

IT-Pflichtenheft: Allgemeine technische Vorgaben zum Einsatz von IT-Systemen im Rahmen der Online-Sozialwahl 2029 (Anlage L3)

26-09148

Inhalt

Allgemeine technische Vorgaben zum Einsatz von IT-Systemen im Rahmen der Online-Sozialwahl 2029	1
Allgemeine Vorgaben zu Anwendungen	2
Qualitätssicherung	2
Vorgaben zu Apps	3
Apps - allgemeine Vorgaben	3
Zugekaufte Apps - MASVS	4
Vorgaben für den Betrieb	4
Antwortzeit	4
Vorgaben zur Netzwirkommunikation	4
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.	4
Vorgaben zum Datenaustausch	4
Verfahren für den Austausch von Dateien	4
Vorgaben zur Datenhaltung	5
Vorgaben zu dezentraler Datenhaltung	5
Sofern Daten bspw. aus Performancegründen dezentral gespeichert werden, so werden Verfahren zur Datensicherung und zum Schutz der Vertraulichkeit und Integrität angegeben und umgesetzt.	5
Vorgaben zum Datenschutz	5
Hosting - Auswertung gesammelter Daten nur mit Auftrag der AG	5
Keine Datenübermittlung an Dritte	5
Vorgaben zur Ergonomie	5
Barrierefreiheit für externe Anwendungen	5
Die Anwendung, welche für die Benutzung durch Kunden, Partner oder die Allgemeinheit gedacht ist, hält die BITV 2.0 oder vergleichbare Vorgaben ein.	5
Vorgaben zur Verfügbarkeit	5
Basisanforderungen zur Verfügbarkeit	5
Erweiterte Anforderungen an die Verfügbarkeit	5
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 den AG offen. Bei festgestellten Mängeln können die AG Nachbesserung verlangen.

Vorgaben zu Apps

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 den AG über den Store-Account des App-Anbieters oder den Store-Account der AG 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 Prüflvel (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

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.

Es 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. Für Anwendungen, bei denen die Antwort über das Internet ausgeliefert wird, kann 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.

Vorgaben zur Netzwirkommunikation

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 zum Datenaustausch

Verfahren für den Austausch von Dateien

Die AG unterstützen 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 oder Dracoon

Für Datentransfers von und zu den AG müssen die unterstützten Verfahren genutzt werden. Das gewählte Verfahren ist zwischen den AG und dem AN individuell 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 Auftrag der AG

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 Kunden, Partner oder die Allgemeinheit gedacht ist, hält die BITV 2.0 oder vergleichbare Vorgaben ein.

Vorgaben zur Verfügbarkeit

Basisanforderungen zur Verfügbarkeit

Der AN legt die von ihm bereitgestellten Dienste und Anwendungen hochverfügbar aus. Sie müssen im Wahlzeitraum Montag bis Sonntag, von 0:00 bis 24:00 Uhr (vereinbarte Betriebszeiten) verfügbar sein. Ihre durchschnittliche Verfügbarkeit im Jahr beträgt mindestens 99,9 % innerhalb der vereinbarten Betriebszeiten. In den vereinbarten Betriebszeiten sind geplante Wartungsfenster nicht zulässig. Über geplante Wartungsfenster außerhalb der vereinbarten Betriebszeiten informiert der AN die AG mit einem Vorlauf von einer Woche. Dies kann schriftlich oder per E-Mail an den vereinbarten Ansprechpartner der AG erfolgen.

Während der Konzeptions- und Bereitstellungsphase, sowie der Wahlnachbereitungsphase ist eine angemessene Verfügbarkeit zu gewährleisten, die eine reibungslose Durchführung der Online-Wahl ermöglicht.

Für die Einhaltung der SLA stellt der AN den AG den Zugriff auf entsprechende Statistiken bereit.

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 nach einem Wiederanlauf nur ein Datenverlust des Transaktionsvolumens von nahe Null auftreten.

Erweiterte Anforderungen an die Verfügbarkeit

Für die Überprüfung der Einhaltung des Service Level Agreements (SLA) hinsichtlich der Transaktionszeiten stellt der AN den AG mind. eine entsprechende offene Schnittstelle (API) bereit, über die Antwortzeit- und Verfügbarkeitsmetriken in Intervallen von maximal 15 Minuten maschinenlesbar abgerufen werden können. Folgende Verfahren stehen dabei alternativ zur Verfügung:

- Die Anwendung bietet einen HTTPS Metricendpoint (z.B. nach Prometheus-Standard bzw. OpenTelemetry Spezifikationen) und liefert darüber detailliert Performancemetriken zu den ausgeführten Transaktionen.
- Die Anwendung bzw. eine eigene Monitoringagentenkomponente unterstützt nativ die Weiterleitung von ihren eigenen Performancedaten an einen InfluxDB kompatiblen Endpoint.
- Sofern es sich um netzwerknahe Services (z. B. Printspool) handelt, ist zusätzlich möglich: Die Anwendung bietet eine SNMP Schnittstelle, welche Abfragen via SNMP (v3) zulässt, um Performancemetriken der Anwendung aktiv auszulesen.

Zur Überprüfung der Erreichbarkeit des Service stellt der AN einen Referenzdienst bereit. Der Referenzdienst simuliert das Verhalten des bereitgestellten Dienstes und muss ein sicherer Indikator für die Verfügbarkeit und Performance aller beteiligten Komponenten sein. Die Details zur Nutzung des Referenzdienstes im Rahmen des Monitorings werden zwischen AG und AN abgestimmt.

Ein Dienst gilt in einem Abfrage-Referenzintervall als nicht verfügbar, wenn entweder der Dienst nicht erreicht werden kann oder in diesem und den beiden vorhergehenden Referenzintervallen die vereinbarten Antwortzeiten nicht eingehalten wurden.

Die Anwendung soll ein automatisches Umschalten beim Schwenken von benutzten Server- und Netzwerk-Ressourcen unterstützen, ohne dass dazu manuelle Eingriffe nötig sind.

Der Auftragnehmer hat ein funktionierendes Business Continuity Management nach BSI-Standard 200-4 oder ISO 22301 BCMS bei sich etabliert.

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 AG können die Liste der zu unterstützenden Browser aktualisieren, z.B. um die Entwicklungen des Marktes zu berücksichtigen. Sie zeigen 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.

- Die vom AN eingesetzten Stylesheets sind entsprechend der aktuellen W3C-Konvention syntaktisch korrekt.