

# eProcurement Plattform

25-08555

## Inhalt

Vorgaben aus IT-Sicht .....	1
Allgemeine Vorgaben zu Anwendungen .....	2
Integrationsfähigkeit in Portale und Workflows .....	2
Qualitätssicherung .....	3
Vorgaben zu Apps .....	3
Zugekaufte Apps - allgemeine Vorgaben .....	3
Vorgaben für den Betrieb .....	4
Antwortzeit .....	4
Vorgaben zur Netzwerkkommunikation .....	4
Vorgaben zu Clients .....	4
Allgemeine Vorgaben für Clients .....	4
Vorgaben zum Datenaustausch .....	4
Verfahren für den Austausch von Dateien .....	4
Vorgaben zur Datenhaltung .....	5
Gebot zentraler Datenhaltung .....	5
Vorgaben zum Datenschutz .....	5
Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag .....	5
Keine Datenübermittlung an Dritte .....	5
Vorgaben zur Ergonomie .....	5
Barrierefreiheit für interne Anwendungen .....	5
Vorgaben zur Verfügbarkeit .....	6
Basisanforderungen zur Verfügbarkeit .....	6
Erweiterte Anforderungen an die Verfügbarkeit .....	<b>Fehler! Textmarke nicht definiert.</b>
Vorgaben zu Webclients .....	6
Lauffähigkeit auf aktuellen Browsern .....	6
Vorgaben für Webclients (allgemein) .....	6

## Allgemeine Vorgaben zu Anwendungen

### Integrationsfähigkeit in Portale und Workflows

Alle Funktionen der Anwendung müssen über eine API und/oder eine URL aufrufbar sein. Eine API soll als REST-API mit der Unterstützung von standardisierten Sicherheitsmechanismen zur Autorisierung ausgestaltet sein. Ein Aufruf per URL soll über Standardbrowser mit standardisierten Sicherheitsmechanismen möglich sein. Die API soll klar und eindeutig nach OpenAPI Standard dokumentiert sein.

**Datenimport über SCIM:** Es muss die Möglichkeit bestehen, Benutzerinformationen über das SCIM-Protokoll (System for Cross-domain Identity Management) zu importieren. Dies umfasst die Unterstützung von Standard-SCIM-Operationen, um einen effizienten und automatisierten Austausch von Benutzerdaten zu gewährleisten. Besonders wichtig ist, dass bei diesem Import auch die Gruppenzugehörigkeiten der Benutzer berücksichtigt werden, um eine korrekte Zuweisung von Berechtigungen und Rollen innerhalb der Software zu gewährleisten.

## Qualitätssicherung

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

- Tests inkl. Dokumentation der Testfälle und -ergebnisse
- Überprüfen von Qualitätsstandards
- Change-Management inkl. Freigabeverfahren
- Problem-Management inkl. Lösungen und Maßnahmen zur künftigen Prävention

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

## Vorgaben zu Apps

### Zugekaufte Apps - allgemeine Vorgaben

#### *Stores*

Apps sind über die Standard-App-Stores der Plattformen Android und iOS verfügbar. Sie entsprechen den dort geltenden Richtlinien. Sie werden nach Absprache mit der TK über den Store-Account des APP-Anbieters oder den store-Acount der TK veröffentlicht.

#### *Berechtigungen*

Es wird dem Kunden explizit erläutert, wozu eine 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.

#### *Unterstützte Versionen*

Apps unterstützen alle Betriebssystemversionen der jeweiligen Plattform (iOS und Android) für einen Zeitraum von mindestens 36 Monaten ab deren Veröffentlichung. Apps sollen stets auch mit den Beta-Versionen der Betriebssysteme getestet werden.

#### *Verwendete Fremdbibliotheken*

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

Sicherheitsupdates für externe Bibliotheken und Frameworks müssen zeitnah integriert und die neuen App-Versionen über die Stores veröffentlicht werden.

Fremdbibliotheken müssen datensparsam konfiguriert werden.

#### *Bedienkonzept*

Apps sind intuitiv bedienbar und folgen dabei dem Bedienkonzept der jeweiligen Plattform.

#### *Aktualisierung*

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

#### *Einverständniserklärung*

Es wird dem Kunden 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 des Kunden dazu wird eingeholt. Der Nutzer kann den Datenverwendungen, die nicht für die Kernfunktionalität der App notwendig sind, widersprechen. In diesem Fall steht die Kernfunktionalität trotzdem zur Verfügung.

#### *Zusätzlicher Zugangsschutz bei sensiblen Daten*

Wenn die App den Zugang zu sensiblen Daten ermöglicht, muss vom Nutzer ein zusätzlicher App-spezifischer Zugangsschutz eingerichtet werden können (z. B. biometrische Merkmale, Hardwaretoken oder Kennwort).

### *Kommunikation*

Daten werden nur über TLS transportiert, die jeweiligen Empfehlungen der Plattform wie „Apple App Transport Security“ oder OkHttp.RESTRICTED\_TLS müssen genutzt werden.

### *Lokale Speicherung von Daten*

Sensible Daten dürfen nur sicher verschlüsselt lokal gespeichert werden.

### *Benachrichtigungen*

Benachrichtigungen durch die App sollen abschaltbar sein.

### *Datenverbrauch*

Die App geht mit dem Datenvolumen des Kunden sparsam um. Aus Sicht des Kunden muss der Verbrauch des Datenvolumens dem Zweck angemessen sein.

### *Stromverbrauch*

Die App geht mit dem Akkuvolumen des Kunden sparsam um. Aus Sicht des Kunden muss der Stromverbrauch dem Zweck angemessen sein.

## Vorgaben für den Betrieb

### Antwortzeit

Die Anwendung muss 95% aller Anfragen in weniger als 2 Sekunden beantworten.

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

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

Die Performancedaten (Antwortzeit, Durchsatz, Fehleranzahl) aller wesentlichen Funktionen/Transaktionen der Anwendung sollen in ein Berichtswesen auf Basis Grafana / InfluxDB integriert werden können, deshalb müssen entsprechende Metriken seitens der Anwendung über offene Schnittstellen bereitgestellt werden können.

### Vorgaben zur Netzwerkkommunikation

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

Das Produkt muss in Netzwerken, in denen IPv4-Netzwerk-Adress-Translation eingesetzt wird, integrierbar sein.

Die Netzwerk-Kommunikation des Produktes muss zwischen per Firewallsystemen getrennten Netzwerkbereichen möglich sein.

## Vorgaben zu Clients

### Allgemeine Vorgaben für Clients

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

Eine clientseitige Validierung von Eingaben (z. B. mit JavaScript ) darf nur ergänzend zu einer serverseitigen Validierung vorgenommen werden.

## Vorgaben zum Datenaustausch

### Verfahren für den Austausch von Dateien

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

- manueller Austausch über Cryptshare (<https://webft.tk.de>)
- Austausch über fest definierte S-FTP bzw. FTP-S Server bei externen Partnern.

Für Datentransfers von und zur TK müssen die unterstützten Verfahren genutzt werden.

Im Falle von Austauschverfahren für den Datenaustausch soll als Transportverschlüsselung eines der Protokolle S-FTP oder FTP-S zum Einsatz kommen.

Das gewählte Verfahren ist zwischen TK und AN zu vereinbaren und vom AN zu beschreiben.

Der Austausch von Daten zwischen dem AN und der TK muss über sichere Protokolle (z.B. S-FTP oder gleichwertig) erfolgen, sofern es sich um personenbeziehbare und/oder sensible Daten handelt.

Für den sicheren Ad-hoc-Datenaustausch muss die durch die TK bereitgestellte Plattform cryptshare genutzt werden.

Alternativ kann die Übertragung von sensiblen Daten auch per S/MIME-verschlüsselter Mail oder über einen sicheren und mit der TK abgestimmten Dienst erfolgen.

Bei Verwendung von S-FTP bzw. FTP-S muss der Auftragnehmer den entsprechenden Server bereitstellen und betreiben.

Wenn ein Datenaustausch regelmäßig vorgesehen ist und eine automatisierte Verarbeitung erfolgen soll, sollen zur Integritäts- und Vollständigkeitskontrolle geeignete Verfahren vom AN unterstützt und eingerichtet werden.

## Vorgaben zur Datenhaltung

### Gebot zentraler Datenhaltung

Die Anwendung soll Daten zentral speichern. Eine dezentrale Speicherung auf Endgeräten soll nicht erfolgen. Sofern es eine Herstellerempfehlung gibt, Daten aus Performancegründen dezentral vorzuhalten, so müssen geeignete Verfahren zur Datensicherung und zum Schutz der Daten angegeben werden.

## Vorgaben zum Datenschutz

### Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag

Der Anbieter darf keine im Rahmen des Hostings gesammelten Daten an Dritte weitergeben oder diese ohne Auftrag auswerten.

### 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 interne Anwendungen

Das User Interface muss barrierefrei sein. Es muss mindestens unterstützen:

- 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 Verfügbarkeit

### Basisanforderungen zur Verfügbarkeit

Der AN hat die von ihm bereitgestellten Dienste und Anwendungen in einer hochverfügbaren Architektur bereitzustellen. Die geforderte Serviceverfügbarkeit sowie die einzuhaltenden Betriebs- und Servicezeiten ergeben sich aus dem vertraglichen Anhang „EVB-IT Cloud-AGB“ in der jeweils vereinbarten Fassung und sind vom AN technisch sicherzustellen.

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, muss der AN die TK mit einem Vorlauf von einer Woche informieren. Dies kann schriftlich oder per E-Mail an den vereinbarten Ansprechpartner der TK erfolgen.

Der AN richtet seine Backup- und Recovery-Verfahren so ein, dass nach einer Störung der Dienst innerhalb von 48h wieder zur Verfügung steht. In jedem Fall darf nach einem Wiederanlauf nur ein Datenverlust des Transaktionsvolumens von maximal 10min auftreten.

Der AN muss das Operating der TK nach Feststellung eines Fehlers und bei Beeinträchtigung des Dienstes unverzüglich per Telefon oder E-Mail informieren. 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 Operating der TK.

Die maximale Ausfallzeit - auch bei Hardware-Defekten - beträgt 48h

## Vorgaben zu Webclients

### Lauffähigkeit auf aktuellen Browsern

Die vom AN bereitgestellte Anwendung bzw. die bereitgestellten Internetseiten müssen von folgenden Browsern vollständig und korrekt dargestellt werden:

- Chrome, Firefox, Edge, Safari: es sind alle Versionen zu unterstützen, deren Nutzung 5% in Deutschland in Bezug auf den jeweiligen Browser überschreitet

Die Anwendung bzw. die Internetseiten sind vom AN fortlaufend mit den zu unterstützenden Browsern zu testen.

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 Fax oder Brief an. Der AN muss die Unterstützung der in der aktualisierten Liste genannten Browser binnen vier Wochen sicherstellen, 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:

- Andere clientseitige Scriptsprachen als JavaScript sind in keinem Fall zu verwenden.
- Framesets dürfen nicht eingesetzt werden.
- 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 müssen entsprechend der aktuellen W3C-Konvention syntaktisch richtig sein.
- Flash-Animationen und andere Plugins dürfen nicht eingesetzt werden.

Die Anwendung muss die Kommunikation mit einem WEB-Proxy grundsätzlich unterstützen. Darüber hinaus entsprechen die verwendeten Technologien und Protokolle den üblichen Internetstandards gemäß Request for Comments (RFC).