*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.*

Änderungsbedarf:

Aufgrund der Anwendbarkeit der DSGVO am 25.5.2018 müssen Anforderungen angepasst werden.

Folgende Spezifkationen sind betroffen:

- gemSpec_X.509_TSP
- gemSpec_VPN_ZugD
- gemRL_Betr_TI
- gemSpec_FD_KOMLE
- gemSpec_InfoNFDM.

Hinweis 1: Die Dokumente gemSpec_Sich_DS und gemSpec_DSM sind ebenfalls von der DSGVO betroffen. Die Anpassung der darin betroffenen Anforderungen erfolgt im Rahmen der Anpassung der übergreifenden Anforderungen zum Datenschutz und der Informationssicherheit. Die Dokumente gemSpec_Sich_DS und gemSpec_DSM werden aufgelöst und durch die Dokumente gemSpec_DS_Anbieter und gemSpec_DS_Hersteller ersetzt. Diese Dokumente werden separat im Rahmen der neuen Spezifikationen der Datenschutz- und Sicherheitsanforderungen an Anbieter und Hersteller der TI freigegeben.

Hinweis 2: Das Dokument gemLF_Int_WA ist ebenfalls von der DSGVO betroffen. Dieser Leitfaden wird aufgelöst. Die Datenschutz- und Sicherheitsanforderungen für weitere Anwendungen ergeben sich dann aus dem Dokument gemSpec_DS_Anbieter, das separat freigegeben wird.

## Änderungen in gemSpec_X.509_TSP

Es sind die Anforderungen TIP1-A_4230 und TIP1-A_4235 betroffen.

### ⌦ TIP1-A_4230 Datenschutzgerechte Antrags- und Sperrprozesse

TSP-X.509 nonQES und gematik-Root-CA MÜSSEN die Antrags- und Sperrprozesse datenschutzgerecht ausgestalten, d.h. insbesondere ~~ist~~ sind für die ~~Erhebung,~~ Verarbeitung ~~und Nutzung~~ der Antrags- und Sperrauftragsdaten ~~das Prinzip der Datensparsamkeit und Zweckbindung~~ die Datenschutzgrundsätze gemäß Art. 5 DSGVO zu berücksichtigen sowie die technischen und organisatorischen Maßnahmen nach ~~Anlage zu § 9 BDSG~~ Art. 25 und Art. 32 DSGVO ~~sind~~ zu treffen.⌫

⌦ **TIP1-A_4235 Fehlerprotokollierung**

Falls es erforderlich sein sollte, dass TSP-X.509 nonQES und gematik-Root-CA eine Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung durchführen, MÜSSEN die Protokolldaten entsprechend ~~des Prinzips der Datenvermeidung und Datensparsamkeit nach §3a BDSG~~ des Datenschutzgrundsatzes der Datenminimierung gemäß Art. 5 Abs. 1 Satz 1 lit.c) DSGVO unter Berücksichtigung der Art. 25, 32 DSGVO derart gestaltet sein, dass nur personenbezogene Daten in der Art und dem Umfang enthalten ~~sein~~ sind, wie sie zur Behebung erforderlich sind.⌫

# *Änderungen in gemSpec_VPN_ZugD*

Es ist die Anforderung TIP1-A_5074 betroffen.

⌦ **TIP1-A_5074 VPN-Zugangsdienst, Einhaltung des Datenschutzes bei Protokollierung**

Der Anbieter des VPN-Zugangsdienstes MUSS unter Berücksichtigung des Art. 25 Abs. 2 DSGVO sicherstellen, dass die Daten aus dem SOAP-Request „registerKonnektorRequest“ nur für den Zweck der Registrierung von Konnektoren und der Missbrauchserkennung für die Dauer der Vertragslaufzeit verwendet werden, sofern nicht ausnahmsweise die Verarbeitung für einen anderen Zweck zulässig ist.

~~Diese Daten unterliegen der besonderen Zweckbestimmung gemäß § 31 BDSG und dienen nur zur Sicherstellung eines ordnungsgemäßen Betriebes des VPN-Zugangsdienstes.~~⌫

# *Änderungen in gemRL_Betr_TI*

Es ist die Anforderung GS-A_3884 betroffen.

⌦ **GS-A_3884 Priorisierung von Incidents**

ITSM-TI-Teilnehmer MÜSSEN jeden im übergreifenden Incident Management bearbeiteten bzw. an diesen Prozess übergebenen Incident gemäß nachfolgendem Schema priorisieren. Dabei ist die Anzahl der möglichen Prioritäten gemäß der Prioritätenmatrix wie folgt festgelegt:

**Tabelle 22: Tab_Betr_TIP_009 INC – Prioritätenmatrix**

| | | Auswirkung | | |
|---|---|---|---|---|
| **Dringlichkeit** | | **Hoch** | **Mittel** | **Niedrig** |
| | **Hoch** | 1 | 2 | 3 |
| | **Mittel** | 2 | 3 | 4 |

| Dringlichkeit | Auswirkung | | | |
|---|---|---|---|---|
| | **Niedrig** | 3 | 4 | 4 |

- Jeder im übergreifenden Incident Management bearbeitete bzw. an diesen Prozess übergebene Incident MUSS entsprechend einer vierstufigen Einteilung - wobei 1 die höchste und 4 die niedrigste Priorität ist - eingestuft werden.
- *Priorität 1- Kritisch,*
- *Priorität 2 - Hoch,*
- *Priorität 3 - Mittel,*
- *Priorität 4 - Niedrig.*

Die für einen Incident anzuwendende Priorität wird abgeleitet aus den beiden Faktoren „Auswirkung“ und „Dringlichkeit“. Folgende Festlegungen sind für eine korrekte Anwendung der beiden Faktoren zu beachten:

**Tabelle 23: Tab_Betr_TIP_026 INC – Festlegung von Dringlichkeit**

| Dringlichkeit | Beschreibung |
|---|---|
| **Hoch** | • Durch die Störung stehen dem Servicenehmer die ihm bereitgestellten Leistungen (und/oder Funktionen) nicht zur Verfügung, bzw. nur so eingeschränkt, dass die Nutzung des Services für den Servicenehmer im Rahmen seiner Aufgabenerfüllung nicht zumutbar ist.<br>• Die Sicherheit der TI ist nicht mehr gewährleistet<br>Die Störung der bereitgestellten Leistungen (und/oder Funktionen) lässt sich nicht durch eine Umgehungslösung für den Servicenehmer unmittelbar beseitigen. |
| **Mittel** | • Durch die Störung stehen dem Servicenehmer die ihm bereitgestellten Leistungen (und/oder Funktionen) erheblich eingeschränkt zur Verfügung. Die Nutzung des Services für den Servicenehmer ist im Rahmen seiner Aufgabenerfüllung jedoch möglich. |
| **Niedrig** | • Durch die Störung stehen dem Servicenehmer die ihm bereitgestellten Leistungen (und/oder Funktionen) ohne nennenswerte Auswirkungen zur Verfügung. |

**Tabelle 24: Tab_Betr_TIP_027 INC – Festlegung von Auswirkung**

| Auswirkung | Beschreibung |
|---|---|
| **Hoch** | • Eine Mehrheit (>50%) der Servicenehmer ist von der Störung betroffen<br>• Der durch die Störung verursachte Schaden weitet sich schnell aus, falls nicht unmittelbar eine Lösung bereitgestellt werden kann.<br>• Die Störung führt zu Verletzung gesetzlicher Vorschriften, wie z.B. |

| Auswirkung | Beschreibung |
|---|---|
| | aus Datenschutz und Informationssicherheit<br>• Die Störung hat eine hohe Auswirkung in der öffentlichen Wahrnehmung und führt zu einem erheblichem Imageverlust der TI |
| **Mittel** | • Eine beträchtliche Anzahl (>10%) der Servicenehmer ist von der Störung betroffen<br>• Die Störung kann zu Verletzung gesetzlicher Vorschriften führen, wie z.B. aus Datenschutz und Informationssicherheit |
| **Niedrig** | • Eine geringe Anzahl (<10%) der Servicenehmer ist von der Störung betroffen<br>• Eine Verletzung gesetzlicher Vorschriften ist nicht gegeben |

Für die Aspekte Informationssicherheit und Datenschutz gelten folgende Festlegungen:

- Jeder Incident MUSS auf die Sicherheitsrelevanz geprüft werden und bei Erfüllung der Sicherheitsrelevanz entsprechend gekennzeichnet werden (Feld 7: Sicherheitsrelevanz in „Tabelle 27: Tab_Betr_TIP_014 INC – Mindestinhalte Incident-Dokumentation“). Die Sicherheitsrelevanz ist gegeben, wenn die Vertraulichkeit bzw. Integrität eines schutzbedürftigen Informationsobjektes gefährdet ist.

- Jeder Incident MUSS auf die Datenschutzrelevanz geprüft werden und bei Erfüllung der Datenschutzrelevanz entsprechend gekennzeichnet werden (Feld 8: Datenschutzrelevanz in Tabelle 27: Tab_Betr_TIP_014 INC – Mindestinhalte Incident-Dokumentation). Datenschutzrelevanz ist gegeben, wenn personenbezogene Daten gemäß ~~§ 3 Abs. 1 [BDSG]~~ Art. 4 Nr. 1 DSGVO betroffen sind. ⌫

# *Änderungen in gemSpec_FD_KOMLE*

Es sind die Anforderungen KOM-LE-A_2135 und KOM-LE-A_2137 betroffen.

⌦ **KOM-LE-A_2135 Protokollierung von Vorgängen**

Für die Nachvollziehbarkeit der Vorgänge am Fachdienst KOM-LE MÜSSEN Maßnahmen und Verfahren gemäß DSGVO i.V.m. BDSG installiert werden. Die Protokollierung der folgenden Informationen ist dabei zulässig:

- Anmeldung von Nutzern (Nutzername und Uhrzeit),
- Informationen über empfangene, weitergeleitete und abgeholte Nachrichten Absender, Empfänger, Uhrzeit) und
- Fehlermeldungen (Fehler mit Beschreibung und Uhrzeit). ⌫

⌦ **KOM-LE-A_2137 Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung**

Falls im KOM-LE-Fachdienst eine Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung erfolgt, MUSS der KOM-LE-Fachdienst unter Berücksichtigung des Art. 25 Abs. 2 DSGVO sicherstellen, dass in den Protokolldaten entsprechend ~~des Prinzips der Datenvermeidung und Datensparsamkeit nach § 3a BDSG~~ dem Datenschutzgrundsatz nach Art. 5 DSGVO nur personenbezogene Daten in der Art und dem Umfang enthalten sind, wie sie zur Behebung erforderlich sind und dass die erzeugten Protokolldaten im Fachdienst nach der Behebung unverzüglich gelöscht werden. ⌫

# *Änderungen in gemSpec_InfoNFDM*

Es ist die Anforderung NFDM-A_2035 betroffen.

| | |
|---|---|
| element name | **NFD_Versicherter_Einwilligung** |
| type | |
| content | complex |
| maxLength | |
| minOccurs | 1 |
| maxOccurs | 1 |
| pattern | |
| Schlüssel-verzeichnis | |
| Beschreibung | Angaben zur Einwilligung des Versicherten in die Nutzung der Notfalldaten (papiergebundene Hinterlegung bei einem Arzt). |
| Kommentar | Die Adressangaben beziehen sich niemals auf den Versicherten, sondern auf den Ort der Ablage der Einwilligung. Dies ist in aller Regel die Praxis eines Arztes.<br><br>Zieht der Versicherte seine Einwilligung in die Anlage und Nutzung der Notfalldaten zurück, ist der Notfalldatensatz zu löschen. Hierbei sind jedoch rechtliche Vorgaben in Bezug auf die Dokumentationspflicht des Arztes zu beachten, so dass der Datensatz dem Anwender ~~zwar~~ nicht mehr zur unmittelbaren Verfügung steht~~,~~ und die Verarbeitung der Daten im Primärsystem des Anwenders eingeschränkt wird ~~an sich aber lediglich gesperrt sind~~. Somit sind sie nur noch für den vorgesehenen Zweck des rechtlichen Nachweises nutzbar. Dies ist bei der Implementierung zu beachten. [NFDM-A_2035]<br><br>⌦ **NFDM-A_2035 PS: Sperrung von NFD bei Widerruf der Einwilligung**<br><br>Das Primärsystem MUSS bei Widerruf der Einwilligung durch den Versicherten sicherstellen, dass der Notfalldatensatz im Rahmen der Löschung der Notfalldaten im Primärsystem des Arztes abgelegt und dort ~~zur weiteren Verwendung gem. § 35 Abs. 3 BDSG gesperrt~~ die Verarbeitung gemäß § 35 Abs. 3 BDSG i.V.m. Artikel 18 DSGVO eingeschränkt wird. ⌫ |