

Anlage L1

TK-Schwangerschaftsapp

Vorgaben aus IT-Sicht (IT-Pflichtenheft)

26-09209

Inhalt

TK-Schwangerschaftsapp	1
Allgemeine Vorgaben zu Anwendungen	3
Qualitätssicherung	3
Vorgaben zu Apps	3
Zugekaufte Apps - allgemeine Vorgaben	3
Zugekaufte Apps – Security	4
Vorgaben für den Betrieb	4
Antwortzeit	4
Herstellersupport	4
Plattform-Konformität	4
Vorgaben zur Netzwirkommunikation	4
Vorgaben zu Clients	4
Allgemeine Vorgaben für Clients	4
Vorgaben zum Datenaustausch	5
Verfahren für den Austausch von Dateien	5
Vorgaben zur Datenhaltung	5
Vorgaben zu dezentraler Datenhaltung	5
Vorgaben zum Datenschutz	5
Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag	5
Keine Datenübermittlung an Dritte	5
Vorgaben zur IT-Sicherheit	5
Eindeutige Authentifizierung	5
Freiheit von Schadsoftware	5
Identity und Access Management	5
Meldung von Sicherheitsvorfällen	6
Nutzung von Cookies in Webanwendungen	6
Patch- und Release-Management (allgemeine Vorgaben)	6
Prüfrechte der TK	6
Transport Layer Security (TLS)	7
Transportverschlüsselung nicht-öffentlicher Daten	7
Überprüfung von Eingaben	7
Vorgaben für öffentlich erreichbare Webanwendungen	7
Wahl von Verschlüsselungsverfahren und Cipher-Suites	7
Sicherheitsrelevante Zufallswerte	7
Vorgaben zur Verfügbarkeit	7
Basisanforderungen zur Verfügbarkeit	7
Vorgaben zu Webclients	8
Lauffähigkeit auf aktuellen Browsern	8
Vorgaben für Webclients (allgemein)	8

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 zu Apps

Zugekaufte Apps - allgemeine Vorgaben

Die App ist über die Standard-App-Stores der Plattformen Android und iOS verfügbar. Sie entspricht den dort geltenden Richtlinien. Sie wird nach Absprache mit der TK über den Store-Account des App-Anbieters oder den Store-Account der TK veröffentlicht.

Es wird dem Kunden explizit erläutert, wozu die App Berechtigungen benötigt, sofern dies nicht offensichtlich ist. Berechtigungen, die für die Kernfunktionalität der App nicht erforderlich sind, sondern nur dem Benutzerkomfort dienen, können vom Nutzer verweigert werden. In diesem Fall steht die Kernfunktionalität der App weiterhin zur Verfügung.

Die App unterstützt alle Betriebssystemversionen der jeweiligen Plattform (iOS und Android) für einen Zeitraum von mindestens 36 Monaten ab deren Veröffentlichung.

Verwendete Fremdbibliotheken sind unter Angabe der genutzten Versionen bei jedem Store-Upload zu dokumentieren.

Sicherheitsupdates für externe Bibliotheken und Frameworks werden innerhalb von 30 Tagen nach deren Verfügbarkeit integriert und die neuen App-Versionen über die Stores veröffentlicht.

Fremdbibliotheken sind datensparsam konfiguriert.

Die App ist intuitiv bedienbar und folgt dem Bedienkonzept der jeweiligen Plattform.

Aktualisierungen der App erfolgen über den App-Store der jeweiligen Plattform.

Es wird den Nutzenden explizit erläutert, welche Daten erhoben, verarbeitet und gespeichert werden. Dies schließt auch die nicht offensichtliche Datenverarbeitung wie z. B. Tracking ein. Die Verwendung dieser Daten wird dargestellt und die Erlaubnis der Nutzenden dazu wird eingeholt. Die Nutzenden können den Datenverwendungen, die nicht für die Kernfunktionalität der App notwendig sind, widersprechen. In diesem Fall steht die Kernfunktionalität trotzdem zur Verfügung.

Wenn die App den Zugang zu sensiblen Daten ermöglicht, haben Nutzende die Möglichkeit, einen zusätzlichen App-spezifischen Zugangsschutz einzurichten (z. B. biometrische Merkmale, Hardwaretoken oder Kennwort).

Daten werden nur über TLS transportiert. Die Empfehlungen der jeweils aktuellen BSI-Vorgaben zu TLS z.B. *TR-02102* und der jeweiligen Plattform wie z.B. „Apple App Transport Security“ oder `OkHttp.RESTRICTED_TLS` werden beachtet.

Sensible Daten werden nur sicher verschlüsselt lokal gespeichert. Die Empfehlungen der jeweiligen Plattform werden beachtet.

Die App geht mit dem Datenvolumen der Nutzenden sparsam um. Aus Sicht der Nutzenden ist der Verbrauch des Datenvolumens dem Zweck angemessen.

Die App geht mit dem Akkuvolumen der Nutzenden sparsam um. Aus Sicht der Nutzenden ist der Stromverbrauch dem Zweck angemessen.

Zugekaufte Apps – Security

Der AN hält die Vorgaben des BSI zu Gesundheits-Apps ein, u.a. die jeweils gültige TR-03161 Teil 1, oder begründet die Abweichungen. Die Checkliste ist der Dokumentation bei jeder Version beizufügen.

Zugekaufte Apps - Vorgaben für das Backend und weitere Datenendpunkte

Der AN hält die Vorgaben des BSI zu Gesundheits-Apps ein, u.a. die jeweils gültige TR-03161 Teil 2&3, oder begründet die Abweichungen. Die Checkliste ist der Dokumentation bei jeder Version beizufügen.

Einhaltung aller TK-Richtlinien

Alle TK-Richtlinien und Vorgaben aus IT-Sicht müssen auch durch das Backend und Provider von weiterem Content eingehalten werden.

Schutz gegen Missbrauch

Alle Schnittstellen des Backends und weiterer Datenendpunkte sind gegen Missbrauch geschützt, beispielsweise durch verpflichtende Authentifizierung und Verschlüsselung.

Vorgaben für den Betrieb

Antwortzeit

Die Anwendungen beantworten 95% aller Anfragen in weniger als 2 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 Anwendungen nicht zur Verfügung stehen, beträgt **8h** im Zeitraum **von Montag bis Freitag, von 9:00 bis 18:00 Uhr**.

Plattform-Konformität

Die Anwendungen (das Backend der App und das Content Management System) werden als Software as a Service ausgeliefert.

Vorgaben zur Netzwerkkommunikation

Alle verwendeten Netzwerk-Kommunikationsprotokolle sind gemäß den jeweils gültigen RFCs implementiert.

Vorgaben zu Clients

Allgemeine Vorgaben für Clients

Die Anwendung (das Content Management System) 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 WebFT(<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 IT-Sicherheit

Eindeutige Authentifizierung

Die Anwendungen besitzen Verfahren für die eindeutige Authentifizierung von Anwendenden.

Freiheit von Schadsoftware

Alle Bestandteile des Angebots sind frei von Schadsoftware (Viren, Würmer, Backdoors usw.). Der AN stellt dies durch geeignete Maßnahmen sicher. Der AN prüft insbesondere sämtliche ausgelieferte Software vor Auslieferung mittels marktgängiger und aktueller Scanner oder mindestens gleichwertiger Technologie.

Identity und Access Management

Die Anwendung (das Content Management System) 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 in Webanwendungen, 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.

Patch- und Release-Management (allgemeine Vorgaben)

Die Anwendungen werden regelmäßig weiterentwickelt und an neue Anforderungen angepasst. Sicherheitsrelevante Patches auf Plattform- und Datenbankebene werden spätestens 2 Wochen nach deren genereller Verfügbarkeit unterstützt. Service Packs und neue Maintenance Level auf Plattform- und Datenbankebene werden spätestens 3 Monate nach der generellen Verfügbarkeit unterstützt. Neue Releases auf Plattform- und Datenbankebene werden spätestens 12 Monate nach deren genereller Verfügbarkeit unterstützt.

Der AN informiert die TK selbstständig und ohne Aufforderung über neue Releasestände und Patches, idealerweise per E-Mail.

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 Härtingsmaßnahmen) 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.

Transport Layer Security (TLS)

Der AN hält sich bei der Wahl von TLS-Version(en) und der eingesetzten Cipher-Suites an die Empfehlungen der jeweils aktuellen Fassung der Technischen Richtlinie BSI TR-02102-2 *“Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)”* des BSI. Der Auftragnehmer stellt sicher, dass alle Kommunikationsteilnehmer mindestens eine der zulässigen Cipher-Suites unterstützen. Der AN gleicht die von ihm gewählte Konfiguration mindestens jährlich gegen die Vorgaben des BSI ab. Bei Abweichungen passt der AN die Konfiguration an, um Konformität mit der o.a. Richtlinie herzustellen.

Transportverschlüsselung nicht-öffentlicher Daten

Nicht-öffentliche Daten werden immer verschlüsselt übertragen.

Überprüfung von Eingaben

Die Anwendungen bzw. die vom AN für die TK bereitgestellten Dienste prüfen alle Eingaben vor der Verarbeitung, um bspw. Buffer-Overflows und Injection-Angriffe auszuschließen.

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.

Es werden keine Profile durch den AN erstellt. Das Surfverhalten der User (Tracking/Webanalytics) wird nicht ausgewertet.

Wahl von Verschlüsselungsverfahren und Cipher-Suites

Sofern in der Software Verschlüsselungsalgorithmen eingesetzt werden, sind diese zur aktuellen Fassung "BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen" konform. Sofern Verschlüsselungsalgorithmen im direkten Umfeld von qualifizierten elektronischen Signaturen nach dem bundesdeutschen Signaturgesetz eingesetzt werden, richten sie sich nach den Veröffentlichungen der Bundesnetzagentur im Bundesanzeiger. Verschlüsselungsverfahren werden vor Ablauf des laut der o.a. genannten Vorschriften zulässigen Verwendungsdatums durch aktuelle Verfahren ersetzt werden.

Sicherheitsrelevante Zufallswerte

Sollen sicherheitsrelevante Zufallswerte (z.B. Session-IDs, kryptographisches Material, Initial-PINs) in einer Anwendung verwendet werden, so müssen diese hinreichend zufällig sein. Die dafür verwendeten Zufallsgeneratoren müssen den Vorgaben aus Kapitel "Zufallszahlengeneratoren" der aktuellen Technischen Richtlinie BSI TR-02102-1 des BSI entsprechen.

Vorgaben zur Verfügbarkeit

Basisanforderungen zur Verfügbarkeit

Der AN legt die von ihm bereitgestellten Dienste und Anwendungen hochverfügbar aus. Sie müssen im Zeitraum **von Montag bis Freitag, von 9:00 bis 18:00 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 **24h** wieder zur Verfügung steht. In jedem Fall darf nach einem Wiederanlauf nur ein Datenverlust des Transaktionsvolumens von maximal **24h** 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 **24h**.

Vorgaben zu Webclients

Lauffähigkeit auf aktuellen Browsern

Falls eine Webanwendung eingesetzt wird (z.B. für das Content Management System), wird sie von folgenden Browsern vollständig und korrekt dargestellt und ist vollständig funktionsfähig unter: 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 Webanwendungen 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).