

Nicht-funktionale Anforderungen an die Software

Tabelle A: Nicht-Funktionale Anforderungen an die Software				
Nr.	Bezeichnung/Inhalte			Anforderung
1	Übergreifende Anforderungen	1.1	Die Software muss eine integrierte Programmbeschreibung besitzen, welche online oder über das jeweilige Software-Modul zugänglich ist und alle wichtigen Programmfunktionen sowie theoretischen Grundlagen hinreichend genau beschreibt.	Muss
		1.2	Das Programm wird für die Verwendung in deutscher Sprache ausgeliefert.	Muss
		1.3	Die Ansprechpartner beim AN im Falle von technischen und fachlichen Problemen (2nd, 3rd level support) sind dokumentiert, vgl. ISO 20000	Muss
2	Virtualisierung	Für diese Ausschreibung nicht relevant		
3	Installation	Für diese Ausschreibung nicht relevant		
4	Lizenzierung			
		4.1	Eine eventuell notwendige Aktivierung kann mit dem Nutzerprofil zwischen mehreren VDI-Instanzen transferiert werden.	Muss
		4.2	Die Lizenzierung/Aktivierung einer einzelnen Installation ist nicht an echte oder emulierte Gerätekennungen gebunden.	Muss
		4.3	Die Nutzung/Aktivierung einer Lizenz ist ohne Verwendung eines physischen Tokens (z.B. USB- Dongle) möglich.	Muss
		4.4	Werden bei der Lizenzierung Drittanbieter Produkte eingesetzt, so müssen diese unterstützt werden und aktuell sein.	Muss
5	Technik / Architektur	5.1	Der Anbieter stellt sicher, dass im System innerhalb der Vertragslaufzeit nur aktuelle (Drittanbieter-) Komponenten/Dependencies/Runtimes eingesetzt werden, deren Produktsupport nicht abgelaufen (EOL) ist und die frei von bekannten Sicherheitslücken sind. Eine aktuelle Liste der Komponenten ist nach Vergabe einzureichen.	Muss

		5.2	Der AN liefert eine Dokumentation der benötigten Ablaufumgebung (nicht nur OS, RAM und CPU, sondern inkl. aller noch zu installierender Bibliotheken, die nicht im Software-Paket enthalten sind, eventuell benötigte offene Ports, Internet-Zugang, etc.).	Muss
		5.3	Die Schnittstellen zwischen der Applikation und den verbundenen Systemen sind mit den genutzten Protokollen dokumentiert. Im Kontextdiagramm ist an alle Schnittstellen das Protokoll, die genutzten Ports sowie die Verschlüsselung zu schreiben.	Muss
		5.4	Der AN dokumentiert, welche Bibliotheken und Applikationen Dritter (z.B. Open-Source) genutzt werden und welche Lizenzen für sie gelten.	Muss
		5.5	Der AN beschreibt die Mindest-Leistungsstandards, zu denen die Anwendung betrieben wird. Hierzu gehören Datendurchsatz, Verfügbarkeit, Reaktionszeiten des Systems Definition: Datendurchsatz: Der maximale Durchsatz an Daten, für den die Anwendung ausgelegt ist Verfügbarkeit: Die von den Parteien definierte und vom Betrieb abgesicherte Verfügbarkeit der Anwendung Reaktionszeiten: Die Zeit, die die Anwendung maximal benötigen darf, um Transaktionen zu verarbeiten	Muss
		5.6	Der AN zeigt auf, dass die Anwendung in die gegebenen Querschnittsfunktionen (SSO, Logging, Monitoring) integrierbar ist.	Muss
6	Unternehmensarchitektur	Für diese Ausschreibung nicht relevant		
7	Datenschutz	7.1	Wird im Rahmen der Leistungserbringung eine Künstliche Intelligenz (KI) gem. der Definition der KI-Verordnung eingesetzt? (Ja/Nein)	muss beantwortet werden
		7.2	Der Auftragnehmer liefert Informationen, ob die KI mit den Daten des AG trainiert wird. <i>Wenn ja, soll dieses Vorgehen nur nach der schriftlichen Freigabe des AG möglich sein.</i> Als separat gekennzeichnete Anlage ist nach Vergabe einzureichen.	Muss (muss beantwortet werden, wenn Nr. 7.1 mit „Ja“ beantwortet wurde)

		7.3	Der Auftragnehmer liefert Informationen, ob die KI eine automatisierte Entscheidung im Sinne des Art. 22 DSGVO durchführt. <i>Wenn ja, soll dieses Vorgehen nur nach der schriftlichen Freigabe des AG möglich sein.</i> Als separat gekennzeichnete Anlage ist nach Vergabe einzureichen.	Muss (muss beantwortet werden, wenn Nr. 7.1 mit „Ja“ beantwortet wurde)
		7.4	Der AN bestätigt und kann auf Anfrage des AG nachweisen, dass die Applikation den Anforderungen des Art. 25 DSGVO (Privacy by Default und Privacy by Design) entspricht.	Muss
		7.5	Die Applikation kann mit Blick auf Anzahl der Datenfelder/Attribute, Anzahl der Betroffenen und Nutzungsintensität auf das erforderliche Maß beschränkt (so wenig wie möglich) werden.	Muss
		7.7	Die Applikation ist in der Lage, die Erfüllung der Betroffenenrechte gem. Art. 12 ff DSGVO zu unterstützen: - Korrektur/Aktualisierung der Daten ist möglich bzw. sichergestellt - Löschung von Daten zu einzelnen Betroffenen ist möglich - Sperrung von Daten zu einer Person im Einzelfall ist möglich - Vollständige Kopie aller Daten zu einer Person ist erstellbar	Muss
		7.9	Der AN muss ein Löschkonzept für die in der Applikation verarbeiteten personenbezogenen Daten vorlegen. Personenbezogene Daten sind u.a. User-IDs, Kontaktdaten, etc. Für den DSGVO-konformen Betrieb der Applikation müssen diese bekannt sein und dann auch im Rahmen der technischen Möglichkeiten gelöscht werden, wenn der Verarbeitungsgrund entfallen ist. Als separat gekennzeichnete Anlage ist nach Vergabe einzureichen.	Muss
7.12	Sollte die Applikation Logfiles erzeugen können, so hat der AN darzulegen, welche Logfiles erzeugt und wie lange diese gespeichert werden können.	Muss		

		7.14	Erfolgt eine Drittstaatenübermittlung von personenbezogenen Daten, d.h. ein Datenexport in Drittländer (außerhalb der EU/EWR)? Ja/Nein Wenn ja: Anforderungen 7.15– 7.17 bearbeiten Wenn nein: weiter ab Anforderung 8.1.	(muss beantwortet werden)
		7.15	Bestätigen Sie, dass die Ausnahmeregelung gemäß Art. 49 DSGVO greift (Ja/Nein). Wenn ja: weiter ab Anforderung 7.17. Wenn nein: weiter ab Anforderung 7.16.	(muss beantwortet werden, wenn Nr. 7.14 mit „Ja“ beantwortet wurde)
		7.16	Legen Sie dar, welche der nachfolgenden Übermittlungsinstrumente für die Drittstaatenübermittlung Anwendung finden: - Angemessenheitsbeschluss der EU-Kommission liegt vor - EU-Standarddatenschutzklauseln wurden geschlossen - Ein anderer Mechanismus zur Sicherstellung der Zulässigkeit des Exports wurde umgesetzt. Bitte angeben, welches der Instrumente Anwendung findet. Hier muss eine konkrete Darlegung erfolgen, welches Übermittlungsinstrument vorliegt.	Muss (muss beantwortet werden, wenn Nr. 7.15 mit „Nein“ beantwortet wurde)
		7.17	Legen Sie dar, welche personenbezogene Daten exportiert werden und zu welchem Zweck. Als separat gekennzeichnete Anlage in tabellarischer Form ist nach Vergabe einzureichen.	(muss beantwortet werden, wenn Nr. 7.14 mit „Ja“ beantwortet wurde)
8	IT-Sicherheit	8.1	Die Übertragung personenbezogener und anderer vertraulicher Daten erfolgt über geschützte Übertragungswege nach aktuellem Stand der Technik (z.B. https).	Muss
		8.2	Die Speicherung personenbezogener und anderer vertraulicher Daten erfolgt verschlüsselt nach aktuellem Stand der Technik (z.B. AES256).	Muss
		8.3	Komponenten und Dienste erhalten nur die minimal für die Anwendungsnutzung notwendigen Rechte (z.B. User Kontext und kein administrativer Laufwerkszugriff o.ä.).	Muss
		8.4	Die Software und ihre mitgelieferten Komponenten sind frei von Schadcode und Code, welcher den Anforderungen der	Muss

			Software nicht zweckdienlich ist oder gar der Sicherheit des Produkts entgegenwirkt.	
		8.5	Der AN hat nach Kenntnisnahme unverzüglich Informationen zu Sicherheitsproblemen dem AG zu melden und geeignete Lösungsvorschläge zu unterbreiten. Siehe Anforderung 8.7 und 8.8	Muss
		8.6	Der AN bestätigt die Authentizität der Anwendung und aller enthaltenen Komponenten mit geeigneten technischen Maßnahmen, wie z.B. signierten Executables. siehe Anforderung 3.7 Erläuterung: Das Ausführen von nicht signierten Dateien wird von den Systemen der Autobahn blockiert.	Muss
		8.7	Der AN dokumentiert, in welcher Form und nach welchem Zeitplan für seine Applikation bekannte Sicherheitsprobleme abgestellt werden und in welcher Form Sicherheitsupdates zur Verfügung gestellt werden.	Muss
		8.8	Die Aktualität und der Support der Software und der Komponenten sind während der gesamten Vertragslaufzeit durchgängig und umfassend zu gewährleisten.	Muss
		Wenn Cloud Services oder eine Client-Server Architektur genutzt werden (auch optional) bitte 8.10 ff. bearbeiten.		
		8.9	Der Anbieter dokumentiert seine Strategien im Falle einer Disaster Recovery Situation	Muss
		8.10	Es muss eine starke Authentifizierung erfolgen.	Muss
		8.11	Als Authentifizierungsprotokoll wird OIDC oder SAML genutzt.	Muss
		8.12	Die Useranlage und Löschung erfolgt automatisiert mittels SCIM bzw. einem API der Applikation.	Muss
		8.13	Wenn entsprechende Protokolldaten erzeugt werden, müssen die Logdaten in einen zentralen Logservice übergeben werden können.	Muss
		8.14	Sofern differenzierte Berechtigungen in der angebotenen Software existieren, müssen diese nach dem Prinzip der least privilege und segregation of duties implementiert sein.	Muss
		8.15	Die Anwendung muss vollständig über eine Cloud aufrufbar sein (Desktop)	Muss

		8.16	Der Zugriff auf die Daten muss sowohl von innerhalb der Autobahn, als auch von Extern unterstützt werden	Muss
9	Barriere-freiheit			
		9.2	Der Anbieter muss die Autobahn GmbH des Bundes über bekannte Einschränkungen bei der Barrierefreiheit informieren.	Muss