht zugeordnet .

Der Verweis auf den konkreten Paragraphen im SGB X ist noch zu ergänzen.

⌦ **GS-A_5552 Angemessene Sicherheitsmaßnahmen**

Der Anbieter MUSS die erforderlichen technischen Maßnahmen treffen, um die Anforderungen an die Sicherheit des Dienstes der TI bzw. der weiteren Anwendung im Hinblick auf die Schutzbedürftigkeit der im Dienst der TI bzw. in der weiteren Anwendung verarbeiteten Daten zu gewährleisten. ⌫

⌦ **GS-A_5553 Sicherheitskonzept**

Der Anbieter MUSS eine aktuelle und nachvollziehbare Dokumentation besitzen, in der der Schutzbedarf der Daten und die technischen Maßnahmen beschrieben werden, die getroffen wurden, um die Anforderungen an die Sicherheit des Dienstes der TI bzw. der weiteren Anwendung im Hinblick auf die Schutzbedürftigkeit der dort verarbeiteten Daten zu gewährleisten. Es sind zudem die Wirksamkeit der Sicherheitsmaßnahmen hinsichtlich des Schutzbedarfs der verarbeiteten Daten, die Restrisiken, ein Netzstrukturplan und die Maßnahmen zum Notfallmanagement zu dokumentierten.⌫

⌦ **GS-A_5554 Aufrechterhaltung der Informationssicherheit**

Der Anbieter MUSS Prozesse zur Gewährleistung der Informationssicherheit aufbauen und kontinuierlich verbessern. ⌫

⌦ **GS-A_4523-01 Bereitstellung Kontaktinformationen für Informations-sicherheit**

Der Anbieter MUSS im Rahmen des Informationssicherheitsmanagements eine Kommunikationsschnittstelle direkt der gematik mitteilen (übliche Kontaktinformationen wie Name eines Ansprechpartners, Stellvertreter, E-Mailadresse, Telefon, Fax, Anschrift, …).⌫

ENTWURF

⌦ **GS-A_4524-01 Meldung von Änderungen der Kontaktinformationen für Informationssicherheit**

Der Anbieter MUSS Änderungen an der Kommunikationsschnittstelle seines Informationssicherheitsmanagements der gematik unverzüglich direkt melden.⌫

⌦ **GS-A_5555 Unverzügliche Meldung von erheblichen Sicherheitsvorfällen und -notfällen**

Der Anbieter MUSS erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit, die zum Ausfall oder zur Beeinträchtigung der Sicherheit oder Funktionsfähigkeit des Dienstes der TI bzw. eines Dienstes der weiteren Anwendung oder zum Ausfall oder zur Beeinträchtigung der Sicherheit oder Funktionsfähigkeit der Telematikinfrastruktur führen können oder bereits geführt haben, unverzüglich nach bekannt werden direkt der gematik melden.⌫

⌦ **GS-A_5556 Unverzügliche Behebung von erheblichen Sicherheitsvorfällen und -notfällen**

Der Anbieter MUSS bei erheblichen Sicherheitsvorfällen oder Sicherheitsnotfällen, die Dienste der TI bzw. Dienste einer weiteren Anwendung betreffen, unverzüglich Maßnahmen zur Behebung des Vorfalls bzw. Notfalls umsetzen und den erfolgreichen Abschluss direkt an die gematik melden.⌫

Hinweis: ITSM-TI-Teilnehmer melden die erfolgreiche Behebung eines Vorfalls gemäß den Vorgaben des Incident Managements (vgl. [gemRL_Betr_TI]).

3.2 Modul „Basis-ISMS“

Die Anforderungen dieses Moduls richten sich an die Ausgestaltung des ISMS beim Anbieter.

⌦ **GS-A_4980-01 Umsetzung der Norm ISO/IEC 27001**

Der Anbieter MUSS für mindestens genau die Umgebungen, in denen die Dienste der TI bzw. die weiteren Anwendungen betrieben werden, die internationale Norm ISO/IEC 27001 umsetzen.⌫

Hinweis: Falls Anbieter direkt von der gematik beauftragt werden, kann zusätzlich eine ISO 27001-Zertifizierung mit einem Geltungsbereich, der den betriebenen Dienst der TI und die unterstützenden Systeme umfasst, gefordert werden.

⌦ **GS-A_4981-01 Erreichen der Ziele der Norm ISO/IEC 27001 Annex A**

Der Anbieter MUSS für mindestens genau die Umgebungen, in denen die Dienste der TI bzw. die weiteren Anwendungen betrieben werden, zu allen gemäß der Erklärung der Anwendbarkeit (engl. „Statement of Applicability“) anwendbaren Maßnahmen (engl. „controls“) der internationalen Norm ISO/IEC 27001 ergreifen und die dort angegebenen Ziele (engl. „objectives“) erreichen. ⌫

⌦ **GS-A_4982-01 Umsetzung der Maßnahmen der Norm ISO/IEC 27002**

Der Anbieter SOLL für mindestens genau die Umgebungen, in denen die Dienste der TI bzw. die weiteren Anwendungen betrieben werden, beim Ergreifen der Maßnahmen (engl. „controls“) aus der internationalen Norm ISO/IEC 27002 die

ENTWURF

dort angegebene „Anleitung zur Umsetzung“ (engl. „implementation guidance“) und die dort angegebenen „Weiteren Informationen“ (engl. „other information“) befolgen.⌫

Hinweis: Der Nachweis der Umsetzung der Anforderungen GS-A_4980, GS-A_4981 und GS-A_4982 kann durch Vorlage eines ISO27001-Zertifikats, welches den Geltungsbereich des Dienstes der TI bzw. der weiteren Anwendung und der unterstützenden Systeme umfasst, erfolgen.

⌦ **GS-A_4983-01 Umsetzung der Maßnahmen aus dem BSI-Grundschutz**

Der Anbieter SOLL für mindestens genau die Umgebungen, in denen die Dienste der TI bzw. die weiteren Anwendungen betrieben werden, bei der Umsetzung der internationalen Normen ISO/IEC 27001 und ISO/IEC 27002 die anwendbaren Anforderungen des BSI-Grundschutzkompendiums oder entsprechende Maßnahmen, die ein vergleichbares Sicherheitsniveau gewährleisten, umsetzen.⌫

Hinweis: Der Anbieter muss aufgrund der Anforderung GS-A_4983 neben der nativen ISO 27001 Vorgehensweise nicht die Grundschutzvorgehensweise (BSI Standard 200-X) umsetzen. Eine zusätzliche Dokumentation ist aufgrund der Anforderung nicht erforderlich. Das BSI Grundschutzkompendium beschreibt zu erreichende Sicherheitsanforderungen detaillierter als die Normen ISO 27001 und ISO 27002. Hierdurch soll eine gemeinsame Baseline anhand des BSI Grundschutzkompendiums über das erforderliche Sicherheitsniveau und die Angemessenheit von Maßnahmen erlangt werden. Beispielsweise wird es einem Sicherheitsgutachter hierdurch erleichtert, die Angemessenheit von getroffenen Sicherheitsmaßnahmen besser einzuschätzen.

⌦ **GS-A_3737-01 Sicherheitskonzept**

Der Anbieter MUSS die von ihm betriebenen Dienste der TI bzw. weiteren Anwendungen in seine bestehende Sicherheitskonzeption einbinden oder ein betreiberspezifisches Sicherheitskonzept erstellen. Folgende Inhalte MÜSSEN vom Anbieter mindestens dokumentiert werden:

- Beschreibung des Dienstes der TI bzw. der weiteren Anwendung bzgl. der Informationssicherheitsaspekte,
- Schutzbedarf der Daten,
- Bedrohungsanalyse,
- Dokumentation und Beschreibung der Erfüllung der Sicherheitsanforderungen der gematik,
- Sicherheitsanalyse (Verifikation der Wirksamkeit der Sicherheitsmaßnahmen),
- Erstellung einer Restrisikoabschätzung.⌫

⌦ **GS-A_3753-01 Notfallkonzept**

Der Anbieter MUSS die von ihm betriebenen Dienste der TI bzw. weiteren Anwendungen in seine bestehende Notfallkonzeption einbinden oder ein betreiberspezifisches Notfallkonzept erstellen. Folgende Inhalte MÜSSEN mindestens dokumentiert werden:

ENTWURF

- übergeordnete Notfallstrategie und Einordnung der Dienste der TI bzw. der weiteren Anwendungen,
- gesetzliche und vertragliche Anforderungen,
- Rollen und Verantwortliche in Bezug auf das Notfall-Management,
- Dokumentation zur Notfallvorsorge inkl. durchgeführter Auswirkungsanalyse (BIA oder vergleichbar),
- szenariounabhängige Notfallbewältigungsstrategie (Hierbei ist insbesondere auch die TI-spezifische Eskalation zu weiteren Anbietern und zur gematik zu beschreiben.),
- Dokumentation der szenariospezifischen Notfallpläne (Hierbei sind neben allgemeinen Notfallplänen für Brand und Wassereinbruch etc. insbesondere auch TI-spezifische Notfallszenarien wie der Ausfall verfügbarkeitskritischer TI-Produkte, Schwächung oder Kompromittierung von kryptographischen Schlüsselmaterial etc. zu dokumentieren.)
- Nachbereitung von Notfällen,
- Prävention und Vorbeugung von Notfällen, inklusive Fachkunde und Schulungen.⌫

⌦ **GS-A_3772-01 Notfallkonzept: Der Dienstanbieter soll dem BSI-Standard 100-4 folgen**

Der Anbieter SOLL bei der Erstellung seines Notfallkonzeptes den inhaltlichen Vorgaben des Dokuments BSI-Standard 100-4 „Notfallmanagement" [BSI 100-4] folgen. ⌫

⌦ **GS-A_2328-01 Pflege und Fortschreibung des Sicherheitskonzeptes und Notfallkonzeptes**

Der Anbieter MUSS die Pflege und Fortschreibung der Sicherheits- und Notfallkonzepte für die von ihm betriebenen Dienste der TI bzw. weiteren Anwendungen durchführen. ⌫

⌦ **GS-A_2329-01 Umsetzung der Sicherheitskonzepte**

Der Anbieter MUSS die Maßnahmen zur Sicherheit des Personals, der Organisation, der Infrastruktur und der eingesetzten Technologien entsprechend der erstellten Sicherheitskonzepte umsetzen und dokumentieren; wozu insbesondere die Implementierung und Einhaltung von organisatorischen und technischen Sicherheitsmaßnahmen und die Kommunikation sowie Durchführung von Sensibilisierungen für den Themenbereich „Informationssicherheit“ und Schulungen gehören. ⌫

⌦ **GS-A_2345-01 regelmäßige Reviews**

Der Anbieter MUSS regelmäßige Reviews seiner bestehenden Sicherheitskonzepte inkl. der organisatorischen und technischen Sicherheitsmaßnahmen durchführen und die sich daraus ergebenen Verbesserungspotenziale umsetzen. ⌫

ENTWURF

⌦ **GS-A_2158-01 Informationstechnische Trennung von Umgebungen mit Echtdaten**

Der Anbieter MUSS sicherstellen, dass die Produktivumgebung der TI des Anbieters (Umgebung mit Echtdaten) informationstechnisch von Testumgebungen getrennt ist. ⌫

Hinweis: Dies bedeutet insbesondere, dass in Testumgebungen keine Echtdaten der TI oder kryptographische Identitäten bzw. Schlüssel der Produktivumgebung der TI verwendet werden dürfen. Genauso dürfen aber auch keine kryptographischen Identitäten bzw. Schlüssel aus Testumgebungen in der Produktivumgebung der TI genutzt werden.

⌦ **GS-A_2160-01 Nachweispflicht der informationstechnischen Trennung**

Der Anbieter MUSS die Wirksamkeit der informationstechnischen Trennung der Produktivumgebung der TI des Anbieters von Testumgebungen nachweisen können. ⌫

Hinweis: Anbietern von Fachdiensten VSDM werden die Anforderungen GS-A_2158-01 und GS-A_2160-01 aufgrund gesetzlicher Regelungen im SGB X nicht zugeordnet.

Der Verweis auf den konkreten Paragraphen im SGB X ist noch zu ergänzen.

⌦ **GS-A_4984-01 Befolgen von herstellerspezifischen Vorgaben**

Der Anbieter SOLL für die von ihm betriebenen Dienste der TI bzw. der weiteren Anwendungen herstellerspezifische Sicherheitsvorgaben und -empfehlungen befolgen.⌫

⌦ **GS-A_2331-01 Sicherheitsvorfalls-Management**

Der Anbieter MUSS Sicherheitsvorfälle („security incidents“) wirksam vorbeugen, diese aufdecken und unterbinden.⌫

⌦ **GS-A_2355-01 Meldung von erheblichen Schwachstellen und Bedrohungen**

Der Anbieter MUSS erhebliche Schwachstellen und erhebliche Bedrohungen, die Dienste der TI bzw. Dienste einer weiteren Anwendung betreffen, unverzüglich nach bekannt werden und direkt an die gematik melden. ⌫

⌦ **GS-A_2332-01 Notfallmanagement**

Der Anbieter MUSS die durch Notfälle aufgetretenen Schäden zeitnah durch entsprechende Maßnahmen seines Notfallmanagements korrigieren. ⌫

Spezialisierung von Anforderungen des Moduls Basis-IS

Das Modul Basis-ISMS spezialisiert die Anforderungen GS-A_5552, GS-A_5553 und GS-A_5554 des Moduls Basis-IS. Werden die Anforderungen des Moduls Basis-ISMS umgesetzt, so auch diese Anforderungen des Moduls Basis-IS. Daher werden die Anforderungen GS-A_5552, GS-A_5553 und GS-A_5554 nicht den Anbietern zugeordnet, denen das Modul Basis-ISMS zugeordnet ist.

3.3 Modul „Erweitertes ISMS“

Von Anbietern, denen das Modul „Erweitertes ISMS“ zugeordnet ist, wird eine enge Zusammenarbeit mit dem CERT der gematik hinsichtlich der Erkennung, Analyse,

ENTWURF

Bewertung und dem Umgang von Sicherheitsvorfällen, Schwachstellen, Bedrohungen und Risiken erwartet. Die folgenden Anforderungen konkretisieren diese Notwendigkeit.

⌦ **GS-A_2343-01 eigene Audits**

Der Anbieter MUSS zur Überprüfung der etablierten Sicherheitsmaßnahmen regelmäßige und ggf. anlassbezogene Audits planen und durchführen.⌫

⌦ **GS-A_5557 Security Monitoring**

Der Anbieter MUSS im Rahmen eines Security Monitoring präventive Maßnahmen zur Erkennung und Analyse von Bedrohungen (z. B. über Korrelation und Auswertung von Log-Daten) durchführen. ⌫

Hinweis: Die durch den Anbieter auszuwertenden Informationen (z. B. Log-Daten der Kommunikationsverbindungen und anwendungsnaher Dienste) sind mit der gematik vor Betriebsaufnahme und im Rahmen der Einführung neuer Produkte und bei Änderungen an bestehenden Produkten abzustimmen.

⌦ **GS-A_5558 Aktive Schwachstellenscans**

Der Anbieter MUSS im Rahmen seines Schwachstellenmanagements mindestens monatliche Schwachstellenscans oder vergleichbare Maßnahmen zur Erkennung und Analyse von technischen Schwachstellen („vulnerabilities“) in den vom ihm betriebenen Dienst der TI bzw. der weiteren Anwendung durchführen. ⌫

Hinweis: Als vergleichbar werden Maßnahmen angesehen, die eine kontinuierliche technisch unterstützte Erkennung von Schwachstellen gewährleisten (z.B. durch Inspektion der auf Systemen laufenden Dienste und Abgleich gegen aktuelle Schwachstelleninformationen).

⌦ **GS-A_5559 Bereitstellung Ergebnisse von Schwachstellenscans**

Der Anbieter MUSS der gematik die Detailergebnisse von durchgeführten Schwachstellenscans oder der vergleichbaren Maßnahmen zur Erkennung und Analyse von technischen Schwachstellen monatlich zur Verfügung stellen. ⌫

Hinweis: Der genaue Detailgrad, das zu verwendende Format und die einzuhaltenden Sicherheitsmaßnahmen für die Übergabe der bereitzustellenden Ergebnisse sind vor Betriebsaufnahme und im Rahmen der Einführung neuer Produkte und bei Änderungen an bestehenden Produkten mit der gematik abzustimmen.

⌦ **GS-A_5017-01 Meldung und Behandlung von Schwachstellen**

Der Anbieter MUSS die gematik unverzüglich und direkt über Schwachstellen in den von ihnen betriebenen Diensten der TI bzw. weiteren Anwendungen informieren und sich mit der gematik anhand einer Einzelfallbetrachtung und -bewertung der Schwachstelle hinsichtlich der einzuleitenden Maßnahmen und der Behebungszeit abstimmen.⌫

⌦ **GS-A_5560 Entgegennahme und Prüfung von Meldungen der gematik**

Der Anbieter MUSS von der gematik übermittelte Meldungen zu Schwachstellen, Bedrohungen und Sicherheitsvorfällen annehmen, bewerten und die erforderlichen Maßnahmen mit der gematik abstimmen und umsetzen. ⌫

⌦ **GS-A_5561 Bereitstellung 24/7-Kontaktpunkt**

ENTWURF

Der Anbieter MUSS der gematik einen Kontaktpunkt benennen, über den der Anbieter jederzeit sicherheitsrelevante Meldungen der gematik entgegennehmen kann, um eine unverzügliche Bearbeitung und Reaktion zu gewährleisten.⌫

⌦ **GS-A_5562 Bereitstellung Produktinformationen**

Der Anbieter MUSS der gematik halbjährlich eine aktuelle Liste aller zur Leistungserbringung von Diensten der TI verwendeten Hard- und Softwareprodukte sowie dem zugehörigen TI Produkttyp übermitteln. ⌫

Hinweis: Die zur Verfügung gestellten Produktinformationen (z.B. Betriebssystem, eingesetzte Webserver, Datenbanken, Netzwerkkomponenten inkl. jeweils aktueller Version) dienen dazu, bei Schwachstellen und Sicherheitsvorfällen die Sicherheitslage der TI besser einschätzen zu können und mit Anbietern gezielt Maßnahmen zur Beseitigung der Schwachstellen zeitnah abstimmen zu können.

Der Detailgrad und das zu verwendende Format der bereitzustellenden Liste der Produktinformationen sind vor Betriebsaufnahme und im Rahmen der Einführung neuer Produkte und bei Änderungen an bestehenden Produkten mit der gematik abzustimmen.

3.4 Modul „TI-Sicherheitsbericht“

⌦ **GS-A_5563 Jahressicherheitsbericht (kurz)**

Der Anbieter MUSS sicherstellen, dass der gematik jährlich ein Sicherheitsbericht vorliegt (spätestens bis Ende Januar des Folgejahres), der mindestens folgende Inhalte hat:

- allgemeine Anbieterinformationen (einschl. Kontaktinformationen des anbieterinternen Informationssicherheitsmanagements)
- allgemeiner Überblick des Sicherheitsstatus der vom Anbieter betriebenen Dienste der TI bzw. weiteren Anwendungen (einschl. sicherheitsrelevanter Erkenntnisse aufgrund gesetzlicher Änderungen, des technischen Fortschritts oder veränderter Bedrohungslage)
- Übersicht der im Jahreszeitraum aufgetretenen Sicherheitsvorfälle und Notfälle bzgl. der Dienste der TI bzw. weiteren Anwendungen des Anbieters (unabhängig von Kritikalität und Ad-Hoc-Meldepflicht)
- Übersicht der im Jahreszeitraum erkannten Schwachstellen bzgl. der Dienste der TI bzw. weiteren Anwendungen des Anbieters (inkl. geplanter risikomindernder Maßnahmen und des Umsetzungsstatus)
- Übersicht der im Jahreszeitraum eigenverantwortlich durchgeführten Audits (Management Summary)
- Handlungsempfehlungen und Entscheidungsbedarf auf Seiten der gematik. ⌫

⌦ **GS-A_4530-01 Maßnahmen zur Behebung von erheblichen Sicherheitsvorfällen und Notfällen**

ENTWURF

Der Anbieter MUSS sich bei erheblichen Sicherheitsvorfällen und Notfällen mit der gematik hinsichtlich der Maßnahmen und deren Umsetzung abstimmen sowie deren erfolgreichen Abschluss direkt der gematik melden.⌫

⌦ **GS-A_4532-01 Nachweis der Umsetzung von Maßnahmen in Folge eines erheblichen Sicherheitsvorfalls oder Notfalls**

Der Anbieter MUSS der gematik auf Anfrage die Umsetzung der Maßnahmen zur Behebung eines erheblichen Sicherheitsvorfalls oder Notfalls, z. B. in Form von zur Verfügung gestellten Dokumentationen, neuen Regelungen oder Prozessen sowie anhand von Auszügen aus der Konfiguration oder Logdaten, nachweisen.⌫

⌦ **GS-A_5324-01 Teilnahme des Anbieters an Sitzungen des kISMS**

Der Anbieter MUSS der gematik zusichern, dass der Anbieter das koordinierende Informationssicherheitsmanagementsystem (kISMS) der gematik unterstützt, indem auf Einladung der gematik ein Sicherheitsbeauftragter des Anbieters am Arbeitskreis Datenschutz und Informationssicherheit (AK DIS) teilnimmt, der sich im Rahmen seiner beruflichen Tätigkeit mit dem operativen Betrieb der vom Anbieter betriebenen Dienste befasst. ⌫

3.5 Modul „Erweiterter TI-Sicherheitsbericht“

Anbieter, denen das Modul „Erweiterter TI-Sicherheitsbericht“ zugeordnet ist, müssen der gematik Quartalsberichte und einen Jahresbericht zur Sicherheit übermitteln.

Die Quartalssicherheitsberichte umfassen die jeweiligen Erfassungszeiträume 1.1. bis 31.3. (Q1), 1.4. bis 30.6. (Q2) und 1.7. bis 30.9. (Q3). Für das vierte Quartal 1.10. bis 31.12. (Q4) ist kein separater Quartalssicherheitsbericht zu erstellen. Diese Quartal ist im Jahressicherheitsbericht zu erfassen.

Der Jahressicherheitsbericht umfasst den Zeitraum vom 1.1. bis 31.12. eines Jahres.

⌦ **GS-A_4507-01 Quartalsweiser Sicherheitsbericht**

Der Anbieter MUSS sicherstellen, dass der gematik für das erste, zweite und dritte Quartal ein Sicherheitsbericht vorliegt (jeweils bis spätestens zum Ende des Folgemonats nach Ablauf des Quartals), der mindestens folgende Inhalte hat:

- allgemeine Anbieterinformationen (einschl. Kontaktinformationen des anbieterinternen Informationssicherheitsmanagements)
- allgemeiner Überblick des Sicherheitsstatus der vom Anbieter betriebenen Dienste der TI (einschl. sicherheitsrelevanter Erkenntnisse aufgrund gesetzlicher Änderungen, des technischen Fortschritts oder veränderter Bedrohungslage)
- Übersicht der im Quartal aufgetretenen Sicherheitsvorfälle und Notfälle bzgl. der Dienste der TI des Anbieters (unabhängig von Kritikalität und Ad-Hoc-Meldepflicht)
- Übersicht der erkannten Schwachstellen bzgl. der Dienste der TI des Anbieters (inkl. geplanter risikomindernder Maßnahmen und des Umsetzungsstatus).

ENTWURF

- Handlungsempfehlungen und Entscheidungsbedarf auf Seiten der gematik.⌫

Sind einem Anbieter die Module „TI-Sicherheitsbericht“ und „Erweiterter TI-Sicherheitsbericht“ zugeordnet, ist nur der jährliche Sicherheitsbericht des Moduls „Erweiterter TI-Sicherheitsbericht“ (s. Afo GS-A_4508-01) zu erstellen, da der jährliche Sicherheitsbericht des Moduls „Erweiterter TI-Sicherheitsbericht“ alle Inhalte des jährlichen Sicherheitsberichtes des Moduls „TI-Sicherheitsbericht“ (s. Afo GS-A_5563) enthält.

⌦ **GS-A_4508-01 Jährlicher Sicherheitsbericht**

Der Anbieter MUSS gewährleisten, dass der gematik jährlich (spätestens bis Ende Januar des Folgejahres) ein Jahressicherheitsbericht bzgl. der vom Anbieter angebotenen Produkte der TI vorliegt, der zum einen die Inhalte eines Quartalssicherheitsberichts bezogen auf das gesamte Berichtsjahr und zusätzlich mindestens folgende Inhalte enthält:

- die Anzahl und durchschnittliche Dauer der Informationssicherheitsschulungen der Mitarbeiter, die sich mit den Diensten der TI befassen,
- die durchschnittliche Reaktionszeit (Zeitraum zwischen interner Erfassung und Weiterleitung der Meldung an die gematik) und durchschnittliche Lösungszeit (Zeitraum zwischen interner Erfassung und Abschluss des Tickets) der Sicherheitsvorfälle. Hier sind nur die Incidents zu betrachten, die einen Bezug zu Diensten der TI haben.
- den durchschnittlichen Schweregrad der erfassten Schwachstellen gemäß Common Vulnerability Scoring System (CVSS), die einen Bezug zu Diensten der TI des Anbieters haben,
- die durchschnittliche Reaktionszeit der meldepflichtigen Schwachstellen (Zeitraum zwischen interner Erfassung und Weiterleitung der Meldung an die gematik) und die durchschnittliche Lösungszeit der Schwachstellen der meldepflichtigen Schwachstellen (Zeitraum zwischen interner Erfassung und Abschluss des Tickets). Hier sind nur die Schwachstellen zu betrachten, die einen Bezug zu Diensten der TI des Anbieters haben,
- die Anzahl aller im Änderungsmanagement des Anbieters behandelten und durchgeführten Änderungen, die Dienste der TI des Anbieters betreffen,
- die Anzahl aller im Änderungsmanagement des Anbieters behandelten und als sicherheitsrelevant gekennzeichneten durchgeführten Änderungen, die die Dienste der TI des Anbieters betreffen. Sowie
- die Anzahl der durchgeführten Notfallübungen, die die Dienste der TI des Anbieters betreffen, deren durchschnittliche Übungsdauer sowie deren Inhalt (Scope).⌫

⌦ **GS-A_4526-01 Aufbewahrungsvorgaben an die Nachweise zu den im Sicherheitsbericht gemachten Angaben**

ENTWURF

Der Anbieter MUSS geeignete Nachweise zu den in Sicherheitsberichten zur Verfügung gestellten Angaben mindestens ein Jahr, nachdem dieser Bericht bei bei der gematik eingegangen ist, vorhalten, um bei einem Informationssicherheitsaudit die Richtigkeit der gemachten Angaben belegen zu können. ⌫

ENTWURF

4 Module des Datenschutzes

Dieses Kapitel beschreibt die Anforderungen der Module zum Datenschutz.

4.1 Modul „Basis-DS“

⌦ **GS-A_2076-01 kDSM: Datenschutzmanagement nach BSI**

Der Anbieter MUSS ein Datenschutzmanagement nach Baustein CON.2 des IT-Grundschutz-Kompendiums umsetzen.⌫

⌦ **GS-A_5564 kDSM: Ansprechpartner für Datenschutz**

Der Anbieter MUSS der gematik eine Kommunikationsschnittstelle für Datenschutz (übliche Kontaktinformationen, wie Name eines Ansprechpartners, Stellvertreter, E-Mail-Adresse, Telefon, Fax, Anschrift, …) mitteilen.⌫

Hinweis: Bei der in GS-A_5564 geforderten Kommunikationsschnittstelle muss es sich nicht notwendigerweise um den betrieblichen Datenschutzbeauftragten handeln.

⌦ **GS-A_4479-01 kDSM: Meldung von Änderungen der Kontaktinformationen zum Datenschutzmanagement**

Der Anbieter MUSS der gematik Änderungen der Kontaktinformationen seines Datenschutzmanagements unverzüglich mitteilen.⌫

⌦ **GS-A_4473-01 kDSM: Unverzügliche Benachrichtigung bei Verstößen gemäß Art. 34 DSGVO**

Der Anbieter MUSS jeden Datenschutzverstoß, der die Voraussetzungen für eine Benachrichtigung der Betroffenen nach Art. 34 DSGVO erfüllt und der sich auf die vom Anbieter betriebenen Dienste der TI bzw. weiteren Anwendungen nach § 291a Abs. 7 S. 3 SGB V bezieht, unverzüglich nach bekannt werden der gematik zusammen mit folgenden Informationen melden:

- Die nach Art. 33 Abs. 3 DSGVO geforderten Informationen. Falls ein Verstoß nach Art. 34 DSGVO vorliegt, ist zudem die nach Art. 33 Abs. 1 DSGVO an die Aufsichtsbehörde gesendete Meldung notwendig.
- Eine Information darüber, ob der Verstoß bei einem Auftragsverarbeiter erfolgte.⌫

Hinweis: Die vorstehende Anforderung knüpft an den Inhalt der DSGVO unabhängig von deren Anwendbarkeit an. Gleiches gilt für nachstehende Anforderungen, in denen auf Voraussetzungen der DSGVO verwiesen wird.

⌦ **GS-A_5565 Unverzügliche Behebung von Verstößen gemäß Art. 34 DSGVO**

Der Anbieter MUSS im Fall von Datenschutzverstößen, die die Voraussetzungen für eine Benachrichtigung der Betroffenen nach Art. 34 DSGVO erfüllen und die sich auf die vom Anbieter betriebenen Dienste der TI bzw. weiteren Anwendungen

ENTWURF

beziehen, unverzüglich Maßnahmen zur Behebung des Verstoßes umsetzen und den erfolgreichen Abschluss unverzüglich an die gematik melden.⌫

Hinweis: ITSM-TI-Teilnehmer melden die erfolgreiche Behebung eines Verstoßes gemäß den Vorgaben des Incident Managements (vgl. [gemRL_Betr_TI]).

4.2 Modul „TI-Datenschutzbericht“

⌦ **GS-A_4468-01 kDSM: Jährlicher Datenschutzbericht (kurz)**

Der Anbieter MUSS gewährleisten, dass der gematik jährlich (spätestens bis Ende Januar des Folgejahres) ein Jahresdatenschutzreport bzgl. der vom Anbieter angebotenen Dienste der TI bzw. weiteren Anwendungen vorliegt, der mindestens folgende Inhalte enthält:

- allgemeine Anbieterinformationen einschl. Kontaktinformationen des anbieterinternen Datenschutzmanagements (wie Name des betrieblichen Datenschutzbeauftragten bzw. eines Ansprechpartners, Stellvertreter, E-Mail-Adressen, Telefonnummern, Anschrift, …) sowie Angabe der für den Anbieter zuständigen datenschutzrechtlichen Aufsichtsbehörde,
- eine Übersicht über die Anzahl der aufgetretenen Datenschutzverstöße, die die Voraussetzungen nach Art. 83 Abs. 4, 5 und 6 DSGVO erfüllen, bei denen Dienste der TI bzw. weitere Anwendungen betroffen waren; hierbei ist jeweils anzugeben, gegen welche Bestimmung verstoßen wurde,
- eine Übersicht über die Anzahl der aufgetretenen Verletzungen des Schutzes personenbezogener Daten, die die Voraussetzungen gemäß Art. 33 und 34 DSGVO erfüllen, bei denen Dienste der TI bzw. weitere Anwendungen betroffen waren,
- eine Übersicht über die Anzahl der von Betroffenen gestellten Anfragen zur Wahrnehmung der Betroffenenrechte aufgeschlüsselt nach Art. 15 (Auskunft), Art. 16 (Berichtigung), Art. 17 (Löschung), Art. 18 (Einschränkung), Art. 20 (Datenübertragbarkeit) und Art. 21 (Widerspruch) DSGVO, bezogen auf Dienste der TI bzw. weitere Anwendungen. Sofern die DSGVO nicht anwendbar ist, sind die vorstehenden Angaben entsprechend bereitzustellen,
- eine Übersicht über die Anzahl der von Betroffenen bei der Aufsichtsbehörde eingereichten Beschwerden gem. Art. 77 DSGVO, die den Anbieter als Betreiber eines Dienstes der TI bzw. weiteren Anwendung betreffen.⌫

Hinweis: Im jährlichen Datenschutzbericht der TI ist jeweils nur die Anzahl der Datenschutzverstöße, Anfragen bzw. Beschwerden zu nennen, nicht jedoch deren Inhalte.

Neben dem Jahresdatenschutzreport ist im Falle gravierender Datenschutzverstöße die erfolgreiche Umsetzung der Maßnahmen zur Behebung des Verstoßes der gematik zu melden.

ENTWURF

⌦ **GS-A_4478-01 kDSM: Nachweis der Umsetzung von Maßnahmen in Folge eines gravierenden Datenschutzverstoßes**

Der Anbieter MUSS der gematik auf Anfrage die Umsetzung der Maßnahmen zur Behebung eines Datenschutzverstoßes, der die Voraussetzungen für eine Benachrichtigung der Betroffenen nach Art. 34 DSGVO erfüllt und der sich auf die vom Anbieter betriebenen Dienste der TI bzw. weiteren Anwendungen bezieht, unter zur Verfügungstellung einer Dokumentation mit den in Art. 33 Abs. 5 DSGVO geforderten Inhalten nachweisen.⌫

⌦ **GS-A_5324-02 kDSM: Teilnahme des Anbieters an Sitzungen des kDSM**

Der Anbieter MUSS der gematik zusichern, dass der Anbieter das koordinierende Datenschutzmanagementsystem der gematik unterstützt, indem auf Einladung der gematik ein sachkundiger Ansprechpartner für Datenschutz des Anbieters am Arbeitskreis Datenschutz und Informationssicherheit (AK DIS) teilnimmt, der sich im Rahmen seiner beruflichen Tätigkeit mit dem operativen Betrieb der vom Anbieter betriebenen Dienste befasst.⌫

4.3 Modul „Erweiterter TI-Datenschutzbericht“

Sind einem Anbieter die Module „TI-Datenschutzbericht“ und „Erweiterter TI-Datenschutzbericht“ zugeordnet, ist nur der im Modul „Erweiterter TI-Datenschutzbericht“ geforderte Datenschutzbericht (GS-A_4468-02) zu erstellen.

⌦ **GS-A_4468-02 kDSM: Jährlicher Datenschutzbericht der TI**

Der Anbieter MUSS gewährleisten, dass der gematik jährlich (spätestens bis Ende Januar des Folgejahres) ein Jahresdatenschutzreport bzgl. der vom Anbieter angebotenen Dienste der TI vorliegt, der mindestens folgende Inhalte enthält:

- allgemeine Anbieterinformationen einschl. Kontaktinformationen des anbieterinternen Datenschutzmanagements (wie Name des betrieblichen Datenschutzbeauftragten bzw. eines Ansprechpartners, Stellvertreter, E-Mail-Adressen, Telefonnummern, Anschrift, …) sowie Angabe der für den Anbieter zuständigen datenschutzrechtlichen Aufsichtsbehörde,
- eine Liste der Verarbeitungsvorgänge nach Art. 35 Abs. 4 DSGVO mit Bezug zu Diensten der TI, für die eine Datenschutz-Folgenabschätzung durchgeführt wurde inkl. der Bewertung der Risiken gemäß Art. 35 Abs. 7 Buchstabe c) DSGVO,
- eine Übersicht über die getroffenen technischen und organisatorischen Maßnahmen zur Umsetzung der Grundsätze für die Verarbeitung personenbezogener Daten entsprechend Art. 5 DSGVO,
- eine Übersicht über die Umsetzung der technischen und organisatorischen Maßnahmen entsprechend Art. 32 DSGVO zum Schutz der personenbezogenen Daten in den Diensten der TI,
- eine Übersicht der durchgeführten Audits mit thematischem Inhalt, bei denen Dienste der TI betroffen waren,

ENTWURF

- eine Übersicht über die Anzahl der aufgetretenen Datenschutzverstöße, die die Voraussetzungen nach Art. 83 Abs. 4, 5 und 6 DSGVO erfüllen, bei denen Dienste der TI betroffen waren; hierbei ist jeweils anzugeben, gegen welche Bestimmung verstoßen wurde,
- eine Übersicht über die Anzahl der aufgetretenen Verletzungen des Schutzes personenbezogener Daten, die die Voraussetzungen gemäß Art. 33 und 34 DSGVO erfüllen, bei denen Dienste der TI betroffen waren,
- eine Übersicht über die Anzahl der von Betroffenen gestellten Anfragen zur Wahrnehmung der Betroffenenrechte aufgeschlüsselt nach Art. 15 (Auskunft), Art. 16 (Berichtigung), Art. 17 (Löschung), Art. 18 (Einschränkung), Art. 20 (Datenübertragbarkeit) und Art. 21 (Widerspruch) DSGVO, bezogen auf Dienste der TI. Sofern die DSGVO nicht anwendbar ist, sind die vorstehenden Angaben entsprechend bereitzustellen,
- den Anteil der fehlerhaft adressierten Datenschutz-Anfragen (d. h. Anfragen, für die der Anbieter nicht Verantwortlicher ist) im Verhältnis zur Gesamtzahl der Datenschutz-Anfragen bzgl. der im Verantwortungsbereich des Anbieters liegenden Dienste der TI**,**
- eine Übersicht über die durchschnittliche Bearbeitungszeit von korrekt an den Anbieter im Berichtszeitraum adressierten Datenschutz-Anfragen bzgl. der Dienste der TI (Zeitspanne vom Eingang der Anfrage beim Anbieter bis zum Abschluss des Vorgangs beim Anbieter),
- eine Übersicht über die Anzahl der gemäß Art. 14 und Art. 19 DSGVO erteilten Auskünfte ggü. Betroffenen bezogen auf Dienste der TI. Sofern die DSGVO nicht anwendbar ist, sind die vorstehenden Angaben entsprechend bereitzustellen,
- eine Übersicht über die Anzahl der von Betroffenen eingereichten Beschwerden gem. Art. 77 DSGVO, die den Anbieter als Betreiber eines Dienstes der TI betreffen,
- eine Liste der Auftragsverarbeiter, die Dienste der TI betreiben; zusätzlich ggf. für jeden Auftragsverarbeiter die von ihm beauftragten weiteren Auftragsverarbeiter,
- eine Übersicht der durchgeführten Schulungen der Mitarbeiter zum Datenschutz (Dauer, thematische Inhalte),
- eine Selbsteinschätzung, ob es Umsetzungsprobleme mit den Anforderungen des Datenschutzes der TI bzgl. der vom Anbieter betriebenen Dienste der TI gibt.⌫

Die im Datenschutzreport genannten Auftragsverarbeiter sind jährlich vom Anbieter zu kontrollieren.

⌦ **GS-A_2214-01 kDSM: Anbieter müssen jährlich die Auftragsverarbeiter kontrollieren**

Falls der Anbieter Auftragsverarbeiter i.S. des Art. 4 Nr. 8 DSGVO beauftragt hat, MUSS er sich jährlich bei den beauftragten Auftragsverarbeitern von der

ENTWURF

Einhaltung der von den Auftragsverarbeitern getroffenen Maßnahmen überzeugen.⌫

⌦ **GS-A_5566 kDSM: Sicherstellung der Datenschutzanforderungen in Unterbeauftragungsverhältnissen**

Der Anbieter MUSS im Falle von Unterbeauftragungen einzelner oder mehrerer Leistungen an Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO in den Unterbeauftragungsverträgen sicherstellen, dass die datenschutzrechtlichen Pflichten, die er zu beachten hat, im gleichen Maße von den Unterauftragnehmern erfüllt werden. Dies gilt gleichermaßen für weitere Unterbeauftragungsverhältnisse.⌫

ENTWURF

5 Spezifische Module

Kapitel 3 und 4 enthalten anbieterübergreifende Module, die unabhängig von einer speziellen Rolle des Anbieters sind. Dieses Kapitel beschreibt die Module für Anbieter in spezifischen Rollen (vgl. spezifische Module (rot) in Abbildung 2). Die spezifischen Module werden Anbietern zusätzlich zu den anbieterübergreifenden Modulen zugeordnet.

5.1 Module für weitere Anwendungen

Anbietern weiterer Anwendungen nach § 291a Abs. 7 S. 3 SGB V wird neben den anbieterübergreifenden Modulen der Informationssicherheit aus Kapitel 3 und des Datenschutzes aus Kapitel 4 auch das spezifische Modul „Weitere Anwendungen (ohne TI-Beeinträchtigung)“ bzw. das Modul „Weitere Anwendungen (mit TI-Beeinträchtigung)“ zugeordnet.

Das Modul „Weitere Anwendungen (ohne TI-Beeinträchtigung)“ ist für Anbieter relevant, bei denen technisch ausgeschlossen ist, dass der Verlust der Sicherheit ihrer Dienste die Sicherheit der TI beeinträchtigen können.

Das Modul „Weitere Anwendungen (mit TI-Beeinträchtigung)“ ist für Anbieter relevant, bei denen technisch nicht ausgeschlossen werden kann, dass sie die Sicherheit der TI beeinträchtigen könnten.

Die Richtlinie für weitere Anwendungen [gemRL_NvTIwA] unterscheidet die folgenden Anwendungskategorien für weitere Anwendungen:

- Andere Anwendungen des Gesundheitswesens (aAdG),
- Andere Anwendungen des Gesundheitswesens mit Zugriff auf Dienste der TI aus angeschlossenen Netzen des Gesundheitswesens (aAdG-NetG-TI),
- Andere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens (aAdG-NetG).

Die aAdG und aAdG-NetG-TI könnten die TI, aufgrund der Anbindungstechnik ihrer Dienste an die TI, beeinträchtigen. Bei den aAdG-NetG ist eine Beeinträchtigung aufgrund der Anbindungstechnik an die TI technisch ausgeschlossen.

Anbieter von aAdG und aAdG-NetG-TI sind daher „Anbieter weiterer Anwendungen mit Beeinträchtigung der TI“ und ihnen wird das Modul „Weitere Anwendungen (mit TI-Beeinträchtigung)“ zugeordnet. Anbieter von aAdG-NetG sind „Anbieter weiterer Anwendungen ohne Beeinträchtigung der TI“, denen das Modul „Weitere Anwendungen (ohne TI-Beeinträchtigung)“ zugeordnet wird.[1]

Abbildung 5 zeigt alle Module der Informationssicherheit für weitere Anwendungen im Überblick.

[1] Die Art der Anbindungstechnik für weitere Anwendungen an die TI wird von der gematik geprüft, mit dem Ziel, die Anbindung für weitere Anwendungen zu vereinfachen und die Sicherheitsanforderungen an die Anbieter zu reduzieren. Ziel ist es, dass auch den aAdG und aAdG-NetG-TI das Modul „Weitere Anwendungen (ohne TI-Beeinträchtigung)“ zugeordnet werden kann.

ENTWURF

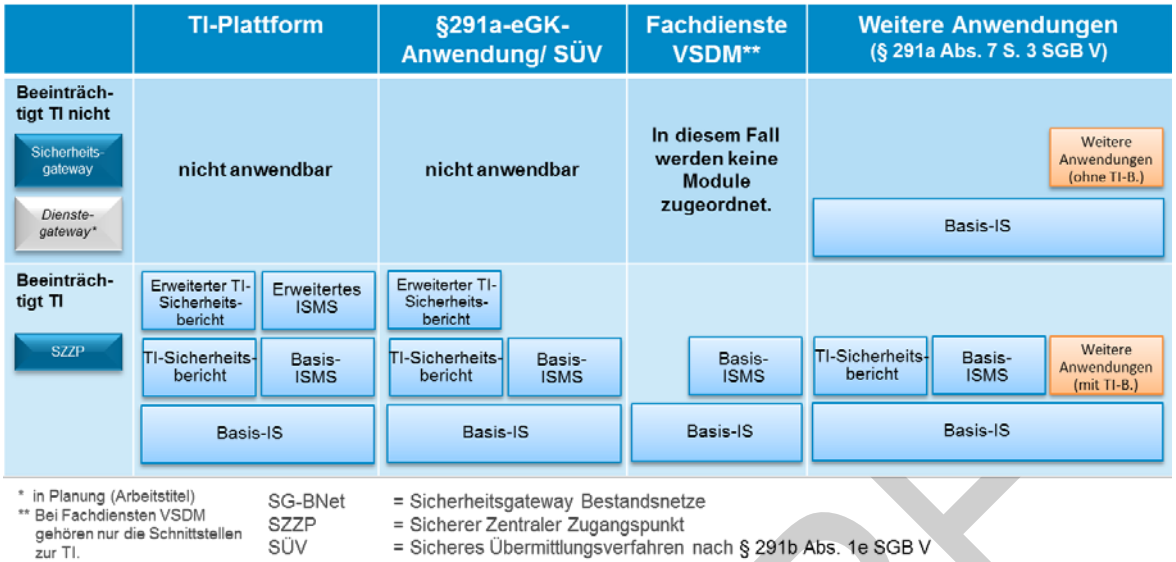

Abbildung 5 – Module für weitere Anwendungen

5.1.1 Modul „Weitere Anwendungen (mit TI-Beeinträchtigung)“

Die Anforderungen des spezifischen Moduls „Weitere Anwendungen (mit TI-Beeinträchtigung)“ gewährleisten eine zulässige Nutzung der Zentralen Dienste der TI durch die weiteren Anwendungen.

⌦ **GS-A_5567 Nutzung Zentraler Dienste der TI nur durch bestätigte Anwendungen**

Ein Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS durch technisch-organisatorische Maßnahmen gewährleisten, dass ausschließlich die bestätigten Anwendungen bestimmte, festgelegte Zentrale Dienste der TI nutzen können.⌫

Hinweis: Die Anforderung GS-A_5567 verbietet insbesondere auch eine reine Proxyfunktion im Sinne der Zurverfügungstellung der Schnittstellen zu den Diensten der TI-Plattform für Dienste, die nicht im Bestätigungs- bzw. Zulassungsumfang enthalten sind.

⌦ **GS-A_5568 Keine Weitergabe von Daten Zentraler Dienste der TI an nicht bestätigte oder zugelassene Anwendungen**

Der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS durch technisch-organisatorische Maßnahmen gewährleisten, dass von Zentralen Diensten der TI zur Verfügung gestellte personenbezogene Daten weder unverändert noch geändert an nicht bestätigte oder nicht zugelassene Anwendungen weitergegeben werden.⌫

⌦ **GS-A_5569 Sicherung der Netzgrenzen**

Der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS ggf. vorhandene Netzgrenzen derart sichern, dass außerhalb der Netzgrenzen nicht auf die TI zugegriffen werden kann.⌫

⌦ **GS-A_5570 Kein Zugriff auf gekoppelte Netze**

ENTWURF

Der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS durch technisch-organisatorische Maßnahmen gewährleisten, dass ggf. an die Netzgrenzen des Bestätigungsumfangs gekoppelte Netze nicht von Nutzern der TI erreichbar sind.⌫

⌦ **GS-A_5571 keine Fälschung von IP-Adressen**

Der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS sicherstellen, dass in allen Netzsegmenten, die zur Verbindung der bestätigten oder zugelassenen Dienste mit dem Netzübergang zur Telematikinfrastruktur genutzt werden, Adressinformationen in IP-Paketen unverändert bleiben und es nicht möglich ist, IP-Pakete mit falschen Adressinformationen einzuschleusen. ⌫

Hinweis: Die Anforderung GS-A_5571 soll unter anderem IP-Spoofing verhindern.

⌦ **GS-A_5572 Sichere Speicherung privater Schlüssel für TI-Identitäten**

Der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS die ihm zugeordneten privaten asymmetrischen Schlüssel von Identitäten der Telematikinfrastruktur sicher speichern, so dass der Schlüssel während der Speicherung insbesondere nicht unautorisiert ausgelesen, unautorisiert verändert, unautorisiert ersetzt oder in anderer Weise unautorisiert benutzt werden kann.⌫

⌦ **GS-A_5573 Qualität der X.509-Identität des Dienstes der Anwendung**

Der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS sicherstellen, dass die zum Komponentenzertifikat gehörende X.509-Identität des Dienstes der weiteren Anwendung die Vorgaben für X.509-Identitäten aus [gemSpec_Krypt] erfüllt.⌫

⌦ **GS-A_5574 Kryptographische Verfahren bei Anbietern mit Beeinträchtigung der TI**

Falls der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI kryptographische Verfahren zum Schutz personenbezogener medizinischer Daten verwendet, MÜSSEN die Vorgaben aus [gemSpec_Krypt] eingehalten werden.⌫

Die folgende Anforderung legt die Auditrechte der gematik für Anbieter weiterer Anwendungen mit Beeinträchtigung der TI fest. Sie entspricht inhaltlich den vertraglich festgelegten Auditrechten der gematik bei Anbietern von Diensten der TI.

⌦ **GS-A_5575 Auditrechte der gematik**

Der Anbieter weiterer Anwendungen mit Beeinträchtigung der TI MUSS zusichern, dass die gematik oder ein von ihr zur Geheimhaltung verpflichteter Bevollmächtigter berechtigt sind,

- pro Kalenderjahr maximal ein Regelaudit durchzuführen. Hiervon unbenommen ist das Recht der gematik, anlassbezogene Audits durchzuführen,
- im Rahmen eines Audits beim Anbieter die konkrete Umsetzung der an den Anbieter gestellten Anforderungen der TI zum Datenschutz und der Informationssicherheit zu überprüfen,
- im Rahmen eines Audits während der üblichen Geschäftszeiten die Geschäftsräume des Anbieters zu betreten,

ENTWURF

- im Rahmen eines Audits alle für das Audit benötigten Informationen zur Verfügung gestellt zu bekommen und insbesondere die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte zu erhalten.

Dies hat der Anbieter im gleichen Maße für Unterauftragnehmer zuzusichern. Die Kosten, die dem Anbieter durch diese Mitwirkungspflichten entstehen, trägt der Anbieter selbst. ⌫

5.1.2 Modul „Weitere Anwendungen (ohne TI-Beeinträchtigung)“

Das spezifische Modul „Weitere Anwendungen (ohne TI-Beeinträchtigung)“ enthält folgende Anforderungen.

⌦ **GS-A_5576 Regelmäßiger Nachweis von Datenschutz- und Sicherheit**

Der Anbieter weiterer Anwendungen ohne Beeinträchtigung der TI MUSS der Zulassungsstelle der gematik alle drei Jahre schriftlich mitteilen, dass in allen Anwendungen des Anbieters, die mittels der TI nutzbar sind, die Datenschutz- und Sicherheitsanforderungen des für die Anwendungen geltenden Produktsteckbriefes umgesetzt sind, die Vorschriften zum Datenschutz eingehalten werden und die Anforderungen an die Sicherheit der Anwendungen gewährleistet ist.⌫

⌦ **GS-A_5577 Erklärung bei Änderungen am Bestätigungsobjekt**

Der Anbieter weiterer Anwendungen ohne Beeinträchtigung der TI MUSS bei Änderungen am Objekt der Bestätigung, die der Zulassungsstelle der gematik angezeigt werden müssen, schriftlich mitteilen, dass durch die Änderungen weiterhin die Vorschriften zum Datenschutz eingehalten werden und die Anforderungen an die Sicherheit gewährleistet sind.⌫

⌦ **GS-A_5578 Kryptographische Verfahren bei Anbietern ohne Beeinträchtigung der TI**

Falls der Anbieter weiterer Anwendungen ohne Beeinträchtigung der TI kryptographische Verfahren zum Schutz personenbezogener medizinischer Daten verwendet, MÜSSEN die Vorgaben aus [gemSpec_Krypt] eingehalten werden.⌫

5.2 Modul „Schlüsselverwaltung“

Dieses Modul ist nur von Anbietern umzusetzen, die eine Schlüsselverwaltung anbieten.[2]

⌦ **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 nachweisen (z. B. durch dokumentierte Notfallübungen, Ablaufprotokolle von abgewickelten Vorfällen).⌫

[2] Die betroffenen zentralen Produkttypen sind CVC-Root, gematik Root-CA, Intermediär VSDM, Namensdienst, TSP CVC, TSP X.509 nonQES (HBA, SMC-B, gSMC, FD, ZD), TSL-Dienst, Fachdienst KOM-LE.

ENTWURF

⌦ **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.⌫

⌦ **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 zu einer Kompromittierung des Ableitungsschlüssels oder anderer abgeleiteter Schlüssel führen.).⌫

⌦ **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.⌫

5.3 Modul „Kartenherausgabe“

Dieses Modul ist von Anbietern umzusetzen, die Karten herausgeben. Die Anforderungen des Moduls sind in [gemSpec_PINPUK_TI, gemSpec_CAN_TI] beschrieben.

ENTWURF

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
aAdG	Andere Anwendungen des Gesundheitswesens
aAdG-NetG	Andere Anwendungen des Gesundheitswesens ohne Zugriff auf Dienste der TI in angeschlossenen Netzen des Gesundheitswesens
aAdG-NetG-TI	Andere Anwendungen des Gesundheitswesens mit Zugriff auf Dienste der TI aus angeschlossenen Netzen des Gesundheitswesens
BIA	Business Impact Analyse
DS	Datenschutz
DSMS	Datenschutzmanagementsystem
eGK	elektronische Gesundheitskarte
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
IS	Informationssicherheit
ISMS	Informationssicherheitsmanagementsystem
kDSM	koordinierendes Datenschutzmanagementsystem
RU	Referenzumgebung
SGB	Sozialgesetzbuch
SG-BNet	Sicherheitsgateway Bestandsnetze
sÜv	sicheres Übermittlungsverfahren
TI	Telematikinfrastruktur
TU	Testumgebung

A2 – Abbildungsverzeichnis

Abbildung 1 – Anforderungen, Module und Anbieter 7
Abbildung 2 – Modulübersicht für Anbietermodule 8
Abbildung 3 – Zuordnung der Module der Informationssicherheit 9
Abbildung 4 – Zuordnung der Module zum Datenschutz 10
Abbildung 5 – Module für weitere Anwendungen 27
Abbildung 6 – Modulübersicht für Anbietermodule 34
Abbildung 7 – Auswirkungen des § 274 SGB V auf die Modulzuordnung (grau = entfällt) 40

ENTWURF

A3 – Tabellenverzeichnis

Tabelle 1 – Modulzuordnung bzgl. der Spezifikationshoheit der gematik 35
Tabelle 2 – Modulzuordnung bzgl. der Möglichkeit, die TI zu beeinträchtigen.....38

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
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemRL_Betr_TI]	gematik: Übergreifende Richtlinien zum Betrieb der TI
[gemRL_NvTIwA]	gematik: Richtlinie – Nutzungsvoraussetzungen der TI für weitere Anwendungen des Gesundheitswesens sowie für die Gesundheitsforschung
[gemSpec_CAN_TI]	gematik: Übergreifende Spezifikation CAN-Policy
[gemSpec_Hersteller_SI]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen an Hersteller
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_PINPUK_TI]	gematik: Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur

ENTWURF

A4.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[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

ENTWURF

Anhang B – Modularisierungskonzept

Kapitel 3 und 4 ordnen die anbieterübergreifenden Module den Anbietern von Diensten der TI, Anbieter von Fachdiensten VSDM gemäß § 291 Abs. 2b SGB V sowie Anbieter weiterer Anwendungen gemäß § 291a Abs. 7 Satz 3 SGB V zu. In diesem Anhang wird dargestellt, nach welchem Schema die Module angeordnet sind und nach welchen Kriterien die Zuordnung der Module zu den Anbietern erfolgt.

B1 – Anordnung der Module

Die Module zur Informationssicherheit und zum Datenschutz sind jeweils in Säulen angeordnet, die auf einem Basis-Modul („Basis-IS“ für Informationssicherheit, „Basis-DS“ für Datenschutz) aufsetzen.

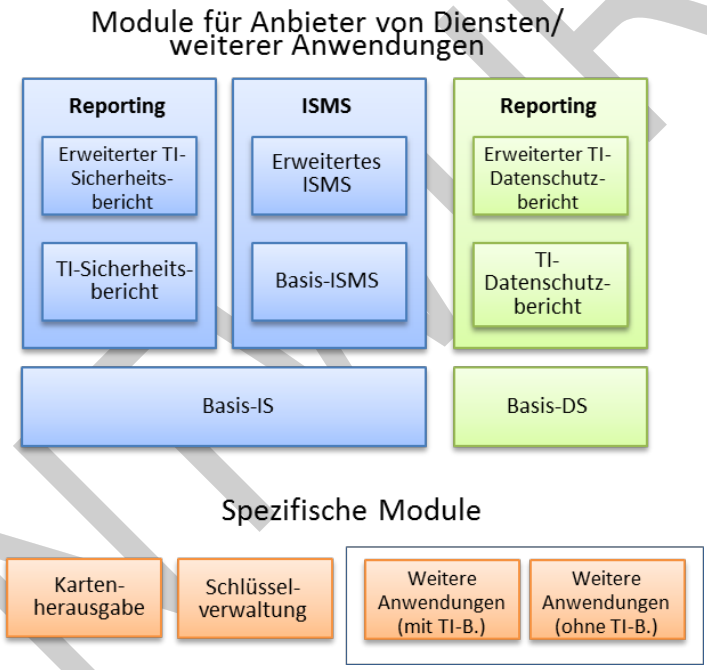

Abbildung 6 – Modulübersicht für Anbietermodule

Wird einem Anbieter ein Modul einer Säule zugeordnet, so gelten für ihn auch alle darunter liegenden Module der Säule. Wird einem Anbieter beispielsweise das Modul „Erweitertes ISMS“ zugeordnet, so gelten für ihn auch die darunter liegenden Module „Basis-ISMS“ und „Basis-IS“.

Für die Informationssicherheit gibt es eine Säule zur Etablierung eines Informationssicherheitsmanagementsystems und eine Säule zum Reporting an die gematik. Für den Datenschutz gibt es nur die Säule zum Reporting. Die Basis-Module enthalten jeweils die Minimalanforderungen zum Managementsystem und zu Meldepflichten.

ENTWURF

B2 – Kriterien der Modulzuordnung

Die Zuordnung der anbieterübergreifenden Module zur Informationssicherheit und des Datenschutzes in Abbildung 3 und Abbildung 4 erfolgt anhand der beiden folgenden Kriterien.

- **Spezifikationshoheit der gematik**, d. h., ist die gematik gesetzlich verantwortlich für die Spezifikation?
- **Beeinträchtigung des Datenschutzes oder der Sicherheit der TI**, d. h., kann der Verlust der Sicherheit oder des Datenschutzes des Dienstes den Datenschutz oder die Sicherheit der TI beeinträchtigen?

Es werden einem Anbieter alle anbieterübergreifenden Module zur Informationssicherheit und zum Datenschutz zugeordnet, die sich für ihn aus diesen beiden Kriterien ergeben.

B2.1 – Kriterium: Spezifikationshoheit der gematik

Die Spezifikationshoheit der gematik unterscheidet sich bei Diensten der TI, den Fachdiensten VSDM und weiteren Anwendungen nach § 291a Abs. 7 S.3 SGB V. Tabelle 1 zeigt die Zuordnung der Module der Informationssicherheit und des Datenschutzes anhand dieses Kriteriums.

Tabelle 1 – Modulzuordnung bzgl. der Spezifikationshoheit der gematik

Anbieter			Module
gematik-Spezifikationshoheit (Dienste der TI)	**zentrale TI-Plattform**	Der Anbieter betreibt einen Dienst der zentralen TI-Plattform. Die Dienste der zentralen TI-Plattform werden von der gematik spezifiziert.	Module Informationssicherheit ☒ Basis-IS ☒ Basis-ISMS ☐ Erweitertes ISMS ☒ TI-Sicherheitsbericht ☒ Erweiterter TI-Sicherheitsbericht Module Datenschutz ☒ Basis-DS☒ TI-Datenschutz-bericht ☒ Erweiterter TI-Datenschutzbericht
	eGK-Anwendung/ sÜv	Der Anbieter betreibt einen Dienst einer eGK-Anwendung oder eines sicheren Übermittlungsverfahrens (sÜv). Dienste der eGK-Anwendungen und der sÜv werden von der gematik spezifiziert.	Module Informationssicherheit ☒ Basis-IS ☒ Basis-ISMS ☐ Erweitertes ISMS ☒ TI-Sicherheitsbericht ☒ Erweiterter TI-Sicherheitsbericht Module Datenschutz ☒ Basis-DS ☒ TI-Datenschutzbericht ☒ Erweiterter TI-Datenschutzbericht
k e i –	**Fachdienste**	Der Anbieter betreibt einen Fachdienst	Module Informationssicherheit

ENTWURF

	VSDM	VSDM gemäß § 291 Abs. 2b SGB V. Die Fachdienste VSDM und deren Spezifikation fallen nicht in den gesetzlichen Aufgabenbereich der gematik gemäß § 291b Abs. 1 SGB V.	☐ Basis-IS ☐ Basis-ISMS ☐ Erweitertes ISMS ☐ TI-Sicherheitsbericht ☐ Erweiterter TI-Sicherheitsbericht Module Datenschutz ☐ Basis-DS ☐ TI-Datenschutzbericht ☐ Erweiterter TI-Datenschutzbericht
	weitere Anwend-ungen	Der Anbieter betreibt eine weitere Anwendung gemäß § 291a Abs. 7 Satz 3 SGB V. Weitere Anwendungen werden nicht von der gematik spezifiziert.	Module Informationssicherheit ☒ Basis-IS ☐ Basis-ISMS ☐ Erweitertes ISMS ☐ TI-Sicherheitsbericht ☐ Erweiterter TI-Sicherheitsbericht Module Datenschutz ☒ Basis-DS ☐ TI-Datenschutzbericht ☐ Erweiterter TI-Datenschutzbericht

Dienste der TI

Für Dienste der TI erstellt die gematik die funktionalen und technischen Vorgaben, legt den Inhalt und die Struktur der Datensätze für deren Bereitstellung und Nutzung fest, erstellt die Vorgaben für einen sicheren Betrieb der TI und überwacht ihre Umsetzung (§ 291b Abs. 1 SGB V).

Die gematik spezifiziert für Dienste der TI insbesondere die Maßnahmen, mit denen der Datenschutz und die Informationssicherheit gewährleistet werden. Die korrekte Umsetzung dieser Maßnahmen durch den Anbieter stellt sicher, dass in der TI die Vorschriften zum Datenschutz eingehalten und ein angemessenes Sicherheitsniveau in den Diensten der TI gewährleistet wird (vgl. § 291b Abs. 1 SGB V).

Anbietern von Diensten der TI werden sämtliche Module des Datenschutzes und, mit Ausnahme des Moduls „Erweitertes ISMS“, sämtliche Module der Informationssicherheit zugeordnet. Diese Module gewährleisten eine sichere Betriebsumgebung beim Anbieter.

Fachdienste VSDM

Die Fachdienste VSDM und deren Spezifikation fallen nicht in den gesetzlichen Aufgabenbereich der gematik gemäß § 291b Abs. 1 SGB V. Die gematik ist insbesondere nicht gesetzlich damit beauftragt – anders als bei den weiteren Anwendungen in § 291a Abs. 7 Satz 3 Nr. 2 SGB V – die Einhaltung der Vorschriften des Datenschutzes und ein angemesseses Sicherheitsniveau im Hinblick auf die Schutzbedürftigkeit der in den Fachdiensten VSDM verarbeiteten Daten zu gewährleisten. Die Fachdienste VSDM gehören nicht zur TI. Lediglich die Schnittstellen der Fachdienste VSDM sind Teil der TI.

Anbietern von Fachdiensten VSDM werden daher aufgrund des Kriteriums der „Spezifikationshoheit der gematik“ keine Module der Informationssicherheit oder des Datenschutzes zugeordnet.

Weitere Anwendungen

Weitere Anwendungen nach § 291a Abs. 7 Satz 3 SGB V werden nicht von der gematik spezifiziert. Der gesetzliche Auftrag der gematik beschränkt sich bzgl. der Spezifikation darauf, zu gewährleisten, dass nur weitere Anwendungen die TI nutzen, die die

ENTWURF

Vorschriften zum Datenschutz einhalten und ein angemessenes Sicherheitsniveau bzgl. ihrer Anwendung bieten (vgl. § 291a Abs. 7 Satz 3 Nr. 2 SGB V). Insbesondere spezifiziert die gematik keine Maßnahmen des Datenschutzes und der Informationssicherheit zum Schutz der Anwendungsdaten.

Es werden die Module „Basis-IS“ und „Basis-DS“ zugeordnet, um gemäß § 291a Abs. 7 Satz 3 Nr. 2 SGB V sicherzustellen, dass die Anbieter die Vorschriften zum Datenschutz und die Anforderungen der Informationssicherheit in ihrer weiteren Anwendung einhalten.

B2.2 – Kriterium: Beeinträchtigung der TI

Dieses Kriterium unterscheidet die Anbieter danach, ob der Verlust der Sicherheit ihres Dienstes den Datenschutz oder die Sicherheit der TI beeinträchtigen kann. Tabelle 2 zeigt die Zuordnung der Module nach diesem Kriterium.

Es werden einem Anbieter nach diesem Kriterium keine Module zugeordnet, falls die Dienste des Anbieters so an die TI angeschlossen werden, dass eine Beeinträchtigung der Sicherheit der TI durch den Verlust der Sicherheit des Dienstes technisch ausgeschlossen ist.

Diensten der TI werden alle Module des Datenschutzes und der Informationssicherheit, mit Ausnahme des Moduls „Erweitertes ISMS“, zugeordnet, da der Verlust der Sicherheit eines Dienstes der TI die Sicherheit der TI per Definition beeinträchtigt.

Das Modul „Erweitertes ISMS“ ist nur von Anbietern der Dienste der zentralen TI-Plattform umzusetzen, da die Aufrechterhaltung von Sicherheit und Datenschutz bei diesen Diensten von besonderer Bedeutung für alle Teilnehmer der TI ist. Sie werden daher gemäß dem Modul „Erweitertes ISMS“ stärker bzgl. der Sicherheit kontrolliert.

Kann für einen Dienst einer weiteren Anwendung eine Beeinträchtigung der TI nicht technisch ausgeschlossen werden, so werden auch dem Anbieter der weiteren Anwendung alle Module zugeordnet, mit Ausnahme der Module „Erweitertes ISMS“, „Erweiterter TI-Sicherheitsbericht“ und „Erweiterter TI-Datenschutzbericht“. Das Modul „Erweitertes ISMS“ wird nicht zugeordnet, da die Dienste der weiteren Anwendung, anders als Dienste der TI-Plattform, nicht von allen Teilnehmern der TI genutzt werden. Für weitere Anwendungen sind die Berichte der Module „TI-Sicherheitsbericht“ und „TI-Datenschutzbericht“ ausreichend zur Erfüllung des gesetzlichen Auftrags der gematik.

Bei den Fachdiensten VSDM wird – analog zu den Diensten der weiteren Anwendungen – bei der Zuordnung der Module berücksichtigt, ob eine Beeinträchtigung der Sicherheit und des Datenschutzes der TI bei Verlust der Sicherheit oder des Datenschutzes eines Fachdienstes VSDM technisch ausgeschlossen werden kann. Ist eine Beeinträchtigung der TI technisch ausgeschlossen, so werden keine Module zugeordnet. Ist eine Beeinträchtigung der TI nicht ausgeschlossen, werden die Module „Basis-IS“ und „Basis-ISMS“ sowie „Basis-DS“ zugeordnet. Zusammen mit der Prüfung der Fachdienste gemäß § 274 Abs. 1 SGB V (vgl. Anhang C) wird so der gesetzliche Auftrag der gematik gemäß § 291b Abs. 1 SGB V zur Gewährleistung eines sichereren Betriebs der TI und zur Sicherstellung der Einhaltung der Vorschriften zum Datenschutz in der TI umgesetzt.

In der derzeitigen Form des Anschlusses der Fachdienste VSDM an die TI ist eine Beinträchtigung der Sicherheit und des Datenschutzes der TI bei Verlust der Sicherheit oder des Datenschutzes eines Fachdienstes VSDM technisch nicht ausgeschlossen.

ENTWURF

Tabelle 2 – Modulzuordnung bzgl. der Möglichkeit, die TI zu beeinträchtigen

Grad der möglichen Beeinträch-tigung der TI	Anbieter	Beschreibung	Module
keine Beeinträchti gung möglich	weitere Anwendungen	Die Sicherheit der Betriebsumgebung des Dienstes der weiteren Anwendung hat keinen Einfluss auf die Sicherheit der TI.	Module Informationssicherheit ☐ Basis-IS ☐ Basis-ISMS ☐ Erweitertes ISMS ☐ TI-Sicherheitsbericht ☐ Erweiterter TI-Sicherheitsbericht Module Datenschutz ☐ Basis-DS ☐ TI-Datenschutzbericht ☐ Erweiterter TI-Datenschutzbericht
	Fachdienste VSDM	Die Sicherheit der Betriebsumgebung des Fachdienstes VSDM hat keinen Einfluss auf die Sicherheit der TI. Hinweis: In der derzeitigen Form des Anschlusses der Fachdienste VSDM an die TI ist dies nicht gegeben.	Module Informationssicherheit ☐ Basis-IS ☐ Basis-ISMS ☐ Erweitertes ISMS ☐ TI-Sicherheitsbericht ☐ Erweiterter TI-Sicherheitsbericht Module Datenschutz ☐ Basis-DS ☐ TI-Datenschutzbericht ☐ Erweiterter TI-Datenschutzbericht
Beeinträch-tigung möglich	zentrale TI-Plattform	Die Sicherheit der Betriebsumgebung des Dienstes der TI hat einen Einfluss auf die Sicherheit der TI. Die Aufrechterhaltung von Informationssicherheit und Datenschutz bei Diensten der zentralen TI-Plattform ist von besonderer Bedeutung, da sie von allen Teilnehmern der TI genutzt werden.	Module Informationssicherheit ☒ Basis-IS ☒ Basis-ISMS ☒ Erweitertes ISMS ☒ TI-Sicherheitsbericht ☒ Erweiterter TI-Sicherheitsbericht Module Datenschutz ☒ Basis-DS ☒ TI-Datenschutzbericht ☒ Erweiterter TI-Datenschutzbericht
	eGK-Anwendung/ sÜv	Die Sicherheit der Betriebsumgebung des Dienstes der TI hat einen Einfluss auf die Sicherheit der TI.	Module Informationssicherheit ☒ Basis-IS ☒ Basis-ISMS ☐ Erweitertes ISMS ☒ TI-Sicherheitsbericht ☒ Erweiterter TI-Sicherheitsbericht Module Datenschutz ☒ Basis-DS ☒ TI-Datenschutzbericht ☒ Erweiterter TI-Datenschutzbericht
	Fachdienste VSDM	Die Sicherheit der Betriebsumgebung des	Module Informationssicherheit

ENTWURF

Grad der möglichen Beeinträch-tigung der TI	Anbieter	Beschreibung	Module
		Fachdienstes VSDM hat einen Einfluss auf die Sicherheit der TI.	☒ Basis-IS ☒ Basis-ISMS ☐ Erweitertes ISMS ☐ TI-Sicherheitsbericht ☐ Erweiterter TI-Sicherheitsbericht Module Datenschutz ☒ Basis-DS ☐ TI-Datenschutzbericht ☐ Erweiterter TI-Datenschutzbericht
	weitere Anwendungen	Die Sicherheit der Betriebsumgebung des Dienstes der weiteren Anwendung hat einen Einfluss auf die Sicherheit der TI.	Module Informationssicherheit ☒ Basis-IS ☒ Basis-ISMS ☐ Erweitertes ISMS ☒ TI-Sicherheitsbericht ☐ Erweiterter TI-Sicherheitsbericht Module Datenschutz ☒ Basis-DS ☒ TI-Datenschutzbericht ☐ Erweiterter TI-Datenschutzbericht

ENTWURF

Anhang C – Modulzuordnung bei Anwendbarkeit des § 274 Abs. 1 SGB V

Für ausgewählte Anbieter legt der § 274 Abs. 1 SGB V eine Aufsichtsbehörde und einen Prüfzyklus fest, nach dem die dort benannte Aufsichtsbehörde die Geschäfts-, Rechnungs- und Betriebsführung beim Anbieter prüft. Die Prüfung erstreckt sich auf den gesamten Geschäftsbetrieb des Anbieters und umfasst die Prüfung seiner Gesetzmäßigkeit und Wirtschaftlichkeit. Die Prüfung beinhaltet die Einhaltung der Vorschriften des Datenschutzes und die Maßnahmen zur Informationssicherheit.

Da die Prüfung des Datenschutzes und der Informationssicherheit inklusive Prüfzyklus gesetzlich geregelt ist, entfallen die Module zum Reporting und das Modul „Erweitertes ISMS“ für Anbieter der Fachdienste VSDM und Anbieter weiterer Anwendungen, für die der § 274 Abs. 1 SGB V anwendbar ist (siehe Abbildung 7).

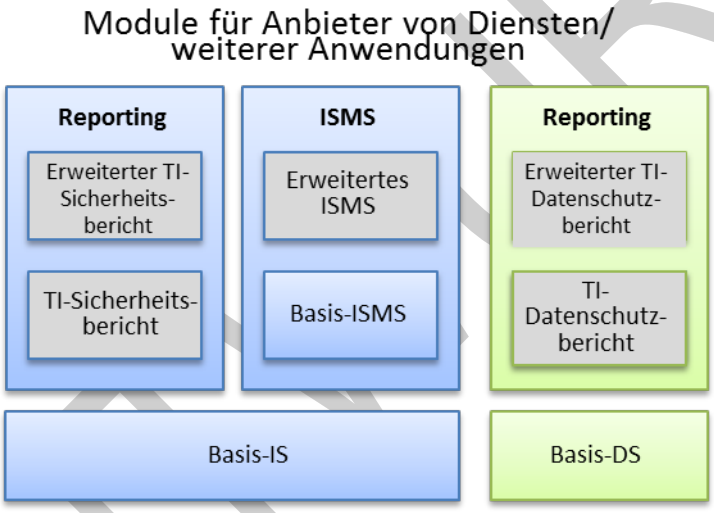

Abbildung 7 – Auswirkungen des § 274 SGB V auf die Modulzuordnung (grau = entfällt)

ENTWURF