# Vorgaben aus IT-Sicht

25-08897 Sektoraler Identity Provider (IDP)

# Inhalt



## 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 eigentwickeltem 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 jeweiligen Plattform wie „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 - MASVS

Der Mobile Application Security Verification Standard (MASVS, siehe *https://github.com/OWASP/owasp-masvs/releases/*) ist eine Community-Initiative mit dem Ziel ein Rahmenwerk von Security-Anforderungen für Design, Entwicklung und Test von mobilen Apps unter iOS und Android zu etablieren. Der MASVS legt für unterschiedliche Bedrohungslevel ("L1", "L2") sowie für Resilienz gegen Reverse Engineering und Manipulation ("R") eine Reihe von Anforderungen fest.

Der AN pflegt bei Einführung und bei jeder größeren Änderung - mindestens aber alle 24 Monate - eine Checkliste, welche Anforderungen des MASVS in der jeweils aktuellen Version (siehe *https://github.com/OWASP/owasp-masvs/releases/*) erfüllt sind und welche noch nicht. Dazu wählt er zunächst den Prüflevel (z. B. "L1"+"R" oder "L2") aus und begründet diese Wahl. Die Checkliste ist der Dokumentation bei jeder Version beizufügen.

### Zugekaufte Apps - Vorgaben für das Backend und weitere Datenendpunkte

*Einhaltung aller TK-Richtlinien*
Alle TK-Richtlinien 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 Anwendung beantwortet 95% aller Anfragen in weniger als 2 Sekunden.

Für Anwendungen, die in der TK betrieben und genutzt werden, zählt dabei die End-2-End-Antwortzeit am Client. Es kann dabei davon ausgegangen werden, dass alle Clients mindestens über ein WAN mit 4 MBit/s angebunden sind. Die aktuellen Hard- und Software-Spezifikationen eines TK-Referenzclients können auf Anfrage entsprechend bereitgestellt werden.

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 gemäß gematik Spezifikation.

Die Integration in die ITSM-Prozesse der TK muss für Second- und Third-Level-Support Ticket-basiert automatisierbar sein. Tickets, die beim AN zur Bearbeitung liegen, müssen durch zuständige TK-Mitarbeiter einsehbar sein.

### Vorgaben zur Netzwerkkommunikation

Alle verwendeten Netzwerk-Kommunikationsprotokolle sind gemäß den jeweils gültigen RFCs implementiert. Die Anwendung ist integrierbar in Netzwerken, in denen IPv4-Netzwerk-Adress-Translation eingesetzt wird. Die Netzwerk-Kommunikation des Produktes ist zwischen per Firewallsystemen getrennten Netzwerkbereichen möglich.

## 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 Emails
- 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 http://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.

## Vorgaben zu Backup & Recovery

Um die Datensicherheit zu gewährleisten, erstellt die Anwendung regelmäßig Backups der zu verarbeiteten Daten. Die dafür notwendige Backupstrategie berücksichtigt den Stand der Technik (insb. einer Verschlüsselung der Daten) sowie die entsprechenden datenschutzrechtlichen Vorgaben (insb. zur Löschung).

## Vorgaben zur Verfügbarkeit

### Basisanforderungen zur Verfügbarkeit

Die Verfügbarkeiten leiten sich grundsätzlich aus der gematik Spezifikation ab.

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

Der AN richtet seine eingesetzten IT-Kontinuitätslösungen so ein, dass nach einer Störung der Dienst innerhalb von einer Stunde wieder zur Verfügung steht. Im Falle des Komplettausfalls eines Rechenzentrums muss der Dienst innerhalb von 24 Stunden wieder zur Verfügung stehen können. In jedem Fall darf nach einem Wiederanlauf nur ein Datenverlust des Transaktionsvolumens von nahe Null auftreten.

## 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 den 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 Email 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 die 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.