Anhang 1: Katalog TS Los 2

Wichtige Bemerkungen zur Bearbeitung des Anforderungskataloges
An den vorgegebenen Zeilen und Spalten wie auch den Inhalten in den Spalten «Nr», «Beschreibung» und «Form des Nachweises» werden keine Veränderungen oder Anpassungen akzeptiert.
Die Anbieterin hat ihre Taxierungen oder Dokumentationen in den grün eingefärbten Zellen aufzuführen.
In der Spalte "Angaben der Anbieterin" hat diese darzulegen respektive mit entsprechenden Unterlagen und Ausführungen die Erfüllung der einzelnen Punkte zu dokumentieren. Verweise auf allfällige Anhänge sind erlaubt, müssen jedoch sehr präzise und nachvollziehbar auf die relevanten Textstellen im Angebot oder entsprechenden Anhänge referenzieren.

Name Anbieterfirma	

Nr.	**Beschreibung**	**Form des Nachweises**	**Angaben der Anbieterin**
Infrastruktur			
L2-TS01	**Plattform-as-a-Service (PaaS)** Die Anbieterin stellt eine gemanagte private Cloud (inkl. Backup) bereit, auf der die Plattform Justitia.Swiss mit allen benötigten Umgebungen für die CI/CD betrieben werden. Die Cloud Umgebung stellt den Containern Infrastrukturfunktionalität und Integrationsmöglichkeiten via deklarativen APIs zur Verfügung. In einer gemanagten private Cloud werden sämtliche Aspekte der Bereitstellung der Cloud Umgebung durch die Anbieterin gemacht. Der Applikationsserver, die Datenbank und Storage werden ausschliesslich für Justitia.Swiss	1) Schriftliche Bestätigung, dass diese Anforderung so erfüllt werden kann und dass die Kosten im Preisangebot berücksichtigt sind. 2) Dokumentation der jeweiligenen Dimensionen der jeweiligen Umgebungen (Entwicklung, Integration, Schulung und Produktion) je Projektphase sowie im Regelbetrieb. 3) Schriftliche Bestätigung, dass die vorgesehenen Dimensionen genügend gross sind, damit eine effiziente Projektumsetzung und Arbeitsweise	

Nr.	Beschreibung	Form des Nachweises	Angaben der Anbieterin
	bereitgestellt und genutzt. Die Produktionsumgebung ist von den restlichen Umgebungen getrennt (siehe Anhang 8, MT 9).	ermöglicht wird und darin sämtliche Vorgaben gemäss Pflichtenheft berücksichtigt sind.	
L2-TS02	**Verwendung von Cloud Native Technologien** Die Private Cloud wird mit cloud native Technologien realisiert. Die zugrundeliegenden Techniken ermöglichen die Umsetzung von entkoppelten Systemen, die belastbar, handhabbar und beobachtbar sind. Die Technologien basieren auf ein Ökosystem von open-source und herstellerneutralen Projekten. Kombiniert mit einer robusten Automatisierung können Softwareentwickler mit geringem Aufwand flexibel und schnell auf Änderungen reagieren (siehe CNCF Cloud Native Definition v1.0; https://github.com/cncf/toc/blob/main/DEFINITION.md).	Dokumentation des verwendeten Technologie Stacks, woraus die Erfüllung dieser Spezifikation/Vorgabe klar erkennbar ist.	
L2-TS03	**Bearbeitung von Daten** Die Bearbeitung von Daten muss in der Schweiz gemäss Schweizer Recht erfolgen. Ein Zugriff ausländischer Behörden auf die Daten aufgrund entsprechender rechtlicher Anknüpfungen der Anbieterin zu ausländischen Rechtsordnungen muss ausgeschlossen werden können. Siehe dazu auch die Bestimmungen des Rahmenvertrages.	Schriftliche Bestätigung und Dokumentation, wie sichergestellt wird, dass - die Daten nur in der Schweiz nach Schweizer Recht bearbeitet werden und - ein fremdstaatlicher Zugriff verhindert wird.	
L2-TS04	**Skalierung der Infrastruktur** Die gesamte IT-Infrastruktur (über alle Ebenen) kann bezüglich Datenvolumen, Durchsatz und Perfomance skalieren. Die dazu nötigen Technologien und Skalierungskonzepte sind vorhanden.	Schriftliche Bestätigung und Dokumentation der entsprechenden Technologien und Skalierungskonzepte.	

Nr.	Beschreibung	Form des Nachweises	Angaben der Anbieterin
L2-TS05	**Unterstützte Protokolle Justitia.Swiss** Die Plattform wird ein- und ausgehende Schnittstellen über APIs verwenden. Die detaillierten Protokolle werden im Lauf des Projekts festgelegt. Die Architektur muss jedoch von Beginn an darauf ausgelegt werden, dass grosse Dateien (grösser als 8.5 GB) übermittelt und gestreamet werden können.	Schriftliche Bestätigung sowie zusätzliche Bestätigung, dass die Streaming Protokolle in Absprache mit der Entwicklerin (Zuschlagsempfängerin Los 1) später realisiert werden.	
L2-TS06	**Service Management Tool** Die Anbieterin stellt für den Betrieb ein mandantenfähiges, professionelles Service Management Tool zur Verfügung, welches das providerübergreifende Management der Service Prozesse inklusive Test-Prozesse unterstützt und eine mehrsprachige (D, F, I, EN), barrierenfreie Benutzeroberfläche enthält. Die Ansichten im Ticketing Tool müssen auf unterschiedlich grossen Endgeräten angezeigt werden können.	Schriftliche Bestätigung und kurze Dokumentation des einzusetzenden Service Management Tools, woraus die Abdeckung der hier aufgeführten Vorgaben erkennbar sind.	
IT-Sicherheit und Betrieb			
L2-TS07	**Föderierte Identitäten** Die Infrastruktur der Anbieterin muss die Anbindung an verschiedene Identitätsprovider erlauben. Es müssen dazu die Standardprotokolle OpenIdConnect/OAuth 2.0 und SAML unterstützt werden.	Schriftliche Bestätigung.	
L2-TS08	**Etablierung und Betrieb von Security Prozessen** Die Anbieterin hat standardisierte Security Prozesse für technische Komponenten etabliert. Die Anbieterin betreibt über die gesamte Vertragslaufzeit mittels eines Security Operations Center (SOC) ein Security Information and Event Management (SIEM).	Schriftliche Bestätigung, dass die Anbieterin ein SIEM aufbaut und dessen Betrieb über die gesamte Vertragsdauer sicherstellt und alle daraus entstehenden Kosten (inkl. allfälliger Kosten für dabei einzusetzende Softwareprodukte) im Rahmen ihrer Preiseingabe bei GL01 resp. OP01 berücksichtigt sind. Dabei ist auch	

Nr.	Beschreibung	Form des Nachweises	Angaben der Anbieterin
	Die Anbieterin pflegt eine Liste von (Cloud-) Security Policies und zeigt die Einhaltung dieser Policies auf.	die laufende Weiterentwicklung zur adäquaten Behandlung von neuen Risiken inkludiert. Dokumentation der initialen Baseline der Security Policies.	
L2-TS09	**Sicherer Administrationszugang** Sämtliche Zugänge zu Daten und Systemen aus Supportprozessen müssen aufgezeichnet werden. Dies betrifft insbesondere: - Zugänge der Entwickung für Fehleranalyse - Lesen von Log/Debug Informationen - Änderung am Log Level - Zugang zu gespeicherten Daten Ein Berechtigungskonzept ist vorhanden, welches die Paradigmen von Least-Privilege und Segregation of Duty aller Beteiligter für Zugriff auf Daten und Systeme regelt. Zugriffe auf Produktivsysteme sind zeitlich beschränkt und nur im Supportfall möglich.	Schriftliche Bestätigung und Dokumentation des entsprechenden Berechtigungskonzepts.	
L2-TS10	**Verschlüsselung sämtlicher Kommunikation** Die Kommunikation übers Netzwerk muss in verschlüsselter Form erfolgen, gemäss dem aktuellen Stand der Technik.	Schriftliche Bestätigung und nachvollziehbare Dokumentation der Sicherheitsarchitektur in Bezug auf Datentransportverschlüsselung.	
L2-TS11	**Verschlüsselung der Daten at Rest** Aktenstücke und Dateien der Eingaben werden nur verschlüsselt abgespeichert.	Schriftliche Bestätigung	
L2-TS12	**Katastrophenvorsorge** Die Plattform soll auch im physischen und logischen Katastrophenfall rasch wieder verfügbar gemacht werden (siehe Anforderungen W1 Service Level Agreement im Anhang 6) können. Die beiden Rechenzentren dürfen nicht in der	Schriftliche Bestätigung sowie Nachweis der Standorte der Datacenters (für Primär- und Sekundärbetrieb) sowie der Standorte der Backups.	

Nr.	Beschreibung	Form des Nachweises	Angaben der Anbieterin
	gleichen Gefährdungszone (insbesondere durch Hochwasser und Erdbeben) liegen. Sie müssen sich in verschiedenen Geländekammern befinden.		
L2-TS13	**Monitoring der Services** Die Verfügbarkeit und Perfomance der Services wird in allen Umgebungen und auf allen Ebenen umfassend (d.h. vom Business Service bis zur Netzauslastung) überwacht und (visuell) rapportiert. Die technischen Logeinträge und der Audit Trail werden sicher aufbewahrt und für die Verwendung von (potentiellen) Sicherheitsvorfällen verwendet (SIEM).	Schriftliche Bestätigung und Dokumentation des verwendeten Monitoring, woraus die Abdeckung der hier aufgeführten Vorgaben erkennbar sind.	
L2-TS14	**Virenscan aller transferierten Dateien** Die Plattform Justitia.Swiss führt für alle transferierten Dateien einen Virenscan durch.	Schriftliche Bestätigung, dass der Betrieb des Virenscanners über die gesamte Laufzeit im Preis GL01 resp. OP01 inkludiert ist.	
Nachhaltigkeit			
L2-TS16	**Technologiemanagement** Sämtliche eingesetzte Technologieprodukte sind beherrschbar punkto Betrieb und kontinuierlicher Weiterentwicklung. Die Anbieterin stellt sicher, dass entsprechende Skills und entsprechendes Knowhow verfügbar sind. Die eingesetzten Technologien werden regelmässig (mind. vor jedem Release) gegen Vorgaben aus Security und Architektur (Baseline) geprüft. Sie sind in einem zentralen Monitoring eingebunden.	Schriftliche Bestätigung.	
L2-TS17	**Transparenz der Konfigurationen und Code-Artefakte**	Schriftliche Bestätigung.	

Nr.	Beschreibung	Form des Nachweises	Angaben der Anbieterin
	Sämtliche Code Artefakte und Konfiguration sind für den Auftraggeber einsehbar. Das Design und der geschäftsspezifische Source Code der Plattform sind öffentlich zugänglich. Nicht öffentlich zugänglich sind demgegenüber sicherheitsrelevante Einstellungen. Der Entscheid über den Umfang der Veröffentlichung liegt bei der Auftraggeberin.		
Vertrag /Bug Bounty Programm			
L2-TS18	**Bug Bounty-Programm** Die Anbieterin akzeptiert, dass die Auftraggeberin Initiativen zu Bug Bounty-Programme starten kann.	Schriftliche Bestätigung.	
L2-TS19	**Akzeptanz der Vertragsentwürfe** Die Anbieterin ist bereit, die Vertragsentwürfe in den Anhängen 6.1, 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.2, 6.2.1, 6.3 und 6.3.1 vom Kapitel 9.1 des Pflichtenhefts vorbehaltlos zu akzeptieren.	Schriftliche Bestätigung.	

Ort/Datum
Rechtsgültige Unterschrift(en) der Anbieterin