Vivantes –
Netzwerk für Gesundheit GmbH

Leistungsbeschreibung

VSG-SEK-2026-48

Beschaffung von KIM Mail Proxys
und KIM Postfächern

Version 1.0

Inhalt

1. Vorbemerkungen ... 3
1.1. Begriffsbestimmungen ... 3
1.2. Gegenstand der Ausschreibung ... 3
1.3. Vorstellung des Vivantes-Konzerns ... 4
1.3.1. Allgemein ... 4
1.3.2. Die Vivantes – Netzwerk für Gesundheit GmbH ... 4
1.4. Nutzungsberechtigte Parteien ... 5
1.5. Laufzeit ... 5
1.6. Mindest- und Höchstabnahmemengen über die Laufzeit ... 5
1.7. Vergütung ... 6
1.8. Abruf von Leistungen ... 6
1.9. Fälligkeit von Vergütungen, Rechnungslegung und Preisanpassungen ... 6
2. Beschreibung des Ausgangszustands ... 6
2.1. Beschreibung des TI-Gateways und des Infomodells ... 7
2.2. Beschreibung der Netzwerktopologie ... 8
3. Beistellungen der AG ... 8
4. Anforderungen ... 9
4.1. Anforderungen an den Fachdienst KOM-LE ... 9
4.2. Anforderungen an die KIM Mail Proxys ... 9
4.3. Anforderungen an das Migrationsprojekt ... 12
4.4. Projekt- und Meilensteinplan ... 13
4.4.1. Abnahme ... 14
4.5. Anforderungen an Betrieb & Support ... 14
4.6. Leistungen bei Vertragsende ... 14
4.7. Allgemeine Anforderungen an Datenschutz & IT-Sicherheit ... 15
4.8. Spezifische Anforderungen: Datenschutz ... 15
4.9. Spezifische Anforderungen: Informationssicherheit ... 16

1. Vorbemerkungen

1.1. Begriffsbestimmungen

Begriff	Erläuterung
KIM Client Modul	Mit „KIM Client Modul“ wird in dieser Ausschreibung ein Produkt bezeichnet, das mindestens die verpflichtenden Anforderungen an den Produkttyp KOM-LE-Clientmodul der Gematik Spezifikation gemSpec_CM_KOMLE erfüllt.
KIM Mail Proxy	Mit „KIM Mail Proxy“ wird in dieser Ausschreibung ein Produkt bezeichnet, dass die Funktionen eines KIM Client Moduls um weitere in dieser Ausschreibung geforderte Fähigkeiten ergänzt. Ein KIM Mail Proxy stellt dabei immer auch die Funktionen eines KIM Client Moduls bereit.
KIM Adresse	Mit „KIM Adresse“ wird in dieser Ausschreibung ein eigenständiges E-Mail-Postfach eines Gematik KOM-LE Fachdiensts im Sinne der Gematik Spezifikation gemSpec_FD_KOMLE bezeichnet.
KIM Postfach	Siehe „KIM Adresse“
Ausführungs-umgebung	Mit „Ausführungsumgebung“ wird in dieser Ausschreibung eine IT-Komponente bezeichnet, die die KIM Mail Proxys ausführt. Eine VM, eine Container Runtime, oder eine Appliance sind Beispiele für eine Ausführungsumgebung.
IT-Gesamtsystem bei der AG	Die zur Erfüllung der Anforderungen dieser Ausschreibung bei der Auftraggeberin zu schaffender Kombination der Ausführungsumgebungen und KIM Mail Proxys wird als „IT-Gesamtsystem bei der AG“ bezeichnet. Der Begriff umfasst nicht die Primärsysteme bei der Auftraggeberin, oder die IT-Komponenten des KOM-LE Fachdiensts bei dem Auftragnehmer.
vKON	Mit vKON wird ein „**v**irtuellen **KON**nektor“ bezeichnet, der durch das bei der Auftraggeberin im Einsatz befindliche TI-Gateway bereitgestellt wird.
Werktag	Als Werktag im Sinne dieser Ausschreibung gelten abweichend von den gesetzlichen Regelungen die Wochentage von Montag bis Freitag.

1.2. Gegenstand der Ausschreibung

Die Vivantes Netzwerk für Gesundheit GmbH (im Weiteren als Vivantes, Auftraggeberin oder die AG bezeichnet) schreibt für ihre neun Klinik-Standorte und Ihre Tochtergesellschaften die Dienst- und Lieferleistung „Adressen für KIM (Kommunikation im Medizinwesen)“ als Rahmenvereinbarung mit einem Bieter (im Weiteren als Auftragnehmer oder der AN bezeichnet) aus.

Vivantes verwendet zum Zeitpunkt der Ausschreibung 12 KIM Adressen unter der Telematik-ID 5-2-261101878-002 „Vivantes Netzwerk für Gesundheit GmbH – KIM“, 66 KIM Adressen unter der Telematik-ID 1-20723216700 „üBAG Vivantes – Vivantes MVZ GmbH“ sowie eine weitere KIM Adresse unter der Telematik-ID 1-20723218600 „MVZ Charité Vivantes“.

Alle 79 KIM Adressen enden mit der Telematik Domain „vivantes.kim.telematik“.

Vivantes plant die Nutzung der Nachrichtenkennungen eNachricht und eArztbriefs des Fachdiensts KOM-LE auch innerhalb der Vivantes Kliniken zu etablieren, die Nutzung von KIM in den stationären Pflegeheimen der Vivantes - Forum für Senioren GmbH zu ermöglichen und weitere KIM Adressen für den Gebrauch in den MVZs bereitzustellen.

Die Rahmenvereinbarung soll die Beschaffung von Adressen und die Bereitstellung der gemeinsamen Telematik Domain für die drei genannten Telematik-IDs – jeweils in der PU-Umgebung der Telematik Infrastruktur – sowie von KIM Mail Proxys umfassen.

Dazu ist ein Migrationsprojekt durchzuführen und anschließend der sichere Betrieb der gelieferten Komponenten, inklusive Support, für die Vertragslaufzeit zu gewährleisten.

Die Rahmenvereinbarung soll zusätzlich die Beschaffung von KIM Adressen und die Bereitstellung der Telematik Domain für noch zu beschaffende Telematik-IDs – jeweils in der RU-Umgebung der Telematik Infrastruktur – sowie zweier KIM Mail Proxys für die RU-Umgebung umfassen.

1.3. Vorstellung des Vivantes-Konzerns

1.3.1. Allgemein

Vivantes - bestehend aus der Vivantes – Netzwerk für Gesundheit GmbH und ihren Tochtergesellschaften - betreibt mit rund 20.000 Mitarbeitern Krankenhäuser an neun Standorten (unselbständige Betriebsstätten) sowie andere gesundheitliche und soziale Einrichtungen in Berlin.

Vivantes versorgt mit jährlich ca. 358.000 ambulanten und ca. 198.000 stationären Fällen ca. 30 Prozent aller Krankenhauspatienten in Berlin. In über 100 Kliniken und medizinischen Instituten stehen ca. 5.900 Krankenhausbetten für die stationäre Behandlung der Patienten zur Verfügung. Zusätzlich werden in allen Kliniken ambulante und teilstationäre Leistungen erbracht.

Zum Vivantes-Konzern gehören weiterhin 19 stationäre Pflegeheime, eine ambulante Rehabilitation, 15 Medizinische Versorgungszentren, eine ambulante Krankenpflege, ein Hospiz sowie Tochtergesellschaften für Catering, Reinigung und Wäsche. Die einzelnen Standorte sind über das gesamte Stadtgebiet von Berlin verteilt.

In allen Einrichtungen wird eine qualitativ hochwertige medizinische, pflegerische und sozialtherapeutische Behandlung gewährleistet. Ein umfangreiches Qualitätsmanagementsystem stellt die ständige Weiterentwicklung der Qualität sicher. Alle Vivantes Krankenhäuser sind akademische Lehrkrankenhäuser der Charité. Vivantes ist der größte kommunale Krankenhauskonzern Deutschlands, alleiniger Gesellschafter ist das Land Berlin.

Weitere Angaben zu Aufgaben, Leistungen und der Organisation von Vivantes entnehmen Sie bitte der Webseite www.vivantes.de.

1.3.2. Die Vivantes – Netzwerk für Gesundheit GmbH

Die Vivantes-Netzwerk für Gesundheit GmbH als Konzern-Mutterunternehmen ist alleinige Vertragspartnerin des vorliegenden Rahmenvertrages und der Einzelabrufe. Sie stellt den untenstehenden nutzungsberechtigten Tochtergesellschaften die gesamte IT-Infrastruktur zur Verfügung, einschließlich der auftragsgegenständlichen Komponenten der dezentralen und zentralen Telematik Infrastruktur.

Die gesamte Abwicklung des gegenständlichen Auftrags wird über die zentrale IT der Vivantes – Netzwerk für Gesundheit GmbH abgewickelt werden, unabhängig davon, in welcher Gesellschaft die Adressen zum Einsatz kommen.

1.4. Nutzungsberechtigte Parteien

Die vertragsgegenständlichen Leistungen können in den folgenden Tochterunternehmen von der Vivantes – Netzwerk für Gesundheit GmbH zum Einsatz kommen:

1. Vivantes Ida-Wolff-Krankenhaus GmbH, Juchaczweg 21, 12351 Berlin
2. SVL Speiseversorgung und -logistik GmbH, Aroser Alle 72-76, 13407 Berlin
3. Vivantes MVZ GmbH, Fröbelstraße 15, 10405 Berlin
4. Vivantes Rehabilitation GmbH, Rubensstraße 125, 12157 Berlin
5. Vivantes Hospiz GmbH, Wenckebachstraße 23, 12099 Berlin
6. Vivantes Service GmbH, Aroser Allee 72-76, 13407 Berlin
7. BBG Berliner Bildungscampus für Gesundheitsberufe gGmbH, Waldstraße 86-90, 13403 Berlin
8. Vivantes – Forum für Senioren GmbH, Alt Wittenau 90, 13437 Berlin
9. VivaClean Nord GmbH, Aroser Allee 72-76, 13407 Berlin
10. VivaClean Süd GmbH, Aroser Allee 72-76, 13407 Berlin
11. MVZ Charité Vivantes, Landsberger Allee 49, 12049 Berlin

1.5. Laufzeit

Zur Laufzeit der Rahmenvereinbarung und der Einzelaufträge siehe EVB-IT digital Rahmenvereinbarung.

1.6. Mindest- und Höchstabnahmemengen über die Laufzeit

Die AG verpflichtet sich, mit Abschluss des Migrationsprojekts 80 KIM Adressen in der Produktivumgebung (PU) der Telematikinfrastruktur abzunehmen. Bis zum 01.02.2028 verpflichtet sich die Auftraggeberin zur Abnahme von mindestens 220 weiteren KIM-Adressen in der Produktivumgebung (PU) der Telematikinfrastruktur. Die verbindliche Mindestabnahmemenge beträgt somit insgesamt 300 KIM-Adressen in der Produktivumgebung (PU) der Telematikinfrastruktur. Darüber hinaus besteht für die gesamte Vertragslaufzeit inkl. Verlängerungsoptionen und automatischen Verlängerungen keine weitere Verpflichtung zum Abruf von Leistungen aus der Rahmenvereinbarung.

Für KIM-Adressen in der Referenzumgebung (RU) besteht keine Mindestabnahmeverpflichtung.

Über die vorgenannten Mindestabnahmemengen hinaus besteht während der gesamten Vertragslaufzeit einschließlich sämtlicher Verlängerungsoptionen und automatischer Verlängerungen keine Verpflichtung zum Abruf weiterer KIM-Adressen oder optionaler Leistungen. Die vereinbarten Höchstabnahmemengen bleiben hiervon unberührt.

Die Gesamtabnahmemenge aus der Rahmenvereinbarung ist über die gesamte Vertragslaufzeit einschließlich sämtlicher Verlängerungsoptionen und automatischer Verlängerungen auf maximal 600 KIM-Adressen in der Produktivumgebung (PU) und zusätzlich maximal 20 KIM-Adressen in der Referenzumgebung (RU) der Telematikinfrastruktur begrenzt.

Diese Höchstmengen gelten jeweils für sämtliche Abrufe aus der Rahmenvereinbarung. Mit Erreichen der jeweiligen Höchstmenge dürfen keine weiteren KIM-Adressen für die betreffende Umgebung aus der Rahmenvereinbarung abgerufen werden. Die Regelungen der EVB-IT digital Rahmenvereinbarung zum Erreichen des Höchstvolumens bleiben unberührt.

Der Auftragnehmer stellt im Rahmen der vereinbarten Grundvergütung die zur Erfüllung der Anforderungen nach Abschnitt 4.2, insbesondere KIM_4.2_30, erforderliche Anzahl an KIM Mail Proxys bereit, mindestens jedoch fünf KIM Mail Proxys für eine Verwendung mit der

Produktivumgebung (PU) der Telematikinfrastruktur, sowie zwei weitere KIM Mail Proxys für eine Verwendung mit der Referenzumgebung (RU) der Telematikinfrastruktur.

Die Anzahl der für die Erfüllung der vereinbarten Mindest- und Höchstabnahmemengen erforderlichen KIM Mail Proxys ist vom Auftragnehmer eigenverantwortlich zu bemessen. Eine gegebenenfalls erforderliche Erweiterung dieser Anzahl zur Verarbeitung des vereinbarten Anfrage- und Verarbeitungsvolumens erfolgt ohne zusätzliche Vergütung.

Unabhängig davon ist die Auftraggeberin berechtigt, während der gesamten Vertragslaufzeit einschließlich sämtlicher Verlängerungen optional bis zu fünf weitere KIM Mail Proxys über den zur Leistungserfüllung erforderlichen Umfang hinaus gesondert abzurufen. Diese zusätzlichen KIM Mail Proxys werden ausschließlich auf Grundlage der hierfür vereinbarten Preise gemäß Anlage 2 (Preisblatt) vergütet.

Eine Verpflichtung zur Abnahme dieser optionalen zusätzlichen KIM Mail Proxys besteht nicht.

1.7. Vergütung

Zur Vergütung der Leistung siehe Anlage 2 (Preisblatt) und EVB-IT Vertrag.

1.8. Abruf von Leistungen

Der Abruf von Leistungen erfolgt ausschließlich durch die zentrale IT der Vivantes-Netzwerk für Gesundheit GmbH.

[KIM_1.8_10] Der Abruf von KIM Postfächern geschieht in Kontingenten von mindestens 20 KIM Postfächern nach separater Beauftragung. Das Kontingent muss der AG erlauben KIM Postfächer mit beliebiger, nach gemSpec_FD_KOMLE konformer, Mail Adresse innerhalb der Vivantes Telematik Domain und beliebiger zugeordneter Vivantes Telematik-ID im Fachdienst KOM-LE bereitzustellen. Das Verfahren zur Bereitstellung von KIM Postfächern im Fachdienst KOM-LE aus dem Kontingent kann bei Erfüllung der folgenden Anforderungen vom AN frei festgelegt werden (z.B. Freischaltcodes zur Verwendung in einem Web Interface).

[KIM_1.8_20] Falls alle KIM Postfächer in allen durch die AG beauftragten Kontingente im Fachdienst KOM-LE bereitgestellt wurden (d.h. das Kontingent erschöpft ist), darf es der AG nicht möglich sein, weitere KIM Postfächer im Fachdienst KOM-LE abzurufen.

[KIM_1.8_30] Die Bereitstellung eines Kontingents an KIM Postfächern muss innerhalb von 10 Werktagen nach Beauftragung des Kontingents erfolgen. Der AN meldet die Bereitstellung des Kontingents an die AG in geeigneter Weise. Die Bereitstellung eines KIM Postfachs aus dem Kontingent zur produktiven Nutzung im Fachdienst KOM-LE muss innerhalb von 5 Werktagen nach Anforderung erfolgen. Der AN meldet die Bereitstellung eines KIM Postfachs in geeigneter Weise.

1.9. Fälligkeit von Vergütungen, Rechnungslegung und Preisanpassungen

Zur Fälligkeit von Vergütungen, Rechnungslegung und Preisanpassungen siehe EVB-IT digital Rahmenvereinbarung.

2. Beschreibung des Ausgangszustands

Vivantes verwendet zum Zeitpunkt der Ausschreibung 12 KIM Adressen unter der Telematik-ID 5-2-261101878-002 „Vivantes Netzwerk für Gesundheit GmbH – KIM“, 66 KIM Adressen unter der Telematik-ID 1-20723216700 „üBAG Vivantes – Vivantes MVZ GmbH“ sowie eine weitere KIM Adresse unter der Telematik-ID 1-20723218600 „MVZ Charité Vivantes“.

Alle 79 KIM Adressen enden mit der Telematik Domain „vivantes.kim.telematik“.

Die 79 KIM Adressen werden über den KOM-LE Fachdienst der Fa. „IBM Deutschland GmbH“ bereitgestellt. Das KIM Client Modul der Fa „IBM Deutschland GmbH“ wird im KIM Mail Proxy „vast.UI“ der Fa. „ITSM HealthCare GmbH“ bereitgestellt.

Der Versand und Empfang von KIM Nachrichten mit einer Größe von maximal 500 MB (KIM 1.5+) ist für keines der KIM Postfächer aktiviert.

Folgende Primärsysteme rufen zum jetzigen Zeitpunkt über vast.UI KIM Nachrichten aus dem KOM-LE Fachdienst ab oder versenden über diesen KIM Nachrichten:

Hersteller	Produkt
DH Healthcare GmbH	Orbis
medatixx GmbH & Co. KG	x.concept
medatixx GmbH & Co. KG	x.vianova
ET Software Developments GmbH	IndiCation
Geocon Software GmbH	Cairful
KHP - Informatik GmbH & Co KG	classyRT

Die Frequenz der POP3 Abrufe der KIM Postfächer aus den Primärsystemen variiert, überschreitet i.d.R. aber nicht 30 POP3 Abrufversuche pro Stunde.

Im Juli 2026 wurden ≈ 9.700 Nachrichten über den bestehenden KIM Mail Proxy empfangen. Informationen über eine Verteilung der Nachrichten auf die KIM Postfächer, über eine Verteilung der Nachrichten auf Nachrichtenkennungen oder das empfangene Datenvolumen sind nicht vorhanden.

Im Juli 2026 wurden ≈ 5800 Nachrichten über den bestehenden KIM Mail Proxy versandt. Informationen über eine Verteilung der Nachrichten auf die KIM Postfächer, über eine Verteilung der Nachrichten auf Nachrichtenkennungen oder das versandte Datenvolumen sind nicht vorhanden.

2.1. Beschreibung des TI-Gateways und des Infomodells

Die TI-Konnektoren der AG werden durch ein TI-Gateway des Vivantes Bestandsanbieters Fa. „Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH“ in der Form von vKONs bereitgestellt.

Der bestehende KIM Mail Proxy verwendet einen (1) vKON für die Verarbeitung von Anfragen des Primärsystems Orbis, sechs (6) vKONs für die Verarbeitung von Anfragen des Primärsystems x.vianova und zwei (2) vKONs für die Verarbeitung von Anfragen des Primärsystems x.concept, einen (1) vKON für die Verarbeitung von Anfragen des Primärsystems Indication und einen (1) vKON für die Verarbeitung von Anfragen des Primärsystems Cairful.

Die vKONs verwenden self-signed ECC Zertifikate an den Außenschnittstellen. Eine Host Name Validation erfolgt über die IP des vKONs im CN Attribut des Zertifikats.

Alle vKONs nutzen verpflichtend TLS Client Auth zur Authentifizierung am Client System. Die Nutzung des LDAP Proxys der vKONs erfordert ebenfalls zwingend ein TLS Client Auth. In der Regel ist für jedes Primärsystem eine Authentifizierung an den vKONs am zugewiesenen Client System Konnektoren-übergreifend über denselben TLS Client Auth Private Key möglich. Die TLS Client Authentifizierung verwendet ECC Private Keys und ECC signierte Zertifikate.

Für die verschiedenen Standorte der Vivantes MVZ sind eigene Mandanten auf den vKONs angelegt worden. Die MVZ Mandanten enthalten stets eine zugewiesene SMC-B.

Die Krankenhäuser und Pflegeeinrichtungen der AG teilen sich einen Mandanten. Dieser Mandant enthält zwei zugewiesene SMC-Bs.

Für das Client System Cairful wurde ein Rewrite der POP3- und SMTP-Anfragen eingerichtet, da die UI im System die Erstellung des notwendigen Benutzernamens nur rudimentär unterstützt – siehe hierzu Kriterium KIM_4.2_50.

Ein separater Mandant mit nur einer SMC-B für das Client System x.concept der Ermächtigungs-ambulanzen der Vivantes Krankenhäuser ist vorhanden.

Für das Client System x.concept der Ermächtigungsambulanzen der Vivantes Krankenhäuser wurde ein Rewrite der POP3- und SMTP-Anfragen eingerichtet, da das Primärsystem mit nativen Mitteln keine Verwendung einer SMC-B für die Fachdienste VSDM, ePA, etc. und einer anderen SMC-B für den Fachdienst KOM-LE erlaubt – siehe hierzu Kriterium KIM_4.2_50.

2.2. Beschreibung der Netzwerktopologie

Die Primärsysteme, die KIM Mail Proxys und die vKONs laufen in separaten Subnetzen. Ein Routing zwischen den Subnetzen wird über die Default Gateways der Subnetze sichergestellt.

Die Anbindung der Rechenzentren der AG an die Rechenzentren des TI-Gateways Anbieters erfolgt über eine VPN Verbindung. Die Verbindung ist transparent für die KIM Mail Proxys.

Die Anbindung der Rechenzentren der AG an die Netzbereiche der Zentralen Telematik-Infrastruktur erfolgt über den Sicheren Zugangsdienst des TI-Gateway Anbieters. Ein Routing von Verbindungen in die Netzbereiche der Zentralen Telematik-Infrastruktur wird über die Default Gateways der Vivantes Subnetze sichergestellt.

3. Beistellungen der AG

Die für die Verwendung der KIM Mail Proxys mit dem KOM-LE Fachdienst notwendigen Komponenten des TI-Gateways (z.B. Konnektoren in der Form von vKONs, TI-Zugangsdienst, eHealth-Kartenterminals, Schlüsselmaterial auf SMC-Bs, SM-Bs, eHBA, etc.) werden von der AG bereitgestellt.

Das für die KIM Client Module notwendige Infomodell wird von der AG gepflegt, der Aufrufkontext pro KIM Mail Adresse, sowie die KonnektorId, werden von der AG benannt. Die AG stellt die benötigten TLS Client Auth Zertifikate für die KIM Client Module zur Authentifizierung als Client System an den Konnektoren zur Verfügung.

Die AG hinterlegt die POP3 und SMTP Benutzernamen, sowie das weitere für die Kommunikation mit den KIM Mail Proxys notwendige Customizing, in den Primärsystemen der AG.

Die AG stellt geeignete TLS Serverzertifikate für die KIM Mail Proxys zur Absicherung der Kommunikation mit den Primärsystemen und die Zertifikatskette zur Absicherung der Kommunikation mit den vKONs bereit.

Die AG stellt Ausführungsumgebungen in Form von VMs einer VMWare Virtualisierungsumgebung und die benötigten Hardwareressourcen (Storage, Compute, Memory, Network) zur Verfügung. Als Betriebssystem der Ausführungsumgebungen können entweder „Windows Server Datacenter 2025“ oder „Ubuntu 24.04 LTS“ bereitgestellt werden. „Ubuntu 24.04 LTS“ kann mit einer Docker Runtime zur Verfügung gestellt werden. Der Betrieb der KIM Mail Proxys in Form von Containern wird präferiert. Eine Kubernetes-basierte Ausführungsumgebung wird aber nicht unterstützt und ist ausgeschlossen. Der Betrieb von Containern auf „Windows Server Datacenter 2025“ mit Hilfe z.B. des

„Windows Subsystem for Linux“ oder der Betrieb von Containern, denen ein Windows-basiertes Container Image zugrunde liegt, wird ebenfalls nicht unterstützt und ist ausgeschlossen.

Die AG stellt eine Certificate Authority zur Verfügung, die das ACME Protokoll unterstützt.

Die AG stellt Accounts mit geeigneten Berechtigungen für die Ausführungsumgebungen bereit.

Die AG stellt Fernwartungszugänge in Form eines Client-2-Site-VPNs über die Lösung Palo Alto Networks GlobalProtect bereit.

4. Anforderungen

4.1. Anforderungen an den Fachdienst KOM-LE

[KIM_4.1_10] Der AN stellt die vollständige Kompatibilität des KOM-LE Fachdiensts mit dem TI-Gateway und den damit bereitgestellten virtuellen Konnektoren und dem Zugangsdienst des Vivantes Bestandsanbieters – der Fa. „Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH“ – sicher.

[KIM_4.1_20] Der zum Einsatz kommende Fachdienst KOM-LE muss vollständig und ausschließlich in Rechenzentren betrieben werden, die ihren physischen Standort innerhalb eines Mitgliedsstaats der Europäischen Union haben.

[KIM_4.1_30] Der zum Einsatz kommende Fachdienst KOM-LE muss vollständig redundant in mindestens zwei geographisch voneinander getrennten Rechenzentren betrieben werden. Ein Mindestabstand wird nicht vorgeschrieben, ein Betrieb der Rechenzentren innerhalb desselben Gebäudes (z.B. in unterschiedlichen Brandabschnitten) ist aber nicht zulässig.

[KIM_4.1_40] Der AN stellt sicher, dass für die Bereiche, die den zum Einsatz kommenden KOM-LE Fachdienst bereitstellen, lückenlos über die gesamte Vertragslaufzeit ein gültiges C5-Typ2-Testat vorliegt. Alternativ kann ein Nachweis über ein gleichwertiges Testat oder Zertifikat nach § 393 Absatz 4 Satz 4 SGB V erbracht werden.

[KIM_4.1_50] Alle KIM Postfächer, die der AG durch den zum Einsatz kommenden KOM-LE Fachdienst bereitgestellt werden, müssen optional den Versand und Empfang von KIM Nachrichten mit einer Größe von maximal 500 MB inklusive aller Anhänge ohne Zusatzkosten für die AG ermöglichen.

4.2. Anforderungen an die KIM Mail Proxys

[KIM_4.2_10] Der AN stellt die vollständige Kompatibilität der KIM Mail Proxys mit dem TI-Gateway und den damit bereitgestellten virtuellen Konnektoren und dem Zugangsdienst des Vivantes Bestandsanbieters – der Fa. „Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH“ – sicher.

[KIM_4.2_20] Die KIM Mail Proxys müssen On-Premise in den Rechenzentren der AG betrieben werden. Ein Betrieb der KIM Mail Proxys in den Rechenzentren des ANs ist aufgrund von datenschutzrechtlichen und IT-sicherheitstechnischen Vorgaben der AG nicht zulässig.

[KIM_4.2_30] Der AN stellt KIM Mail Proxys in ausreichender Menge zur Verfügung. Der AN berücksichtigt dabei das initiale und maximale zu erwartende Anfrage- und Verarbeitungsvolumen der KIM Mail Proxys. Das initiale Anfrage- und Verarbeitungsvolumen ergibt sich aus der Mindestabnahmemenge zum 01.02.2028, das maximale Anfrage- und Verarbeitungsvolumen aus der Höchstabnahmemenge. Der AN berücksichtigt dabei die Notwendigkeit, dass für einige Adressen die SMTP und POP3 Benutzernamen überschrieben werden müssen – siehe hierzu Kriterium KIM_4.2_50. Um die Auswirkungen eines Ausfalls eines KIM Mail Proxys zu minimieren, stellt der AN

aber mindestens 5 KIM Mail Proxys (1 für die Vivantes MVZ, 1 für Vivantes Forum für Senioren, 3 für die Vivantes Kliniken) zur Verfügung. Zur Verarbeitung des maximal zu erwartenden Anfrage- und Verarbeitungsvolumens ist die Bereitstellung von KIM Mail Proxys zu einem späteren Zeitpunkt zulässig, muss dann aber ohne Zusatzkosten für die AG erfolgen.

[KIM_4.2_40] Prozesse der KIM Mail Proxys müssen unter einem Daemon oder Service mit einer Autostart Funktion bei einem Neustart der Ausführungsumgebung ausgeführt werden. In Windows Ausführungsumgebungen müssen die Services der KIM Mail Proxys unter einem Service Account ausgeführt werden.

[KIM_4.2_50] Die Verwendung von getrennten Telematik-IDs für den Fachdienst KOM-LE und die restlichen Fachdienste (VSDM, ePA für Alle, etc.) erfordert bei der Verwendung eines KIM Client Moduls, dass mindestens zwei SMC-Bs in den Mandanten auf den Konnektoren hinterlegt werden müssen. Der AG sind in den Primärsystemen, die bei der AG im Einsatz sind, Probleme bekannt, die durch eine dann zufällige Auswahl der für Telematik Interaktionen verwendeten SMC-B resultieren.

Vivantes plant daher einen separaten Mandanten für Interaktionen mit dem Fachdienst KOM-LE in den Konnektoren zu hinterlegen, der nur die für den Fachdienst KOM-LE vorgesehene Telematik-Id im Zugriff hat.

Erschwert wird dieses Vorhaben dadurch, dass nicht in allen Primärsystemen der Benutzername nach gemspec_CM_KOMLE Absatz 3.3.2.2 oder Absatz 3.4.2.2 frei festgelegt werden kann.

Der AN stellt eine Funktion des KIM Mail Proxys bereit, die vor einer Interaktion mit den Konnektoren oder dem Fachdienst KOM-LE die Verwendung einer durch die AG definierten SMC-B, individuell pro KIM Mail Proxy, z.B. durch einen Rewrite der Felder MandantId, ClientsystemId, WorkplaceId, oder KonnektorId eines übergebenen POP3- oder SMTP-Benutzernamens, ermöglicht.

[KIM_4.2_51] Der AN stellt eine Funktion des KIM Mail Proxys bereit, die vor einer Interaktion mit den Konnektoren oder dem Fachdienst KOM-LE die Verwendung einer durch die AG definierten SMC-B, individuell pro KIM Mail Adresse, z.B. durch einen Rewrite der Felder MandantId, ClientsystemId, WorkplaceId, oder KonnektorId eines übergebenen POP3- oder SMTP-Benutzernamens, ermöglicht.

[KIM_4.2_52] Der AN stellt eine Funktion des KIM Mail Proxys bereit, die vor einer Interaktion mit den Konnektoren oder dem Fachdienst KOM-LE die Verwendung einer durch die AG definierten SMC-B, individuell pro KIM Mail Adresse, z.B. durch einen Rewrite der Felder MandantId, ClientsystemId, WorkplaceId, oder KonnektorId eines übergebenen POP3- oder SMTP-Benutzernamens ermöglicht, unabhängig von Präsenz oder Wert der Felder im initial übergebenen Benutzernamen, überschreibt.

[KIM_4.2_60] Um der veränderten Bedrohungslage der IT-Sicherheit durch kriminelle und staatliche Akteure gerecht zu werden, minimiert Vivantes aktiv die Zahl der auf den Clients und Ausführungsumgebungen installierten oder ausgeführten Programme. Aus diesem Grund muss die Administration der KIM Mail Proxys mit angemessener Ergonomie durch die auf den Vivantes Admin Clients installierten Browser Microsoft Edge oder Mozilla Firefox ohne eine Installation von Plugins möglich sein. Die Verwendung der Standardprogramme der Ausführungsumgebungen zur Durchführung von Tätigkeiten auf Ebene der Ausführungsumgebungen ist zulässig.

[KIM_4.2_70] Alle durch die KIM Mail Proxys verwendeten Key Stores und Trust Stores, die Schlüsselmaterial oder Zertifikate für die Verbindungen zwischen Primärsystemen, KIM Mail Proxys, Admin Clients und Konnektoren enthalten, können durch einen von der AG zu implementierenden oder zu konfigurierenden ACME Client automatisch, d.h. ohne händisches Zutun, über die Challenge Types HTTP-01 oder TLS-ALPN-01 aktualisiert werden. Das Kriterium betrifft nicht die Verwaltung von Schlüsselmaterial zur Absicherung der Verbindungen zwischen KIM Client Modul und KOM-LE Fachdienst. Nach einem von der AG selbst festgelegten Zeitplan kann der ACME Client einen Wechsel

auf die neuen Zertifikate durch Reload oder Restart der KIM Mail Proxys anstoßen. Der Rollout und Wechsel der Zertifikate müssen auf allen KIM Mail Proxys regelmäßig in einem Abstand von höchstens 30 Tagen stattfinden können. Alle dafür notwendigen Kenntnisse über die interne Funktion und Konfiguration der KIM Mail Proxys (z.B. Passwörter, Pfade, API-Spezifikationen) werden der AG durch den AN zur Verfügung gestellt.

[KIM_4.2_71] Der AN implementiert oder konfiguriert einen ACME Client in den KIM Mail Proxys und/oder auf den Ausführungsumgebungen. Das Kriterium betrifft nicht die Verwaltung von Schlüsselmaterial zur Absicherung der Verbindungen zwischen KIM Client Modul und KOM-LE Fachdienst. Der ACME Client aktualisiert automatisch, d.h. ohne händisches Zutun, über die Challenge Types HTTP-01 oder TLS-ALPN-01 alle verwendeten Key Stores und Trust Stores der KIM Mail Proxys auf den Ausführungsumgebungen die Schlüsselmaterial oder Zertifikate für die Verbindungen zwischen Primärsystemen, KIM Mail Proxys, Admin Clients und Konnektoren enthalten und führt nach einem mit der AG abzustimmenden Zeitplan den Wechsel auf die neuen Zertifikate durch Reload oder Restart der KIM Mail Proxys durch. Der Rollout und Wechsel der Zertifikate müssen auf allen KIM Mail Proxys regelmäßig in einem Abstand von höchstens 30 Tagen stattfinden.

[KIM_4.2_80] Die Funktion der Softwareprodukte im Umfeld der Telematik Infrastruktur werden bei Vivantes durch eine Kombination der Softwareprodukte Grafana, Alloy, Loki und Prometheus überwacht. Die Produkte sind in der Lage text-basierte Log Dateien auf den Ausführungsumgebungen über z.B. Regular Expressions oder JSON Parsing auszuwerten, können aber auch über den OpenTelemetry Standard oder proprietäre Methoden Metriken auslesen. Der AN stellt sicher, dass über die Kombination Grafana, Alloy, Loki und Prometheus mindestens folgende Metriken der KIM Mail Proxys ermittelbar sind:

- Anzahl der versandten Mails in den letzten 15 Minuten
- Anzahl der empfangenen Mails in den letzten 15 Minuten
- Anzahl der erfolgreichen und fehlgeschlagenen Mail Empfangsversuche in den letzten 15 Minuten
- Anzahl der erfolgreichen und fehlgeschlagenen Mail Sendeversuche in den letzten 15 Minuten
- Anzahl der erfolgreichen und fehlgeschlagenen Operationen mit den Konnektoren in den letzten 15 Minuten
- Anzahl der erfolgreichen und fehlgeschlagenen Operationen mit dem KOM-LE Fachdienst in den letzten 15 Minuten

Im Falle von text-basierten Logs ist es nicht notwendig, dass die Metriken an sich in den Logs aufgeführt sind, sondern dass für jede beschriebene Metrik bei einem zu zählenden Ereignis eine eindeutige Nachricht mit einem Zeitstempel in den Logs ausgegeben wird, die mit Regular Expressions mindestens in die Teile Zeitstempel und Nachricht geparst werden kann.

[KIM_4.2_90] Der KIM Mail Proxy unterstützt das Scannen von eingehenden Mails und Mailanhängen über eine ICAP Schnittstelle. Die ICAP Schnittstelle ist kompatibel mit dem bei der AG verwenden Trend Micro ICAP Server. Der AN konfiguriert oder implementiert bei Inbetriebnahme der KIM Mail Proxys die ICAP Schnittstelle mit Zuarbeit der AG. Bei einem positiven Befund weist der KIM Mail Proxy die Mail mit allen Mailanhängen ab und liefert sie nicht an die Primärsysteme der AG aus. Der KIM Mail Proxy oder der KOM-LE Fachdienst stellen über geeignete Mechanismen sicher, dass die Mail bei zukünftigen Verarbeitungsläufen nicht erneut verarbeitet wird.

Der KIM Mail Proxy versendet bei einem positiven Virenbefund eine Benachrichtigung in Form einer KIM Nachricht an den Empfänger der betroffenen Mail über den Virenfund. Der AN stellt über die Wahl geeigneter E-Mail-Header sicher, dass die Benachrichtigungsmail in den Primärsystemen der AG gelesen werden kann.

[KIM_4.2_91] Der Textinhalt der Benachrichtigungsmail aus Kriterium KIM_4.2_90 kann durch die AG selbst festgelegt werden.

[KIM_4.2_92] Der Textinhalt und die Gestaltung der Benachrichtigungsmail aus Kriterium KIM_4.2_90 kann durch die AG vollständig selbst festgelegt werden.

[KIM_4.2_100] Der AN macht der AG alle im KIM Mail Proxy vorhandenen API und Web Interface Endpunkte, die nicht durch gemSpec_CM_KOMLE spezifiziert wurden, bekannt. Die Vertraulichkeit aller genannten Endpunkte ist durch die Verwendung von TLS Server Zertifikaten abgesichert. Eine erfolgreiche Interaktion mit den genannten Endpunkten ohne vorherige Authentifizierung ist nicht möglich, außer es handelt sich um Endpunkte, die keine vertraulichen Informationen exponieren und nur einen lesenden Zugriff erlauben (z.B. Health-, Liveness-, Readiness-Endpunkte).

4.3. Anforderungen an das Migrationsprojekt

[KIM_4.3_10] Der Beginn der Leistungserbringung erfolgt beim Beginn der Laufzeit der Rahmenvereinbarung.

[KIM_4.3_20] Ein Kick-Off-Workshop findet innerhalb von 2 Wochen nach Beginn der Leistungserbringung statt.

[KIM_4.3_30] Der AN stellt für die gesamte Dauer des Migrationsprojektes vom Kick-Off Workshop bis zur Abnahme durch die AG eine*n Projektmanager*in/Projektleiter*in als technische*n Ansprechpartner*in zur Verfügung.

[KIM_4.3_40] Der AN bietet 2 Termine für Schulungen zur Administration der KIM Mail Proxys für je bis zu 5 Personen aus dem Telematik Basis Team der AG an.

[KIM_4.3_50] Der AN benennt bei Beginn der Leistungserbringung die Anzahl und die Beschaffenheit (z.B. Hardwareressourcen) der Ausführungsumgebungen, die durch die AG bereitgestellt werden müssen. Der AN berücksichtigt dabei das initiale und final zu erwartende Anfrage- und Verarbeitungsvolumen der KIM Mail Proxys aus Mindest- und Höchstabnahmemengen über die Laufzeit, sowie die Mindestanforderungen aus Anforderungen an die KIM Mail Proxys. Die AG stellt die ggf. notwendigen Ausführungsumgebungen bereit. Der AN benennt bei Beginn der Leistungserbringung die für eine Migration der bestehenden KIM Postfächer und Telematik Domain notwendigen Leistungen des Bestandsanbieters, die durch die AG veranlasst werden müssen. Der AN passt die Ausführungsumgebungen an die Anforderungen der KIM Mail Proxys an. Der AN installiert und konfiguriert die Mail Proxys, so dass sie für eine produktive Nutzung inklusive der vereinbarten Zusatzfunktionen bereitstehen. Die Bereitstellung muss innerhalb von 2 Wochen nach Lieferung aller notwendigen Beistellungen der AG erfolgen. Mit der Bestätigung der Bereitstellung durch die AG ist Meilenstein MS 2 „Bereitstellung KIM Mail Proxys“ erreicht.

[KIM_4.3_60] Der AN erstellt in Zusammenarbeit mit der AG ein Datensicherungs- und Wiederherstellungskonzept und setzt es mit der AG zur Sicherung der KIM Mail Proxys um. Das Konzept enthält mindestens:

- Benennung und Klassifizierung der zu sichernden Daten auf den IT-Systemen
- Sicherungsstrategien der Daten (Sicherungsart, Sicherungsfrequenz, Sicherungsort)
- Monitoring der Backups und Alarmierung bei einem Fehlschlag
- Definition der Wiederherstellungsstrategie und Runbooks zur Umsetzung der Strategie bei:
  - notwendige Wiederherstellung des IT-Gesamtsystems bei der AG von Grund auf
  - notwendiger Wiederherstellung der Applikation auf der Ausführungsumgebungen
  - notwendiger Wiederherstellung der Bewegungsdaten
  - notwendiger Wiederherstellung der Konfigurationsdaten

[KIM_4.3_70] Der AN erstellt in Zusammenarbeit mit der AG ein System- und Betriebskonzept. Das Konzept enthält mindestens:

- Eine Auflistung der zum IT-Gesamtsystem bei der AG gehörenden Ausführungsumgebungen, die Konfiguration der Ausführungsumgebungen zur Anbindung ans Netzwerk und die Einbindung von Speichersystemen
- Eine Auflistung der zum IT-Gesamtsystem bei der AG gehörenden Applikations-, Konfigurations- und Bewegungsdaten und eine Beschreibung der Funktion der Daten
- Eine Auflistung aller an der Ausführungsumgebung vorgenommenen Konfigurationsänderungen, um eine Funktion des IT-Gesamtsystems bei der AG zu erreichen (Kernel Parameter, Jobs, Dienste, etc.)
- Eine Auflistung aller an den KIM Mail Proxys vorgenommenen Konfigurationsänderungen, um eine Funktion des IT-Gesamtsystems bei der AG zu erreichen.
- Runbooks zur Umsetzung regelmäßig notwendiger Tätigkeiten zur Aufrechterhaltung der Betriebsfähigkeit des IT-Gesamtsystems oder zur Korrektur der zu erwartenden Fehlerzustände.

Die Fertigstellung der Konzepte muss innerhalb von 4 Wochen nach Erreichung des Meilensteins MS-2 erfolgen. Mit der Bestätigung der Fertigstellung durch die AG ist Meilenstein MS 3 „Betriebsbereitschaft KIM Mail Proxys“ erreicht.

[KIM_4.3_80] Nach Bereitstellung der KIM Mail Proxys schließt sich die Migration der bestehenden KIM Postfächer und Vivantes Telematik Domain an. Der AN ist für die Planung und Durchführung der Migration verantwortlich. Der AN benennt die durch die AG zu beauftragenden oder veranlassenden Mitwirkungsleistungen des Bestandsanbieters schriftlich mit ausreichendem Vorlauf. Der AN stellt sicher, dass durch die Migration kein Datenverlust in Form von empfangenen oder versandten KIM Nachrichten entsteht. Der AN stellt sicher, dass eine aus der Migration resultierende Nicht-Verfügbarkeit der KIM Postfächer innerhalb der Zeiten von Montag – Freitag 07:00 Uhr – 17:00 Uhr nicht länger als 30 Minuten andauert. Anderenfalls ist die Migration außerhalb der genannten Zeiten durchzuführen. Die Konfiguration der Primärsysteme bei der Migration wird durch Mitarbeitende der AG erfolgen. Die Migration muss vollständig innerhalb von 4 Wochen nach Erreichung des Meilensteins MS-3 erfolgen. Mit der Bestätigung des Abschlusses der Migration durch die AG ist Meilenstein MS 4 „Fertigstellung Migration KIM Postfächer und Telematik Domain“ erreicht.

[KIM_4.3_90] Der AN reicht bei Angebotsabgabe ein Lösungs- und Migrationskonzept ein. Das Konzept enthält mindestens:

- Auflistung der zu einem KIM Mail Proxy des ANs gehörenden Komponenten und deren Beziehung zueinander
- Beschreibung der Funktion der zu einem KIM Mail Proxy des ANs gehörenden Komponenten
- Notwendige Anpassungen an den Ausführungsumgebungen der AG und notwendige Schritte zur Bereitstellung der KIM Mail Proxys auf den Ausführungsumgebungen
- Gestaltung und Verhalten der Funktion zum Rewrite von POP3- und SMTP-Benutzernamen
- Gestaltung und Verhalten der Funktion zur Erstellung kundenindividueller Benachrichtigungen bei einem Virenfund
- Erläuterungen zur Gestaltung der KIM Mail Proxys, die eine Kompatibilität mit ACME Zertifikat-Update Mechanismen sicherstellen
- Erläuterungen zum Ablauf der Migration der KIM Postfächer und der Telematik Domain vom Bestandsanbieter der AG

4.4. Projekt- und Meilensteinplan

Meilenstein	Beschreibung / Abnahmekriterien	Fertigstellung
MS 0	**Kick-Off-Workshop hat stattgefunden.** Anzahl und Beschaffenheit der ggf. notwendigen Ausführungsumgebungen wurde benannt und an AG übergeben.	2 Wochen nach Beginn der Laufzeit der Rahmenvereinbarung
MS 1	**Ausführungsumgebungen wurden durch die AG bereitgestellt und an den AN übergeben.**	Planmäßig 4 Wochen nach Erreichen des Meilensteins MS 0. Spätestens 8 Wochen nach Erreichen des Meilensteins MS 0.
MS 2	**Bereitstellung der KIM Mail Proxys ist abgeschlossen.** Die Ausführungsumgebungen wurden an die Erfordernisse des ANs angepasst, die KIM Mail Proxys stehen für eine produktive Nutzung inklusive der vereinbarten Zusatzfunktionen bereit.	Spätestens 2 Wochen nach Erreichen des Meilensteins MS 1.
MS 3	**Betriebsbereitschaft der KIM Mail Proxys ist erreicht.** System- und Betriebskonzept wurde erstellt. Datensicherungs- und Wiederherstellungskonzept wurde erstellt und darin beschriebene Maßnahmen umgesetzt.	Spätestens 4 Wochen nach Erreichen des Meilensteins MS 2.
MS 4	**Die Migration der bestehenden KIM Postfächer und der Telematik Domain vom Bestandsanbieter zum Fachdienst des ANs ist vollständig erfolgt.**	Spätestens 4 Wochen nach Erreichen des Meilensteins MS 3.

4.4.1. Abnahme

Der AN kann die Betriebsbereitschaft des Gesamtsystems im Sinne des EVB-IT Vertrags frühestens bei Erreichen des Meilensteins MS 4 erklären. Es werden keine Teilabnahmen ausgesprochen.

4.5. Anforderungen an Betrieb & Support

[KIM_4.5_10] Der AN stellt sicher, dass das verwendete KIM Client Modul und der KOM-LE Fachdienst lückenlos über die gesamte Vertragslaufzeit eine laufende Zulassung der gematik besitzen. Tätigkeiten, die der Umsetzung neuer Versionen der gematik Spezifikationen mit Bezug auf das KIM Client Modul und dem KOM-LE Fachdienst dienen, sowie die Bereitstellung der neuen Versionen im IT-Gesamtsystem der AG, setzt der AN innerhalb einer angemessenen Frist ohne zusätzliche Kosten für die AG um.

[KIM_4.5_20] Ergänzend zu den Vereinbarungen der EVB-IT digital Rahmenvereinbarung sind allein durch die AG zu benennenden Personen aus dem Telematik Basis Team der AG berechtigt die Hotline des ANs in Anspruch zu nehmen.

[KIM_4.5_30] Empfänger von Störungsmeldungen ist die Hotline des ANs. Der AN teilt der AG bei Beginn der Vertragslaufzeit schriftlich mit, wie die Hotline des ANs erreicht werden kann.

4.6. Leistungen bei Vertragsende

Zu den Leistungen bei Vertragsende siehe EVB-IT digital Rahmenvereinbarung.

4.7. Allgemeine Anforderungen an Datenschutz & IT-Sicherheit

[A_1.1] Im Rahmen der Angebotsabgabe wird ein IT-Sicherheits- und Datenschutzkonzept vorgelegt, in dem dargestellt wird, wie die Lösung, Infrastruktur und der Betrieb vor ungewollten Kompromittierungen bzw. Angriffen geschützt sind (z.B. durch Verschlüsselungen) und wie die nachstehenden Informationssicherheitsanforderungen erfüllt werden. Es ist ausreichend, das Sicherheits- und Datenschutzkonzept, welches bei der Zulassung des KOM-LE Fachdiensts und des KOM-LE Client Moduls durch die Gematik geprüft wurde, zur Verfügung zu stellen.

[A_1.2] Es existiert für die Lösung eine Datenschutzfolgenabschätzung nach DSGVO (sofern erforderlich) oder anderweitige Risikobetrachtung(en), die bei Bedarf dem AG zur Verfügung gestellt werden können.

[A_1.3] Es können Zugriffe (Anlage/Lesen/Ändern/Löschen von Informationen) unter Angabe von Zeitpunkt und ausführendem Nutzer protokolliert werden. Der Zugriff auf die Protokolldaten ist nur durch berechtigte Nutzer möglich ("Need-to-Know-Prinzip").

[A_1.4] Der AN verpflichtet sich, dass er hinsichtlich seiner Produkte mit geeigneten Maßnahmen und Protokollen nachweist, dass alle in diesem Abschnitt genannten Anforderungen eingehalten werden.

Der AN stimmt zu, dass die AG oder ein anderer beauftragter Dritter im Auftrag der AG die Organisation des ANs in Bezug auf die Informationssicherheit und die Einhaltung des Datenschutzes auditieren darf. Dies kann anlassbezogen oder regelmäßig geschehen. Der genaue Umfang, die Dauer und die Organisation werden jeweils einvernehmlich vereinbart.

Zusätzlich muss der AN die Abweichungen von den vereinbarten Sicherheitsanforderungen melden.

Der AN hat dem Antrag der AG nachzukommen, Informationen seiner Sicherheitsorganisation offenzulegen, auf dessen Basis die AG eine Auftragnehmerbewertung durchführen kann. Diese Einschätzung ist ein interner Prozess, der die AG dabei unterstützt, die Metriken und Reife der Sicherheitsorganisation des ANs zu beurteilen.

Der AN kann auch durch entsprechende Zertifizierungen nachweisen, dass die Vorgaben der Informationssicherheit bzw. des Datenschutzes erfüllt werden.

[A_1.5] Die Lösung muss sichere Authentifizierungsmechanismen nach dem Stand der Technik unterstützen. Hierzu zählt neben der Möglichkeit komplexe Passworte verwenden zu können und diese ggf. individuell an die Mindestanforderungen von Vivantes anpassen zu können, insbesondere auch die Möglichkeit zur Nutzung einer Multi-Faktor-Authentifizierung, falls möglich.

4.8. Spezifische Anforderungen: Datenschutz

[D_1.1] Bei der rechtskonformen Verarbeitung personenbezogener Daten sind insbesondere die Anforderungen zur Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f und Artikel 32 Abs. 1 lit a)-c) DSGVO) zu berücksichtigen. Die systemseitigen Voraussetzungen hierfür sind in einer aussagefähigen Dokumentation dem Angebot beizufügen.

Die Anwendung bzw. das Produkt muss darüber hinaus eine rechtskonforme Verarbeitung personenbezogener Daten erlauben. Die aktuelle Fassung des § 24 Abs.7 LKG Berlin wird vollumfänglich eingehalten und die technische Umsetzung im Rahmen eines IT-Sicherheits- und Datenschutzkonzeptes inkl. TOMS nachgewiesen.

[D_1.2] Sozialrechtliche Bedingungen für das Cloud Computing – Im Fall einer Cloud-Verarbeitung von Gesundheitsdaten sind die Bedingungen des § 393 Abs. 2-6 SGB V nachweislich zu erfüllen.

[D_1.8] Der AN erfüllt die Anforderungen, die im beigefügten Muster des Auftragsverarbeitungs-Vertrags (AVV) definiert sind.

4.9. Spezifische Anforderungen: Informationssicherheit

[I_1.1] Der AN muss Informationssicherheitsmanagementprozesse (ISMS) nach einem anerkannten Sicherheitsstandard vorweisen können. Diese Prozesse sowie entsprechende Rollen und Verantwortlichkeiten müssen als Teil seiner Informationssicherheitsrichtlinien dokumentiert sein. Die Richtlinien müssen seiner Belegschaft bekannt sein und regelmäßig auf Aktualität und Richtigkeit überprüft werden.

[I_1.2] AN müssen ihre Produkte einer kontinuierlichen Prüfung auf Schwachstellen unterziehen, um in der Lage zu sein, auf neue Schwachstellen so schnell wie möglich zu reagieren.
Sind vom AN entwickelte Software-, Firmware- oder Hardware-Komponenten betroffen, ist der AN verpflichtet, umgehend die Schwachstellen an die AG zu melden. Jede Schwachstelle ist vom AN bzgl. möglicher funktionaler und sicherheitsrelevanter Auswirkungen zu bewerten. Dies umfasst jede potenzielle Schwachstelle, die möglicherweise Einfluss auf die Verfügbarkeit, Integrität und Vertraulichkeit der Daten hat.

Der AN ist verpflichtet, kontinuierlich Quellen für Sicherheitsempfehlungen zu sichten und diese in Bezug auf die an die AG gelieferten Produkte zu bewerten. Sollte eine Komponente von der Sicherheitslücke betroffen sein, wird von dem AN erwartet, die Einstufung der Kritikalität und die „zeitliche“ Bewertung durchzuführen.

Vom AN wird erwartet, dass eine Lösung zur Behebung bzw. Neutralisierung (Zeit für eine vorläufige Lösung oder einen Workaround für den Fall, dass der Patch nicht innerhalb eines bestimmten Zeitrahmens verfügbar ist.) von Schwachstellen mit einem Best-Effort-Ansatz und nach bestem Wissen erarbeitet wird.

[I_1.4] Sollte es zu der Situation kommen, in der der Drittanbieter eines Betriebssystems oder einer anderen Komponente (Software, Datenbanken, Anwendungen, etc.) das Ende des Lifecycles verkündet, wird vom AN erwartet, entweder die Komponente auf die aktualisierte neuere Version zu erweitern, eine adäquate Alternative einsetzen oder er muss den weiteren Support von Sicherheitspatches für die ältere Version vertraglich mit dem Drittanbieter sicherstellen.

[I_1.5] Der AN verpflichtet sich, alle Softwarebestandteile und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe durch das Programm nicht zwingend notwendig sind, zu entfernen, um die Auswirkungen potenzieller Sicherheitsrisiken zu minimieren. Dies beinhaltet auch nicht benötigte Netzwerkfreigaben. Dies muss vor der Erklärung der Betriebsbereitschaft durch die AG geschehen sein.

Die Grundkonfiguration von Softwareprodukten sollte dem Grundsatz der datenschutzfreundlichen Voreinstellungen (Privacy by Design & by Default) folgen.

[I_1.6] Der AN stellt sicher, dass jedes Standardpasswort in allen möglichen Fällen nachvollziehbar geändert werden kann.

[I_1.7] Der AN muss im Rahmen seiner Möglichkeiten sicherstellen, dass seine Lösungen frei von „Backdoors“ sind, die die verwendeten Sicherheitsmechanismen umgehen können.

[I_1.8] Fernzugänge von Drittanbietern zum Netzwerk der AG und/oder dessen zugehörigen Unternehmen werden ausschließlich gemäß der beigefügten Vivantes-Fernwartungsvereinbarung gestattet.

Der AN muss sicherstellen, dass bei Fernzugängen die Vertraulichkeit, Verfügbarkeit und Integrität der Daten und Systeme der AG gewährleistet sind. Dies beinhaltet auch die nachträgliche

Verwendung von Informationen, von denen der AN während eines Fernzugriffes Kenntnis erlangt hat. Er ist für alle Aktionen der Benutzerkonten mit Fernzugangsfunktion auf Systemen der AG verantwortlich.

Es wird allgemein erwartet, dass jeder Nutzer im Rahmen des Fernzugangs ein eigenes Nutzerkonto bereitgestellt bekommt. Ausnahmen müssen vorab dokumentiert und in einem SLA (Service Level Agreement) festgehalten werden. In diesem Fall wird der AN die komplette Rückverfolgbarkeit der Nutzung eines Accounts (wer, wann) festhalten und diese der AG auf Verlangen aushändigen. Sollte die Situation auftreten, dass der AN ein Nutzerkonto nicht mehr benötigt, muss die AG darüber unverzüglich informiert werden, so dass das entsprechende Konto gesperrt werden kann. Die AG kann durch eine Betriebsfunktion oder eine alternative Service-Management-Funktion repräsentiert werden. Derartige Kontakte sind im SLA zu definieren. Es wird vom AN erwartet, Nutzerkonten mit Fernzugangsfunktion alle sechs Monate zu überprüfen und die AG über notwendige Änderungen zu informieren.

[I_1.9] Die Softwareentwicklungsprozesse des ANs müssen so ausgelegt sein, dass der Informationssicherheit und dem Datenschutz der entwickelten Software angemessene Beachtung in allen wichtigen Entwicklungsphasen geschenkt wird und die Prozesse sich an den allgemein anerkannten Standards orientieren. Bei Benutzung von Open-Source-Komponenten ist auf eine angemessene Konfiguration, Dokumentation und Wartung zu achten.

Die Entwickler müssen sich an vorhandene Standards zur sicheren Programmierung halten, um Schwachstellen vorzubeugen. Diese Standards müssen dokumentiert werden und den Entwicklern z. B. in Schulungen bekannt gemacht werden. Datenschutzrechtliche Anforderungen (z. B. zu Privacy by Design / Privacy by Default) müssen bereits im Entwicklungsprozess der Software beachtet werden.

Die Testverfahren beim AN müssen die implementierten Sicherheitsmechanismen und -funktionen (Verschlüsselung, Zugriffskontrollen, Authentisierung und andere) explizit beinhalten.

Secure-Code-Reviews müssen Teil der Qualitätssicherung und des Testing sein (z. B. müssen die eigenentwickelten Webapplikationen, die für den Betrieb in nicht geschützten Netzen vorgesehen sind, ein Code-Review nach einem Industriestandard wie OWASP durchlaufen.).

Sicherheitsüberprüfungen müssen entsprechend den vorgesehenen Betriebsumgebungen erfolgen, z. B. unabhängige Penetrationstests für die Systeme, die aus den externen bzw. nicht abgesicherten Netzen erreichbar sein sollen. Ergebnisse der Secure-Code-Reviews bzw. Penetrationstests müssen der AG (zumindest für die finale Version des Produktes) auf Anfrage zur Verfügung gestellt werden.

[I_1.11] Der AN hat alle IT-Komponenten in seinem Informationssystem zu identifizieren und zu dokumentieren, die einen Bezug zum Informationssystem der AG zwecks Wartung oder Betriebszugang haben können. Die Verantwortung für die Aufrechterhaltung der entsprechenden Sicherheitskontrollen dieser IT-Komponenten muss zugewiesen werden. Die IT-Komponenten sind zu dokumentieren. Diese Dokumentation ist möglicherweise Teil des Audits, demnach werden alle Unterlagen vom AN schriftlich gepflegt.

Zum Schutz der IT-Komponenten kann der AN die Anwendung spezifischer Sicherheitsmaßnahmen delegieren, jedoch bleibt der AN für den angemessenen Schutz der IT-Komponenten, die in Bezug zu dem Informationssystem der AG stehen, verantwortlich.

[I_1.12] Der AN ist verpflichtet, Sicherheitsvorfälle in seiner Organisation, die potenziell einen negativen Effekt auf materielle und immaterielle gelieferte oder auf dem Informationssystem gespeicherte Vermögenswerte haben könnten, umgehend ohne Zeitverzug der AG zu melden. Prozesse zur Reaktion auf Sicherheitsvorfälle, sowie die dazugehörigen Rollen und Verantwortlichkeiten müssen definiert sein. Der AN wird im Falle eines Vorfalls auf Nachfrage der AG

Ressourcen zur Minderung und/oder Beseitigung des Vorfalles sowie den finalen Korrekturbericht bereitstellen.

[I_1.13] Jeder, der im Namen des ANs agiert, der entfernten oder lokalen Zugriff auf das Informationssystem der AG haben muss, muss Informationen zu seiner Identität bereitstellen. Der AN stellt sicher, dass in seinem Namen kein Zugang missbraucht wird und er die volle Verantwortung übernimmt, sollte sich herausstellen, dass dieser Fall eintritt.

Sollte der AN mit Subunternehmern zusammenarbeiten, um den Vertrag mit der AG zu erfüllen, muss der AN diesen ausdrücklich als Subunternehmer identifizieren und er muss sicherstellen, dass der Subunternehmer die gleichen Anforderungen erfüllt.

Auf Verlangen der AG ist der AN verpflichtet, nur überprüftes Sicherheitspersonal, z. B. geprüft von nationalen Behörden, zum Umgang mit sensiblem Equipment einzusetzen, sowohl vor der der Integration in das Netzwerk der AG als auch für die Wartung des sensiblen Equipments während der gesamten Betriebsphase. Relevante Informationen (insbesondere die Identifizierung und Bestimmung des sensiblen Equipments) müssen schriftlich vereinbart werden. Die von den lokalen gesetzlichen Bestimmungen festgelegten Ausnahmen sind zu beachten.

Der AN beauftragt nur Personen, die über entsprechende Kenntnisse und Fähigkeiten bzgl. Installation, Soft- oder Hardware, Wartung oder Betrieb der Lösung verfügen.

Security-Awareness-Trainings für die Mitarbeiter müssen periodisch durchgeführt werden. Die Inhalte der Schulungen müssen entsprechend den aktuellen Erkenntnissen regelmäßig aktualisiert werden.

[I_1.14] Wenn der AN Teile der Betriebsleistung oder anderer Dienstleistungen für die AG an weitere Dienstleister auslagert, müssen Sicherheitsanforderungen in den Vereinbarungen mit den Dienstleistern berücksichtigt werden. Die Sicherheitsanforderungen mit den Dienstleistern müssen so definiert werden, dass die Sicherheitsstandards für die Daten der AG und Leistungen für die AG in jedem Fall eingehalten werden können und dass der AN in der Lage ist, eigene Verpflichtungen zur Sicherheit gegenüber der AG vollumfassend zu erfüllen. Eine transparente Darstellung der durchgehenden Lieferkette einschließlich Subunternehmer ist gegenüber der AG nachzuweisen. Der AN muss der AG im Vorfeld von Entscheidungen über die Auslagerung von Betriebs- oder Dienstleistungen informieren.