

Inhalt

1.	Einleitung .....	2
2.	Allgemeine Vorgaben zu Anwendungen .....	2
2.1.	Qualitätssicherung .....	2
3.	Vorgaben für den Betrieb .....	2
3.1.	Antwortzeit .....	2
3.2.	Plattform-Konformität .....	2
3.3.	Vorgaben zur Netzwirkkommunikation .....	2
4.	Vorgaben zu Clients .....	2
4.1.	Allgemeine Vorgaben für Clients .....	2
5.	Vorgaben zum Datenschutz .....	3
5.1.	Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag .....	3
5.2.	Keine Datenübermittlung an Dritte .....	3
6.	Vorgaben zur Ergonomie .....	3
6.1.	Barrierefreiheit für interne Anwendungen .....	3
7.	Vorgaben zur IT-Sicherheit .....	3
7.1.	Eindeutige Authentifizierung .....	3
7.2.	Freiheit von Schadsoftware .....	3
7.3.	Hosting - Administrationsrechte und Funktionstrennung .....	3
7.4.	Hosting - Sicherheitsmaßnahmen .....	3
7.5.	Hosting nur mit Sicherheitskonzepten .....	4
7.6.	Identity und Access Management .....	4
7.7.	Meldung von Sicherheitsvorfällen .....	4
7.8.	Nutzung von Cookies in Webanwendungen .....	4
7.9.	Patch Management Prozess bei gehosteten Anwendungen .....	5
7.10.	Prüfrechte der TK .....	5
7.11.	Transport Layer Security (TLS) .....	5
7.12.	Transportverschlüsselung nicht-öffentlicher Daten .....	5
7.13.	Überprüfung von Eingaben .....	5
7.14.	Vorgaben für öffentlich erreichbare Webanwendungen .....	5
7.15.	Vorgaben zur Datenlöschung .....	5
7.16.	Wahl von Verschlüsselungsverfahren und Cipher-Suites .....	6
7.17.	Sicherheitsrelevante Zufallswerte .....	6
8.	Vorgaben zur Verfügbarkeit .....	6
8.1.	Basisanforderungen zur Verfügbarkeit .....	6
9.	Vorgaben zu Webclients .....	6
9.1.	Lauffähigkeit auf aktuellen Browsern .....	6
9.2.	Vorgaben für Webclients (allgemein) .....	7

## 1. Einleitung

Die Anforderungen aus dieser Vertragsanlage gelten für den tool-gestützten Services des AN, also das Terminplanungstool.

## 2. Allgemeine Vorgaben zu Anwendungen

### 2.1. 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

Bei festgestellten Mängeln kann die TK Nachbesserung verlangen.

## 3. Vorgaben für den Betrieb

### 3.1. 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.

### 3.2. Plattform-Konformität

Die Anwendung wird als Software as a Service ausgeliefert.

### 3.3. 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.

## 4. Vorgaben zu Clients

### 4.1. 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).

## 5. Vorgaben zum Datenschutz

### 5.1. 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.

### 5.2. 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.

## 6. Vorgaben zur Ergonomie

### 6.1. 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).

## 7. Vorgaben zur IT-Sicherheit

### 7.1. Eindeutige Authentifizierung

Die Anwendung besitzt Verfahren für die eindeutige Authentifizierung von Anwendenden. Bei Anwendungen, die sich an TK-Mitarbeitende richten, entsprechen die Benutzernamen dem bei der TK verwendeten Schema. Das Schema wird dem Auftragnehmer durch die TK auf Anforderung bereitgestellt.

### 7.2. Freiheit von Schadsoftware

Alle Bestandteile des Angebots sind frei von Schadsoftware (Viren, Würmer, Backdoors usw.). Der AN stellt dies durch geeignete Maßnahmen sicher. Der AN prüft insbesondere sämtliche ausgelieferte Software vor Auslieferung mittels marktgängiger und aktueller Scanner oder mindestens gleichwertiger Technologie.

### 7.3. Hosting - Administrationsrechte und Funktionstrennung

Der Auftragnehmer stellt für alle für die TK bereitgestellten IT-Komponenten (Server, Dienste und Anwendungen) sicher, dass seine Mitarbeiter - insbesondere Systemadministratoren - nur die für die jeweilige Aufgabenerfüllung notwendigen Rechte besitzen. Der Auftragnehmer setzt für kritische administrative Prozesse das Vier-Augen-Prinzip um.

### 7.4. Hosting - Sicherheitsmaßnahmen

Der AN ergreift geeignete technische und organisatorische Maßnahmen, die einen unbefugten und missbräuchlichen Zugriff auf die Anwendungen und/oder Internetseiten, zugehörige Komponenten sowie zugehörige Daten unterbinden. Dies gilt insbesondere für die Abwehr von Bedrohungen, die die Integrität, die Verfügbarkeit und die Vertraulichkeit der Anwendung bzw. des Internetauftritts gefährden oder eine Gefährdung (z.B. durch Exploits, Malicious Software) Dritter (z.B. Besucher eines Internetauftritts) darstellen. Die getroffenen Maßnahmen entsprechen dabei dem jeweils aktuell

gültigen Stand der Technik. Ferner vermeidet der AN bei der Erstellung und Pflege sowie beim Hosting generell Techniken, die bekanntermaßen hohe Sicherheitsrisiken bzw. Sicherheitslücken enthalten, welche nicht durch entsprechende flankierende Maßnahmen geschlossen werden können.

Sollten sich aufgrund neuer Erkenntnisse und Bedrohungen Lücken ergeben, so zeigt der AN diese unverzüglich der TK an und beseitigt diese durch geeignete Maßnahmen. Der AN schreibt die zugehörigen Sicherheitskonzepte fort und stellt sie der TK zur Prüfung zur Verfügung. Sofern die Maßnahmen die Verfügbarkeit der für die TK zur Verfügung gestellten Dienste beeinflussen, stimmt der AN diese mit der TK ab.

#### 7.5. Hosting nur mit Sicherheitskonzepten

Der AN dokumentiert alle von ihm ergriffenen Sicherheitsmaßnahmen in zugehörigen Sicherheitskonzepten. Vor der Produktivsetzung sowie bei wesentlichen Änderungen stellt der AN der TK die Sicherheitskonzepte zur Prüfung zur Verfügung. Die Konzepte adressieren mindestens folgende Punkte:

- Schutz vor Malware
- Systemhärtung
- Patch-Management-Prozess
- Verschlüsselung bei Datenübertragungen
- Lösungsverfahren
- Umgang mit Zugangsdaten und anderen sensiblen Informationen
- Rechtekonzept für Administratoren
- Umgang mit Sicherheitsvorfällen (insbesondere Erkennung, Meldung, Behebung)

#### 7.6. Identity und Access Management

Die Anwendung ist in ein Single Sign On bei der TK integrierbar. Es wird Entra ID bei der Anmeldung unterstützt.

Zur Authentifizierung wird mindestens eines der folgenden Protokolle unterstützt:

- OpenID/OAuth2 über Microsoft Entra ID Enterprise Application (siehe <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-application-management>)
- SAML über Microsoft Entra ID Enterprise Application (siehe <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-application-management>)

Die Anwendung verfügt über ein für den Anwendungszweck geeignetes Rollen- und Rechte-Management. Dieses stellt insbesondere sicher, dass:

- Die Rechte für administrative Tätigkeiten von den Rechten zur regulären Nutzung getrennt sind.
- Auf von der Anwendung verarbeitete Daten nur von denjenigen Mitarbeitern zugegriffen werden kann, die den Zugriff für die Erfüllung ihrer Aufgaben benötigen.

#### 7.7. Meldung von Sicherheitsvorfällen

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

#### 7.8. 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.

#### 7.9. Patch Management Prozess bei gehosteten Anwendungen

Der AN gewährleistet über einen Patch-Management-Prozess, dass alle von ihm eingesetzten Systeme, Systemkomponenten und Entwicklungswerkzeuge jeweils auf einem aktuellen Versionsstand und insbesondere frei von Schwachstellen sind. Der AN stellt sicher, dass je nach Risiko für die Anwendung (bewertet durch den AN) Sicherheitspatches - innerhalb von 1-18 Arbeitstagen nach Veröffentlichung des Patches eingespielt sind. Darüber sorgt der AN für eine angemessene Härtung der Systeme.

#### 7.10. Prüfrechte der TK

Die TK ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Die TK ist berechtigt, regelmäßig (mindestens monatlich, höchstens täglich) oder anlassbezogen (z.B. Bekanntwerden einer über das Netzwerk ausnutzbaren Schwachstelle oder Nachverfolgung von Härtungsmaßnahmen) nichtinvasive Prüfungen wie Portscans und Aufrufe der Webschnittstellen durchzuführen. Darüber hinaus hat die TK das Recht, die Sicherheit der beteiligten Systeme und Prozesse im Rahmen von Assessments zu überprüfen. Insbesondere stimmt der AN zu, dass die TK bzw. ein von ihr beauftragter Prüfer nach Vorankündigung eigene Penetrationstests durchführen darf.

#### 7.11. Transport Layer Security (TLS)

Der AN hält sich bei der Wahl von TLS-Version(en) und der eingesetzten Cipher-Suites an die Empfehlungen der jeweils aktuellen Fassung der Technischen Richtlinie BSI *TR-02102-2 "Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)"* des BSI. Der Auftragnehmer stellt sicher, dass alle Kommunikationsteilnehmer mindestens eine der zulässigen Cipher-Suites unterstützen. Der AN gleicht die von ihm gewählte Konfiguration mindestens jährlich gegen die Vorgaben des BSI ab. Bei Abweichungen passt der AN die Konfiguration an, um Konformität mit der o.a. Richtlinie herzustellen.

#### 7.12. Transportverschlüsselung nicht-öffentlicher Daten

Nicht-öffentliche Daten werden immer verschlüsselt übertragen.

#### 7.13. 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.

#### 7.14. Vorgaben für öffentlich erreichbare Webanwendungen

Eine Anwendungssitzung wird nach maximal 30 Minuten Inaktivität serverseitig beendet.

Die Anwendung setzt KEINE 3rd Party Cookies im Browser der Anwendenden.

Es werden keine Profile durch den AN erstellt. Das Surfverhalten der User (Tracking/Webanalytics) wird nicht ausgewertet.

#### 7.15. Vorgaben zur Datenlöschung bei Clouddiensten

Bei der Verwendung von SaaS werden Storage-Komponenten (die zur persistenten Speicherung von Daten verwendet werden) bei Außerbetriebnahme einer Appliance, des Services und bei der Beendigung des Vertrages gelöscht. Die Löschung einer Speicherkomponente entspricht einer physischen Vernichtung. Die Löschung aller virtuellen Ressourcen muss in einem Protokoll dokumentiert werden. Dieses Protokoll muss der TK zur Verfügung gestellt werden. Gelöschte Speicherressourcen dürfen nicht wiederherstellbar sein.

#### 7.16. Wahl von Verschlüsselungsverfahren und Cipher-Suites

Sofern in der Software Verschlüsselungsalgorithmen eingesetzt werden, sind diese zur aktuellen Fassung "BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen" konform. Sofern Verschlüsselungsalgorithmen im direkten Umfeld von qualifizierten elektronischen Signaturen nach dem bundesdeutschen Signaturgesetz eingesetzt werden, richten sie sich nach den Veröffentlichungen der Bundesnetzagentur im Bundesanzeiger. Verschlüsselungsverfahren werden vor Ablauf des laut der o.a. genannten Vorschriften zulässigen Verwendungsdatums durch aktuelle Verfahren ersetzt werden.

#### 7.17. Sicherheitsrelevante Zufallswerte

Sollen sicherheitsrelevante Zufallswerte (z.B. Session-IDs, kryptographisches Material, Initial-PINs) in einer Anwendung verwendet werden, so müssen diese hinreichend zufällig sein. Die dafür verwendeten Zufallsgeneratoren müssen den Vorgaben aus Kapitel "Zufallszahlengeneratoren" der aktuellen Technischen Richtlinie BSI TR-02102-1 des BSI entsprechen.

### 8. Vorgaben zur Verfügbarkeit

#### 8.1. Basisanforderungen zur Verfügbarkeit

Der AN legt die von ihm bereitgestellten Dienste und Anwendungen hochverfügbar aus. Sie müssen im Zeitraum werktags (Mo-Sa) 6 bis 22 Uhr verfügbar sein. **Ihre durchschnittliche Verfügbarkeit im Jahr beträgt mindestens 99,9 % innerhalb der vereinbarten Betriebszeiten.**

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

Der AN richtet seine eingesetzten IT-Kontinuitätslösungen so ein, dass nach einer Störung der Dienst innerhalb von 168 Stunden wieder zur Verfügung steht. In jedem Fall darf nach einem Wiederanlauf nur ein Datenverlust des Transaktionsvolumens von maximal 72 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.

Die maximale Ausfallzeit - auch bei Hardware-Defekten - beträgt 168 Stunden.

### 9. Vorgaben zu Webclients

#### 9.1. 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 wird die jeweils aktuelle sowie vorherige Major-Version unterstützt. 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.

### 9.2. 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.