

BPM-Software

26-09021

Inhalt

BPM-Software.....	1
Allgemeine Vorgaben zu Anwendungen.....	2
Integrationsfähigkeit in Portale und Workflows.....	2
Qualitätssicherung.....	2
Vorgaben für den Betrieb.....	3
Antwortzeit.....	3
Vorgaben zu Backup & Recovery.....	3
Vorgaben zur Netzwirkommunikation.....	3
Vorgaben zu Clients.....	3
Allgemeine Vorgaben für Clients.....	3
Vorgaben zum Datenaustausch.....	3
Verfahren für den Austausch von Dateien.....	3
Vorgaben zum Datenschutz.....	3
Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag.....	3
Keine Datenübermittlung an Dritte.....	4
Vorgaben zur Ergonomie.....	4
Barrierefreiheit für interne Anwendungen.....	4
Nutzung von Cookies in Webanwendungen.....	4
Patch- und Release-Management (allgemeine Vorgaben).....	4
Überprüfung von Eingaben.....	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

Allgemeine Vorgaben zu Anwendungen

Integrationsfähigkeit in Portale und Workflows

Alle Funktionen der Anwendung sind über eine API und/oder eine URL aufrufbar.

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 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.

Vorgaben zu Backup & Recovery

Die Anwendung besitzt die Fähigkeit zu Backup & Recovery.

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.

Vorgaben zum Datenaustausch

Verfahren für den Austausch von Dateien

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

- Austausch über fest definierte S-FTP bzw. FTP-S Server bei externen Partnern
- S/MIME-gesicherte E-Mails
- 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.

Bei Verwendung von S-FTP bzw. FTP-S stellt der Auftragnehmer den entsprechenden Server bereit und betreibt diesen.

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 interne Anwendungen

Das User Interface ist barrierefrei. Es unterstützt mindestens:

- 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).

Nutzung von Cookies in Webanwendungen

Cookies, 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 Anwendung wird 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.

Sofern Anwendungskomponenten auf Windows-Clientsystemen vorgesehen sind, unterstützen diese neue Windows-Funktionsupdates innerhalb von 6 Monaten nach genereller Verfügbarkeit.

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

Überprüfung von Eingaben

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

Vorgaben zur Verfügbarkeit

Basisanforderungen zur Verfügbarkeit

Der AN legt die von ihm bereitgestellten Dienste und Anwendungen hochverfügbar aus. Die geforderte Verfügbarkeit ergibt sich aus Nr. 9.6 des Vertrags sowie Ziffer 8.3 der EVB-IT Cloud-AGB. Ergänzend gilt:

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

Störungen sind zu beseitigen. Es gelten die Service-, Reaktions- und Wiederherstellungszeiten aus Nr. 9.6 des Vertrags.

Nach einem Wiederanlauf darf nur ein Datenverlust des Transaktionsvolumens von maximal 12 Stunden 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.

Erweiterte Anforderungen an die Verfügbarkeit

Für die Überprüfung der Einhaltung des Service Level Agreements (SLA) hinsichtlich der Transaktionszeiten stellt der AN der TK 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 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 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 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 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.