

Anlage L1

Vorgaben aus IT-Sicht

Fotorealistischer Beratungssavatar

Inhalt

Vorgaben aus IT-Sicht	1
Allgemeine Vorgaben zu Anwendungen	2
Qualitätssicherung	2
Vorgaben für den Betrieb	3
Antwortzeit	3
Herstellersupport	3
Plattform-Konformität	3
Vorgaben zu Clients	3
Allgemeine Vorgaben für Clients	3
Vorgaben zum Datenaustausch	3
Verfahren für den Austausch von Dateien	3
Vorgaben zur Datenhaltung	4
Vorgaben zu dezentraler Datenhaltung	4
Vorgaben zum Datenschutz	4
Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag	4
Keine Datenübermittlung an Dritte	4
Vorgaben zur Ergonomie	4
Barrierefreiheit für externe Anwendungen	4
Barrierefreiheit für interne Anwendungen	4
Vorgaben zur IT-Sicherheit	4
Eindeutige Authentifizierung	4
Identity und Access Management	4
Meldung von Sicherheitsvorfällen	5
Nutzung von Cookies in Webanwendungen	5
Prüfrechte der TK	5
Vorgaben für öffentlich erreichbare Webanwendungen	5
Vorgaben zur Verfügbarkeit	6
Basisanforderungen zur Verfügbarkeit	6
Vorgaben zu Webclients	6
Lauffähigkeit auf aktuellen Browsern	6
Vorgaben für Webclients (allgemein)	6

Allgemeine Vorgaben zu Anwendungen

Qualitätssicherung

Der AN unterzieht den Content, die Funktionalitäten und die Anwendungen einer inhaltlichen und technischen, nachhaltigen Qualitätssicherung (QS). Folgende Maßnahmen werden durch den AN im Rahmen der QS mindestens eingesetzt:

- Tests inkl. Dokumentation der Testfälle und -ergebnisse
- Statische und dynamische Verfahren zum Aufspüren von Schwachstellen in eigenentwickeltem Code

- Verfahren zur Erkennung von Schwachstellen in verwendeten Drittanbieterkomponenten
- Überprüfen von Code-Qualitätsstandards in eigenentwickeltem Code
- Change-Management inkl. Freigabeverfahren
- Problem-Management inkl. Lösungen und Maßnahmen zur künftigen Prävention

Der AN legt im Rahmen der Auftragsdurchführung das Verfahren zur QS gegenüber der TK offen. Bei festgestellten Mängeln kann die TK Nachbesserung verlangen.

Vorgaben für den Betrieb

Antwortzeit

Die Anwendung beantwortet 95% aller Anfragen in weniger als 0,8 Sekunden.

Für Anwendungen, bei denen die Antwort über das Internet ausgeliefert wird, kann seitens TK mit einem für die Anwendung zur Verfügung stehenden/zugesicherten Bandbreitendurchsatz von 5 MBit/s gerechnet werden, bei einer Latenz von max. 100ms.

Auf Basis dieser Kennzahlen muss die Anwendung für die geforderten Transaktionen die entsprechende Antwortzeiten einhalten.

Herstellersupport

Der AN leistet Support mit garantierten Responsetimes. Die Responsetime in dem Fall, dass die Anwendung nicht zur Verfügung steht, beträgt **24 Std** im Zeitraum von **Montag bis Freitag, von 6:00 bis 22:00 Uhr**.

Plattform-Konformität

Die Anwendung wird als Software as a Service ausgeliefert.

Vorgaben zu Clients

Allgemeine Vorgaben für Clients

Die Anwendung reagiert auf die Eigenschaften des jeweils benutzten Endgerätes und unterstützt eine geräteoptimierte Darstellung, die gute Lesbarkeit und einfache Navigation mit einem Minimum an Verschieben und Blättern ermöglicht (Responsive Design).

Die Validierung von Eingaben erfolgt immer serverseitig und ggf. **ergänzend** clientseitig (z.B. durch JavaScript).

Vorgaben zum Datenaustausch

Verfahren für den Austausch von Dateien

Die TK unterstützt für den Austausch mit externen Stellen folgende Verfahren:

- Automatisierte Austauschverfahren für den Datenaustausch im Gesundheitswesen (s. "Gemeinsame Grundsätze Technik", https://www.gkv-datenaustausch.de/technische_standards_1/technische_standards.jsp)
- Austausch über fest definierte S-FTP bzw. FTP-S Server bei externen Partnern.
- S/MIME-gesicherte E-Mails
- Manueller Austausch über Cryptshare (<https://webft.tk.de>)

Für Datentransfers von und zur TK müssen die unterstützten Verfahren genutzt werden. Das gewählte Verfahren ist zwischen TK und AN zu vereinbaren und vom AN zu beschreiben. Soweit technisch machbar und wirtschaftlich umsetzbar, sind die Verfahren des Datenaustausches im Gesundheits- und Sozialwesen über Datenannahmestellen (siehe <https://www.gkv-datenaustausch.de>) bevorzugt zu verwenden.

Bei Verwendung von S-FTP bzw. FTP-S stellt der Auftragnehmer den entsprechenden Server bereit und betreibt diesen.

Vorgaben zur Datenhaltung

Vorgaben zu dezentraler Datenhaltung

Sofern Daten bspw. aus Performancegründen dezentral gespeichert werden, so werden Verfahren zur Datensicherung und zum Schutz der Vertraulichkeit und Integrität angegeben und umgesetzt.

Vorgaben zum Datenschutz

Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag

Der Auftragnehmer gibt keine im Rahmen des Betriebes gesammelten personenbezogenen Daten an Dritte weiter oder wertet diese ohne Auftrag aus.

Keine Datenübermittlung an Dritte

Personenbezogene Daten gem. Art. 4 Nr. 1 DSGVO sowie Sozialdaten gem. § 67 Abs. 2 SGB X dürfen nicht an Dritte gem. Art. 4 Nr. 10 DSGVO übermittelt werden, sofern sich dies nicht explizit aus dem Vertrag oder einer gesetzlichen Verpflichtung nach deutschem oder europäischem Recht ergibt.

Vorgaben zur Ergonomie

Barrierefreiheit für externe Anwendungen

Die Anwendung, welche für die Benutzung durch TK-Kunden, Partner oder die Allgemeinheit gedacht ist, hält die BITV 2.0 oder vergleichbare Vorgaben ein.

Barrierefreiheit für interne Anwendungen

Das User Interface ist barrierefrei. Es unterstützt mindestens:

Vollständige Tastaturbedienbarkeit

Unterstützung von Screenreadern und Braille-Zeilen

Alternativtexte für Bilder

Bedienbarkeit auch bei Einsatz eines Skalierungsfaktors von 250% gegenüber der von der Berufsgenossenschaft empfohlenen Schriftgröße (Zeichenhöhe für Großbuchstaben in mm = Sehabstand in mm / 155; entsprechend 20-22 Bogenminuten Sehwinkel).

Bedienbarkeit bei Einsatz der durch das Betriebssystem bereitgestellten Mittel zur erleichterten Bedienung (insbesondere die Nutzung der vom Betriebssystem vorgegebenen Standards, damit individuell angepasste Farbschemata verwendet werden können).

Vorgaben zur IT-Sicherheit

Eindeutige Authentifizierung

Die Anwendung besitzt Verfahren für die eindeutige Authentifizierung von Anwendenden. Bei Anwendungen, die sich an TK-Mitarbeitende richten, entsprechen die Benutzernamen dem bei der TK verwendeten Schema. Das Schema wird dem Auftragnehmer durch die TK auf Anforderung bereitgestellt.

Identity und Access Management

Die Anwendung ist in ein Single Sign On bei der TK integrierbar. Es wird das Microsoft Active Directory oder Entra ID bei der Anmeldung unterstützt.

Zur Authentifizierung wird mindestens eines der folgenden Protokolle unterstützt:

OpenID/OAuth2 über Microsoft Entra ID Enterprise Application
(siehe <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-application-management>)

SAML über Microsoft Entra ID Enterprise Application (siehe <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-application-management>)

Kerberos über Microsoft Active Directory. Dies ist jedoch NICHT zulässig für Anwendungen, die über eine HTTP-Schnittstelle angesprochen werden. In diesem Fall unterstützt die Anwendung mindestens eines der beiden anderen genannten Protokolle.

Die Anwendung verfügt über ein für den Anwendungszweck geeignetes Rollen- und Rechte-Management. Dieses stellt insbesondere sicher, dass:

Die Rechte für administrative Tätigkeiten von den Rechten zur regulären Nutzung getrennt sind.

Auf von der Anwendung verarbeitete Daten nur von denjenigen Mitarbeitern zugegriffen werden kann, die den Zugriff für die Erfüllung ihrer Aufgaben benötigen.

Meldung von Sicherheitsvorfällen

Der AN meldet der TK unverzüglich Sicherheitsvorfälle, die direkt oder indirekt den vom AN für die TK bereitgestellten Dienst betreffen. Die Meldung erfolgt an die jeweils verantwortlichen Ansprechpartner sowie an von der TK nach Zuschlag zur Verfügung gestellte E-Mailadressen. Reaktionen auf diese Vorfälle werden gemeinsam abgestimmt.

Nutzung von Cookies in Webanwendungen

Cookies, welche für serverseitiges Tracking von Loginsessions verwendet werden, erfüllen folgende Anforderungen

- Das Attribut "Expires" ist nicht gesetzt.
- Die Attribute "Secure" und "HttpOnly" sind beide gesetzt.
- Das Cookie wird bei jedem Authentisierungsvorgang neu gesetzt.
- Das Cookie wird bei Logout serverseitig invalidiert.

Prüfrechte der TK

Die TK ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Die TK ist berechtigt, regelmäßig (mindestens monatlich, höchstens täglich) oder anlassbezogen (z.B. Bekanntwerden einer über das Netzwerk ausnutzbaren Schwachstelle oder Nachverfolgung von Härtungsmaßnahmen) nichtinvasive Prüfungen wie Portscans und Aufrufe der Webschnittstellen durchzuführen. Darüber hinaus hat die TK das Recht, die Sicherheit der beteiligten Systeme und Prozesse im Rahmen von Assessments zu überprüfen. Insbesondere stimmt der AN zu, dass die TK bzw. ein von Ihr beauftragter Prüfer nach Vorankündigung eigene Penetrationstests durchführen darf.

Vorgaben für öffentlich erreichbare Webanwendungen

Eine Anwendungssitzung wird nach maximal 30 Minuten Inaktivität serverseitig beendet.

Die Anwendung setzt KEINE 3rd Party Cookies im Browser der Anwendenden.

Die Einbindung von externem JavaScript Code (insb. "Pixel" und "Tags") erfolgt ausschließlich mittels des Tag Management Systems der TK.

Es werden keine Profile durch den AN erstellt. Das Surfverhalten der User (Tracking/Webanalytics) wird nicht ausgewertet. Ggf. wird die TK eine Auswertung des Surfverhaltens vornehmen wollen. In diesem Fall bindet der AN das Tag Management

System der TK ein, auch wenn dieser keinen externen JavaScript Code verwendet. In diesem Fall verwendet der AN auch das Consent Management der TK.

Vorgaben zur Verfügbarkeit

Basisanforderungen zur Verfügbarkeit

Der AN legt die von ihm bereitgestellten Dienste und Anwendungen hochverfügbar aus. Sie müssen im Zeitraum **Montag bis Freitag, von 6:00 bis 22:00 Uhr** verfügbar sein. Ihre durchschnittliche Verfügbarkeit im Jahr beträgt mindestens 99,9 % innerhalb der vereinbarten Betriebszeiten.

Sofern das Internet verwendet wird, stellt der AN eine leistungsfähige und redundante Anbindung an den Internet-Backbone sicher.

Bei geplanten Änderungen an Systemen und Anwendungen, die zu einer Abweichung von den vereinbarten Betriebszeiten führen oder führen können, informiert der AN die TK mit einem Vorlauf von einer Woche. Dies kann schriftlich oder per E-Mail an den vereinbarten Ansprechpartner der TK erfolgen.

Der AN richtet seine eingesetzten IT-Kontinuitätslösungen so ein, dass nach einer Störung der Dienst innerhalb von **48 Std** wieder zur Verfügung steht. In jedem Fall darf nach einem Wiederanlauf nur ein Datenverlust des Transaktionsvolumens von maximal **4 Std** auftreten.

Der AN informiert das Network Operations Center der TK nach Feststellung eines Fehlers und bei Beeinträchtigung des Dienstes unverzüglich per Telefon oder E-Mail. Er gibt dabei die Art der Störung und die voraussichtliche Zeitdauer der Beeinträchtigung bzw. des Ausfalls an. Nach Beseitigung der Störung gibt der AN eine Entwarnung per Telefon oder E-Mail an das Network Operations Center der TK.

Die maximale Ausfallzeit - auch bei Hardware-Defekten - beträgt **48 Std**.

Vorgaben zu Webclients

Lauffähigkeit auf aktuellen Browsern

Die vom AN bereitgestellte Anwendung bzw. die bereitgestellten Internetseiten werden von folgenden Browsern vollständig und korrekt dargestellt und sind vollständig funktionsfähig: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari.

Von jedem Browser werden diejenigen Versionen unterstützt, welche von dem jeweiligen Hersteller innerhalb den letzten 24 Monaten veröffentlicht wurden. Dies gilt fortlaufend über die komplette Vertragslaufzeit. Der AN testet die Anwendung bzw. die Internetseiten mit den zu unterstützenden Browsern.

Die TK kann die Liste der zu unterstützenden Browser aktualisieren, z.B. um die Entwicklungen des Marktes zu berücksichtigen. Sie zeigt dem AN die Aktualisierung schriftlich per E-Mail oder über ein Ticketsystem (falls vorhanden) an. Der AN stellt die Unterstützung der in der aktualisierten Liste genannten Browser binnen vier Wochen sicher, sofern die neu hinzugekommenen Browser vergleichbar kompatibel mit der aktuellen HTML Spezifikation des W3C sind.

Vorgaben für Webclients (allgemein)

Für die Internetseiten und -anwendungen gelten nachstehende Anforderungen und Pflichten zu den verwendeten Sprachen und Gestaltungstechniken:

- Als clientseitige Scriptsprache wird nur JavaScript eingesetzt.
- Flash-Animationen und andere Plugins werden nicht eingesetzt.
- Framesets werden nicht eingesetzt.
- Die Anwendung unterstützt die Kommunikation mit einem WEB-Proxy grundsätzlich unterstützen. Darüber hinaus entsprechen die verwendeten Technologien und Protokolle den üblichen Internetstandards gemäß Request for Comments (RFC).

- Der AN setzt konsequent Cascading Style Sheets ein und gewährleistet damit die Trennung von Inhalt und Darstellung - unter Einhaltung des Corporate Design der TK.
- Die vom AN eingesetzten Stylesheets sind entsprechend der aktuellen W3C-Konvention syntaktisch korrekt.
- Der AN muss die vom AG bereitgestellten UI Bausteine aus der TK UI Library in Form von "Web Components" verwenden. Der AG stellt diese in Form von statischen Dateien (JS & CSS) bereit, die vom CDN des AG durch den AN einzubinden und zu verwenden sind.
- Sämtliche UI Komponenten, die in der Library enthalten sind, sind für gleichartige Anwendungsfälle in der vom AN zu entwickelnden Oberfläche zu verwenden.
- Der AN hat dabei die zum Zeitpunkt der Entwicklung aktuellste Version der UI Library zu verwenden und
- Auf explizite Anweisung des AG ist die verwendete Version der UI Library innerhalb von 4 Wochen auf einen genannten Stand zu aktualisieren. Es steht dem AN frei selbständig aktuellere Versionen der UI Library zu verwenden, sowie diese im Laufe des Vertragsverhältnisses vom AG veröffentlicht werden.