gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

**Einführung der Gesundheitskarte**

# Koordinierendes Datenschutzmanagement in der Telematikinfrastruktur

| | |
|---|---|
| Version: | 1.2.0 |
| Revision: | \main\rel_online\rel_ors1\5 |
| Stand: | 21.02.2014 |
| Status: | freigegeben |
| Klassifizierung: | öffentlich |
| Referenzierung: | [gemSpec_DSM] |

# Dokumenteninformation

**Änderungen zur Vorversion**

Losübergreifende Synchronisation

**Dokumentenhistorie.**

| Version | Datum | Kap./ Seite | Grund der Änderung, besondere Hinweise | Bearbeitung |
|---|---|---|---|---|
| 0.5.0 | 29.06.12 | | freigegeben zur Abstimmung | PL P77 |
| 0.6.0 | 07.09.12 | | freigegeben zur Abstimmung | PL P77 |
| 1.0.0 | 15.10.12 | | freigegeben | gematik |
| | | | Kommentare aus einer internen Änderungsliste | P77 |
| 1.0.9 | 22.04.13 | | zur Abstimmung freigegeben | PL P77 |
| 1.1.0 RC | 30.05.13 | | zur Freigabe empfohlen | PL P77 |
| 1.1.0 | 06.06.13 | | freigegeben | gematik |
| | | | Einarbeitung gemäß Änderungsliste | gematik |
| | | | Losübergreifende Synchronisation | PL P77 |
| 1.2.0 | 21.02.14 | | freigegeben | gematik |

# Inhaltsverzeichnis


**Dokumenteninformation** ..... 2

**Inhaltsverzeichnis** ..... 3

**1 Einordnung des Dokumentes** ..... 5

**1.1 Zielsetzung** ..... 5

**1.2 Zielgruppe** ..... 5

**1.3 Geltungsbereich** ..... 5

**1.4 Methodik** ..... 6

**2 Kennzahlensystem des Datenschutzes in der TI** ..... 7

**2.1 Kennzahl: Häufung von Datenschutzbeschwerden als Indiz** ..... 7

**2.2 Kennzahl: Anzahl der Datenschutz-Anfragen** ..... 8

**2.3 Kennzahl: Anteil der fehlerhaft adressierten Datenschutz-Anfragen** ..... 9

**2.4 Kennzahl: Bearbeitungszeit für Datenschutz-Anfragen** ..... 9

**2.5 Kennzahl: Anzahl der gravierenden Datenschutzverstöße** ..... 10

**2.6 Kennzahl: Anzahl der Datenschutz-Schulungstage je Mitarbeiter** ..... 10

**2.7 Kennzahl: Anteil der Verfahren, die im internen Verfahrensverzeichnis abgebildet sind** ..... 11

**2.8 Kennzahl: Anzahl der externen und internen Datenschutz-Audits** ..... 12

**3 Anforderungen an das DSM der Anbieter** ..... 13

**3.1 Dokumentation des Datenschutzmanagements** ..... 13

**3.2 Reports an das koordinierende DSM der TI** ..... 13

3.2.1 Monatliche Reports der Anbieter in der Erprobung ..... 14

3.2.2 Jährliche Reports der Anbieter im Produktivbetrieb ..... 17

3.2.3 Format zur Bereitstellung des Kennzahlen-Reports ..... 18

**3.3 Behandlung von gravierenden Datenschutzverstößen** ..... 21

**3.4 Meldung von Kontaktinformationen zum Datenschutzmanagement** ..... 22

**3.5 Berücksichtigung von Informationen des koordinierenden DSM** ..... 22

**Anhang A** ..... 24

**A1 – Abkürzungen** ..... 24

**A2 – Glossar** ..... 24

**A3 – Tabellenverzeichnis ..... 24**

**A4 - Referenzierte Dokumente ..... 24**

A5.1 – Dokumente der gematik ..... 24

A5.2 – weitere Referenzierungen ..... 25

# 1 Einordnung des Dokumentes

## 1.1 Zielsetzung

Die vorliegende übergreifende Spezifikation definiert die Anforderungen für die Koordination der Datenschutzmanagements (DSM) der Anbieter bei der übergreifenden Sicherstellung des Datenschutzes in der TI. Diese Anforderungen sind als übergreifende Regelungen relevant für Interoperabilität und Verfahrenssicherheit. Die Bereitstellung eines koordinierenden DSM ist Aufgabe der gematik, um den Sicherstellungsauftrag nach § 291b SGB V wahrzunehmen.

Anbieter von zentralen Diensten der TI-Plattform und Anbieter von fachanwendungsspezifischen Diensten, die personenbezogene Daten erheben, verarbeiten oder nutzen, müssen zum Schutz dieser Daten eine Datenschutzorganisation mit für diesen Bereich verantwortlichen fachkundigem und zuverlässigem Personal haben (i.d.R. bestellter Datenschutzbeauftragter). Das Datenschutzmanagement ist entsprechend der Maßnahmen des IT-Grundschutzkatalogs für Datenschutzmanagement zu gestalten. Im Übrigen ergeben sich die Anforderungen an die Datenschutzorganisation aus dem Bundesdatenschutzgesetz (BDSG) und spezialgesetzlichen Regelungen. Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind (z. B. SGB X für Sozialdaten), gehen sie den Vorschriften des BDSG vor (vgl. § 1 Abs. 3 BDSG).

In diesem Dokument wird zudem ein Kennzahlenmodell festgelegt, mit dem die Einhaltung der Anforderungen des Datenschutzes bei den Anbietern von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten kontrolliert werden kann. Des Weiteren werden die Prozesse des koordinierenden Datenschutzmanagements der TI beschrieben, die die Einhaltung der Vorschriften zum Schutz personenbezogener Daten in der TI im Wirkbetrieb sicherstellen soll.

Kennzahlen zur Informationssicherheit der TI werden in [gemSpec_ISM] beschrieben. Mit ihnen soll insbesondere die Wirksamkeit der getroffenen Maßnahmen zur Informationssicherheit betrachtet werden, die zum Schutz der personenbezogenen Daten dienen.

## 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 geson-

derten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Die Regelungen des Dokumentes sind für Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten relevant und beziehen sich auf die IT-Systeme des Anbieters, die zum Betrieb des Produktes der TI genutzt werden. Im Rahmen der Zulassung ist geregelt, welche Produkte der TI die Anforderungen erfüllen müssen.

Die Regelungen des Dokumentes gelten nicht für Leistungserbringer, Leistungserbringerinstitutionen, die Ärzte- und Zahnärztekammern und die Kassenärztlichen und Kassenzahnärztlichen Vereinigungen, sofern sie nicht selbst Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten sind.

Die Regelungen des Dokumentes gelten ebenfalls nicht für nach dem Signaturgesetz (SigG) akkreditierte Zertifizierungsdiensteanbieter, die von der BNetzA beaufsichtigt werden.

## 1.4 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_0000 <Titel der Afo>**

Text/Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

# 2 Kennzahlensystem des Datenschutzes in der TI

Dieses Kapitel beschreibt das Kennzahlensystem des Datenschutzes in der TI. Die folgenden Kennzahlen sind von Anbietern von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten zu erheben und an das koordinierende Datenschutzmanagement (DSM) der TI zu berichten (siehe Kap. 3.2). Werden die Kennzahlen von einem Anbieter nicht oder nicht rechtzeitig geliefert, behält sich das koordinierende DSM der TI Maßnahmen vor, die zur Durchsetzung des Sicherstellungsauftrags der gematik nach § 291b SGB V [SGB V] erforderlich sind.

Die Kontaktinformationen des koordinierenden DSM der TI sind im öffentlichen Datenschutzverzeichnis der gematik hinterlegt.

## 2.1 Kennzahl: Häufung von Datenschutzbeschwerden als Indiz

Datenschutzbeschwerden sind alle Beschwerden von Betroffenen, die sich auf die Erhebung, Verarbeitung und Nutzung ihrer personenbezogenen Daten beziehen.

**Erwartete Werte**

Es wird die Anzahl der Datenschutzbeschwerden von Betroffenen im Berichtszeitraum erwartet. Die Beschwerden sind nach den folgenden Beschwerdegründen aufzuschlüsseln:

- Verwendung unzutreffender Daten,
- Verlust von Daten,
- unautorisierte Kenntnisnahme durch Dritte,
- sonstige Gründe: stellt eine Datenschutz-Beschwerde auf andere als die vorgenannten Gründe ab, sind diese von den Anbietern zu nennen.

**Ziel der Kennzahl**

Ziel der Kennzahl soll die Erfassung der Gründe der Datenschutzbeschwerden sein (Verwendung unzutreffender Daten, Verlust von Daten, unautorisierte Kenntnisnahme, sonstige Gründe). Datenschutzbeschwerden können darauf hinweisen, dass die Vorschriften des Datenschutzes von Anbietern der TI nicht eingehalten werden. Die übermittelte Anzahl an Datenschutzbeschwerden kann jedoch lediglich als Indiz für etwaige Nichteinhaltungen der Datenschutzvorschriften dienen, da nicht ausgeschlossen werden kann, dass Beschwerden der Betroffenen unberechtigt erfolgen.

Anhand der von allen Anbietern gelieferten Kennzahlen kann die gematik bewerten, ob sich Beschwerden verstärkt auf einzelne Anbieter beziehen oder übergreifende Beschwerden an die TI als Ganzes existieren. Darüber hinaus gibt die Aufschlüsselung Hinweise auf den Grund der Beschwerden und lässt eine zielgerichtete Behebung der Ursache zu.

Die Kennzahl lässt keinen generellen Rückschluss auf die Umsetzung der Anforderungen an das Datenschutzmanagement des Anbieters zu, da Beschwerden nur mittelbar als Reaktion der Betroffenen auftreten und eine Prüfung ihrer Gültigkeit durch die gematik nicht erfolgt.

Kein Ziel der Kennzahl ist die Kontrolle eines einzelnen Anbieters. Die Erfassung der gravierenden Datenschutz-Verstöße (dies wäre eine berechtigte Datenschutz-Beschwerde) erfolgt in einer anderen Kennzahl.

## 2.2 Kennzahl: Anzahl der Datenschutz-Anfragen

Datenschutz-Anfragen sind alle Anfragen von Betroffenen, durch welche sie ihre Rechte als Betroffener auf Auskunft, Berichtigung, Löschung oder Sperrung entsprechend § 6 BDSG (bzw. § 83-84a [SGB X]) geltend machen.

**Erwartete Werte**

Es wird die Anzahl der Datenschutz-Anfragen von Betroffenen im Berichtszeitraum erwartet. Personenbezogene Daten selbst dürfen dabei nicht übermittelt werden (vgl. § 6 Abs. 3 [BDSG]). Falls Anbieter Auftragnehmer beauftragen, ist die Anzahl der Datenschutz-Anfragen nach den Beauftragten aufzuschlüsseln.

Neben der Angabe der Gesamtanzahl der Anfragen sind die Anfragen in folgenden Kategorien aufgeschlüsselt darzustellen:

- Auskunftsanfragen,
- Löschungs- bzw. Sperranfragen,
- Berichtigungsanfragen.

**Ziel der Kennzahl**

Die Anzahl aller Datenschutz-Anfragen bzgl. der Produkte der TI bei einem Anbieter zeigt den Aufwand an, den Anbieter bei der Gewährleistung der Wahrnehmung der datenschutzrechtlichen Betroffenenrechte durch den Betrieb von Produkten der TI haben. Die Kenntnis des tatsächlichen Aufwands für Anbieter durch die Bearbeitung von Datenschutz-Anfragen kann dazu führen, dass übergeordnete Prozesse oder technische Geräte in der TI etabliert werden müssen, die den Aufwand auf Seiten der Anbieter sowie der Betroffenen reduzieren.

Durch die Aufschlüsselung der Datenschutz-Anfragen können zusätzlich Tendenzen hinsichtlich eines nicht datenschutzkonformen Umgangs mit personenbezogenen Daten bei den Anbietern erkennbar gemacht werden. Gehen z.B. bei einem Anbieter vermehrt Löschungs-, Sperr- oder Berichtigungsanfragen ein, kann dies auf eine mangelnde Einhaltung der Vorschriften zum Schutz personenbezogener Daten hindeuten. Handelt es sich hingegen vorwiegend um Auskunftsanfragen, kann hieraus nicht unbedingt ein Schluss auf die fehlende Einhaltung der Datenschutzvorschriften gezogen werden. Auskunftsanfragen sind vielmehr ein Ausdruck einer gesteigerten Sensibilisierung des Datenschutzes bei den Betroffenen.

## 2.3 Kennzahl: Anteil der fehlerhaft adressierten Datenschutz-Anfragen

In der TI gibt es mehrere verantwortliche Stellen. Nach § 6 Abs. 2 BDSG bzw. § 84a Abs. 2 SGB X müssen die speicherberechtigten Stellen Anfragen an die zuständige Stelle weiterleiten und den Betroffenen hierüber unterrichten.

**Erwartete Werte**

Es wird das Verhältnis der fehlerhaft adressierten Datenschutz-Anfragen zur Gesamtzahl der Datenschutz-Anfragen bzgl. der im Verantwortungsbereich liegenden Produkte der TI in Prozent erwartet.

**Ziel der Kennzahl**

Mit dieser Kennzahl soll bewertet werden, ob Anbieter viele Anfragen von Betroffenen bzgl. der Produkte der TI erreichen, für die sie nicht zuständig sind. In diesem Fall wäre der Informationsfluss an die Betroffenen zur Frage der Zuständigkeiten zu verbessern. Zudem können hierdurch koordinierende Prozesse abgeleitet werden, welche die Pflicht nach § 6 Abs. 2 Satz 2 BDSG (bzw. § 84a Abs. 2 SGB X) zur Weiterleitung der Datenschutzanfragen an die zuständige Stelle beschleunigen können.

Die Kennzahl soll letztlich sicherstellen, dass die Betroffenen ihre Anfrage an die richtige verantwortliche Stelle adressieren und soll somit eine zeitnahe Geltendmachung ihrer Rechte sicherstellen.

## 2.4 Kennzahl: Bearbeitungszeit für Datenschutz-Anfragen

Diese Kennzahl erhebt die durchschnittliche Bearbeitungszeit (Zeitspanne vom Eingang der Anfrage beim Anbieter bis zum Abschluss des Vorgangs beim Anbieter) von korrekt an den Anbieter adressierten Datenschutz-Anfragen. Datenschutzanfragen sind nach dem Schutzzweck der §§ 34, 35 BDSG (bzw. §§ 83, 84 SGB X) unverzüglich und schnell zu erteilen.

**Erwartete Werte**

Es wird die durchschnittliche Bearbeitungszeit (Zeitspanne vom Eingang der Anfrage beim Anbieter bis zum Abschluss des Vorgangs beim Anbieter) von korrekt an den Anbieter im Berichtszeitraum adressierten Datenschutz-Anfragen bzgl. eines Produktes der TI erwartet.

Neben der Angabe der Bearbeitungszeit der Anfragen sind die Anfragen in folgenden Kategorien aufgeschlüsselt darzustellen:

- Auskunftsanfragen,
- Lösch- und Sperranfragen,
- Berichtigungsanfragen.

**Ziel der Kennzahl**

Die Bearbeitungszeit von Datenschutzanfragen kann ein Indiz für die Umsetzung der Anforderungen an die Organisation des Datenschutzmanagements eines Anbieters liefern. Ist die Bearbeitungszeit für Anfragen in der TI zu hoch, müssen durch die Anbieter zusätzliche Maßnahmen ergriffen werden, um Betroffenen zumutbare Antwortzeiten zu gewährleisten. Dabei können für die Bearbeitungszeiten für Auskunfts-, Lösch-, Sperr- und Berechtigungsanfragen unterschiedliche Bearbeitungszeiten als angemessen angesehen werden. Dennoch ist zu berücksichtigen, dass einzelne Anfragen längere Bearbeitungszeiten haben können.

## 2.5 Kennzahl: Anzahl der gravierenden Datenschutzverstöße

Diese Kennzahl erfasst die Anzahl der beim Anbieter aufgetretenen Datenschutzverstöße, die nach § 42a BDSG (bzw. § 83a SGB X) benachrichtigungspflichtig sind oder formelle und materielle Verstöße darstellen (insbesondere Verstöße gemäß §§ 43, 44 BDSG bzw. § 85, 85a SGB X), die von der Aufsichtsbehörde sanktioniert wurden oder wegen denen eine strafrechtliche Verurteilung ausgesprochen wurde. Bei dieser Kategorie von Datenschutzverstößen muss das koordinierende DSM die Auswirkungen auf andere Beteiligte der TI und schwerwiegende Beeinträchtigungen auf die Rechte und schutzwürdigen Interessen der Betroffenen prüfen und ggf. Maßnahmen ergreifen.

**Erwartete Werte**

Es wird die Anzahl der im Berichtszeitraum beim Anbieter aufgetretenen Datenschutzverstöße erwartet. Es müssen alle Fälle der §§ 42a, 43 und 44 BDSG (bzw. § 83a, 85, 85a SGB X) berücksichtigt werden.

Im Falle von Datenschutzverstößen nach § 42a BDSG (bzw. § 83a SGB X) ist jeder einzelne Datenschutzverstoß unverzüglich nach bekannt werden, spätestens jedoch zeitgleich mit Erfüllung der Informationspflicht nach § 42a Abs. 1 Satz 1 BDSG (bzw. § 83a SGB X), der gematik zu melden.

**Ziel der Kennzahl**

Diese Kennzahl macht gravierende Datenschutzverletzungen offenkundig. Die Kenntnis solcher Verstöße ermöglicht dem koordinierenden DSM, Kontakt zu den jeweiligen Anbietern aufzunehmen und zu prüfen, ob ggf. technische oder organisatorische Mängel den Schutz der personenbezogenen Daten von Patientinnen und Patienten verletzen und schwerwiegende Nachteile drohen. Zudem kann hierdurch ggf. unmittelbar auf die jeweilige Stelle eingewirkt werden, um den Schutz personenbezogener Daten sicherzustellen.

## 2.6 Kennzahl: Anzahl der Datenschutz-Schulungstage je Mitarbeiter

Ein effektiver Datenschutz ist in aller Regel nicht gesichert, wenn die mit der TI-befassten Mitarbeiter des Anbieters nicht ausreichend in datenschutzrechtlichen Aspekten sowie

zur Umsetzung datenschutzrechtlicher Bestimmungen geschult und darin kontinuierlich weitergebildet sind.

**Erwartete Werte**

Es werden die Anzahl und Dauer der Datenschutz-Schulungstage je mit der TI-befasstem Mitarbeiter im Berichtszeitraum erwartet. Personenbezogene Daten sind dabei nicht zu übermitteln.

**Ziel der Kennzahl**

Diese Kennzahl gibt Aufschluss über das Engagement eines Anbieters, seine Mitarbeiter hinsichtlich datenschutzrechtlicher Themen zu schulen. Werden regelmäßig und in angemessenem Umfang gemäß § 4g BDSG (bzw. § 81 Abs. 4 SGB X) solche Schulungen durchgeführt, ist zumindest davon auszugehen, dass die Mitarbeiter auf das Thema Datenschutz sensibilisiert sind. Diese Kennzahl gibt jedoch nicht zwingend eine Auskunft über den Umfang und die Qualität des vermittelten Wissens. Insofern kann auch bei vielen Schulungstagen kein direkter Rückschluss auf tatsächlich vorhandene datenschutzrechtliche Kenntnisse der Mitarbeiter gezogen werden. Andererseits liegt die Annahme jedoch nahe, dass die Kenntnisse gering sein werden, wenn ein Anbieter keine Datenschutz-Schulungen durchführt.

## 2.7 Kennzahl: Anteil der Verfahren, die im internen Verfahrensverzeichnis abgebildet sind

Verfahren automatisierter Verarbeitungen zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten der TI sind von der verantwortlichen Stelle in einem Verfahrensverzeichnis zu führen. Das Verfahrensverzeichnis enthält die Angaben nach §§ 4d und 4e BDSG (bzw. § 81 Abs. 4 SGB X) und dient zur Information von Betroffenen und zur Kontrolle des Datenschutzes. Das öffentliche Verfahrensverzeichnis enthält die Informationen nach §4e Nr. 1 bis Nr. 8 BDSG (bzw. § 81 Abs. 4 SGB X) und behandelt in der Regel die eingesetzten Verfahren nicht im Detail. Das interne Verfahrensverzeichnis enthält die Informationen des öffentlichen Verfahrensverzeichnisses zuzüglich der Angaben nach § 4e Nr. 9 BDSG (bzw. § 81 Abs. 4 SGB X) und behandelt die eingesetzten Verfahren im Detail.

**Erwartete Werte**

Es wird das Verhältnis der im internen Verfahrensverzeichnis dokumentierten und vom Datenschutzbeauftragten regelmäßig kontrollierten Verfahren zur Gesamtzahl der Verfahren mit personenbezogenen Daten in Prozent erwartet.

**Ziel der Kennzahl**

Der Anteil der im internen Verfahrensverzeichnis abgebildeten und vom Datenschutzbeauftragten geprüften Verfahren zeigt an, welcher Anteil der Verfahren des Anbieters des TI-Produkttyps bereits kontrolliert und dokumentiert wurde. Je höher der Anteil ist, desto einfacher können Betroffene informiert werden bzw. je einfacher können Kontrollen, insbesondere durch den betrieblichen Datenschutzbeauftragten, durchgeführt werden. Es

wird angenommen, dass durch die Prüfung des Datenschutzbeauftragten eine datenschutzgerechte Gestaltung der Verfahren gewährleistet wird.

## 2.8 Kennzahl: Anzahl der externen und internen Datenschutz-Audits

Durch externe oder interne Datenschutz-Audits wird die Einhaltung des Datenschutzes im laufenden Betrieb kontrolliert. Die bei einem Audit festgestellten Befunde können durch Maßnahmen behoben und so das Datenschutzmanagement verbessert werden.

**Erwartete Werte**

Es wird die Anzahl und thematischer Inhalt der durchgeführten externen und internen Datenschutz-Audits sowie Anzahl der Beauftragten, die Produkte der TI betreiben, erwartet. Dabei sind die Auditanlässe nach den folgenden Kriterien aufzuschlüsseln:

- Auftragsdatenverarbeitung nach § 11 BDSG oder § 80 SGB X,
- anlassbezogene Audits, insbesondere bei Datenschutzverstößen beim Anbieter,
- Regelprüfungen durch den Datenschutzbeauftragten des Anbieters.

**Ziel der Kennzahl**

Diese Kennzahl zeigt, welche Anbieter darum bemüht sind, ihre Datenschutzorganisation auf dem aktuellen Stand zu halten. Dabei wird angenommen, dass eine Kontrolle des Datenschutzes durch Audits zu einer Verbesserung bzw. Aufrechterhaltung des Datenschutzes führt. Insbesondere nach § 11 BDSG bzw. § 80 SGB X verpflichtend durchzuführende Kontrollen bei Aufragnehmern sind hierbei zu berücksichtigen.

Die Anzahl der Audits lässt jedoch keinen Rückschluss auf den Umgang mit Ergebnissen der Audits zu.

# 3 Anforderungen an das DSM der Anbieter

Dieses Kapitel beschreibt die Prozessschnittstellen zwischen dem koordinierenden Datenschutzmanagement der TI und dem jeweiligen Datenschutzmanagement der Anbieter. Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten müssen die Anforderungen dieses Kapitels umsetzen.

Die Vorgaben dieses Kapitels richten sich nicht an die Systeme der Leistungserbringer, Leistungserbringerinstitutionen und Bestandssysteme der Kartenherausgeber und ihrer IT-Dienstleister, soweit sie keine zentralen Produkte der TI betreiben. Sie haben gleichwohl die datenschutzrechtlichen Vorgaben aus den jeweils für sie geltenden allgemeinen und speziellen Gesetzen und berufsspezifischen Regelungen zu erfüllen. Die derzeitigen Prozesse bei diesen Stellen werden als ausreichend angesehen, um die Interessen von Patientinnen und Patienten zu wahren und die Einhaltung der Vorschriften zum Schutz personenbezogener Daten sicherzustellen.

## 3.1 Dokumentation des Datenschutzmanagements

⌦ **GS-A_4435 kDSM: Dokumentation des DSM**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN die Umsetzung ihres Datenschutzmanagements mit seinen relevanten Maßnahmen derart dokumentieren, dass es von sachverständigen Dritten mit angemessenem Aufwand nachvollzogen und geprüft werden kann.⌫

⌦ **GS-A_4436 kDSM: Bereitstellung der Dokumentation des DSM bei Audits**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN die Dokumentation der Maßnahmen ihres Datenschutzmanagements bei einem durch die gematik veranlassten Datenschutz-Audit zur Verfügung stellen.⌫

⌦ **GS-A_4437 kDSM: Jährliche Prüfung der Dokumentation des DSM**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN die Dokumentation der Maßnahmen ihres Datenschutzmanagements mindestens jährlich überprüfen und ggf. überarbeiten. ⌫

## 3.2 Reports an das koordinierende DSM der TI

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten müssen dem koordinierenden DSM in regelmäßigen Reports über die Einhaltung der Vorschriften zum Datenschutz bzgl. der von ihnen betriebenen Produkte der TI berichten. Hierbei wird zwischen monatlichen Reports im Rahmen der Erprobung und mindestens jährlichen Reports im Produktivbetrieb unterschieden.

**GS-A_4448 kDSM: Übermittlung von Reports**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN Datenschutz-Reports gemäß den Regelungen zum Reporting aus den übergreifenden Richtlinien zum Betrieb der TI übermitteln.

### 3.2.1 Monatliche Reports der Anbieter in der Erprobung

Zielgruppe dieses Reports ist das koordinierende DSM der TI. Das koordinierende DSM kann anhand der Kennzahlen aller Anbieter die Einhaltung des Datenschutzes in der TI bewerten und über die monatlichen Verläufe Trends und Tendenzen erkennen.

Das koordinierende DSM der TI prüft regelmäßig die Effektivität der Kennzahlen und passt diese ggf. an. Das koordinierende DSM informiert die Anbieter über das geänderte Kennzahlenmodell. Die Anbieter müssen dann die Kennzahlen entsprechend des geänderten Kennzahlenmodells melden.

**GS-A_4449 kDSM: Monatliche Reports in der Erprobung**

Während der Erprobung MÜSSEN Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten die von der gematik geforderten Kennzahlen des Datenschutzes in einem Kennzahlen-Report monatlich an das koordinierende Datenschutzmanagement der TI liefern.

**GS-A_4450 kDSM: Erfassungszeitraum monatlicher Reports**

Während der Erprobung MÜSSEN Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten sicherstellen, dass der monatliche Kennzahlen-Report einen Erfassungszeitraum vom ersten bis zum letzten Tag eines Kalendermonats abdeckt und innerhalb von zwei Wochen nach Ende des Erfassungszeitraums an das koordinierende Datenschutzmanagement der TI übermittelt wird.

**GS-A_4451 kDSM: Kein Personenbezug in Kennzahlen**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN sicherstellen, dass in den gemeldeten Kennzahlen keine personenbezogenen Daten übermittelt werden.

**GS-A_4453 kDSM: Sicherstellung der Kennzahl-Meldung in Unterbeauftragungsverhältnissen**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN im Falle von Unterbeauftragungen im Sinne des § 11 BDSG bzw. des § 80 SGB X in den Unterbeauftragungsverträgen sicherstellen, dass die in den Kennzahlen vorgesehen eigenen Meldepflichten auch vom Unterauftragnehmer unterstützt werden.

**GS-A_4455 kDSM: Anpassung der Reports bei geänderten Kennzahlen**

Nachdem Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten über eine Anpassung der Kennzahlen des Datenschutzes durch das koordinierende Datenschutzmanagement der TI informiert wurden, MÜSSEN Anbieter die Kennzahlen spätestens ab dem übernächsten Kennzahlen-Report oder einem in der Information genannten Zeitpunkt entsprechend des geänderten Kennzahlenmodells an das koordinierende Datenschutzmanagement der TI melden.⌫

**⌦ GS-A_4456 kDSM: Dateiformat des Kennzahlen-Reports**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN den Kennzahlen-Report im CSV-Format entsprechend des Schemas in Tabelle *Tab_kDSM_001_Inhalte Kennzahlen-Report* übermitteln und innerhalb der CSV-Datei als Trennzeichen ein Semikolon (;) und für Werte vom Typ Double ein Komma (,) als Dezimaltrennzeichen benutzen. ⌫

**⌦ GS-A_4457 kDSM: Anpassung an geändertes CSV-Format**

Nachdem Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten über eine Anpassung des CSV-Formats in Tabelle *Tab_kDSM_001_Inhalte Kennzahlen-Report* durch das koordinierende Datenschutzmanagement der TI informiert wurden, MÜSSEN Anbieter die Kennzahlen ab dem nächsten Kennzahlen-Report oder einem in der Information genannten Zeitpunkt entsprechend des geänderten CSV-Formats an das koordinierende Datenschutzmanagement der TI übermitteln.⌫

**⌦ GS-A_4458 kDSM: Identifizierung der Ursachen von auffälligen Kennzahlenwerten**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN der gematik Audits zur Feststellung der Ursachen von auffälligen Kennzahlenwerten beim Anbieter ermöglichen.⌫

**⌦ GS-A_4459 kDSM: Meldung der Anzahl der Datenschutzbeschwerden**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN im Kennzahlen-Report die Anzahl der Datenschutzbeschwerden, die Betroffene im Berichtszeitraum bei ihm einreichten, unter Nennung der Beschwerdegründe melden und dabei folgende Beschwerdegründe berücksichtigen:

- Verwendung unzutreffender Daten,
- Verlust von Daten,
- unautorisierte Kenntnisnahme durch Dritte,
- sonstige Gründe: stellt eine Datenschutz-Beschwerde auf andere als die vorgenannten Gründe ab, sind auch diese zu nennen.⌫

**⌦ GS-A_4460 kDSM: Meldung der Anzahl der Datenschutzanfragen**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN im Kennzahlen-Report die Anzahl der Datenschutz-Anfragen nach § 6 BDSG (bzw. §§ 81-84a SGB X), die Betroffene im

Berichtszeitraum bei ihm einreichten, melden und nach folgenden Kategorien aufschlüsseln: Auskunftsanfragen, Löschungs- bzw. Sperranfragen und Berichtigungsanfragen. ⌫

⌦ **GS-A_4461 kDSM: Meldung der fehlerhaft adressierten Datenschutzanfragen**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN im Kennzahlen-Report das Verhältnis der fehlerhaft adressierten Datenschutz-Anfragen zur Gesamtzahl der Datenschutzanfragen bzgl. der in seinem Verantwortungsbereich liegenden Produkte der TI in Prozent melden.⌫

⌦ **GS-A_4462 kDSM: Durchschnittliche Bearbeitungszeit für Datenschutzanfragen**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN im Kennzahlen-Report die durchschnittliche Bearbeitungszeit (Zeitspanne vom Eingang der Anfrage beim Anbieter bis zum Abschluss des Vorgangs beim Anbieter) von korrekt an den Anbieter im Berichtszeitraum adressierten Datenschutz-Anfragen bzgl. eines Produktes der TI melden und entsprechend der folgenden Kategorien aufschlüsseln: Auskunftsanfragen, Löschungs- bzw. Sperranfragen und Berichtigungsanfragen.⌫

⌦ **GS-A_4463 kDSM: Meldung der Anzahl gravierender Datenschutzvorfälle**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN im Kennzahlen-Report die Anzahl der im Berichtszeitraum beim Anbieter aufgetretenen Datenschutzvorfälle nach §§ 42a, 43, 44 BDSG bzw. §§ 83a, 85, 85 a SGB X melden. ⌫

⌦ **GS-A_4464 kDSM: Meldung der Datenschutzschulungstage**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN im Kennzahlen-Report bzgl. der mit der TI befassten Mitarbeiter die durchschnittliche Anzahl und Dauer der Datenschutzschulungstage je Mitarbeiter im Berichtszeitraum melden.⌫

⌦ **GS-A_4465 kDSM: Meldung des Anteils der Verfahren im internen Verfahrensverzeichnis**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN im Kennzahlen-Report das Verhältnis der im internen Verfahrensverzeichnis dokumentierten und vom Datenschutzbeauftragten regelmäßig geprüften Verfahren zur Gesamtzahl der Verfahren mit personenbezogenen Daten in Prozent melden.⌫

⌦ **GS-A_4466 kDSM: Meldung der Anzahl externer und interner Datenschutz-Audits**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN im Kennzahlen-Report die Anzahl und den thematischen Inhalt der bei ihnen durchgeführten externen und internen Datenschutz-Audits, liefern. Dabei sind die Auditanlässe nach den folgenden Kriterien aufzuschlüsseln:

- Audit gemäß Auftragsdatenverarbeitung nach § 11 BDSG bzw. § 80 SGB X,
- anlassbezogenes Audit, insbesondere bei Datenschutzverstößen beim Anbieter,
- Regelprüfungen durch den Datenschutzbeauftragten des Anbieters. ⌫

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten müssen eine eigene Einschätzung zum Umsetzungsstand des Datenschutzes in der eigenen Datenschutzorganisation abgeben. Diese Information zielt darauf ab, die Ergebnisse der gesammelten von einem Anbieter vorgelegten Kennzahlen mit seiner Selbsteinschätzung abzugleichen. Hierdurch können Fehleinschätzungen der Anbieter aufgedeckt und ihnen entgegen gewirkt werden. Ebenso wird erkennbar, inwieweit Umsetzungsprobleme mit Anforderungen bestehen, die im Zuge des regelmäßigen Evaluierungsprozesses des Datenschutzmanagements der TI berücksichtigt werden kann.

⌦ **GS-A_4467 kDSM: Selbsteinschätzung zum Datenschutz**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN im Kennzahlen-Report eine eigene Einschätzung zum Umsetzungsstand des Datenschutzes bzgl. ihrer eigenen Datenschutzorganisation abgeben, insbesondere bzgl. folgender Fragen:

Wie schätzen Sie den Stand des Datenschutzes in Ihrem Hause auf einer Schulnotenskala von 1 (sehr gut) – 6 (ungenügend) ein?

Sind Sie der Meinung, dass es in Ihrem Hause Umsetzungsprobleme mit den Anforderungen des Datenschutzes der TI bzgl. der von ihnen angebotenen Produkte der TI gibt?

Wo sehen Sie in Ihrem Hause ggf. Verbesserungsbedarf?

Sind Sie der Meinung, dass sie durch die eingeholten Kennzahlen den Stand des Datenschutzes in Ihrem Hause geeignet ausdrücken können? Falls nein, welche weitere Kennzahl würden sie vorschlagen bzw. welche Kennzahl als weniger relevant erachten? ⌫

### 3.2.2 Jährliche Reports der Anbieter im Produktivbetrieb

⌦ **GS-A_4468 kDSM: Jährlicher Datenschutzreport der TI**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN das koordinierende Datenschutzmanagement der TI über die Einhaltung der Vorschriften zum Datenschutz der von ihnen angebotenen Produkte der TI in Form eines jährlichen Datenschutzreports der TI informieren.⌫

⌦ **GS-A_4470 kDSM: Informationen zu Kennzahlen im Datenschutzreport der TI**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN ihrem jährlichen Datenschutzreport der TI eine Zusammenfassung über die bei ihnen erhobenen Datenschutz-Kennzahlen

der TI zufügen, wobei für jeden Monat erkennbar sein muss, welche Kennzahlen in diesem Monat erhoben wurden. ⌫

⌦ **GS-A_4471 kDSM: Auftragsdatenverarbeitung im Datenschutzreport der TI**

Falls Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten Auftragnehmer beauftragen, MUSS der Anbieter das koordinierende Datenschutzmanagement der TI im jährlichen Datenschutzreport der TI über die Ergebnisse der bei den Auftragnehmern nach § 11 BDSG bzw. § 80 SGB X (Auftragsdatenverarbeitung) durchgeführten Überprüfungen seiner Produkte der TI zusammenfassend und in übersichtlicher Form informieren.⌫

⌦ **GS-A_4472 kDSM: Allgemeiner Datenschutzbericht**

Neben dem zu übersendenden Datenschutzreport der TI MÜSSEN Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten dem koordinierenden Datenschutzmanagement der TI zusätzlich den im Rahmen des Datenschutzmanagements zu erstellenden allgemeinen Datenschutzbericht übersenden.⌫

### 3.2.3 Format zur Bereitstellung des Kennzahlen-Reports

Anbieter müssen den Kennzahlen-Report als CSV-Datei nach folgendem Schema (die Reihenfolge ist verbindlich) aufbereiten:

**Tabelle 1: Tab_kDSM_001_Inhalte Kennzahlen-Report**

| # | Spaltenname | Beschreibung | Wertebereich |
|---|---|---|---|
| 1 | Teilnehmer-ID | ID des Anbieters | [String] |
| 2 | Name des Anbieters | Kurzform der Anbieterfirma | [String] |
| 3 | Name des betrieblichen Datenschutzbeauftragten des Anbieters | vollständiger Name des bDSB | [String] |
| 4 | E-Mail-Adresse des betrieblichen Datenschutzbeauftragten des Anbieters | E-Mail-Adresse des betrieblichen Datenschutzbeauftragten des Anbieters | [String], z.B. name@anbieter.de |
| 5 | Anzahl der Auftragnehmer des Anbieters | Anzahl der Auftragnehmer des Anbieters, die Produkte der TI betreiben. | [Integer] z. B. 3 |
| 6 | Gesamtanzahl der Datenschutzbeschwerden des Anbieters | Summe der beim Anbieter und allen seinen Auftragnehmern eingegangenen Datenschutzbeschwerden im Erfassungszeitraum | [Integer] |
| 7 | Gesamtanzahl der Datenschutzbeschwerden des Anbieters bzgl. der Verwendung unzutreffender Daten | Summe der beim Anbieter und allen seinen Auftragnehmern eingegangenen Datenschutzbeschwerden bzgl. | [Integer] |

| # | Spaltenname | Beschreibung | Wertebereich |
|---|---|---|---|
| | | der Verwendung unzutreffender Daten im Erfassungszeitraum | |
| 8 | Gesamtanzahl der Datenschutzbeschwerden des Anbieters bzgl. des Verlustes von Daten | Summe der beim Anbieter und allen seinen Auftragnehmern eingegangenen Datenschutzbeschwerden bzgl. des Verlustes von Daten im Erfassungszeitraum | [Integer] |
| 9 | Gesamtanzahl der Datenschutzbeschwerden des Anbieters bzgl. der unautorisierten Kenntnisnahme durch Dritte | Summe der beim Anbieter und allen seinen Auftragnehmern eingegangenen Datenschutzbeschwerden bzgl. der unautorisierten Kenntnisnahme durch Dritte im Erfassungszeitraum | [Integer] |
| 10 | Gesamtanzahl der Datenschutzbeschwerden des Anbieters bzgl. sonstiger Gründe | Summe der beim Anbieter und allen seinen Auftragnehmern eingegangenen Datenschutzbeschwerden bzgl. bzgl. sonstiger Gründe im Erfassungszeitraum | [Integer] |
| 11 | Gesamtanzahl aller Datenschutz-Anfragen des Anbieters | Summe der beim Anbieter und allen seinen Auftragnehmern eingegangenen Datenschutzanfragen nach § 6 BDSG (§ 84a SGB X) im Erfassungszeitraum | [Integer] |
| 12 | Gesamtanzahl der Datenschutz-Anfragen des Anbieters bzgl. Auskunft | Summe der beim Anbieter und allen seinen Auftragnehmern eingegangenen Datenschutzanfragen nach § 6 BDSG (§ 83 SGB X) bzgl. Auskunft im Erfassungszeitraum | [Integer] |
| 13 | Gesamtanzahl der Datenschutz-Anfragen des Anbieters bzl. Löschung bzw. Sperrung | Summe der beim Anbieter und allen seinen Auftragnehmern eingegangenen Datenschutzanfragen nach § 6 BDSG (§ 84 Abs. 2-4 SGB X) bzgl. Löschung bzw. Sperrung im Erfassungszeitraum | [Integer] |
| 14 | Gesamtanzahl der Datenschutz-Anfragen des Anbieters bzgl. Berichtigung | Summe der beim Anbieter und allen seinen Auftragnehmern eingegangenen Datenschutzanfragen nach § 6 BDSG (§ 84 Abs. 1 SGB X) bzgl. Berichtigung im Erfassungszeitraum | [Integer] |
| 15 | Fehlerhaft adressierte Datenschutzanfragen beim Anbieter | Verhältnis der Summe der beim Anbieter und allen seinen Auftragnehmern fehlerhaft | [Prozent %] |

| # | Spaltenname | Beschreibung | Wertebereich |
|---|---|---|---|
| | | adressierten Datenschutzanfragen zur Gesamtzahl der Datenschutzanfragen im Erfassungszeitraum | |
| 16 | Durchschnittliche Bearbeitungszeit für Datenschutz-Anfragen beim Anbieter | Durchschnittliche Bearbeitungszeit in Tagen für Datenschutz-Anfragen beim Anbieter über alle Anfragearten | [Double] |
| 17 | Durchschnittliche Bearbeitungszeit für Datenschutz-Anfragen beim Anbieter bzgl. Auskunft | Durchschnittliche Bearbeitungszeit in Tagen für Datenschutz-Anfragen beim Anbieter bzgl. Auskunft | [Double] |
| 18 | Durchschnittliche Bearbeitungszeit für Datenschutz-Anfragen beim Anbieter bzgl. Löschung oder Sperrung | Durchschnittliche Bearbeitungszeit in Tagen für Datenschutz-Anfragen beim Anbieter bzgl. Löschung oder Sperrung | [Double] |
| 19 | Durchschnittliche Bearbeitungszeit für Datenschutz-Anfragen beim Anbieter bzgl. Berichtigung | Durchschnittliche Bearbeitungszeit in Tagen für Datenschutz-Anfragen beim Anbieter bzgl. Berichtigung | [Double] |
| 20 | Anzahl gravierender Datenschutzverstöße beim Anbieter | Summe der beim Anbieter und allen seinen Auftragnehmern aufgetretenen gravierenden Datenschutzverstöße im Erfassungszeitraum | [Integer] |
| 21 | Anzahl der Datenschutz-Schulungstage beim Anbieter | Durchschnittliche Anzahl von Datenschutz-Schulungstagen je Mitarbeiter beim Anbieter | [integer] |
| 22 | Dauer der Datenschutzschulungstage | Durchschnittliche Dauer der Datenschutz-Schulungstage in Stunden je Mitarbeiter beim Anbieter | [double] |
| 23 | Anteil der dokumentierten Verfahren im internen Verfahrensverzeichnis | Verhältnis der Summe der beim Anbieter in seinem internen Verfahrensverzeichnis dokumentierten Verfahren zur Gesamtzahl der Verfahren des Anbieters im Erfassungszeitraum | [Prozent %] |
| 24 | Anzahl der externen und internen Datenschutz-Audits des Anbieters gemäß § 11 BDSG bzw. § 80 SGB X | Summe der beim Anbieter durchgeführten externen und internen Datenschutz-Audits gemäß § 11 BDSG bzw. § 80 SGB X im Erfassungszeitraum | [Integer] |
| 25 | Anzahl der externen und internen anlassbezogenen Datenschutz-Audits des Anbieters | Summe der beim Anbieter durchgeführten anlassbezogenen externen und internen Datenschutz-Audits im | [Integer] |

| # | Spaltenname | Beschreibung | Wertebereich |
|---|---|---|---|
| | | Erfassungszeitraum | |
| 26 | Anzahl der externen und internen Datenschutz-Audits des Anbieters im Rahmen der Regelprüfung durch den bDSB | Summe der beim Anbieter im Rahmen der Regelprüfung durch den bDSB durchgeführten externen und internen Datenschutz-Audits im Erfassungszeitraum | [Integer] |
| 27 | Thematische Inhalte der Datenschutz-Audits | Zusammenfassung der thematischen Inhalte der beim Anbieter durchgeführten externen und internen Datenschutz-Audits im Erfassungszeitraum | [String] |
| 28 | Selbsteinschätzung des Anbieters zum Datenschutz | Selbsteinschätzung des Anbieters | [String] |

## 3.3 Behandlung von gravierenden Datenschutzverstößen

⌦ **GS-A_4473 kDSM: Unverzügliche Benachrichtigung bei Verstößen gemäß § 42a BDSG bzw. § 83a SGB X**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN jeden Datenschutzverstoß nach § 42a BDSG bzw. § 83a SGB X, der sich auf die vom Anbieter verantworteten Systeme der TI bezieht, unverzüglich nach Bekannt werden, spätestens jedoch zeitgleich mit Erfüllung der Informationspflicht nach § 42a Abs. 1 Satz 1 BDSG bzw. § 83a SGB X, dem koordinierenden Datenschutzmanagement der TI melden. ⌫

⌦ **GS-A_4474 kDSM: Nutzung des Incident Managements der gematik**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN Meldungen von gravierenden Datenschutzverstößen nach § 42a BDSG bzw. § 83a SGB X gemäß den Regelungen zum übergreifenden Incident Management aus den übergreifenden Richtlinien zum Betrieb der TI [gemRL_Betr_TI] mit der Priorität 1 klassifizieren und übermitteln. ⌫

⌦ **GS-A_4475 kDSM: Stellungnahme bei gravierenden Datenschutzverstößen gemäß § 42a BDSG bzw. § 83a SGB X**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN im Fall von gravierenden Datenschutzverstößen nach § 42a BDSG bzw. § 83a SGB X die an die Aufsichtsbehörde gesendete Meldung mit den Angaben nach § 42a Satz 3 und Satz 4 BDSG bzw. § 83a SGB X an das koordinierende Datenschutzmanagement der TI senden.⌫

⌦ **GS-A_4476 kDSM: Maßnahmen zur Behebung gravierender Datenschutzverstöße**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN bei gravierenden Datenschutzverstößen,

von denen sie betroffen sind, bei der Behebung der Ursachen des Verstoßes mitwirken.⌫

⌦ **GS-A_4477 kDSM: Umgehende Umsetzung von Maßnahmen bei gravierenden Datenschutzverstößen**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN bei gravierenden Datenschutzverstößen die mit dem koordinierenden Datenschutzmanagement der TI abgestimmten Maßnahmen umgehend umsetzen und den erfolgreichen Abschluss an das koordinierende Datenschutzmanagement der TI melden.⌫

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

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN der gematik zusichern, dass die gematik die Umsetzung der Maßnahmen, die sich aufgrund eines Datenschutzverstoßes beim Anbieter ergaben und mit dem koordinierenden Datenschutzmanagement der TI abgestimmt wurden, beim Anbieter kontrollieren kann.⌫

## 3.4 Meldung von Kontaktinformationen zum Datenschutzmanagement

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

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN Änderungen an den Kontaktinformationen ihres Datenschutzmanagements umgehend dem koordinierenden Datenschutzmanagement der TI melden.⌫

Die gematik veröffentlicht die übermittelten Kontaktinformationen zum Datenschutzmanagement der Anbieter auf ihren Internetseiten.

## 3.5 Berücksichtigung von Informationen des koordinierenden DSM

Das koordinierende DSM informiert Anbieter der TI

- über wesentliche Änderungen im Datenschutzrecht und wesentliche Ergebnisse des technischen Fortschritts, sofern diese Auswirkungen auf die Einhaltung der Vorschriften zum Schutz personenbezogener Daten der vom Anbieter betriebenen Produkte der TI haben,
- über Änderungen von Datenschutzanforderungen der TI, sofern diese Auswirkungen auf die vom Anbieter betriebenen Produkte haben,
- bei gravierenden Datenschutzverstößen in der TI, die mehrere Beteiligte der TI und insbesondere Anbieter betreffen.

Eigene gesetzliche oder vertragliche Pflichten der Anbieter bleiben durch die Information des koordinierenden DSM der TI unberührt.

⌦ **GS-A_4480 kDSM: Berücksichtigung von Änderungen im Datenschutzrecht und Ergebnissen des technischen Fortschritts**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN die vom koordinierenden Datenschutzmanagement der TI bereitgestellten Informationen zu Änderungen im Datenschutzrecht und zu Ergebnissen des technischen Fortschrittes in ihrem Datenschutzmanagement berücksichtigen.⌫

⌦ **GS-A_4481 kDSM: Berücksichtigung von Änderungen der Datenschutzanforderungen der TI**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN Änderungen der Datenschutzanforderungen der TI in ihrem Datenschutzmanagement berücksichtigen.⌫

⌦ **GS-A_4482 kDSM: Kontrolle der Umsetzung von Maßnahmen durch die gematik**

Anbieter von zentralen Diensten der TI-Plattform und Anbietern von fachanwendungsspezifischen Diensten MÜSSEN der gematik zusichern, dass die gematik die Umsetzung der Maßnahmen, die sich aus Änderungen der Datenschutzanforderungen der TI ergaben, beim Anbieter kontrollieren kann.⌫

# Anhang A

## A1 – Abkürzungen

| Kürzel | Erläuterung |
|---|---|
| bDSB | betrieblicher Datenschutzbeauftragter |
| BDSG | Bundesdatenschutzgesetz |
| DSM | Datenschutzmanagement |
| ISM | Informationssicherheitsmanagement |
| SGB | Sozialgesetzbuch |
| TI | Telematikinfrastruktur |

## A2 – Glossar

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

## A3 – Tabellenverzeichnis

Tabelle 1: Tab_kDSM_001_Inhalte Kennzahlen-Report ..... 18

## A4 - Referenzierte Dokumente

### A5.1 – 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 |
|---|---|
| [gemRL_Betr_TI] | gematik: Übergreifende Richtlinien zum Betrieb der Telematikinfrastruktur |

| | |
|---|---|
| [gemSpec_ISM] | gematik: Koordinierendes Informationssicherheitsmanagement der Telematikinfrastruktur |

## A5.2 – weitere Referenzierungen

| [Quelle] | Herausgeber (Erscheinungsdatum): Titel |
|---|---|
| [BDSG] | Bundesdatenschutzgesetz (Fassung der Bekanntmachung vom 14.01.2003; zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009) |
| [RFC2119] | RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2119 |
| [SGB V] | BGBl. I S.2477 (20.12.1988):<br>Sozialgesetzbuch, Fünftes Buch<br>Zuletzt geändert durch Art. 4 G v. 14.4.2010 I 410<br>Gesetzliche Krankenversicherung |
| [SGB X] | Sozialgesetzbuch, Zehntes Buch<br>Zuletzt geändert durch Art. 4 Abs. 15 G v. 29.7.2009 I 2258<br>Sozialverwaltungsverfahren und Sozialdatenschutz |