

IT-Vorgaben

Stand: 07-2026

Inhalt

IT-Vorgaben.....	1
Vorgaben für den Betrieb	2
Antwortzeit.....	2
Herstellersupport	2
Vorgaben zu Clients	3
Allgemeine Vorgaben für Clients.....	3
Vorgaben zum Datenschutz	3
Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag	3
Keine Datenübermittlung an Dritte.....	3
Vorgaben zur Ergonomie.....	3
Barrierefreiheit für interne Anwendungen.....	3
Vorgaben zur IT-Sicherheit.....	3
Eindeutige Authentifizierung	3
Identity und Access Management	3
Meldung von Sicherheitsvorfällen	4
Nutzung von Cookies in Webanwendungen.....	4
Vorgaben für öffentlich erreichbare Webanwendungen.....	4
Vorgaben zur Verfügbarkeit.....	4
Basisanforderungen zur Verfügbarkeit.....	4
Erweiterte Anforderungen an die Verfügbarkeit	5
Vorgaben zu Webclients	5
Lauffähigkeit auf aktuellen Browsern	5
Vorgaben für Webclients (allgemein)	6
Anforderung an APIs und API-Dokumentation.....	6
Standardkonforme Schnittstellen	6
Bereitgestellte Informationen je Asset.....	6
API-Dokumentation (Umfang und Form).....	7

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.

Herstellersupport

Der AN hat Support mit garantierten Responsetimes zu leisten.

Die Responsetime in dem Fall, dass die Anwendung nicht zur Verfügung steht, beträgt weniger als 8 Stunden im Zeitraum von Montag bis Sonntag, von 0:00 bis 24:00 Uhr.

Tickets, die beim AN zur Bearbeitung liegen, sollen durch zuständige TK-Mitarbeiter einsehbar 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 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 IT-Sicherheit

Eindeutige Authentifizierung

Die Anwendung muss Verfahren für die eindeutige Authentifizierung von Anwendenden besitzen.

Identity und Access Management

Es muss das Microsoft Active Directory oder AzureAD bei der Anmeldung unterstützt werden.

Die Anwendung muss in ein Single Sign On bei der TK integriert werden können.

Zur Authentifizierung soll mindestens eines der folgenden Protokolle unterstützt werden:

- Kerberos

- SAML über Azure AD Enterprise Application (siehe <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management>)
- OAuth2 über Azure AD Enterprise Application (siehe <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management>)

Die Anwendung muss über ein für den Anwendungszweck geeignetes Rollen- und Rechte-Management verfügen, welches sicherstellt, dass auf personenbezogene Daten nur von denjenigen Mitarbeitern zugegriffen werden kann, die den Zugriff für die Erfüllung ihrer Aufgaben benötigen.

Meldung von Sicherheitsvorfällen

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

Nutzung von Cookies in Webanwendungen

Attribute und Präfixe müssen entsprechend der Kritikalität der Daten, welche in dem jeweiligen Cookie verarbeitet werden, angemessen gesetzt sein. Die Lifetime von Cookies muss -dem Anwendungszweck entsprechend- möglichst kurz sein. Cookies sollen nicht für die Speicherung von Daten verwendet werden, welche nur auf Clientseite verarbeitet werden. Stattdessen sollen -sofern im Client verfügbar- die dafür vorgesehenen APIs (z.B. Web Storage API) verwendet werden.

Für Cookies, welche für serverseitiges Tracking von Login-Sessions verwendet werden, gelten folgende detaillierte Anforderungen:

- Das Attribut "Expires" darf nicht gesetzt sein.
- Die Attribute "Secure" und "HttpOnly" müssen gesetzt sein.
- Das Attribut "SameSite" soll auf den Wert "Strict" gesetzt sein.
- Das Attribut "Domain" soll nicht gesetzt sein.
- Das Präfix des Cookies soll "__Host-" sein.
- Das Cookie muss bei jedem Authentisierungsvorgang neu gesetzt werden.
- Das Cookie muss bei Logout serverseitig invalidiert werden.

Vorgaben für öffentlich erreichbare Webanwendungen

Eine Anwendungssitzung muss nach maximal 30 Minuten Inaktivität serverseitig beendet werden.

Der Auftragnehmer darf keine 3rd Party Cookies im Browser des Kunden setzen.

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

Die Erstellung von Profilen und die Auswertung des Surfverhaltens der User durch den Auftragnehmer (Tracking/Webanalytics) darf nicht erfolgen. Ggf. wird die TK eine Auswertung des Surfverhaltens vornehmen wollen. In diesem Fall muss das Tag Management System der TK durch den AN eingebunden werden, auch wenn dieser keinen externen JavaScript Code verwendet. In diesem Fall muss auch das Consent Management der TK verwendet werden.

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 Sonntag, von 0:00 bis 24:00 Uhr verfügbar sein. Ihre durchschnittliche Verfügbarkeit im Jahr muss mindestens 99,7 % innerhalb der vereinbarten Betriebszeiten betragen.

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 8 Stunden wieder zur Verfügung steht. In jedem Fall darf nach einem Wiederanlauf nur ein Datenverlust des Transaktionsvolumens von maximal 4 Stunden 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 EMail an das Operating der TK.

Die maximale Ausfallzeit - auch bei Hardware-Defekten – beträgt 8 Stunden.

Erweiterte Anforderungen an die Verfügbarkeit

Für die Überprüfung der Einhaltung des Service Level Agreements (SLA) hinsichtlich der Transaktionszeiten soll der AN der TK mind. eine entsprechende offene Schnittstelle (API) bieten, 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 Performance Metriken zu den ausgeführten Transaktionen.
- Die Anwendung bzw. eine eigene Monitoring-Agentenkomponente 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 Performance Metriken der Anwendung aktiv auszulesen.

Zur Überprüfung der Erreichbarkeit des Service soll der AN einen Referenzdienst bereitstellen. 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 TK 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 AN soll nachweisen, dass er ein funktionierendes Business Continuity Management bei sich etabliert hat und soll der TK gegenüber diesbezüglichen Tests nachweisen.

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. 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.
- 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).

Anforderung an APIs und API-Dokumentation

Standardkonforme Schnittstellen

- Das DAM stellt vollständig dokumentierte, standardkonforme REST- und/oder GraphQL-APIs zur Verfügung, über die sämtliche Medienobjekte (Assets) sowie deren Metadaten automatisiert abgerufen und verarbeitet werden können.
- Die APIs sind so ausgelegt, dass ein performanter und skalierbarer Zugriff durch Drittsysteme (insbesondere CMS-, Frontend- und Streaming-Integrationen) gewährleistet ist.

Bereitgestellte Informationen je Asset

Über die API sind für jedes Asset mindestens folgende Informationen bereitzustellen:

- eine eindeutige Asset-ID,
- der Medientyp (z. B. Bild, Audio, Video),
- sämtliche zugehörigen Metadaten gemäß dem im System verwendeten Datenmodell,
- Verweise auf inhaltlich verbundene Assets, insbesondere auf:
 - Untertitel,
 - Audiodeskriptionen,
 - Posterframes bzw. Vorschaubilder.

Darüber hinaus müssen für alle zur Ausspielung vorgesehenen Medien über die API Streaming-URLs (z. B. HLS, MPEG-DASH) abrufbar sein.

API-Dokumentation (Umfang und Form)

- Die API-Dokumentation ist vollständig, konsistent und technisch detailliert bereitzustellen.
- Sie umfasst insbesondere:
 - eine Beschreibung des Datenmodells (inkl. Felddefinitionen und Datentypen),
 - eine Auflistung und Beschreibung sämtlicher Endpunkte bzw. Schemata,
 - Informationen zu Authentifizierungs- und Autorisierungsverfahren (z. B. OAuth2, tokenbasierte Verfahren),
 - Beispiele für typische Anwendungsfälle (Request-/Response-Beispiele).
- Die Dokumentation ist in einer für Entwickler gängigen Form bereitzustellen (z. B. OpenAPI-/Swagger-Definition, HTML- oder Markdown-Dokumentation) und fortlaufend aktuell zu halten. Sollte es diesbezüglich Änderungen geben, sind diese vorab mit der TK abzustimmen.