# Bestätigung zur Erfüllung der vollständigen Anforderungslage

Verfahrensschlüssel: [Verfahrensschlüssel eintragen]

Hiermit bestätigen wir, dass der Anbieter [Name des Anbieters] die [Firmenname des Betreibers] mit der Erbringung der betrieblichen Leistungen beauftragt hat.

Der Betreiber wird den Anbieter gemäß den erbrachten Nachweisen und Eigenerklärungen aus dem Anbieterzulassungsverfahren bei der Erfüllung der im Anbietertypsteckbrief [Referenz ATSB] aufgeführten Anforderungen unterstützen.

In diesem Zusammenhang bestätigen Anbieter und Betreiber außerdem, folgende Anforderungen zu erfüllen:
*(Es sind alle zutreffenden Punkte explizit anzukreuzen, bis auf den Punkt zur Datenlieferung, bei dem die gewählte Variante anzukreuzen ist.)*

☐ Der Anbieter hat die Vertragsbeziehung mit den Endkunden.

☐ Sämtliche Anforderungen des Anbietertypsteckbriefs [Referenz Steckbrief] werden durch den Anbieter mit Unterstützung des Betreibers erfüllt.

☐ Der Anbieter gewährleistet ein durchgängiges IT-Service-Management vom UHD bis zum Betrieb des TI-Gateways (TIP1-A_6388-02). Das gilt unabhängig davon, ob der Anbieter den UHD selber erbringt (Anbieter Typ II) oder durch einen Unterauftragnehmer erbringen lässt (Anbieter Typ III).

☐ Die Ansprechpartner für die gematik entsprechend GS-A_4088-01 sind seitens des Anbieters und Betreibers benannt.

☐ Die Ansprechpartner für Informationssicherheitsthemen für die gematik sind seitens des Anbieters benannt (GS-A_4523-01, GS-A_4524-01).

Die notwendigen Datenlieferungen an die gematik und die Beteiligung an betrieblichen Sicherheitsprozessen (A_20719, A_20720, A_21719, GS-A_5559-01, GS-A_5562, GS-A_5558, A_19175)

☐ werden durch den Anbieter erfüllt

ODER

☐ hat der Anbieter auf den Betreiber übertragen wie folgt:

_____

_____

_____

☐ Die Ansprechpartner für Datenschutzthemen beim Anbieter sind benannt (GS-A_5564, GS-A_4479-01)

☐ Ein koordinierendes Datenschutzmanagement (GS-A_2076-01, GS-A_2214-01, GS-A_5626) ist beim Anbieter etabliert, das für die das TI-Gateway betreffenden Aspekte mit jenem des Betreibers verbunden ist, wobei mindestens der

Kontaktpunkt für Anfragen hinsichtlich der Erfüllung von Betroffenenrechten durch den Anbieter selbst umgesetzt ist.

☐ Die im Anforderungshaushalt enthaltenen notwendigen Informationslieferungen an die Endkunden und Kommunikationen mit den Endkunden bzw. die dafür notwendigen Prozesse werden seitens des Anbieters umgesetzt (A_23340, A_23382, A_23393).

☐ Sämtliche am Betrieb des TI-Gateways beteiligten Betriebsstätten – insbesondere auch jene des Anbieters selbst – befinden sich innerhalb der EU bzw. des EWR (GS-A_5551).

☐ Sämtliche im Sicherheitsgutachten des Betreibers ggf. als „durch den Anbieter umzusetzen" deklarierten Punkte werden vom Anbieter selbst umgesetzt.

☐ Der Anbieter hat den Betreiber im Verhältnis zur gematik zur Abgabe und Entgegennahme aller erforderlichen Erklärungen sowie zur Durchführung aller tatsächlichen Handlungen berechtigt und verpflichtet, soweit diese zur Erbringung der Betriebsleistung erforderlich sind. Insbesondere hat er ihn zur Teilnahme an den Service-Reviews als Vertreter des Anbieters bevollmächtigt.

☐ Der Anbieter und der Betreiber bestätigen, dass der Anbieter gegenüber dem Betreiber über die zur ordnungsgemäßen Erbringung der Betriebsleistung notwendigen Weisungs- und Kontrollrechte verfügt.*

Uns ist bewusst, dass es sich bei allen oben genannten Punkten um Zulassungsvoraussetzungen handelt. Wird einer dieser Punkte nicht erfüllt, kann keine Anbieterzulassung erteilt werden. Die Nichteinhaltung eines dieser Punkte während der Dauer der Zulassung kann zum Verlust der Zulassung führen. Änderungen zu den in diesem Schreiben bestätigten Sachverhalten nach Erteilung der Zulassung sind daher der gematik unverzüglich mitzuteilen.

…….  …….

Unterschrift Anbieter  Unterschrift Betreiber

…….

Unterschrift Dritte (falls zutreffend)

*) Dies muss auch dann zutreffen, wenn Anbieter und Betreiber kein unmittelbares Vertragsverhältnis haben. Diese Erklärung muss dann durch sämtliche zwischengeschaltete Dritte mit unterzeichnet werden.

## Anhang - Referenzierte Anforderungen:

**TIP1-A_6388-02 - Bereitstellung eines lokalen IT-Service-Managements durch Anbieter für ihre zu verantwortenden Servicekomponenten**
Anbieter MÜSSEN für die von ihnen verantworteten Servicekomponenten ein lokales ITSM etablieren.**[<=]**

**GS-A_4088-01 - Benennung von Ansprechpartnern**
TI-ITSM-Teilnehmer MÜSSEN Kontaktdaten von Ansprechpartnern im TI-ITSM-System eintragen und aktuell halten für

- die Rolle Service Delivery Manager (agiert auch als 1. Eskalationsstufe),
- die 2. Eskalationsstufe,
- für alle für den TI-ITSM-Teilnehmer relevanten Prozesse gemäß Tabelle gemKPT_Betr#Tab_KPT_Betr_TI_003 Mitwirkungsverpflichtung im TI-ITSM
- das Notfall-Management,
- die Unternehmenskommunikation (u.a. Krisenkommunikation).
- die Informationssicherheit,
- den Datenschutz,
- vertragliche und kaufmännische Fragestellungen.

Die benannten Ansprechpartner MÜSSEN mit der entsprechenden Fach- und Entscheidungskompetenz ausgestattet sein.
**[<=]**

**GS-A_4523-01 - Bereitstellung Kontaktinformationen für Informationssicherheit**
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, …).**[<=]**

**GS-A_4524-01 - Meldung von Änderungen der Kontaktinformationen für Informationssicherheit**
Der Anbieter MUSS Änderungen an der Kommunikationsschnittstelle seines Informations-sicherheits-managements der gematik unverzüglich direkt melden.**[<=]**

**A_20719 - Weiterleitung erkannter Alarme an TI SIEM**
Der Anbieter MUSS für in seinem Security Monitoring Konzept festgelegten Systeme erkannte Anomalien technisch automatisiert über die von der gematik angebotene Schnittstelle an das TI SIEM System übermitteln. **[<=]**

**A_20720 - Weiterleitung von Logdaten (Rohdaten) an TI SIEM**
Der Anbieter MUSS der gematik auf Nachfrage Stichproben der Rohdaten für die in seinem Security Monitoring Konzept festgelegten Systeme automatisiert über die von der gematik angebotene Schnittstelle an das TI SIEM System übermitteln. **[<=]**

**A_21719 - Weiterleitung von Reports TI SIEM**
Der Anbieter MUSS für die in seinem Security Monitoring Konzept festgelegten Systeme aggregierte Informationen (Reports) technisch automatisiert über die von der gematik angebotene Schnittstelle an das TI SIEM System übermitteln.**[<=]**

**GS-A_5559-01 - Bereitstellung Ergebnisse von Schwachstellenscans**
Der Anbieter MUSS der gematik die Ergebnisse von durchgeführten Schwachstellenscans oder der vergleichbaren Maßnahmen zur Erkennung und Analyse von technischen Schwachstellen monatlich in maschinenlesbarer Form zur Verfügung stellen. Dabei MÜSSEN mindestens die folgenden Inhalte enthalten sein: Scandatum, betroffene Umgebung (PU/RU/TU), betroffenes System (interner/externer Name), betroffenes System (IP-Adresse), betroffene Software, eindeutige Bezeichnung der Schwachstelle als CVE, Schweregrad der Schwachstelle als CVSS, Information zum Umgang mit der Schwachstelle.**[<=]**

**GS-A_5562 - Bereitstellung Produktinformationen**
Der Anbieter MUSS der gematik halbjährlich eine aktuelle Liste der zur Leistungserbringung von Diensten der TI bzw. RZ-Consumern verwendeten Hard- und Softwareprodukte sowie dem zugehörigen TI-Produkttyp übermitteln. **[<=]**

**GS-A_5558 - Aktive Schwachstellenscans**
Der Anbieter MUSS im Rahmen seines Schwachstellenmanagements mindestens monatliche Schwachstellenscans oder vergleichbare Maßnahmen zur Erkennung und Analyse von tech-nischen Schwachstellen („vulnerabilities") in den vom ihm betriebenen Dienst der TI bzw. RZ-Consumer durchführen.**[<=]**

**A_19175 - Zustimmung zu regelmäßigen Schwachstellenscans durch die gematik**
Der Anbieter MUSS zustimmen, dass die gematik monatliche nicht-invasive Schwachstellenscans auf die Außenschnittstellen ihrer TI-Produkte durchführen darf.**[<=]**

**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, …) sowie die für den Anbieter zuständige datenschutzrechtliche Aufsichtsbehörde mitteilen.**[<=]**

**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_2076-01 - kDSM: Datenschutzmanagement nach BSI**
Der Anbieter MUSS ein Datenschutzmanagement nach Baustein CON.2 des IT-Grundschutzkompendiums umsetzen**[<=]**

**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 Einhaltung der von den Auftragsverarbeitern getroffenen Maßnahmen überzeugen.**[<=]**

**GS-A_5626 - kDSM: Auftragsverarbeitung**
Falls ein Anbieter als Auftragsverarbeiter i. S. des Art. 4 Nr. 8 DSGVO tätig ist, MUSS dieser mit dem Auftraggeber als Verantwortlichen i. S. des Art. 4 Nr. 7 DSGVO verbindlich regeln, wie die Pflichten des Anbieters gegenüber der gematik, die sich aus den Sicherheits- und Datenschutzanforderungen der gematik ergeben, erfüllt werden.**[<=]**

**A_23340 - TI-Gateway Zugangsmodul - Beschreibung Authentifizierung & Verifikation HSK-Instanz**
Der Anbieter TI-Gateway MUSS seinen Nutzern (Leistungserbringer bzw. deren DVO) Informationen zur Hand geben, dass beim initialen Verbindungsaufbau zur Administrationsschnittstelle der HSK-Instanz deren Authentizität überprüft werden muss und wie dies möglich ist. Dies umfasst mindestens

- die technische Prüfung des TLS-Zertifikats C.AK.AUT des HSK mittels des Software-Clients (seihe A_23341*)
- Bei Verwendung eines Webbrowsers zur Administration:
  - der Abgleich des SHA-256 Werts des im Browser bei der Verbindung zur Management-Schnittstelle der HSK-Instanz mit einer Sicherheitswarnung angezeigten Zertifikats gegen den durch den Software-Client angezeigten SHA-256 Wert
- die Verifikation, dass die HSK-Instanz zur Änderung des Passworts für den Admin-Account auffordert,
- die Änderung des Passworts des Admin-Accounts,
- die Verifikation, dass keine weiteren Admin-Nutzer in der HSK-Instanz angelegt sind,
- die Verifikation, dass das Informationsmodell der HSK-Instanz leer/unkonfiguriert ist bei der Ersteinrichtung,
- Import der individuellen HSK-Instanz-Identität in die "Allowlist" der Clientsysteme und den ggf. für die Administration genutzten Webbrowser
  - entweder durch die Erzeugung oder den Import einer HSK-Instanz-individuellen Server-Identität
  - oder durch die Nutzung der AK.AUT-Identitäten sofern diese HSK-Instanz-individuell sind, also genau eine AK.AUT-Identität immer genau einer HSK-Instanz zugeordnet ist.

Zudem MUSS der Nutzer darauf hingewiesen werden im Nutzer-Portal zu prüfen, dass initial keine Freischaltung für Remote-Zugänge zur HSK-Instanz aus DVO-Netzen konfiguriert sind.
**[<=]**

**A_23382 - TI-Gateway VPN-Client - Nutzerinformation**
Der Anbieter des TI-Gateways MUSS seine Nutzer verständlich zum sicheren Umgang mit den privaten VPN-Client-Schlüsseln und zur korrekten Installation und Nutzung des VPN-Clients informieren.**[<=]**

**A_23393 - Prozesse zur schnellen Kommunikation und Entsperrung von VPN-Zugängen**
Der Anbieter TI-Gateway MUSS Prozesse zur Behandlung und Klärung erkannter Angriffe aus Nutzer-Netzen etablieren, sodass eine schnelle Kommunikation mit betroffenen Kunden und eine Klärung der Situation möglich ist und eine Sperrung möglichst, vermieden werden kann, sofern dies sicherheitstechnisch vertretbar ist. Ebenso müssen Situationen, die zu einer Sperrung geführt haben, schnellst möglich geklärt werden können um den Zugang wieder zu entsperren.**[<=]**

**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.**[<=]**