

# IT-Standardanforderungen

Die folgenden Rahmenbedingungen und IT-Standardanforderungen sind zwingend zu berücksichtigen.

Die entsprechenden Systemvoraussetzungen der Auftragnehmer-Geräte ergeben sich (nachrangig zu den hiesigen Bestimmungen) aus den vor Vertragsschluss übergebenen Datenblättern.

## **Serverlandschaft**

Ein großer Teil der von Vivantes betriebenen Server wird im zentralen Rechenzentrum virtualisiert betrieben. Für die Bereitstellung der virtuellen Umgebung wird aktuell VMware vSphere auf aktuell HP-Serverhardware eingesetzt. Die Virtualisierung der Server wird für alle neuen Systeme und Anwendungen verwendet. Mindestvoraussetzung eines Server-Betriebssystems ist Windows Server 2022, diese werden in die Vivantes Domäne integriert.

## **Fernwartungszugriff**

Der administrative Zugriff auf Server und Geräte im Vivantes Netzwerk erfolgt entweder über einen von Vivantes vorgegebenen VPN-Client (Client-Gateway-Verbindung) oder eine Gateway-Gateway-Verbindung. Für weitere Informationen mit technischen und organisatorischen Angaben wird auf Anlage 3 zum Vertrag zur Auftragsverarbeitung: Fernwartung von Systemen der Vivantes – Netzwerk für Gesundheit GmbH verwiesen. Der Bieter stellt sicher, dass gemäß den angegebenen Informationen der Fernwartungszugriff erfolgen kann und stellt seinerseits alle notwendigen Informationen für die Einrichtung des Fernwartungszugangs mit Vertragsabschluss zur Verfügung.

## **Virenschutz**

Zum Schutz gegen Schadsoftware wird auf allen Clients und Servern bei Vivantes ein zentral administrierter Virens Scanner (TrendMicro Apex One) installiert. Diese Software arbeitet als „on access“ Scanner. Applikationen müssen ohne Einschränkungen mit der Virenschutzsoftware funktionieren. Ggf. notwendige Einschränkungen sind nur dann vom Auftraggeber zu dulden, wenn der Auftragnehmer vor Vertragsschluss explizit hierauf hingewiesen hat.

## **Browser**

Vivantes setzt als Standardbrowser den MS Edge und / oder den Firefox Browser ein. Die Unterstützung dieser Browser in der jeweils aktuellen Version ist ohne funktionale Einschränkungen für eingesetzte Softwarelösungen sicherzustellen.

## Mobile Endgeräte

Für mobile Endgeräte (Smartphones und Tablets) hat sich Vivantes auf iOS festgelegt. Die Geräteregistrierung von Apple Geräten auf Vivantes erfolgt über den Apple DEP Mechanismus. Android Systeme werden nicht unterstützt.

Die Anbindung kann über WLAN- oder Mobilfunkverbindungen (IP VPN) erfolgen.

Zur Verwaltung der Geräte, der Betriebssysteme und der auf den Geräten nutzbaren Apps setzt Vivantes das MDM Tool Mobile Iron ein.

## Verträge

Verträge für Softwarepflege (inkl. Updates und Upgrades) werden ggf. auf Basis der entsprechenden EVB-IT Vertragstypen des BMI in der jeweils aktuellen Version zu schließen.

## Informations- und Datensicherheit

Der unberechtigte Zugriff auf die Daten muss ausgeschlossen sein. Die gesetzlichen Datenschutzbestimmungen der DS-GVO, des Bundes und des Landes Berlin einschließlich des Landeskrankenhausgesetzes sind zu erfüllen. Gesetzliche Änderungen müssen in Produktentwicklungen einfließen.

Es gilt der Leitfaden des BSI zu den „Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte „Manufacturer Disclosure Statement for Medical Device Security“ (MDS2). Die notwendigen Angaben zur Beschreibung des Medizinproduktes sind bereits dem Angebot in elektronischer Form beizufügen (**siehe Anlage Ergänzende Vertragsbedingungen für MP (Anlage EVB-MP)**).

Für Support und Wartung bzw. Cloud-Hosting-Leistungen wird **die Anlage Vertrag zur Auftragsverarbeitung der Vivantes Netzwerk für Gesundheit GmbH** der Vivantes GmbH nach Art. 28 DS-GVO inklusive Anlage Vertragsbestandteil, sofern personenbezogene Daten verarbeitet werden akzeptiert werden.

## Informations- und Datensicherheit

Der unberechtigte Zugriff auf die Daten muss ausgeschlossen sein. Die gesetzlichen Datenschutzbestimmungen der DS-GVO, des Bundes und des Landes Berlin einschließlich des Landeskrankenhausgesetzes sind zu erfüllen. Gesetzliche Änderungen müssen in Produktentwicklungen einfließen.

Es gilt der Leitfaden des BSI zu den „Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte „Manufacturer Disclosure Statement for Medical Device Security (MDS2). Die notwendigen Angaben zur Beschreibung des Medizinproduktes sind bereits dem Angebot in elektronischer Form beizufügen (siehe Anlage Ergänzende Vertragsbedingungen für MP)

Es ist ein Informationssicherheits- und Datenschutzkonzept auf Basis der für Krankenhäuser im Land Berlin geltenden Rechtsvorschriften vorzulegen (DSGVO, LKG Berlin,...).

Das Konzept sollte insbesondere folgende Informationen bereitstellen:

- Informationen, welche sich aus dem Risikomanagementprozess nach DIN EN 80001-1 ergeben
- Umsetzung von Netzwerksicherheitsanforderungen
- Schutz vor schadhafter Software
- Protokollierungsmöglichkeiten
- Eingesetzte Verschlüsselungsverfahren (z.B. TLS 1.3)
- Business Continuity oder Disaster Recovery Pläne (BCP/DRP)
- Wartungsfähigkeit (z.B. Update- und Patchmanagement)
- Vertraulichkeitsvereinbarung (z.B. mit Medizinprodukteberater)
- Compliance-Aspekte (z.B. Datenschutz, Medizinproduktesicherheit)
- Reaktionszeiten des Dienstleisters
- Vorgaben zum Umgang mit Daten nach Vertragsende

Für Support und Wartung bzw. Cloud-Hosting-Leistungen muss der Auftragsdatenverarbeitungsvertrag der Vivantes GmbH (siehe Anlage 3) nach §28 DS-GVO inklusive Anlage unterschrieben werden sofern personenbezogene Daten verarbeitet werden.