Elektronische Gesundheitskarte und Telematikinfrastruktur

Datennutzungskonzept Betriebsdaten der dezentralen Komponenten

Version:	1.0.1
Stand:	04.08.2021
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemKPT_Betriebsdaten_Kon]

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um eine Erstveröffentlichung.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
	09.03.21		Initialer Entwurf	Team Edge Cyber Defense Center
1.0.0 CC	12.03.21		Zur Abstimmung freigegeben	gematik
	22.03.21		Rückmeldungen vom BFDI eingearbeitet; Darstellung des Personenbezuges und Handhabung personenbezogener Daten; Rückmeldung des BSI eingearbeitet: Historie aus 3.2.1 entfernt	gematik
	16.04.21		Rückmeldungen aus Kommentierung eingearbeitet um das KIM Clientmodul in der Betrachtung einzuschließen	gematik
1.0.0 CC 2	22.04.21		Weitere Abstimmungen	gematik
	15.07.21	3.1.3	Anpassung Personenbezug der Betriebsdaten nach Abstimmung mit BfDI Beispielwerte SiteType an Enummeration des Schemas angepasst.	gematik
1.0.1	04.08.21		freigegeben	gematik

 © gematik - öffentlich

Inhaltsverzeichnis

Dokumentinformationen 2

Inhaltsverzeichnis 3

1 Einordnung des Dokuments 4

1.1 Einleitung 4

1.2 Zielgruppe 4

1.3 Geltungsbereich 4

1.4 Abgrenzung des Dokuments 4

2 Zweck der Datenerhebung 5

2.1 Rechtsgrundlage 5

3 Umfang und Nutzung der Datenerhebung 6

3.1 Betriebsdaten 6

3.1.1 Ablauf der Datenübertragung 6

3.1.2 Beschreibung der Datenstrukturen 6

3.1.3 Personenbezug der Betriebsdaten 10

3.2 Scan öffentlicher IP-Adressen 10

3.2.1 Ausgangslage 10

3.2.2 Maßnahmen 10

3.2.2.1 Ablauf *11*

3.2.2.2 Weiterführende Informationen *12*

3.2.3 Personenbezug der IP-Adressen 12

4 Löschfristen 14

4.1 Betriebsdaten 14

4.2 IP-Adressen 14

Anhang A – Verzeichnisse 15

A1 – Tabellenverzeichnis 15

A2 – Referenzierte Dokumente 15

A3 – Offene Punkte/Klärungsbedarf 15

1 Einordnung des Dokuments

1.1 Einleitung

Dieses Dokument beschreibt die Erfassung und Übermittlung von Betriebsdaten der Konnektoren und von öffentlichen IP-Adressen der Leistungserbringerumgebungen zu dem Zweck, die Sicherheit, Verfügbarkeit und Nutzbarkeit der Telematikinfrastruktur zu gewährleisten.

1.2 Zielgruppe

Dieses Konzept richtet sich an Gesellschafter der gematik und Leistungserbringer, die Konnektoren betreiben.

1.3 Geltungsbereich

Die in diesem Dokument beschriebenen Sachverhalte und Abläufe gelten für alle Leistungserbringerumgebungen, in denen Konnektoren betrieben werden. Die Übermittlung von Betriebsdaten der Konnektoren über den VPN-Zugangsdienst an die gematik ist ab Konnektor PTV5 geplant.

1.4 Abgrenzung des Dokuments

Die technische Spezifikation zum Senden der Betriebsdaten vom Konnektor an den VPN-Zugangsdienst (Betriebsdatenerfassung) ist in [gemSpec_Kon], [gemSpec_VPN_ZugD] und [gemSpec_SST_LD_BD] beschrieben.

Die Anforderungen zur Übermittlung der öffentlichen IP-Adressen der Kunden des VPN-Zugangsdienstes an die gematik sind in [gemSpec_VPN_ZugD] und [gemSpec_DS_Anbieter] beschrieben.

 © gematik - öffentlich

2 Zweck der Datenerhebung

2.1 Rechtsgrundlage

Die Rechtsgrundlage für die Übermittlung der Daten ist SGB V. Gemäß § 331 SGB V hat die gematik den gesetzlichen Auftrag, im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik Maßnahmen zur Überwachung des Betriebs zu treffen, die erforderlich sind, um die Sicherheit, Verfügbarkeit und Nutzbarkeit der Telematikinfrastruktur zu gewährleisten. Dies umfasst auch Komponenten und Dienste der Telematikinfrastruktur, die im dezentralen Bereich betrieben werden und Komponenten und Dienste, die die Telematikinfrastruktur nutzen, aber außerhalb der Telematikinfrastruktur betrieben werden.

Betriebsdaten aus den Leistungserbringerumgebungen werden benötigt, damit die gematik bei technischen Fehlersituationen in Zusammenarbeit mit den Industriepartnern schnell und gezielt Maßnahmen ergreifen kann, um die Verfügbarkeit der Anwendungen (ePA, KIM, E-Rezept, VSDM) sicherzustellen bzw. wiederherzustellen. Die gematik darf nach § 331 Abs. 4 SGB V Daten sammeln zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse der Telematikinfrastruktur. Dem Leistungserbringer wird keine Möglichkeit gegeben, dem Senden der Betriebsdaten zu widersprechen. Der Widerspruch wird ausgeschlossen, weil andernfalls Störungen nicht wirksam vermieden bzw. beseitigt werden können.

Um sicherheitskritische Fehlkonfigurationen von Internetanschlüssen von Leistungserbringerumgebungen zu identifizieren, führt die gematik Sicherheitsscans auf öffentlichen IP-Adressen von Vertragspartnern der VPN-Zugangsdienstanbieter aus. Entsprechende Fehlkonfigurationen können unautorisierte Zugriffe auf die Telematikinfrastruktur zur Folge haben. Bei den Sicherheitsscans folgt die gematik Grundsätzen der Datensparsamkeit und Zweckbindung auf Basis ihres gesetzlichen Auftrags gemäß § 330 und § 331 SGB V.

In Fällen, in denen eine unmittelbare Gefahr für die Telematikinfrastruktur entsteht, kann die gematik eine temporäre Sperrung des VPN-Zugangs zur TI anordnen (§ 329 SGB V).

Die personenbezogenen Daten (Vertragsnummern und öffentliche IP-Adressen) unterliegen der DSGVO. Die Rechtmäßigkeit der Verarbeitung dieser Daten ergibt sich aus SGB V und Art. 6 Abs. 1 lit. c) und e) DSG-VO i.V.m. § 331 Abs. 1 und 4 SGB V.

 © gematik - öffentlich

3 Umfang und Nutzung der Datenerhebung

In Kapitel 3 werden die Datenelemente der erhobenen Daten beschrieben. Es wird dargestellt, welche Informationen die einzelnen Datenelemente beinhalten, an wen die Daten übermittelt werden, welchem Zweck die Datenerhebung dient und wozu die Daten verwendet werden.

3.1 Betriebsdaten des Konnektors

3.1.1 Ablauf der Datenübertragung

Der Konnektor übermittelt dem VPN-Zugangsdienst über eine technische Schnittstelle Betriebsdaten. Die Betriebsdaten werden täglich automatisch gesendet, wenn der Konnektor eine Verbindung zum VPN-Zugangsdienst aufgebaut hat.

Die Betriebsdaten werden automatisch durch die Firmware des Konnektors erzeugt.

Damit der VPN-Zugangsdienstanbieter die Betriebsdaten dem jeweiligen Vertragspartner zuordnen kann, fügt der Konnektor dem Betriebsdatensatz die Contract ID bei. Die Contract ID ist ein personenbezogenes Datum. Außer der Contract ID übermittelt der Konnektor keine personenbezogenen Daten an den VPN-Zugangsdienst. Die Contract ID wird nicht an die gematik gesendet. Andere Daten mit möglichem Personenbezug (z. B. Kartenterminal-IDs) werden von der Firmware des Konnektors automatisch vor dem Übermitteln an den VPN-Zugangsdienst entfernt.

Vor dem Weiterleiten der Betriebsdaten an die gematik, entfernt der VPN-Zugangsdienst die Contract ID und den Update Mode und fügt dem Betriebsdatensatz die Betriebsstättenart hinzu. Die Betriebsstättenart umfasst Kategorien von Leistungserbringerumgebungen, z. B. Einzelpraxis, Berufsausübungsgemeinschaft, MVZ, Krankenhaus, Apotheke.

3.1.2 Beschreibung der Datenstrukturen

Tabelle 1: Datenelemente Betriebsdaten

Datenelemente	
Contract ID	
Klassifikation	unmittelbar identifizierendes Merkmal
Empfänger	VPN-ZugD-Anbieter
Beschreibung	Die Contract ID ist die Vertragsnummer des TI-Teilnehmers beim VPN-Zugangsdienst. Über seine Kundendatenbank kann der VPN-ZugD-Anbieter dieser ID die Person zuordnen, die den Konnektor betreibt. Der Konnektor sendet die Contract ID nur an den VPN-ZugD. Vor Übermittlung der Betriebsdaten an die gematik entfernt der VPN-ZugD-Anbieter die Contract ID. Diese wird nicht an die gematik übermittelt.
Verwendung	Die Contract ID dient dem VPN-ZugD-Anbieter zur Identifikation des Vertragspartners und der Zuordnung der Betriebsdaten zum Vertragspartner. Dem VPN-ZugD sind die Vertragsnummern aller seiner Kunden bekannt.
Product Information	

Datenelemente		
Klassifikation	keine	
Empfänger	VPN-ZugD-Anbieter, gematik	
Beschreibung	Produktinformationen des Konnektors Produkttypversion, Informationen über den Hersteller, Produktbezeichnung, Version des Konnektorprodukts (Hardware und Firmware)	
Verwendung	Die Produktinformationen werden zur Identifikation sicherheitskritischer oder nicht (mehr) zugelassener Konnektorversionen verwendet, um den Einsatz solch kritischer Versionen nachzuvollziehen und notwendige Schritte zu Updates oder Außerbetriebnahme einzuleiten.	
Configuration		
Klassifikation	keine	
Beschreibung	Konfigurationseinstellungen des Konnektors	
	TI Connection Mode	
	Empfänger	VPN-ZugD-Anbieter, gematik
	Beschreibung	Einstellung, ob der Konnektor „In Reihe" oder „parallel" geschaltet ist.
	Verwendung	Fehlerkonstellationen in den einzelnen Connection Modes können beim Auftreten von Fehlern zur Fehleranalyse herangezogen werden.
	Standalone Mode	
	Empfänger	Keiner *(Das Datenelement wird aus dem Schema der Betriebsdaten entfernt.)*
	Internet Mode	
	Empfänger	VPN-ZugD-Anbieter, gematik
	Beschreibung	Einstellung, ob und auf welche Weise der Konnektor Pakete ins Internet weiterleitet. Mögliche Einstellungen sind: • Weiterleiten in den VPN-Tunnel zum Sicheren Internet Service (SIS) • Weiterleiten über das Internet Access Gateway (IAG) der Leistungserbringerumgebung • kein Weiterleiten ins Internet
	Verwendung	Durch Wechselwirkungen im VPN-Modul kann der Internetmodus im Störungsfall auf die Verfügbarkeit der Telematikinfrastruktur wirken. Die Information hilft, Störungsursachen und betroffene Institutionen zu identifizieren.
	Client Connection Mode	
	Empfänger	VPN-ZugD-Anbieter, gematik

 © gematik - öffentlich

Datenelemente		
	Beschreibung	Einstellungen, die sich auf die technische Anbindung der Primärsysteme beziehen: • Verschlüsselte Verbindung über Transport Layer Security (TLS) • Art der Authentisierung der Primärsysteme
	Verwendung	An diesen Parametern ist ableitbar, in wie vielen Leistungserbringerinstitutionen die Schnittstellen zur Telematikinfrastruktur unverschlüsselt bzw. ohne Authentifizierung verfügbar sind. Die Daten ermöglichen, betroffene Institutionen zu identifizieren, sobald solche Konstellationen als unzulässig eingestuft werden.
	Update Mode	
	Empfänger	VPN-ZugD-Anbieter
	Beschreibung	Verhalten des Konnektors bei vorliegenden Firmwareupdates auf dem KSR: • Einstellung, ob vorliegende Updates automatisch heruntergeladen werden • Einstellung, ob heruntergeladene Updates automatisch installiert werden Der Konnektor sendet den Update Mode nur an den VPN-ZugD. Vor Übermittlung der Betriebsdaten an die gematik entfernt der VPN-ZugD-Anbieter den Update Mode. Dieser wird nicht an die gematik übermittelt.
	Verwendung	Die Information ermöglicht dem VPN-Zugangsdienst die Identifikation von Kunden, die keine automatischen Updates konfiguriert haben. Damit können die Betreiber vom Dienstleister bzw. VPN-ZugD-Anbieter direkt angesprochen werden, um bei dringenden Updates eine schnelle Aktivierung zu erreichen.
Connector		
Klassifikation	keine	
Empfänger	VPN-ZugD-Anbieter, gematik	
Beschreibung	Verbindungsstatus zu VPN-Konzentrator TI und VPN-Konzentrator SIS, mit Angabe des Zeitpunkts der Änderung des Verbindungsstatus Liste der Fehlerzustände des Konnektors	
Verwendung	Aus den Verbindungsstatus zum VPN-Konzentrator TI und VPN-Konzentrator SIS ist die Auswirkung von Fehlerfällen in diesem Bereich erkennbar. Die Fehlerzustände liefern Informationen zu konkreten Fehlern bei betroffenen Geräten. Die Information erlaubt Fehlerzustände mit spezifischen Konfigurationen zu korrelieren und so Störungsursachen zu ermitteln. Außerdem wird das Ausmaß und der Umfang einer Störung erkennbar.	
Trust Status		
Klassifikation	keine	
Empfänger	VPN-ZugD-Anbieter, gematik	

Datenelemente	
Beschreibung	Informationen über aktuelle Vertrauens- und Sperrlisten im Konnektor: • Certificate Revocation List (CRL) • Trust Service Status List (TSL) • Vertrauensliste der Bundesnetzagentur (BNetzA-VL) Die Informationen umfassen Nummer der Liste, Gültigkeitsbeginn bzw. Erstellungsdatum und Zeitpunkt der nächsten Aktualisierung.
Verwendung	Die Informationen sollen dazu genutzt werden, kritische Gerätezustände bzgl. der Vertrauens- und Sperrlisten vorab zu erkennen. Der gematik ermöglicht die Information, Störungen bei zentralen Diensten frühzeitig zu erkennen und so die Verfügbarkeit der TI sicherzustellen.
Connector Certificates	
Klassifikation	keine
Empfänger	VPN-ZugD-Anbieter, gematik
Beschreibung	Ablaufdaten der Kartenzertifikate der gSMC-K
Verwendung	Die Ablaufdaten ermöglichen es, eine rechtzeitige Transition bzw. einen Austausch der Geräte sicherzustellen, und somit Funktionsausfälle zu verhindern. Der gematik ermöglichen diese Informationen, einen drohenden Ausfall von vielen Konnektoren zu erkennen und Gegenmaßnahmen einzuleiten.
Card Terminals	
Klassifikation	keine
Empfänger	VPN-ZugD-Anbieter, gematik
Beschreibung	Produktinformationen der angeschlossenen Kartenterminals • Produkttypversion, Informationen über den Hersteller, Produktbezeichnung, Version des KT-Produkts (Hardware und Firmware) Ablaufdaten der Kartenzertifikate der gSMC-KT
Verwendung	Die Produktinformationen der KTs werden zur Identifikation sicherheitskritischer oder nicht (mehr) zugelassener KT-Versionen verwendet, um den Einsatz solch kritischer Versionen nachzuvollziehen und notwendige Schritte zu Updates oder Außerbetriebnahme einzuleiten. Die Ablaufdaten der Kartenzertifikate gSMC-KT dienen der rechtzeitigen Wartung der Geräte durch Austausch der gSMC-KT, um Funktionsausfälle zu vermeiden. Der gematik ermöglichen diese Informationen, einen drohenden Ausfall von vielen Kartenterminals zu erkennen und Gegenmaßnahmen einzuleiten.
Site Type	
Klassifikation	keine
Empfänger	gematik
Beschreibung	Kategorie der Leistungserbringerumgebung, in der der Konnektor eingesetzt ist, z. B. Arztpraxis, Zahnarztpraxis, MVZ, Krankenhaus, Apotheke.
Verwendung	In Fehlerfällen sind aus den betroffenen Kategorien von Leistungserbringerumgebungen Aussagen zum Lagebild der TI ableitbar.

 © gematik - öffentlich

3.1.3 Personenbezug der Betriebsdaten

Der Datensatz Betriebsdaten, wie er vom Konnektor zum VPN-Zugangsdienst übertragen wird, ist personenbezogen, weil es dem Zugangsdienstbetreiber möglich ist, die Contract-ID als unmittelbar identifizierendes Merkmal, auf die Person des Vertragspartners aufzulösen. Der VPN-Zugangsdienst muss hier die Grundsätze für die Verarbeitung personenbezogener Daten aus Artikel 5 DSGVO beachten. Die gematik hat in der Definition des Datensatzes dem Prinzip der Datenminimierung folgend nur Daten aufgenommen, die für den in diesem Dokument erläuterte Verwendung notwendig sind.

Der Datensatz Betriebsdaten, wie er zur gematik übertragen wird, enthält keine unmittelbar identifizierenden Merkmale. Durch die Anzahl der Merkmale kann jedoch nicht ausgeschlossen werden, dass Merkmalskombinationen nur bei einzelnen bzw. wenigen Konnektoren vorkommen. Durch die geringe Zahl an Merkmalen gegenüber ca 150.000 Datensätzen, den Mangel an personenbeziehbaren Informationen sowie das Fehlen von Daten für eine Korrellation mit personenbezogenen Daten, fällt die Verarbeitung dieser Daten durch die gematik nicht unter die Regelung der DSGVO.

3.1.4 Nutzung der Betriebsdaten

Die vom Konnektor gesendeten Betriebsdaten sollen dazu genutzt werden um das Sicherheitsniveau der TI auch im dezentralen Bereich unterstützend durch den VPN-Zugangsdienst im konkreten Fall und durch die gematik in der Rolle des Gesamtverantwortlichen für die TI aufrecht zu erhalten. Dies bedeutet, dass die gesendeten Daten und Konfigurationen auf kritische Zustände hin geprüft werden und ggf. eine Meldung an den entsprechenden Nutzer gegeben wird.

Dies bedeutet, dass auch die Gültigkeit der Produkttypen gegen die Zulassungen der gematik analog zum bisherigen Verfahren über den KSR, jetzt direkt über den VPN-Zugangsdienst erfolgt. Dabei steht die umfassende, proaktive Einbindung aller Stakeholder mit dem Ziel des Supports im Vordergrund. Eine Sperrung eines TI-Zugangs ist nur das Mittel der letzten Wahl, wenn Gefährdungen der TI über andere organisatorische Maßnahmen nicht beseitigt werden konnten.

Die Betriebsdaten aus dem dezentralen Bereich werden bei der gematik dabei auf dem gleichen Weg wie das Anbieterreporting verarbeitet, also über die Betriebsdatenerfassung. Allerdings ohne Prüfung gegen Servicelevel, sondern ausschließlich zu den vorab beschriebenen Zwecken.

3.2 Scan öffentlicher IP-Adressen

3.2.1 Ausgangslage

Durch Fehlkonfigurationen der Internetanschlüsse von Praxen ist es möglich, dass Konnektoren über das Internet erreichbar sind, und teilweise auch weitere IT-Systeme der Praxen.

3.2.2 Maßnahmen

Fehlkonfigurationen des Internetanschlusses lassen sich durch einen Scan der IP-Adresse erkennen. Die Scans haben das Ziel zu verhindern, dass Fehlkonfigurationen des Internetanschlusses zu einer Gefährdung der Telematikinfrastruktur führen. Weiterhin möchte die gematik die Leistungserbringer dabei unterstützen, die Sicherheit der von ihnen verantworteten Versichertendaten zu gewährleisten.

Die gematik folgt bei den Scans Grundsätzen der Datensparsamkeit und Zweckbindung auf Basis ihres gesetzlichen Auftrags gemäß § 330 und § 331 SGB V. Die gematik hat das

Vorgehen mit Vertretern des BSI und BfDI im Vorfeld abgestimmt. Für eine möglichst hohe Transparenz ist das Vorgehen im Folgenden detailliert dargestellt.

3.2.2.1 Ablauf

Tabelle 2: Datenelement IP-Adresse

Datenelement	
IP-Adressbereiche angeschlossener Konnektoren	
Klassifikation	unmittelbar identifizierendes Merkmal
Empfänger	gematik
Beschreibung	IP-Adressen der an den VPN-Zugangsdienst angeschlossenen Leistungserbringerinstitutionen. Diese Daten sind nicht mit den Betriebsdaten aus Tabelle 1 verknüpft.
Verwendung	Die gematik nutzt die IP-Adressen, um zu prüfen, ob wegen falscher Konfigurationen des Internetzugangs ungesicherte Schnittstellen der Telematikinfrastruktur aus dem Internet erreichbar sind.

Schritt 1

Konnektoren melden sich mit der vom Internetprovider vergebenen IP-Adresse am VPN-Zugangsdienst der Telematikinfrastruktur an.

Schritt 2

Die IP-Adresse wird durch den VPN-Zugangsdienstanbieter gespeichert und an die gematik übermittelt.

Schritt 3

Die gematik führt auf diese IP-Adressen einen Sicherheitsscan durch. Hierbei wird ausschließlich geprüft, ob und wenn ja welche eingehenden Verbindungen in das jeweilige Netz zugelassen werden. Die gematik konzentriert sich hierbei auf ausgewählte Ports, um negative Auswirkungen auf die Internetverbindung der Praxis auszuschließen.

Auf Port 80 (http) und 443 (https) wird – sofern einer dieser Ports eingehende Verbindungen zulässt - ein http Request ausgelöst, um zu prüfen, ob eine spezielle Konfigurationsdatei des Konnektors (SDS) abrufbar ist und somit ein Zugriff auf den Konnektor möglich ist. Die SDS-Datei liefert Angaben über den Hersteller, das Konnektormodell, die Liste der Dienste, Dienstversionen und Endpunkte der Dienste. Die SDS-Datei enthält keine personenbezogenen oder personenbeziehbaren Informationen der Leistungserbringerumgebung oder von Versicherten.

Zum Abschluss des Scans werden alle IP-Adressen, bei denen keine Auffälligkeiten festgestellt wurden, gelöscht, da die Zweckbindung der Datenspeicherung entfällt.

Schritt 4

Sofern bei einzelnen Internetanschlüssen Fehlkonfigurationen oder Auffälligkeiten erkannt wurden, wendet sich die gematik mit den dazugehörigen IP-Adressen erneut an den VPN-Zugangsdienstanbieter, um den dazugehörigen Vertragspartner, die Contract ID und die ICCSN der SMC-B/gSMC-K zu ermitteln.

Schritt 5

Diese Informationen (ICCSN und Contract ID) werden durch den VPN-Zugangsdienstanbieter bzw. die gematik nachfolgend an den Vertragspartner (Dienstleister vor Ort) weitergereicht und dieser wird aufgefordert, die Fehlkonfiguration des Internetanschlusses zu beheben. In Fällen, in denen eine unmittelbare Gefahr für die Telematikinfrastruktur entsteht, kann die gematik auch eine temporäre Sperrung des VPN-Zugangs zur TI anordnen (§ 329 SGB V).

Schritt 6

Nach Behebung der Fehlkonfigurationen löscht die gematik die IP-Adressen und die in diesem Zusammenhang erhobenen Daten (Contract ID, ICCSN).

3.2.2.2 Weiterführende Informationen

Bei den Scans oder im Nachgang werden keine Aktionen ausgelöst, die zu einem Verlust der Verfügbarkeit des Internetanschlusses oder exponierter Systeme führen können. Weiterhin werden keine Aktionen ausgelöst, die einen Zugriff auf personenbezogene Daten von Mitarbeitern in der Leistungserbringerumgebung oder von Versicherten zur Folge haben könnten. Anhand der Scanergebnisse kann keine vollständige Aussage über die Sicherheit des Internetanschlusses der Praxis getroffen werden. Die Scanergebnisse können jedoch dazu beitragen, den direkten Zugriff auf Konnektoren aus dem Internet zu unterbinden. Weiterhin können die Scans dazu beitragen, die Konfiguration der Internetanschlüsse in den Leistungserbringerumgebungen durch den IT-Dienstleister oder den versierten Leistungserbringer selbst zu überprüfen. Grundsätzlich gilt: Es sollten keine eingehenden Verbindungen an der Internetfirewall erlaubt werden, sofern hierfür keine Erforderlichkeit besteht. Sofern eingehende Verbindungen zugelassen werden, müssen zusätzlich Sicherheitsmaßnahmen getroffen werden, um den unberechtigten Zugriff auf das Netz der Leistungserbringerumgebung aus dem Internet wirksam zu verhindern.

3.2.3 Personenbezug der IP-Adressen

IP-Adressen werden als personenbezogene Daten klassifiziert. Zwar hat die gematik keine Daten, über die sie die IP-Adressen Personen zuordnen kann, anderen Akteuren im Internet kann dieses jedoch möglich sein. Die Anforderungen der DSGVO werden durch die gematik beim Umgang mit den IP-Adressen sichergestellt.

3.3 Betriebsdaten des KIM-Clientmoduls

Das KIM-Clientmodul sendet im Mail Header seine Versionsinformationen an den KIM-Fachdienst, den der Leistungserbringer als KIM-Dienst nutzt. Der KIM-Fachdienst kann diese Information mit den anderen Informationen im unverschlüsselten Teil der KIM-Nachricht korrelieren, wie der Absender-KIM-Adresse als unmittelbar identifizierendem Merkmal.

Der KIM-Anbieter MUSS der gematik auf Anfrage eine nicht-personenbezogene Gesamtübersicht, der sich im Feld befindenden aktiven KIM-Clientmodule zur Verfügung stellen. (gemSpec_CM_KOMLE#A_21389)

Die gematik verwendet die Daten in ihrer Rolle einer koordinierenden Instanz mit dem Blick auf konsolidierte Daten. Eine Zuordnung der Informationen zu Personen oder Institutionen ist der gematik nicht möglich.

Tabelle 3: Datenelemente KIM-Clientmodul

Datenelemente (gemSpec_CM_KOMLE#A_21388)	
X-KIM-CMVersion: VendorID mit Produktversion	
Klassifikation	keine
Empfänger	KIM-Anbieter, aggregiert: gematik
Beschreibung	Über die VerdorID in Verbindung mit der Produkterversion wird die zugelassene Version des Clientmoduls identifiziert
Verwendung	Die Informationen werden vom KIM-Anbieter aggregiert und der gematik auf Verlangen zur Verfügung gestellt, um die Verbreitung unterschiedlicher Produktversionen nachzuvollziehen. Die Daten dienen dem KIM-Anbieter dazu, bei Verarbeitungsfehlern betroffene CM-Versionen zu identifizieren. Der KIM-Anbieter kommt mit der Information in die Lage, Leistungserbringer mit fehlerhaften CM-Versionen direkt zu adressieren. Die Daten werden auf Verlangen aggregiert der gematik bereitgestellt. Die gematik ermittelt die Verbreitung nicht zugelassener Version und nutzt die Information zur Ermittlung des Rolloutfortschrittes. Im Falle von Versionen mit Sicherheitsmängeln nutzt die gematik die Information zur Kommunikation mit Fachdienstbetreibern.
X-KIM-PTVersion: Produkttypversion des CM	
Klassifikation	keine
Empfänger	KIM-Anbieter, aggregiert: gematik
Beschreibung	Über Produkttypversion wird der Spezifikationsstand des CM identifiziert, mit dem das CM zugelassen wurde
Verwendung	Die Informationen werden vom KIM-Anbieter aggregiert und der gematik auf Verlangen zur Verfügung gestellt, um die Verbreitung unterschiedlicher Produkttypversionen nachzuvollziehen. Die gematik erkennt mit der Information die Verbreitung von nicht kompatiblen Clientmodulversionen und nutzt die Information zur Kommunikation mit Fachdienstbetreibern.

© gematik - öffentlich

4 Löschfristen

4.1 Betriebsdaten

Der VPN-Zugangsdienst löscht die vom Konnektor empfangenen Betriebsdaten nach spätestens 6 Wochen.

Die gematik löscht die vom VPN-Zugangsdienstanbieter empfangenen Betriebsdaten nach spätestens 3 Monaten.

Zusammengefasste Auswertungen sind von der Löschpflicht nicht betroffen.

4.2 IP-Adressen

IP-Adressen, bei denen keine Auffälligkeiten festgestellt wurden, löscht die gematik unmittelbar nach jedem Scan.

Daten, die die gematik im Zusammenhang mit IP-Adressen gespeichert hat, bei denen Auffälligkeiten festgestellt wurden, löscht die gematik unmittelbar nachdem die Fehlkonfigurationen vom Vertragspartner (Dienstleister vor Ort) behoben wurden, spätestens jedoch nach 3 Monaten.

 © gematik - öffentlich

Anhang A – Verzeichnisse

A1 – Tabellenverzeichnis

Tabelle 1: Datenelemente Betriebsdaten 6
Tabelle 2: Datenelement IP-Adresse 11
Tabelle 3: Datenelemente KIM-Clientmodul 13

A2 – Referenzierte Dokumente

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_DS_Anbieter]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter
[gemSpec_Kon]	gematik: Spezifikation Konnektor
[gemSpec_SST_LD_BD]	gematik: Spezifikation Logdaten- und Betriebsdatenerfassung
[gemSpec_VPN_ZugD]	gematik: Spezifikation VPN-Zugangsdienst

A3 – Offene Punkte/Klärungsbedarf

Kap.	Offener Punkt	Zuständig

 © gematik - öffentlich