

Leistungsbeschreibung

„Beschaffung und Einführung einer Enterprise Architecture Suite (SaaS) inkl. Migration der bestehenden IT-Anwendungslandschaft aus unserer aktuellen ARIS-Lösung“

Inhaltsverzeichnis

Abkürzungsverzeichnis.....	4
Glossar.....	6
1. Einleitung	10
1.1 Zweck des Dokuments.....	10
1.2 Auftraggeberin	10
1.3 Ausgangslage	11
1.4 Rollen und Berechtigungen.....	11
2. Vergabegegenstand	12
2.1 Sprache	13
2.2 Mengengerüst für die SaaS-Lösung.....	13
3. Beschreibung der Leistungserbringung	15
3.1 Funktionale Anforderungen.....	15
3.1.1 Repository & Metamodell	15
3.1.2 Application Portfolio Management (APM).....	15
3.1.3 Roadmap & Szenarioplanung	15
3.1.4 Transparente Visualisierungen.....	15
3.1.5 Datenqualität & Kollaboration.....	15
3.1.6 Integrationen	16
3.1.7 Compliance, Risiko, Security.....	16
3.1.8 Berichte & Self-Service	16
3.1.9 Mehrsprachigkeit & Mandantenfähigkeit.....	17
3.1.10 Datenmodell.....	17
3.1.11 Darstellbarkeit und Exportierbarkeit von Daten.....	17
3.1.12 Rechteverwaltung und rollenbasierte Nutzengruppen.....	17
3.1.13 Funktionalitäten zur kollaborativen Zusammenarbeit.....	18
3.1.14 Austausch von Datenbankinhalten	18
3.1.15 Workflowbasiertes Arbeiten.....	18
3.1.16 Obsoleszenz- und Schwachstellenmanagement	18
3.1.17 Capability-basierte Budgetierung und Wertstrom-Sichten.....	18

3.1.18	KI-Assistenzfunktionen (z. B. Auto Discovery, Impact-Analysen, Report-Generierung).....	19
3.1.19	KI-Assistenzfunktionen (z. B. Auto Discovery, Impact-Analysen, Report-Generierung).....	19
3.2	Nicht-funktionale Anforderungen.....	19
3.2.1	SaaS-Betrieb (EU/EWR-Optionen/UK/Schweiz / weltweite Verfügbarkeit, Verfügbarkeit ≥ 99,0 %).....	19
3.2.2	Datenschutz und Datensicherheit (EU DSGVO, Verschlüsselung, Datenresidenz) 20	
3.2.3	Skalierbarkeit (>1000 Applikationen, >2000 Komponenten, >100.000 Relationen) 20	
3.2.4	Performance (interaktive Reports < 3 s bei typischen Abfragen)	20
3.2.5	Erweiterbarkeit (konfigurierbares Metamodell, API First).....	20
3.2.6	Dokumentation.....	21
3.2.7	Informationssicherheit.....	22
3.2.8	Datenschutz.....	30
3.2.9	Anforderungen an den Betrieb	30
3.2.10	Incident- und Problemmanagement.....	32
3.2.11	Wartung, Pflege und Support	32
3.2.12	Optionale Schnittstellenanbindung an weitere Third Party Anwendungen	33
3.3	Leistungen in der Implementierungsphase.....	33
3.3.1	Einrichtung der SaaS-Lösung	34
3.3.2	Einrichtung der Rollen und Berechtigungen	35
3.3.3	Datenmodell-Analyse und Modellierung	35
3.3.4	Datenmigration.....	36
3.3.5	Einrichtung der Schnittstellenanbindung zu ARIS	36
3.3.6	Workflows	36
3.4	Schulungen.....	37
3.4.1	Zielgruppen und Lernziele.....	38
3.4.2	Schulungsunterlagen	39
3.4.3	Rahmenbedingungen.....	39
3.5	Vertragsende	40

3.6	Optionale Leistungen	40
4.	Liefergegenstände.....	42
5.	Anhang.....	46
5.1	Inhaltsverzeichnis des Betriebshandbuchs.....	46

Abkürzungsverzeichnis

Begriff	Abkürzung
ME-ID	Entra ID
AG	Auftraggeberin
AN	Auftragnehmer
BHB	Betriebshandbuch
DSGVO	Datenschutz-Grundverordnung
E3/E5	Microsoft 365 (E3/E5)
LLMs	Large Language Models
ARIS	Architektur Integrierter Informationssysteme
SaaS	Software-as-a-Service
ERP	Enterprise Resource Planning
DevOps	Development und Operations
SAP-BTP	SAP-Business Technology Platform

EAS	Enterprise Architecture Suite
-----	-------------------------------

Glossar

Begriff	Erläuterung
Ausfall	Nichtverfügbarkeit der Leistung innerhalb der Betriebszeit.
Begriff	Denkeinheit, die aus einer Menge von Gegenständen unter Ermittlung der diesen Gegenständen gemeinsamen Eigenschaften mittels Abstraktion gebildet wird. Begriffe sind dabei nicht an einzelne Sprachen gebunden, sie sind jedoch vom jeweiligen gesellschaftlichen und kulturellen Hintergrund einer Sprachgemeinschaft beeinflusst.
Benennung	Sprachliche Bezeichnung eines Begriffs, die entweder aus einem Wort (Einwortbenennung, Fachwort) oder mehreren Wörtern (Mehrwortbenennung, Fachausdruck) besteht, aber auch Symbole oder Formeln enthalten kann (@-Zeichen, CO ₂ -Ausstoß).
Bericht	Jegliche Art von Ergebnisdokumenten.
Betriebsbereitschaft	Die Leistung funktioniert störungsfrei.
Betriebshandbuch	beinhaltet die Beschreibung aller für die Serviceerbringung geltenden übergreifenden und spezifischen Rahmenbedingungen bzw. Voraussetzungen sowie die Dokumentation aller betrieblichen Aktivitäten, Abläufe und Handlungsanweisungen zur Aufnahme, Ausführung und Kontrolle des Betriebs. Das BHB wird regelmäßig bei Veränderungen angepasst.
Betriebszeit	Zeiten, innerhalb derer die AG Anspruch auf Bereitstellung der Leistung hat. Die Betriebszeit ist abzugrenzen von der Servicezeit (siehe unten).

Bezeichnung	Repräsentation eines Begriffs mit sprachlichen oder anderen Mitteln (z. B. ein Wort, aber auch ein Symbol oder eine Formel).
ARIS	Das ARIS-System bietet aktuell in der GIZ Transparenz über Prozesse und IT-Anwendungen und hilft, Komplexität zu reduzieren und zu beherrschen. Es ermöglicht die gemeinsame Nutzung von Funktionalitäten und Daten.
Concept Map	Darstellung eines Begriffssystems aus gleich- oder verschiedenartigen Begriffsbeziehungen in Form eines Netzes, ähnlich einer Mindmap
Datenkategorie	Klasse von sprachlichen oder verwaltungstechnischen Informationen, mit denen ein Eintrag näher bestimmt wird – Datenkategorien können sich dabei auf den ganzen Eintrag oder Begriff, auf eine einzelne Sprache oder eine einzelne Benennung beziehen (z.B. wird die Datenkategorie „Genus“ auf Benennungsebene angelegt und beschreibt, welches grammatikalische Geschlecht ein Wort hat).
Datensicherung	Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der auf der Cloudinfrastruktur gespeicherten und für Verarbeitungszwecke genutzten Daten und Software.
Endnutzende*r	In dieser Rolle werden GIZ-Mitarbeitende weltweit sowie externe Dienstleister*innen mit GIZ-Kennung zusammengefasst. Allen Endnutzenden ist gemein, dass sie Inhalte nur passiv nutzen, ohne Sie selbst zu erarbeiten.
Hot-Fix	Softwareaktualisierung, die bereitgestellt wird, um einen oder mehrere Fehler zu korrigieren.

Informationssicherheitsvorfall	Ereignis, durch welches eine Beeinträchtigung der Informationssicherheit möglich oder bereits erfolgt ist, z.B. durch unberechtigte Einsichtnahme/Weitergabe von Informationen (Verlust der Vertraulichkeit), Modifikation von Informationen (Verlust der Integrität) oder Löschen von Informationen/Behinderung des Zugriffs auf Informationen (Verlust der Verfügbarkeit).
Lösungszeit	Mit „Lösungszeit“ meinen wir „Wiederherstellungszeit“ im Sinne der EVB-IT Cloud AGB: Zeitraum, innerhalb dessen der Auftragnehmer die Störungs- bzw. Mängelbehebungsarbeiten erfolgreich abzuschließen hat. Der Zeitraum beginnt mit dem Auftreten der Störung, läuft jedoch nur in den vereinbarten Servicezeiten. Tritt die Störung außerhalb dieser Zeiten ein, beginnt die Wiederherstellungszeit mit der nächsten Servicezeit.
Patch	Temporäre Behebung eines Mangels und/oder einer Störung in der Software ohne Eingriff in den Quellcode.
Reaktionszeit	Zeitraum, innerhalb dessen der AN mit den Störungs- bzw. Mängelbehebungsarbeiten zu beginnen hat. Der Zeitraum beginnt mit dem Auftreten der Störung, läuft jedoch nur in den vereinbarten Servicezeiten. Tritt die Störung außerhalb dieser Zeiten ein, beginnt die Reaktionszeit mit der nächsten Servicezeit.
Release	Neue Entwicklungsstufe einer Software, die sich gegenüber dem vorherigen Release bzw. der Version im Funktions- und/oder Datenspektrum erheblich unterscheidet.
Schlagwort	Eine von mehreren Bezeichnungen innerhalb eines Sprachraums, die innerhalb desselben Begriffssystems angesiedelt sind.
Servicezeit	Zeiten, innerhalb derer die AG Anspruch auf Bereitstellung von Support-Leistungen und auf die

	Beseitigung von Störungs- bzw. Mangelbehebungsarbeiten hat. Der Begriff Servicezeit ist abzugrenzen von dem Begriff „Betriebszeit“ (s.o.) und wird synonym für den Begriff „Geschäftszeit“ des EVB-IT-Cloud-Vertrag genutzt.
Sicherheitsvorfall	Angriff auf die Cloud-Infrastruktur und die Leistungen des Auftragnehmers, der die Vertraulichkeit, Verfügbarkeit oder Integrität derselben derart gefährdet, dass ein erheblicher Schaden eintreten kann oder tatsächlich beeinträchtigt.
single source of truth	Die zentrale Datenquelle für alle sprachlichen Entscheidungen des Unternehmens.
Software as a Service	Bereitstellung von Software bzw. Funktionen von Software in einer vom Auftragnehmer betriebenen Infrastruktur.
Störung	Beeinträchtigung der Eignung der Leistung zur vertraglich vereinbarten, bzw. soweit eine solche Vereinbarung fehlt, zur vorausgesetzten der sonst zur gewöhnlichen Verwendung. Dies gilt unabhängig von einem Vertretenmüssen und unabhängig davon, ob diese Abweichung bereits bei Leistungsbeginn vorlag.
Synonym	Eine von mehreren Bezeichnungen innerhalb eines Sprachraums, die alle denselben Begriff repräsentieren.
Update	Bündelung mehrerer Mängelbehebungen und/oder Störungsbeseitigungen sowie geringfügige funktionale Verbesserungen und/oder Anpassungen der Software in einer einzigen Lieferung.

1. Einleitung

1.1 Zweck des Dokuments

In der Leistungsbeschreibung sind die Art und der Umfang der zu erbringenden Leistung wie auch die dazugehörigen Rahmenbedingungen beschrieben, die Bewerber*innen für die Erstellung eines Angebotes und zur Realisierung der Leistungen benötigen. Die Leistungsbeschreibung wird im Anschluss des Vergabeverfahrens Teil des Vertrags zwischen der Auftraggeberin (AG) und dem Auftragnehmer (AN). Aus der Leistungsbeschreibung gehen die Anforderungen an die einzelnen Positionen im Preisblatt hervor. Außerdem verweist die Leistungsbeschreibung auf ergänzende Anforderungen zur Leistungserbringung, wie zum Beispiel auf Datenschutz- oder Sicherheitsbestimmungen.

1.2 Auftraggeberin

AG ist die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.

Die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH ist ein weltweit tätiges Bundesunternehmen. Sie unterstützt die Bundesregierung in der internationalen Zusammenarbeit für nachhaltige Entwicklung und in der internationalen Bildungsarbeit.

Als Dienstleisterin der internationalen Zusammenarbeit für nachhaltige Entwicklung und internationalen Bildungsarbeit engagiert sich die GIZ weltweit für eine lebenswerte Zukunft. Die GIZ hat mehr als 50 Jahre Erfahrung in unterschiedlichsten Feldern, von der Wirtschafts- und Beschäftigungsförderung über Energie- und Umweltthemen bis hin zur Förderung von Frieden und Sicherheit.

Das vielfältige Know-how des Bundesunternehmens GIZ wird rund um den Globus nachgefragt – von der deutschen Bundesregierung, Institutionen der Europäischen Union, den Vereinten Nationen, der Privatwirtschaft und Regierungen anderer Länder. Wir kooperieren mit Unternehmen, zivilgesellschaftlichen Akteuren und wissenschaftlichen Institutionen und tragen so zu einem erfolgreichen Zusammenspiel von Entwicklungspolitik und weiteren Politik- und Handlungsfeldern bei. Unser Hauptauftraggeber ist das Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ).

Alle Auftraggeber*innen und Kooperationspartner*innen schenken der GIZ ihr Vertrauen, Ideen für politische, gesellschaftliche und wirtschaftliche Veränderungen mit ihnen gemeinsam zu entwickeln, konkret zu planen und umzusetzen. Als gemeinnütziges Bundesunternehmen steht die GIZ für deutsche und europäische Werte. Gemeinsam mit den Partner*innen in den nationalen Regierungen weltweit sowie mit Kooperationspartner*innen aus Wirtschaft,

Wissenschaft und Zivilgesellschaft arbeitet die GIZ flexibel an wirksamen Lösungen, die Menschen Perspektiven bieten und deren Lebensbedingungen dauerhaft verbessern.

Die GIZ hat zwei Unternehmenssitze in Deutschland: Einen in Bonn und einen in Eschborn bei Frankfurt am Main. Von diesen aus wird das Unternehmen geleitet, wesentliche Teile der fachlichen Arbeit verrichtet und die Auslandstätigkeit der GIZ koordiniert.

1.3 Ausgangslage

Die GIZ befindet sich aktuell auf einem Transformationspfad, welche bis 2028 eine zukunftsgerichtet anpassungsfähige und effiziente IT benötigt. Sie muss neben der Stärkung der IT-Leistungsfähigkeit gleichzeitig vielfältigen Anforderungen aus transformativen Vorhaben sowie der Sicherung des Technologiebetriebes gerecht werden.

Ein durchgängiges, kollaboratives und belastbares EA-Ökosystem, das Geschäftsziele, Fähigkeiten (Capabilities), Prozesse, Applikationen, Daten und Technologien nachvollziehbar verknüpft, Entscheidungen datenbasiert unterstützt und Veränderungen planbar macht (Enterprise Architecture Management) stellt die Grundlage für etliche Handlungsfelder des Betriebsmodelles dar.

Gegenstand der Ausschreibung ist die Einführung einer zentralen Enterprise-Architecture-Lösung als Software-as-a-Service (SaaS), inklusive Implementierungs- und Migrationsdienstleistung der bestehenden ARIS-Datenbankinhalte in die neue Lösung.

1.4 Rollen und Berechtigungen

Grundsätzlich müssen in der SaaS-Lösung folgende Berechtigungen umsetzbar sein:

Administrative Berechtigungen	
Lesen	Konsumiert den ihm zur Verfügung gestellten Content.
Schreiben	Erstellt neue Inhalte, kann aber auch Inhalte konsumieren und dazu beitragen.
Administrator*in	Besitzt automatisch alle Rechte der anderen Benutzerrollen (also Anzeigen, Erstellen, Bearbeiten) plus die vollständige Steuerung über Workspace-Konfiguration, Rollen, Berechtigungen, Nutzerverwaltung und technische Einstellungen.

Nutzenden- und Nutzenden-gruppenverwaltung	Erstellen, Bearbeiten und Löschen von Nutzenden, Gruppenzugehörigkeiten und Berechtigungen
Workflow-Erstellung und -Verwaltung	Workflows zur kollaborativen Arbeit erstellen, um <ul style="list-style-type: none"> • den Nutzenden unterschiedliche Aufgaben zur Erstellung und Bearbeitung zuzuweisen • unterschiedliche Aufgaben und Aufgabenpakete mit einem Status zu versehen, um den Arbeitsstand anzuzeigen. • diese automatisiert an andere Nutzende weiterzugeben • den aktuellen Stand und Status jeder Aufgabe einzusehen
Datenmigration	Datenbanken und Daten vollständig oder teilweise und manuell oder (halb-)automatisiert zu importieren und exportieren.

Alle Nutzenden (unabhängig von ihrer Rollenzuordnung) sollen mindestens die Berechtigungen zum **Lesen**, Verfassen von **Kommentaren** zu bestehenden Einträgen und **Antragstellen** für das Erfassen neuer Datenbankinhalte erhalten.

2. Vergabegegenstand

Es wird eine **unternehmensweite Enterprise Architecture Suite (EAS)** als **vollständig cloud- und webbasierte SaaS-Lösung** ausgeschrieben. Gegenstand der Ausschreibung ist die **Bereitstellung, Wartung, Pflege, Support und der Betrieb** der Lösung auf **Servern innerhalb der Europäischen Union**.

Die EAS muss eine zentrale Plattform zur **Erfassung, Verwaltung, Analyse und Bereitstellung** von Unternehmensarchitekturen, Geschäftsprozessen, Anwendungs- und Datenlandschaften sowie IT-Systemen bieten. Ziel ist die **einheitliche, kollaborative und unternehmensweite Nutzung** architekturrelevanter Informationen.

Die Lösung muss folgende Anforderungen erfüllen:

- **Cloud- und webbasierte Bereitstellung** als Software-as-a-Service (SaaS)
- **Hosting ausschließlich auf Servern innerhalb des Europäischen Wirtschaftsraum/Vereinigten Königreich/Schweiz** (vgl. Kap. 3.2.7.3)
- **Mehrsprachige Nutzung** in den Unternehmenssprachen Deutsch, Englisch, Französisch und Spanisch
- **Zugriffsmöglichkeit für interne und externe Nutzende** mit rollenbasierten Berechtigungen

- **Kollaborative Funktionen** zur gemeinsamen Bearbeitung und Abstimmung von Architekturelementen

Zusätzlich sind Leistungen in der Implementierungsphase gemäß Kapitel 3.3, weitere angrenzende Dienstleistungen gemäß Kap. 3.2.6.1 und 3.2.6.2, sowie optionale Leistungen gemäß Kap. 3.1.6, 3.2.12 und 3.6, sowie **Schulungsleistungen in Form von Webinaren** gemäß Kapitel 3.4 Bestandteil der Ausschreibung.

2.1 Sprache

Die Projektsprache ist deutsch. Dokumente, die zwischen der AG und dem AN ausgetauscht werden, z. B. Dokumentationen oder Besprechungsprotokolle, sind ausschließlich in deutscher Sprache zu erstellen und vorzuhalten, ausgenommen sind englische Fachbegriffe. Die Kommunikation im Rahmen der Vertragserfüllung hat in deutscher Sprache zu erfolgen.

2.2 Mengengerüst für die SaaS-Lösung

Die SaaS-Lösung soll unternehmensweit eingesetzt werden.

Mit der Nutzung der Lizenzen verbunden ist die Wartung, Pflege sowie der Support und Betrieb der Lizenzen durch den AN.

Die Anzahl der benötigten Lizenzen für die SaaS-Lösung steigt während der Vertragslaufzeit voraussichtlich an. Die SaaS-Lösung muss paralleles Arbeiten ermöglichen.

In den ersten sechs Monaten (bis Ende Monat 6) nach Vertragsschluss werden für eine kleinere Nutzendengruppe voraussichtlich folgende Lizenzen benötigt:

Gesamtanzahl potenzieller Nutzer*innen je Rolle	Anzahl Nutzer*innen je Rolle im parallelen Zugriff
Bis zu 6 Administrator*innen	Bis zu 6 Administrator*innen
Bis zu 6 Schreibende	Bis zu 6 Schreibende
Bis zu 6 Lesende (Endnutzende)	Bis zu 6 Lesende

Nach sechs Monaten (ab Monat 7) nach Vertragsschluss startet die unternehmensweite Betriebsphase. Dafür werden voraussichtlich folgende Lizenzen benötigt:

Gesamtanzahl potenzieller Nutzenden je Rolle	Anzahl Nutzende je Rolle im parallelen Zugriff
Bis zu 15 Administrator*innen	Bis zu 15 Administrator*innen
Bis zu 500 Schreibende	Bis zu 50 Schreibende
20.000 Lesende (Endnutzende)	100-200 Endnutzende

In der Betriebsphase (ab Monat 7) besteht die Möglichkeit der nutzungsbezogenen Erweiterungen der SaaS-Lösung über die Gesamtlaufzeit (nach Bedarf). Hierbei muss es möglich sein, bis zu 15 Mal Endnutzenden-Lizenzen im parallelen Zugriff (bei 20.000 Endnutzenden) in 50er-Paketen (eine bzw. mehrere Lizenzen, die jeweils mindestens 50 weiteren Endnutzenden einen zeitgleichen Zugriff ermöglichen) dazubuchen zu können:

Gesamtanzahl potenzieller Nutzenden je Rolle	Anzahl Lesende (Endnutzende) im parallelen Zugriff je Paket
20.000 Lesende (Endnutzende)	50 Lesende (Endnutzende)

Dabei meint die „Gesamtanzahl potenzieller Nutzenden je Rolle“ die Anzahl aller Nutzenden der jeweiligen Rolle, die im genannten Zeitraum (ab Anfang Monat 7 nach Vertragsschluss) grundsätzlich mit der SaaS-Lösung arbeiten können.

Die „Anzahl Nutzende je Rolle im parallelen Zugriff“ meint die Anzahl der Nutzenden der jeweiligen Rolle, die gleichzeitig in der SaaS-Lösung arbeiten können.

Es muss gewährleistet sein, dass eine Erhöhung der Endnutzendenzahlen im parallelen Zugriff, der verwalteten Elemente und/oder der Datenmenge durch eine Erweiterbarkeit der Systemressourcen abgesichert ist.

Die konkrete Ausgestaltung des Termin- und Leistungsplans für die Herbeiführung der Betriebsbereitschaft wird im Kick-Off mit dem AN abgestimmt. Der Kickoff findet innerhalb von 2 Wochen nach Vertragsschluss statt.

Ein lauffähiges System ist voraussichtlich ab April 2027 vorgesehen.

3. Beschreibung der Leistungserbringung

3.1 Funktionale Anforderungen

3.1.1 Repository & Metamodell

Änderungen im Repository müssen versioniert und nachvollziehbar sein (Change History).

3.1.2 Application Portfolio Management (APM)

Es muss Funktionen zur Rationalisierung des Applikationsportfolios bieten (z. B. Zusammenlegung, Ablösung, Investitionsentscheidungen).

Für jede Anwendung muss ein Lebenszyklusmanagement (Planung, aktiv, auslaufend, außer Betrieb) vorhanden sein.

3.1.3 Roadmap & Szenarioplanung

Es muss Funktionen zur **Sequenzierung** von Maßnahmen geben (z. B. Programm- oder Projekt-Epics, Roadmap-Phasen).

Das System muss **Szenarien** abbilden können (z. B. "Was-wäre-wenn"-Analysen bei Projektverschiebungen oder Technologieänderungen).

3.1.4 Transparente Visualisierungen

Es muss Abdeckungsmatrizen unterstützen (z. B. Business Capabilities vs. Applikationen).

Es muss Kontextlandkarten erzeugen können (Darstellung von Applikationen im Kontext von Geschäftsprozessen oder Organisationen).

3.1.5 Datenqualität & Kollaboration

Es muss Aufgabenmanagement und Surveys unterstützen, um Datenqualität aktiv zu verbessern.

Benutzer müssen Kommentare zu Objekten hinterlassen können.

Das System muss Änderungsverfolgung und Historie je Fact Sheet bereitstellen.

Es muss Benachrichtigungen oder Erinnerungen bei Aufgaben und Änderungen auslösen.

Das System muss Änderungsverfolgung und Historie bereitstellen.

3.1.6 Integrationen

Das System muss die Integration in SAP-ALM und Entra-ID für SSO ermöglichen.

Das System muss für Discovery und Integration mind. Lesenden Zugriff zu folgenden Systemen bereitstellen:

- CMDB (z. B. ServiceNow, Serviceware Processes)
- Entra-ID
- ALM-Systeme (z. B. SAP Solution Manager, SAP Cloud ALM)
- ERP-Systeme (z. B. SAP S/4HANA)
- BPM-Tools (z. B. ARIS)

Integrationen sollen bidirektional möglich sein (lesen und schreiben von Daten).

Das System muss eine offene API (REST/GraphQL) zur Anbindung weiterer Systeme bereitstellen.

3.1.7 Compliance, Risiko, Security

Das **Rollen- und Berechtigungsmodell** muss nach dem **Least-Privilege-Prinzip** aufgebaut sein.

Das System muss **Mandantentrennung** (Tenant Isolation) gewährleisten.

3.1.8 Berichte & Self-Service

Eine **Self-Service-Reporting-Funktion** muss es Anwendern ermöglichen, eigene Berichte zu erstellen, ohne IT-Unterstützung.

Über eine **API** müssen Reportdaten abgerufen werden können (z. B. Integration mit Power BI oder Tableau).

3.1.9 Mehrsprachigkeit & Mandantenfähigkeit

Die Lösung muss **global skalierbar** sein, um mehrere Regionen, Zeitzonen und regulatorische Anforderungen (z. B. DSGVO, US Data Residency) abzudecken.

Systemmeldungen, Reports und Benachrichtigungen müssen **in der Sprache des Nutzers** angezeigt oder versendet werden.

3.1.10 Datenmodell

Die Daten müssen auf Eintrags- und Datenkategorieebene filterbar sein.

3.1.11 Darstellbarkeit und Exportierbarkeit von Daten

Die SaaS-Lösung muss ermöglichen, dass Datenkategorien (z.B. Attribuierungen von Objekten) auf der Nutzeroberfläche der SaaS-Lösung visuell unterscheid- und darstellbar sind (z. B. fett, ausgegraut, farbig, Icons, Kategorien).

Die SaaS-Lösung muss ermöglichen, dass Datenkategorien (z.B. Attribuierungen von Objekten) auf der Nutzeroberfläche nach unterschiedlichen Kategorie Werten gefiltert werden können.

Die SaaS-Lösung muss ermöglichen, dass Inhalte/Einträge entsprechend bestimmten Filtern exportiert werden können.

Die SaaS-Lösung muss ermöglichen, dass Datenkategorien rollenspezifisch angezeigt oder ausgeblendet werden können.

Die SaaS-Lösung muss ermöglichen, dass bei einem Export nur bestimmte Datenkategorien exportiert werden.

3.1.12 Rechteverwaltung und rollenbasierte Nutzendengruppen

Die Zugriffs-, Lese- und Schreibrechte für die unterschiedlichen Datenbanken, Datenebenen (Eintrags-, Sprach- oder Benennungsebene) und Datenkategorien müssen individuell und gruppenbezogen (d.h. entsprechend der Rollen aus Kap. 1.4 der Leistungsbeschreibung) feingranular vergeben werden können.

3.1.13 Funktionalitäten zur kollaborativen Zusammenarbeit

Die SaaS-Lösung muss es ermöglichen, zu jedem Datenbankeintrag einen Kommentar zu hinterlegen.

3.1.14 Austausch von Datenbankinhalten

Die SaaS-Lösung muss den Export und Import von Datenbankinhalten in bzw. aus folgenden Dateiformaten unterstützen: .csv, .csv js, .xml, .tbx, .xlsx, bpmn.

3.1.15 Workflowbasiertes Arbeiten

Die kollaborative Zusammenarbeit entsprechend dem Rollenkonzept (siehe Leistungsbeschreibung Kap. [1.4](#)) muss über frei konfigurierbare und automatisierbare Workflows in der SaaS-Lösung erfolgen.

Unter Workflow wird verstanden, dass Aufgaben unterschiedlichen Nutzenden in einer bestimmten Reihenfolge zugewiesen werden können, der Bearbeitungsstatus im System manuell geändert werden kann oder beim Erledigen bestimmter (Teil-)Aufgaben automatisch umspringt und dass der Bearbeitungsstatus von berechtigten Personen zu jedem Zeitpunkt eingesehen werden kann.

3.1.16 Obsoleszenz- und Schwachstellenmanagement

Die SaaS-Lösung **muss ermöglichen, dass** Obsoleszenzrisiken frühzeitig identifiziert und Handlungsempfehlungen (z. B. für Migration oder Ersatz) generiert werden.

3.1.17 Capability-basierte Budgetierung und Wertstrom-Sichten

Die SaaS-Lösung **muss ermöglichen, dass** eine unternehmensweite Capability-Map gepflegt und zur Budget- und Investitionsplanung genutzt werden kann.

Die SaaS-Lösung **muss ermöglichen, dass** Capabilities, Wertströmen und Domänen zugeordnet werden können.

3.1.18 KI-Assistenzfunktionen (z. B. Auto Discovery, Impact-Analysen, Report-Generierung)

Die SaaS-Lösung **muss ermöglichen, dass** Systeme, Schnittstellen und Abhängigkeiten KI-gestützt automatisch erkannt und klassifiziert werden („Auto Discovery“).

Die SaaS-Lösung **muss ermöglichen, dass** Auswirkungen von Änderungen im Tech-Stack automatisiert analysiert werden (Impact-Analysen).

3.1.19 KI-Assistenzfunktionen (z. B. Auto Discovery, Impact-Analysen, Report-Generierung)

Die SaaS-Lösung **muss ermöglichen, dass** standardisierte Schnittstellen (APIs, Konnektoren) zur Integration mit einem bestehenden Data Mesh bereitgestellt werden.

Die SaaS-Lösung **muss ermöglichen, dass** Domänen, Datenprodukte und Metadaten automatisiert erkannt und synchronisiert werden können.

Die SaaS-Lösung **muss ermöglichen, dass** Data-Governance- und Compliance-Anforderungen (z. B. DSGVO) eingehalten und dokumentiert werden können.

3.2 Nicht-funktionale Anforderungen

3.2.1 SaaS-Betrieb (EU/EWR-Optionen/UK/Schweiz / weltweite Verfügbarkeit, Verfügbarkeit $\geq 99,0$ %)

Die SaaS-Lösung **muss ermöglichen, dass** der Betrieb wahlweise innerhalb der Europäischen Union (EU) / Europäischen Wirtschaftsraums (EWR)/ UK oder der Schweiz erfolgen kann.

Die SaaS-Lösung **muss ermöglichen, dass** der Betrieb in einer hochverfügbaren Cloud-Infrastruktur mit einer garantierten Mindestverfügbarkeit von $\geq 99,0$ % erfolgt.

Die SaaS-Lösung **muss ermöglichen, dass** Wartungsfenster und Ausfallzeiten transparent kommuniziert und geplant werden.

3.2.2 Datenschutz und Datensicherheit (EU DSGVO, Verschlüsselung, Datenresidenz)

Die SaaS-Lösung **muss ermöglichen, dass** die Datenresidenz innerhalb der EU oder in einem vom Auftraggeber festgelegten Rechtsraum konfigurierbar ist.

Die SaaS-Lösung **muss ermöglichen, dass** sämtliche gespeicherten Daten sowohl im Ruhezustand (at rest) als auch während der Übertragung (in transit) verschlüsselt werden.

Die SaaS-Lösung **muss ermöglichen, dass** alle Funktionen im Einklang mit der EU-Datenschutz-Grundverordnung (DSGVO) betrieben werden.

3.2.3 Skalierbarkeit (>1000 Applikationen, >2000 Komponenten, >100.000 Relationen)

Die SaaS-Lösung **muss ermöglichen, dass** mehr als **1.000 Applikationen, 2.000 Komponenten** und **100.000 Relationen** performant verwaltet werden können.

Die SaaS-Lösung **muss ermöglichen, dass** eine horizontale und vertikale Skalierung der Plattformressourcen (z. B. Rechenleistung, Speicher, Datenbankkapazität) automatisiert erfolgt.

3.2.4 Performance (interaktive Reports < 3 s bei typischen Abfragen)

Die SaaS-Lösung **muss ermöglichen, dass** interaktive Berichte und Dashboards bei typischen Abfragen innerhalb von **< 3 Sekunden** geladen werden.

Die SaaS-Lösung **muss ermöglichen, dass** auch bei hohen Datenvolumina (> 100.000 Relationen) eine stabile Performance gewährleistet bleibt.

3.2.5 Erweiterbarkeit (konfigurierbares Metamodell, API First)

Die SaaS-Lösung **muss ermöglichen, dass** das zugrunde liegende Metamodell konfigurierbar und erweiterbar ist (z. B. eigene Objekttypen, Relationen, Attribute).

Die SaaS-Lösung **muss ermöglichen, dass** sämtliche Funktionen über eine **offene, dokumentierte API** verfügbar sind („API First“-Prinzip).

3.2.6 Dokumentation

Für die SaaS-Lösung sind folgende Dokumentationen – teilweise unter Mitwirkung sowie teilweise eigenständig durch den AN – zu erstellen:

- Betriebshandbuch
- Digitales Benutzerhandbuch.

Die gesamte Dokumentation ist wie nachfolgend beschrieben zu erstellen.

3.2.6.1 Betriebshandbuch

Das Betriebshandbuch gemäß ISO 27001 und BSI-Grundschutz wird von der AG unter Mitwirkung des AN erstellt und stellt sicher, dass alle Betriebsaktivitäten und die dazu notwendigen Ressourcen identifiziert und zugeordnet sind. Insbesondere muss der AN für folgende Kapitel Inhalt zuliefern: 2.3 Datenschutz, 2.4 Verträge, Anforderungen und Vereinbarungen, 2.4 Lizenzmanagement, 2.8 Technische Beschreibung, 2.8.1 Systemkomponenten, 2.8.2 Systemarchitektur, 2.8.3 Datenflüsse und Schnittstellen, 2.8.4 Weiterführende Dokumentation, 3.5.1 Meldungen und Patches der Hersteller.

Das Betriebshandbuch beinhaltet sämtliche Themenbereiche, die für den regulären Betrieb der SaaS-Lösung erforderlich sind und beschreibt die zwischen der AG und dem AN abgestimmten betriebsrelevanten Prozesse und enthält ein Glossar mit Erklärungen der Fachbegriffe. Das Betriebshandbuch wird auf Grundlage eines Standarddokumentes der AG erzeugt. Die Vorlage wird nach Zuschlag bereitgestellt. Das Inhaltsverzeichnis zum Betriebshandbuch befindet sich in Kap. [5.1](#). Das Betriebshandbuch muss zu Beginn der Betriebsphase (siehe auch Kap. [2.2](#)) vorliegen.

Auf Grundlage der Prozesse der AG wird mit dem AN abgestimmt, wie der Prozess auf Seiten des AN integriert werden kann. Falls es Abweichungen und Ergänzungen zu den von der AG dokumentierten Prozessen gibt, sind diese im Betriebshandbuch zu beschreiben.

Das Betriebshandbuch, inklusive evtl. Anhänge muss in deutscher Sprache vorliegen, mit Ausnahme von englischen Fachbegriffen. Sind die englischen Fachbegriffe nicht allgemein gebräuchlich, so müssen diese in Form eines Glossars oder vergleichbar in deutscher Übersetzung oder entsprechender Erläuterung angegeben werden.

Die Kosten pro Fachkrafttag für Unterstützungsleistungen bei der Erstellung des Betriebshandbuchs sind im Preisblatt unter Position 5.1 anzugeben.

3.2.6.2 Benutzerhandbuch

Das Benutzerhandbuch stellt eine ausführliche Dokumentation für die Nutzung der SaaS-Lösung dar. Es ermöglicht Administrator*innen, Schreiben und Lesenden Endnutzenden, alle Funktionalitäten entsprechend dem aktuellen Funktionsumfang der SaaS-Lösung und deren Handhabung in deutscher und ggf. englischer Sprache nachzulesen und mit aktuellen Screenshots und Beschreibungen nachzuvollziehen. Das Handbuch erläutert zudem alle Einstellmöglichkeiten sowie Pflegeoptionen für Templates, die u.a. mit der Erstellung von Datenbankeinträgen zusammenhängen.

Das Benutzerhandbuch muss vom AN zum Tag der ersten Schulung sowohl bearbeitbar (im docx.-Format) als auch im Format PDF zur Verfügung stehen.

Die Inhalte des Benutzerhandbuchs umfassen mindestens:

- Grundlegende Bedienungsanleitung (Erklärung zur Steuerung und zu Bedienelementen)
- Informationen zur spezifischen Funktionalität der Software gemäß der in Kap. 1.4 benannten Rollen
- Informationen zu den konfigurierten Auftraggeber spezifischen Inhalten der Anwendung wie Datenmodell, Datenmigration, Berechtigungen, Workflows, Begriffsnetze, Verbindung zu angebundenen Systemen.
- Ratschläge zur Problembehebung, Fehleranalysen mit Gegenmaßnahmen
- Frequently Asked Questions (FAQ) in übersichtlicher Gliederung
- Glossar mit Erklärung der Fachbegriffe.

Das digitale Benutzerhandbuch muss barrierefrei sein. Bei seiner Gestaltung sollen, die in Abschnitt 12 der DIN EN 301 549 aufgeführten Anforderungen zur Barrierefreiheit eingehalten werden. Das digitale Benutzerhandbuch muss alle in der Implementierungsphase konfigurierten Auftraggeber spezifischen Inhalte der Anwendung enthalten.

Der Aufwand für die Erstellung des Benutzerhandbuchs wird durch den AN geschätzt und im Preisblatt unter Position 5.2 als Pauschal-Festpreis angegeben.

3.2.7 Informationssicherheit

Anforderungen bezüglich Informationssicherheit an den AN und das von ihm eingesetzte Personal:

3.2.7.1 Aufbewahrung von GIZ-bezogenen Unterlagen

Auftragsbezogene Unterlagen und Arbeitsergebnisse, einschließlich der finanziellen Dokumentation, sind von dem AN zehn Jahre nach Abnahme des Schlussberichts bzw. der Werkleistung aufzubewahren. Auf Verlangen der AG sind diese zu übergeben.

3.2.7.2 Zugriff auf Informationen

Der AN darf ausschließlich auf die im Rahmen der Leistungserbringung spezifizierten Informationen analog oder über technische Zugänge zugreifen.

Der Zugriff auf davon abweichende Bereiche und Informationen ist untersagt.

Die AG legt bei Bedarf fest, wie der Auftragnehmer mit Metadaten umzugehen hat (unter Berücksichtigung des Vertraulichkeitsprinzips; Need-to-Know).

3.2.7.3 Ort der Leistungserbringung

Zugriff auf die SaaS-Lösung und die Daten der GIZ durch den Betreiber und Support-Dienstleister soll von einem Standort innerhalb des europäischen Wirtschaftsraums, dem Vereinigten Königreich oder der Schweiz erfolgen. Davon ausgenommen ist die zu Grunde liegende SaaS-Plattform, wenn durch technisch nachweisbare Verfahren sichergestellt ist, dass ein Zugriff auf die Daten der GIZ ausgeschlossen ist und dies durch ein anerkanntes Prüfinstitut verifiziert und bestätigt wird.

3.2.7.4 Auditrecht

- a. Der Auftragnehmer ist verpflichtet, die Einhaltung der Anforderungen der Auftraggeberin an die Informationssicherheit nachzuweisen.
- b. Auf Anforderung der Auftraggeberin legt der Auftragnehmer außerdem Nachweise über die regelmäßige Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests oder Schwachstellenanalysen vor, z.B. durch entsprechende Bestätigungen von unabhängigen Auditoren.
- c. Bei konkretem Anlass räumt der Auftragnehmer der Auftraggeberin das Recht ein während der gesamten Projektlaufzeit Prüfungen zur Informationssicherheit durchzuführen. Ein solcher Anlass liegt insbesondere vor, wenn Hinweise auf Sicherheitsvorfälle, Unregelmäßigkeiten, Vertragsverstöße, wesentliche Änderungen der Leistung oder Unzulänglichkeiten der in a. angeforderten Nachweise bestehen.
- d. Das Prüfungsrecht umfasst ausschließlich die für die Leistungserbringung relevanten infrastrukturellen, organisatorischen, personellen und technischen Bereiche, soweit dies zur Überprüfung der Einhaltung der vereinbarten Informationssicherheitsanforderungen erforderlich ist.

- e. Die Auftraggeberin kann sich hierbei auch durch entsprechend zur Vertraulichkeit verpflichtete Dritte vertreten lassen. Das zur Prüfung eingesetzte Personal der Auftraggeberin muss über entsprechende branchenübliche Qualifikationen (z.B. ISO 27001 Lead Auditor o.ä.) verfügen.
- f. Prüfungen werden in der Regel remote durchgeführt und finden zu normalen Geschäftszeiten statt. In Ausnahmefällen kann eine Prüfung vor Ort durchgeführt werden, wenn relevante Informationssicherheitsanforderungen nicht remote prüfbar sind.
- g. Die Auftraggeberin kündigt Prüfungen frühzeitig an und informiert den Auftragnehmer über Prüfungsgegenstand und voraussichtlichen Umfang, damit dieser sich angemessen vorbereiten kann
- h. Aufwände des Auftragnehmers zur Begleitung/Durchführung der Prüfungen der Auftraggeberin und Bereitstellung der erforderlichen Nachweise werden nicht gesondert vergolten.

3.2.7.5 Mindestanforderungen an Authentisierungsmittel/ Passwörter

Der Auftragnehmer muss mindestens folgende Anforderungen an die Passwortqualität für alle Accounts, mit denen auf GIZ-Informationen zugegriffen wird/werden kann, umsetzen:

- Passwörter müssen mindestens 10 Zeichen lang sein, für privilegierte Konten mindestens 16 Zeichen
- Passwörter für technische Konten müssen mindestens 20 Zeichen lang sein, sofern ein regelmäßiger Passwortwechsel (z.B. über Managed Service Accounts) nicht gewährleistet werden kann
- Das Passwort muss sich aus 3 der 4 folgenden Merkmale zusammensetzen: Großbuchstaben (A bis Z), Kleinbuchstaben (a bis z), Ziffern (0 bis 9) und Sonderzeichen (zum Beispiel: !, \$, #, %)
- Passwörter, die leicht zu erraten sind, dürfen nicht verwendet werden.
- Passwörter dürfen nicht identisch zu einem der letzten 10 benutzten Passwörter sein.
- Passwörter müssen regelmäßig geändert werden.

Für Konten mit administrativen Berechtigungen muss eine Multi-Faktor-Authentifizierung (mindestens zwei Faktoren) genutzt werden.

3.2.7.6 Zertifikatsfehler bei Nutzenden

Es muss gewährleistet sein, dass bei der Nutzung von Zertifikaten, keine Zertifikatsfehler auftreten.

3.2.7.7 Mindestanforderungen an die Datensicherung

Der Auftragnehmer muss folgende Anforderungen an das Verfahren für die Datensicherung für die verarbeiteten Daten erfüllen:

- Aus der Datensicherung müssen sich die für die bereitgestellte Leistung notwendigen technischen Komponenten/Anwendungen entsprechend der aufgeführten Parameter vollständig wiederherstellen lassen:
 - Die Häufigkeit der Datensicherung ist (RPO/maximal zulässiger Datenverlust): mindestens 7 Tage
 - Die Wiederherstellung aller technischen Komponenten/Anwendungen beträgt (RTO/geforderte Wiederanlaufzeit): höchstens 48 Stunden
 - Die Aufbewahrungszeit für die Datensicherungen beträgt: mindestens 21 Tage
- Die technischen Komponenten und der Ort der Speicherung der Datensicherung müssen sich mindestens in zwei unterschiedlichen Brandabschnitten befinden.

3.2.7.8 Leistungskennzahlen

Für die Erbringung der Leistung und die Berichte werden folgende für die Informationssicherheit relevante Leistungskennzahlen vereinbart:

- Verfügbarkeit des Systems in 99,0% innerhalb der Betriebszeit (24/7/365)
- Verfügbarkeit des Services in 99,0% innerhalb der Servicezeit (Mo-Fr 8-16 Uhr)

Während der gesamten Vertragslaufzeit muss auf Anforderung der AG ein Bericht (maximal halbjährlich) zur Informationssicherheit zur Verfügung gestellt werden, über deren Inhalt sich AG und AN abstimmen. Es erfolgt keine gesonderte Vergütung.

3.2.7.9 ISMS des Auftragnehmers

Der Auftragnehmer muss über ein angemessenes, dokumentiertes und implementiertes Informations-Sicherheits-Management-System (ISMS) verfügen, das dem Standard ISO/IEC 27001:2022 (bzw. aktuelle Folgeversionen) oder vergleichbar entspricht. Das ISMS muss die zu erbringende Leistung inklusive der verarbeitenden Informationen mit den dazu notwendigen infrastrukturellen, organisatorischen, personellen und technischen Komponenten umfassen.

Der Auftragnehmer muss eine*n Informationssicherheitsbeauftragte*n (Chief Information Security Officer) benennen, welche*r über die erforderliche Fachkunde verfügt und teilt der AG dessen/deren Kontaktdaten auf Anforderung mit.

Die AG wird einen Kontakt als ausschließliche*n Ansprechpartner*in in allen Fragen des Auftragnehmers bezüglich der Informationssicherheit benennen.

3.2.7.10 Benutzermanagement

Das ISMS des Auftragnehmers muss Verfahren zur dokumentierten Vergabe, Änderung, Sperrung, Entsperrung, Deaktivierung und Reaktivierung von (privilegierten, internen, externen und anderen) Benutzerkonten sowie zur zweifelsfreien Identifikation berechtigter Personen und zur Rücksetzung von Passwörtern beinhalten.

Diese Verfahren müssen technische Maßnahmen zum Schutz vor Brute-Force Angriffen (z.B. Sperrung von Benutzeraccounts nach mehrmaliger fehlerhafter Authentisierung) beinhalten.

Der Auftragnehmer muss im Rahmen seines ISMS für das Benutzermanagement folgendes sicherstellen:

- Benutzerkennungen müssen deaktiviert werden, wenn sie nicht mehr oder für mehr als 6 Monate nicht mehr benötigt werden.
- Benutzerkennungen dürfen nur gelöscht werden, wenn durch die Löschung keine Gefahr besteht, dass vorhandene Protokolle, Logdateien oder sonstige Aufzeichnungen innerhalb des Archivierungszeitraums nicht mehr eindeutig einer Person zugeordnet werden können.
- Werden nicht-personalisierte Benutzerkonten (z.B. root-Account, Benutzerkonten für den IT-Notfall) eingesetzt, so muss durch geeignete Maßnahmen sichergestellt werden, dass die mit diesem Konto durchgeführten Aktivitäten jederzeit zweifelsfrei einer handelnden bzw. verantwortlichen Person (möglichst automatisiert) zugeordnet werden können.
- Technische Benutzerkonten dürfen ausschließlich von Services oder Skripten benutzt werden. Die Nutzung des Kontos darf nicht durch eine Person erfolgen.
- Technische Benutzerkonten dürfen nur mit minimalen Berechtigungen entsprechend dem Berechtigungskonzept konfiguriert werden. Es muss das „Least-Privilege“ Prinzip umgesetzt werden.
- Privilegierte Benutzerkonten dürfen ausschließlich für administrative Tätigkeiten benutzt werden.
- Privilegierte Benutzerkonten für externe Benutzer*innen müssen auf maximal 6 Monate befristet eingerichtet werden und können bei Bedarf nach Ablauf verlängert werden.
- Benutzerkonten für externe Benutzer*innen dürfen nur befristet, jedoch maximal für ein Jahr vergeben werden. Die Befristung muss sich an der Vertragslaufzeit der extern nutzenden Person orientieren. Accounts können ggf. aktiv erneuert werden.

Der Auftragnehmer muss sicherstellen, dass administrative Tätigkeiten nur über personalisierte Konten durchgeführt werden und dass diese Konten ausschließlich für administrative Zwecke genutzt werden.

3.2.7.11 Berechtigungsmanagement

Das ISMS des Auftragnehmers muss ein dokumentiertes Verfahren zur dokumentierten Genehmigung, Vergabe, Änderung, Korrektur, regelmäßigen Aktualisierung und dem zeitnahen Entzug von Berechtigungen enthalten.

Die Berechtigungskonzepte des Auftragnehmers müssen auf den Prinzipien "Need-to-know" und "Least-Privilege " basieren und wirksam durchgesetzt sein.

Im Rahmen des Berechtigungsmanagements müssen die Anforderungen an die Funktionstrennung (Segregation of Duties) umgesetzt werden.

Das Berechtigungskonzept muss technische und organisatorische Maßnahmen beinhalten, welche die Wirksamkeit des Berechtigungskonzepts sicherstellen.

3.2.7.12 Change- und Patchmanagement

Das ISMS des Auftragnehmers muss Verfahren für das Test-, Change- und Patchmanagement in Anlehnung an gängige Standards (z.B. ITIL) beinhalten, dass die sichere, regelmäßige (mindestens alle 6 Monate) und anlassbezogen unverzügliche Implementierung von (Sicherheit-)Patches und Updates für die bereitgestellte Leistung gewährleistet.

3.2.7.13 Trennung von Test- und Produktivumgebung

Durch das ISMS des Auftragnehmers und technische Maßnahmen muss sichergestellt sein, dass Schwachstellen, Bedienfehler oder technische Fehler in Testumgebungen kein Risiko für die Produktivumgebung darstellen (z.B. durch Trennung von Testumgebung und Produktivumgebung durch eine Firewall).

Testumgebungen müssen den zugehörigen Produktivumgebungen entsprechen.

3.2.7.14 Management von Sicherheitsvorfällen

Der Prozess zur Erkennung, Priorisierung, Behandlung und Dokumentation von Sicherheitsvorfällen (Security Incidents) und anderen Störungen muss die zentrale Erfassung und Auswertungen von relevanten Loginformationen beinhalten.

3.2.7.15 Schwachstellenmanagement

Der Auftragnehmer muss ein Verfahren zur Erkennung, Bewertung (z.B. CVSS), Priorisierung, Beseitigung und Dokumentation von Schwachstellen für die bereitgestellte Leistung umsetzen.

Der Auftragnehmer muss an die AG quartalsweise über die für die zu erbringende Leistung relevanten erkannten Schwachstellen, sowie deren Bewertung und Beseitigung berichten.

Der AG muss ein Verfahren für regelmäßige (mindestens jährlich), automatisierte und protokollierte Schwachstellenscans umsetzen.

3.2.7.16 Härtungskonzept

Der Auftragnehmer muss ein Verfahren zur Härtung der technischen Komponenten umsetzen. Das Verfahren muss insbesondere sicherstellen, dass

- nicht benötigte oder unerwünschte Dienste oder Schnittstellen deaktiviert sind,
- nicht benötigte Benutzerkennungen deaktiviert oder gelöscht sind und
- voreingestellte Passwörter geändert werden.

3.2.7.17 Interne Audits

Der Auftragnehmer muss ein Verfahren umsetzen, das sowohl regelmäßige als auch anlassbezogene Prüfungen der Sicherheitsmaßnahmen auf Angemessenheit und Wirksamkeit (wie zum Beispiel Soll-Ist-Vergleiche von Konfigurationen, Firewall-Regelwerken oder Penetrationstests) beinhaltet und die Prüfergebnisse protokolliert.

3.2.7.18 Arbeitsplätze von Administrator*innen

Der AN stellt sicher, dass der Zugang zu Systemen zu Administrationszwecken nur von gehärteten, zugangsbeschränkten und überwachten Arbeitsplätzen erfolgen kann.

3.2.7.19 Schutz vor Schadsoftware

Der AN muss ein Verfahren zum kontinuierlichen Schutz technischer Komponenten vor Schadsoftware und ein Reaktionskonzept für großflächig auftretende Schadsoftware (z.B. Ransomware) umsetzen.

3.2.7.20 Datensicherungskonzept

Der AN muss ein Verfahren für die Datensicherung umsetzen, das regelmäßige und dokumentierte Tests der Wiederherstellung von Datensicherungen beinhaltet.

3.2.7.21 Mandantentrennung

Der AN muss ein technisches Verfahren zur Mandantentrennung umsetzen, das sicherstellt, dass Informationen und Verarbeitungskontexte verschiedener Kunden getrennt gehalten werden.

3.2.7.22 Umgang mit Authentisierungsmitteln

Der AN muss ein Verfahren zur Verwendung, zum sicheren Wechsel, Austausch, Speichern und Hinterlegen von Authentisierungsmitteln (z.B. Passwörtern), sowie eine Regelung zum sicheren Umgang mit Authentisierungsmitteln (z.B. Passwörtern) umsetzen.

Der Missbrauch von Authentisierungsmitteln muss als Sicherheitsvorfall bewertet und behandelt werden.

3.2.7.23 Löschkonzept

Der AN muss ein Verfahren für die Rückgabe, das vollständige Löschen (d.h. nicht rekonstruierbar) und das Vernichten von Daten umsetzen, so dass von der Auftraggeberin als „nicht mehr benötigt“ klassifizierte Daten umgehend gelöscht werden, sofern sie keiner gesetzlichen oder vertraglichen Aufbewahrungs- oder Sperrfrist unterliegen und eine Löschung mit technisch vertretbarem Aufwand möglich ist.

Insbesondere muss dieses Verfahren Anwendung finden für Informationen der AG bei der geplanten oder ungeplanten Beendigung der Leistungserbringung.

Die Löschung ist der AG auf Verlangen und durch entsprechende Erklärung oder anderweitig nachzuweisen. Das Löschverfahren muss auf Anforderung nachgewiesen werden.

3.2.7.24 Sicherer Betrieb von Firewalls

Der AN muss durch ein geeignetes Verfahren sicherstellen, dass alle Firewalls mit einem minimalen Regelwerk (Whitelisting) betrieben werden.

Die Regelwerke müssen dokumentiert sein und der IST-Stand der Regelwerkskonfiguration der Firewalls muss regelmäßig mit dem dokumentierten SOLL-Zustand verglichen werden.

3.2.7.25 Einsatz von Kryptographie – Kryptokonzept

Der AN muss ein Verfahren umsetzen, das den wirksamen Gebrauch von Kryptographie und das Schlüsselmanagement zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen beinhaltet.

Der AN muss bei Übertragung und Speicherung von Daten der AG eine angemessene Verschlüsselung sicherstellen (d.h. sowohl "In Transit" als auch "At Rest").

Insbesondere die Kommunikation über nicht vertrauenswürdige Verbindungen (z.B. WAN, Internet) muss angemessen verschlüsselt erfolgen.

Die Verschlüsselungsprotokolle und -verfahren des AN müssen dem aktuellen Stand der Technik entsprechen.

3.2.7.26 IT-Notfallmanagement

Der AN muss über ein angemessenes, dokumentiertes und implementiertes IT-Notfallmanagement verfügen, welches die zu erbringende Leistung inklusive der

verarbeitenden Informationen mit den dazu notwendigen infrastrukturellen, organisatorischen, personellen und technischen Komponenten umfasst.

Das IT-Notfallmanagement des AN muss einem kontinuierlichen Verbesserungsprozess unterliegen.

Das IT-Notfallmanagement muss mindestens die folgenden Szenarien beinhalten:

- Ausfall eines Gebäudes
- Ausfall eines Rechenzentrums
- Ausfall von Kommunikationsinfrastruktur

Notfalltests für diese Szenarien müssen regelmäßig durchgeführt und dokumentiert werden. Die Ergebnisse der Notfalltests müssen zur Verbesserung genutzt werden.

3.2.8 Datenschutz

Es werden personenbezogene Daten im Auftrag der AG verarbeitet. Daher wird mit dem AN eine Vereinbarung zur Auftragsverarbeitung (AuV) gemäß Art. 28 DSGVO geschlossen. Dafür sind vor Vertragsschluss die technisch-organisatorischen Maßnahmen (TOM) zur Einhaltung der Datenschutzvorgaben darzulegen. Sollte das Unternehmen in der Vergangenheit von der GIZ bereits geprüft worden sein, ist dennoch eine Aktualisierung gemäß DSGVO zu senden. Nach positiver Prüfung wird der Vertrag mit der Anlage AuV abgeschlossen.

3.2.9 Anforderungen an den Betrieb

3.2.9.1 Authentisierung

Der Cloud-Anbieter muss die Anbindung an die GIZ-Systeme zu Authentisierung/Authentifizierung ermöglichen und unterstützt dafür Microsoft SAML, OAuth2.0 oder OIDC Connect.

3.2.9.2 Cloudbasierte SaaS-Lösung

Bei dem System muss es sich um eine cloudbasierte SaaS-Lösung handeln. Der AN muss sicherstellen, dass eine dem Schutzbedarf der Daten angemessene Trennung der GIZ-Daten von den Daten anderer Kunden stattfindet.

3.2.9.3 Serverstandort

Die SaaS-Lösung muss auf Servern innerhalb des EWR/ UK oder der Schweiz betrieben werden.

Die SaaS-Lösung muss in einem gesicherten Rechenzentrum laufen, das die Kriterien der EN 50600 (oder DIN ISO 27001; NIST SP 800-53; SSAE 16 SOC 2; FedRAMP oder vergleichbar) erfüllt.

3.2.9.4 Zugang und Zugriff

Das Betriebssystem bei der GIZ ist Windows 11. Der Standard-Browser ist Microsoft Edge (Version 148.0.3967.70 oder aktueller), d.h. die SaaS-Lösung muss uneingeschränkt in der Microsoft-Umgebung (Windows 11, Edge) der GIZ funktionieren.

Die SaaS-Lösung soll über eine giz.de-Adresse erreichbar sein.

Die SaaS-Lösung muss den Zugang über Single Sign on (SSO) und Multifaktorauthentifizierung (MFA) ermöglichen.

Die SaaS-Lösung muss die Möglichkeit zum Austausch von Authentifizierungs- und Autorisierungsidentitäten zwischen Sicherheitsdomänen über SAML 2.0 oder OAuth bieten.

3.2.9.5 SSL-Zertifikate Web-Oberfläche

Der Schutz der Web-Oberfläche und der Kommunikation zwischen den beteiligten Komponenten inkl. des Clients muss mit Hilfe von SSL-Zertifikaten gewährleistet sein.

3.2.9.6 Schnittstellen

Der allgemeine Datenaustausch über Schnittstellen muss mittels verschlüsselter Datenübertragung (SSL) erfolgen.

Die SaaS-Lösung muss in der Lage sein auf Synchronisationskonflikte hinzuweisen und Lösungen zu unterstützen.

Die SaaS-Lösung muss eine Schnittstelle (Graph API oder REST API) mit entsprechender Dokumentation bieten.

3.2.9.7 Testumgebung

Der AN muss der AG über die gesamte Vertragslaufzeit hinweg eine Testumgebung zur Verfügung stellen. Die Testumgebung muss die Produktivumgebung technisch und funktional abbilden (spiegeln).

3.2.10 Incident- und Problemmanagement

Der AN muss der AG den Service „Incident- und Problemmanagement“ bereitstellen. Die Reaktions- und Wiederherstellungszeiten des AN bei Störungen sind dem EVB-IT-Cloudvertrag Nr. 9.2 zu entnehmen.

Für die Meldung, Klassifizierung und Bestätigung von Störungen, Service-Requests und sonstigen Anfragen oder Meldungen (sowie die Beobachtung und Überwachung des Bearbeitungsfortschritts) erfolgt die Kommunikation über E-Mail. Die AG benennt vier Personen über die gebündelt die Meldungen eingehen. Die Kommunikation erfolgt in deutscher Sprache.

Neben der Erreichbarkeit muss der AN zu den Servicezeiten gem. Kap. 3.2.11 die Beseitigung von Störungen, inkl. Bereitstellung von Hot-Fixes ermöglichen. Dabei müssen die vereinbarten Wiederherstellungszeiten nach den dortigen Störungsklassen eingehalten werden. Das System muss eine Verfügbarkeit von mindestens 99,0% gewährleisten.

3.2.11 Wartung, Pflege und Support

Wartung und Pflege sowie Support sind ab Inbetriebnahme für die im Vertrag vereinbarte Dauer durch den AN durchzuführen. Dies umfasst auch funktionale Erweiterungen (Lieferung neuer Programmstände – Updates, Upgrades, Patches) sowie Wartung und Pflege aller zum Zeitpunkt der Auslieferung bzw. Abnahme mitgelieferten Schnittstellen (Software-seitig).

- Neue Versionsstände inkl. Aktualisierungen aller erforderlichen Drittanbieter-Lizenzen, die zur Anwendung der SaaS-Lösung erforderlich sind.
- Dokumentation zu Minor und Major Releases:
 - Dokumentation der neuen Funktionen und Änderungen
 - Dokumentation der durch den AN für das neue Release durchzuführenden notwendigen Änderungen
 - Dokumentation der durch den AN durchzuführenden Tests zur Prüfung der Funktionsfähigkeit der neuen Version im Falle von Änderungen, die eine Konvertierung der Daten oder Ähnliches notwendig machen

Support-Services über die gesamte Vertragslaufzeit in Form eines telefonischen und eines E-Mail-Supports müssen während der Servicezeiten von Montag bis Freitag von 8:00 Uhr bis 17:00 Uhr zur Verfügung stehen.

Der AN muss jede neue Entwicklungsstufe der SaaS-Lösung (Release) verantworten und betreuen, die Release Notes bereitstellen und den Support für die jeweils zuletzt eingespielte

Version sicherstellen. Die AG muss bei jedem Release mit einem Vorlauf von 2 Wochen per E-Mail an den/die zu benennende*n Ansprechpartner*in vorher informiert werden.

Für die Fehlerklassifizierung wird zwischen den gem. EVB-IT-Cloud-AGB definierten Störungsklassen unterschieden.

Die Einordnung der festgestellten Mängel in schwerwiegende, erhebliche und leichte Störung erfolgt durch die AG anhand der Kriterien in Ziffer 10 EVB IT Cloud AGB und unter angemessener Berücksichtigung der Auffassung des AN.

Dabei führen in der Regel mehr als 20 gleichzeitig auftretende leichte Störungen zu einer erheblichen Störung und mehr als 5 gleichzeitig auftretende erhebliche Störungen zu einer schwerwiegenden Störung.

AN und AG können auch eine andere Fehlerklassifizierung festlegen, soweit diese im Kern nicht hinter der o.g. zurücksteht. Der AN nimmt, falls erforderlich, Anpassung an der Lösung hinsichtlich der aktuellen Gesetzeslage vor. Sollten für den Betrieb zusätzliche Softwarekomponenten nötig sein, stellt der AN diese bereit. Zudem nimmt der AN Anpassungen hinsichtlich Änderungen der Betriebssystemversionen der AG vor.

Neue Versionen, Updates, Patches oder Hot-Fixes dürfen nicht dazu führen, dass bereits durchgeführte Customizing- und Entwicklungsarbeiten in der GIZ-Umgebung nochmals angepasst werden müssen. Es sei denn, dies wurde vorher via E-Mail kommuniziert und von der GIZ akzeptiert (Releasefähigkeit).

Releases sollen einer Planung unterliegen.

3.2.12 Optionale Schnittstellenanbindung an weitere Third Party Anwendungen

Es soll möglich sein, die SaaS-Lösung gemäß Kap. 3.1.6 an weitere Quellsysteme und Anwendungen anderer Hersteller wie etwa CMDB, ServiceWare / ServiceNow, Business Process Management, ERP und weiteren Third Party Anwendungen über eine Schnittstelle zu verbinden.

3.3 Leistungen in der Implementierungsphase

Die Implementierungsphase (Testphase) wird als der ca. 6-monatige Zeitraum nach Zuschlagserteilung definiert, während dem die Betriebsbereitschaft herbeigeführt wird. Der AN muss die AG bei der Inbetriebnahme der SaaS-Lösung unterstützen und die Durchführung

von Abnahmetests ermöglichen. Abschließend sind die Leistungen durch die AG abzunehmen und die Betriebsbereitschaft festzustellen.

Der Kickoff findet innerhalb von zwei Wochen nach Vertragsschluss statt. Im Kickoff wird ein detaillierter Projektplan vom AN in Abstimmung mit der AG erstellt.

Die grundlegenden Abnahmekriterien werden nachfolgend in der Leistungsbeschreibung beschrieben. Die konkreten Abnahmekriterien der in der Leistungsbeschreibung definierten Anforderungen werden jedoch nach Bezuschlagung und Kick-off zwischen Auftraggeber und Auftragnehmer definiert. Die konkreten Abnahmebedingungen werden gem. den Anforderungen in A03_GIZ_EA_Suite _Leistungsbeschreibung und B03_GIZ_EA_Suite_Zuschlagskriterienkatalog nach Art- und Umfang definiert und werden Vertragsbestandteil.

Alle erforderlichen Meetings werden online über Microsoft Teams abgehalten.

Folgende Leistungen müssen während der Implementierungsphase erbracht werden.

3.3.1 Einrichtung der SaaS-Lösung

Der AN richtet die SaaS-Lösung ein. Tests müssen von der AG unter Mitwirkung des AN durchgeführt werden, um die Funktionalitäten und die Performanz des Systems zu überprüfen.

Aus technischer Sicht zu testen sind:

- Zugriff mit dem Edge Chromium auf die Anwendung.
- Anmeldung mit GIZ-Kennung über SAML (SSO).
- Korrekte Rechtezuordnung innerhalb der Anwendung.
- Zugriff auf Produktiv- und Testumgebung der SaaS-Lösung.

Folgende Abnahmekriterien gelten seitens der GIZ: Aus technischer Sicht muss die Authentifizierung (gem. Kap.3.2.9.4.1), das Rollen- und Berechtigungsmanagement (Kap.3.2.9.42) funktionieren und der oben genannte Edge-Browser (gem. Kap.3.2.9.4) auf das Tool zugreifen können. In der Testumgebung sind die Anforderungen aus Kap. 3.3.2 bis Kap. 3.3.6, umgesetzt und abgenommen und in der Produktivumgebung produktivgesetzt und abgenommen.

3.3.2 Einrichtung der Rollen und Berechtigungen

Der AN richtet die Rollen und Berechtigungen entsprechend den Anforderungen aus Kap. 1.4 im System ein. Der AN übergibt die Verwaltung von Rollen und Berechtigungen an die Administrator*innen der SaaS-Lösung.

Tests müssen durchgeführt werden, um die folgenden Funktionalitäten zu überprüfen:

- Einrichtung von Rollen und Berechtigungen gem. Anforderungen aus Kap. [1.4](#)
- Vergabe von Rollen und Berechtigungen für Nutzende und Nutzendengruppen
- Übereinstimmung der konkreten Darstellung für Nutzende und Nutzendengruppen mit den eingerichteten Rollen und Berechtigungen.

Folgende Abnahmekriterien gelten seitens GIZ: Die Rollen und Berechtigungen sind entsprechend Kap. [1.4](#) umgesetzt und funktionieren. Die Vergabe von Rollen- und Berechtigungen durch die Rolle Administrator funktioniert. Nutzende und Nutzendengruppen können in ihrer eigenen Ansicht im System nur die Daten einsehen und bearbeiten, für die sie eine Berechtigung erhalten haben.

3.3.3 Datenmodell-Analyse und Modellierung

Der AN analysiert das aktuelle Datenmodell zusammen mit der AG und berät hinsichtlich der Umsetzung der bisherigen Datenmodelle entsprechend den Bedarfen im neuen System.

Der AN modelliert auf Grundlage dieser Analyse und des bestehenden Datenmodells im neuen System das von der AG zukünftig genutzte Datenmodell.

Tests müssen durchgeführt werden, um die folgenden Funktionalitäten zu überprüfen:

- Kompatibilität zwischen altem und neuem Datenmodell
- Nutzbarkeit des neuen Datenmodells im neuen System

Folgende Abnahmekriterien gelten seitens der GIZ: Das neue Datenmodell wurde so modelliert, dass bestehende Daten problemlos in das neue Datenmodell überführt werden können. Das neue Datenmodell ist für alle Nutzenden entsprechend ihren Rollen und Berechtigungen einsehbar und bearbeitbar.

3.3.4 Datenmigration

In Abstimmung mit der AG wird erörtert welche Daten migriert werden müssen und welche Anforderungen diesbezüglich erfüllt werden müssen.

Die AG stellt die Daten aus dem bisher genutzten System zur Verfügung und der AN übernimmt die Datenmigration in das neue System mit dem zuvor erstellten Datenmodell.

Tests müssen durchgeführt werden, um die folgenden Funktionalitäten zu überprüfen:

- Vollständigkeit der migrierten Daten in der SaaS-Lösung
- Verfügbarkeit der migrierten Daten in der SaaS-Lösung

Folgende Abnahmekriterien gelten seitens der GIZ: Die Daten wurden entsprechend der Datenanalyse und -modellierung (Kap. 3.3.3) in das System migriert. Die Einträge sind vollständig. Es stehen alle notwendigen Sprachen, Datenkategorien und Daten zur Verfügung. Die migrierten Daten sind in der SaaS-Lösung für alle Nutzenden entsprechend ihren Rollen und Berechtigungen einsehbar, bearbeitbar, löschar und exportierbar.

3.3.5 Einrichtung der Schnittstellenanbindung zu ARIS

Sofern eine Schnittstellenanbindung zu ARIS für die Datenmigration in Kap. 3.3.4 der Leistungsbeschreibung erforderlich ist richtet der AN zwischen der SaaS-Lösung und der ARIS-Lösung (aktuell genutzte Version: 10.0.27.0.310016225) eine Schnittstelle ein, um einen Datenaustausch zwischen beiden Systemen zu ermöglichen.

In diesem Fall müssen Tests durchgeführt werden, um die folgenden Funktionalitäten zu überprüfen:

- Verfügbarkeit des Datenaustauschs zwischen SaaS-Lösung und ARIS zu den Betriebszeiten
- Übertragbarkeit von Daten aus der ARIS-Lösung in die SaaS-Lösung

3.3.6 Workflows

Der AN berät die AG technisch und fachlich zur Erstellung von Workflows im Sinne von Kap. 3.1.15 und unterstützt bei deren Einrichtung.

Unter anderem sollen folgende Workflows eingerichtet werden:

- Workflow ausgehend von der Erstellung eines neuen Eintrags durch Lesende über die initiale Prüfung durch Schreibende, die Bearbeitung des Eintrags durch den Schreibenden User bis zur Veröffentlichung (ggf. mehrsprachig).
- Workflow ausgehend vom Eingang eines Änderungsantrags durch Lesende über die initiale Prüfung durch Schreibende, die Bearbeitung des Eintrags durch den Schreibenden User bis zur Veröffentlichung (ggf. mehrsprachig).
- Workflow ausgehend von einem Kommentar durch einen beliebigen Nutzenden zum Ändern und Abstimmen bestehender Einträge unter Einbindung der dazu notwendigen Rollen (Schreibend, ggf. Administrator*in).
- Workflow zum Vervollständigen bestehender Einträge unter Einbindung der dazu notwendigen Nutzenden (Schreibend, ggf. Administrator*in).

Die konkreten Funktionalitäten und Abnahmekriterien innerhalb von Workflows werden im Kickoff sowie im Rahmen der technischen und fachlichen Beratung zwischen AN und AG definiert. Tests müssen durchgeführt werden, um zu überprüfen, ob die Workflows entsprechend den vereinbarten Funktionalitäten nutzbar sind.

3.4 Schulungen

Der AN ist verpflichtet, auf Einzelabruf der AG für Schreibende und Administratoren Rollen Schulungen durchzuführen.

Eine Schulung entspricht einer Einheit, in der alle Teilnehmer*innen der Schulung die Kenntnisse vermittelt bekommen, die sie zum Arbeiten in ihrer Rolle benötigen. Dazu zählen Vorbereitung, Durchführung und Nachbereitung sowie das Bereitstellen der Schulungsunterlagen. Die Schulungen sind entsprechend der im Preisblatt angegebenen Preisposition 6.1, 6.2, 7.3 und 7.4 abzurechnen. Die Gruppengröße soll jeweils bei bis zu 15 Teilnehmenden pro Schulung liegen.

Die Schulungen finden online statt (Online-Schulungen werden im folgenden „Webinar“ genannt). Für die Durchführung von Webinaren muss Microsoft Teams genutzt werden.

Die Schulungen finden in deutscher und ggf. in englischer Sprache statt.

Der AN stellt den Zugang zu einer Trainingsumgebung (z. B. Testumgebung) zur Verfügung, auf der die Schulungen stattfinden und die die Schulungsteilnehmenden von ihren eigenen Laptops aus aufrufen können. In konkreten Übungsszenarien können die Schulungsinhalte so von den Teilnehmenden über den eigenen Laptop nachvollzogen werden.

Bei den Schulungen handelt es sich um Standardschulungen. Die schulenden Trainer*innen des AN berücksichtigen jedoch neben den Vorkenntnissen der Mitarbeitenden auch den unternehmensspezifischen Einsatz der SaaS-Lösung in der GIZ und die damit

einhergehenden Arbeitsabläufe. Die spezifischen Ausbildungskonzepte und Schulungsinhalte für die einzelnen Zielgruppen sind mit der AG im Vorfeld abzustimmen.

3.4.1 Zielgruppen und Lernziele

Die Schulungen richten sich entsprechend der Rollenbeschreibungen aus Kap. 1.4. ausschließlich an die beiden Rollen „Schreibende + Administrator*in“.

3.4.1.1 Zielgruppe Administrator*in

Bereits während der Implementierungsphase sollen Administrator*innen im Rahmen einer Standardschulung in alle administrativen Funktionalitäten der SaaS-Lösung eingewiesen werden und diese entsprechend der Rollenbeschreibung in Kap. 1.4 eigenständig bedienen können.

Bis zu 15 Personen werden gleichzeitig geschult.

Während des Betriebs sind bei wesentlichen Funktionsergänzungen sowie bei Personalwechsel zusätzliche Schulungen nach Bedarf geplant.

3.4.1.2 Zielgruppe Schreibende

Während der Implementierungsphase sind Schulungen für Schreibende User*innen vorzusehen. In diesen Schulungen lernen sie die Funktionalitäten der SaaS-Lösung entsprechend ihrer in Kap. 1.4 beschriebenen Berechtigungen zu bedienen.

Es werden bis zu 15 Personen geschult.

Während des Betriebs sind bei wesentlichen Funktionsergänzungen sowie bei Personalwechsel zusätzliche Schulungen nach Bedarf geplant.

3.4.1.3 Zielgruppe Endnutzende (Lesende)

Endnutzende (Lesende) erhalten keine gesonderten Schulungen. Ihnen wird das Schulungsmaterial bereitgestellt, um die SaaS-Lösung entsprechend ihrer in Kap. 1.4 beschriebenen Berechtigungen zu bedienen. Die Materialien sind so bereitzustellen, dass alle Endnutzende (Lesende) ohne vertiefte Systemkenntnisse in die Lage versetzt werden, die SaaS-Lösung eigenständig aufzufinden, einzusehen, in ihren Grundzügen zu verstehen und für die eigene Aufgabenerfüllung zu nutzen.

3.4.2 Schulungsunterlagen

Die Schulungsunterlagen werden auf Deutsch und ggf. auf Englisch erstellt und in einem bearbeitbaren Format (z.B. .docx) mit jeder Schulung entsprechend dem aktuellen Funktionsumfang der SaaS-Lösung bereitgestellt. Bei Release-Anpassungen in der Implementierungsphase, und während des Betriebs werden diese Änderungen in den Schulungsunterlagen durch den AN ergänzt.

Digitale Schulungsunterlagen müssen barrierefrei sein. Bei ihrer Gestaltung sollen, die in Abschnitt 12 der DIN EN 301 549 aufgeführten Anforderungen zur Barrierefreiheit eingehalten werden.

3.4.3 Rahmenbedingungen

Zusammenfassend gelten folgende Rahmenbedingungen für die Schulungsformate:

Schulungen für Administrator*in	
Form	Webinar (online)
Durchführung	live moderiert inkl. Schulungsunterlagen
Moderation	interaktiv
Sprache der Schulung und der Schulungsunterlagen	Deutsch und ggf. Englisch
Zeitraumen	Vorschlag des AN, in Abstimmung mit der AG. In der entsprechenden Preisposition in der Anlage (B02_V0_GIZ-EA_Suite_Preisblatt) muss vom AN ein Preis pro Schulungstag inkl. Schulungsunterlagen angegeben werden.
Teilnehmendenanzahl	Bis zu 15 Personen.
Inhalte und Lernziele	Vorschlag des AN gemäß Rollenbeschreibungen in Kap. 1.4 , in Abstimmung mit der AG.

Tabelle 1: Schulung für Administrator*innen

Schulungen für Schreibende	
Form	Webinar (online)
Durchführung	live moderiert inkl. Schulungsunterlagen.
Moderation	interaktiv
Sprache der Schulung und der Schulungsunterlagen	Deutsch und ggf. Englisch
Zeitraumen	Vorschlag des AN, in Abstimmung mit der AG. In der entsprechenden Preisposition in der Anlage Preisblatt (B02_GIZ-EA_Suite_Preisblatt) muss vom AN ein Preis pro Schultag inkl. Schulungsunterlagen angegeben werden.
Teilnehmendenanzahl	Bis zu 15 Personen
Inhalte und Lernziele	Vorschlag des AN gemäß Rollenbeschreibungen in Kap. 1.4 , in Abstimmung mit der AG.

Tabelle 2: Schulung für Schreibende

3.5 Vertragsende

Der AN ist verpflichtet, die Daten der AG zum Vertragsende ohne zusätzliche Vergütung verfügbar zu machen. Dies umfasst sowohl die Daten zum Datenmodell im Format .xml oder .json als auch die Datenbankinhalte selbst sowie alle Einstellungen zu Benutzern, Berechtigungen und Workflows im Format .xlsx bzw .csv. Die Daten sind verschlüsselt an das IT-Architektur Team der AG zu übermitteln.

3.6 Optionale Leistungen

Bei Bedarf können während der Vertragslaufzeit optionale Beratungs- und Programmierleistungen u.a. zu folgenden Punkten abgerufen werden, ohne dass dies eines gesonderten Vergabeverfahrens bedarf (§ 132 Abs. 2 Nr. 1 und 2 GWB):

- Datenmodellierung
- Begriffsnetze

- Datenmigration
- Einrichtung von Rollen und Berechtigungen
- Workflows
- Integration in bestehende Systeme
- Unterstützung bei der Behebung von Problemen und Durchführung von Optimierungen
- Unterstützungsleistungen bei Release-Wechsel
- Unterstützung bei der Anpassung des Systems an neue Anforderungen, die während der Vertragslaufzeit auftauchen, z.B. das Hinzufügen von neuen Funktionen oder Modulen
- Weitere Customizing-Leistungen, falls Bedarf besteht.

Hierzu ist im Preisblatt unter Position 7.5 ein entsprechender Preis zu hinterlegen. Eine vertragliche Verpflichtung zur Abnahme dieser Leistung besteht nicht.

4. Liefergegenstände

Preis Pos.	Bezeichnung
1.	Lizenzen SaaS-Lösung inkl. Wartung, Pflege und Support (bis Ende Monat 6)
1.1	Paralleler Zugriff für 6 Lesende (Endnutzende) für eine funktionsfähige, mandantenfähige, vollständig cloudbasierte SaaS-Lösung inkl. Wartung, Pflege und Support und Betrieb gem. den Anforderungen in Kap. 1.3, 1.4, 2 und 3 der Leistungsbeschreibung.
1.2	Paralleler Zugriff für 6 Schreibende für eine funktionsfähige, mandantenfähige, vollständig cloudbasierte SaaS-Lösung inkl. Wartung, Pflege und Support und Betrieb gem. den Anforderungen in Kap. 1.3, 1.4, 2 und 3 der Leistungsbeschreibung.
1.3	Paralleler Zugriff für 6 Administrator*innen für eine funktionsfähige, mandantenfähige, vollständig cloudbasierte SaaS-Lösung inkl. Wartung, Pflege und Support und Betrieb gem. den Anforderungen in Kap. 1.3, 1.4, 2 und 3 der Leistungsbeschreibung.
2	Lizenzen SaaS-Lösung inkl. Wartung, Pflege und Support (ab Anfang Monat 7)
2.1	Zugriff für 20.000 Lesende (Endnutzende) (davon 100 Endnutzende im parallelen Zugriff) für eine funktionsfähiges, mandantenfähiges, vollständig cloudbasierte SaaS-Lösung inkl. Wartung, Pflege und Support und Betrieb gem. den Anforderungen in Kap. 1.3, 1.4, 2 und 3 der Leistungsbeschreibung.
2.2	Zusätzliche Lizenzen / Zugriff-Pakete für 50 Endnutzende im parallelen Zugriff (20.000 Endnutzende aus Position 2.1 bleiben bestehen, nur zusätzlicher paralleler Zugriff) für eine funktionsfähige, mandantenfähige, vollständig cloudbasierte SaaS-Lösung inkl. Wartung, Pflege und Support und Betrieb gem. den Anforderungen in Kap. 1.3, 1.4, 2 und 3 der Leistungsbeschreibung.
2.3	Zugriff für 500 Schreibende (davon 50 Schreibende im parallelen Zugriff) für eine funktionsfähige, mandantenfähige, vollständig cloudbasierte SaaS-Lösung inkl. Wartung, Pflege und Support und Betrieb gem. den Anforderungen in Kap. 1.3, 1.4, 2 und 3 der Leistungsbeschreibung.

2.4	Paralleler Zugriff für Administrator*innen für eine funktionsfähige, mandantenfähige, vollständig cloudbasierte SaaS-Lösung inkl. Wartung, Pflege und Support und Betrieb gem. den Anforderungen in Kap. 1.3, 1.4, 2 und 3 der Leistungsbeschreibung.
3	Lizenzpositionen für Leistungen zur Bereitstellung der SaaS-Lösung
3.1	Unternehmensweite Pauschallizenz (Flat Rate) für eine funktionsfähige, mandantenfähige, vollständig cloudbasierte SaaS-Lösung inkl. Wartung, Pflege und Support und Betrieb gem. den Anforderungen in Kap. 1.3, 1.4, 2 und 3 der Leistungsbeschreibung. Unabhängig von der Anzahl der Nutzer, Nutzerrollen sowie der Anzahl gleichzeitiger Zugriffe für eine unternehmensweite Nutzung (Alternative zu 1. und 2.)
4	Dienstleistungen in der Implementierungsphase
4.1.	Initiale Herbeiführung der Betriebsbereitschaft und Einrichtung der Rollen und Berechtigungen gem. den Anforderungen in Kap. 3.3.1 und 3.3.2 der Leistungsbeschreibung.
4.2	Analyse und Beratung zum aktuellen Datenmodell und Modellierung des bestehenden Datenmodells im neuen System gem. den Anforderungen in Kap. 3.3.3 der Leistungsbeschreibung, sofern nicht in Preisblattposition 4.1 enthalten.
4.3	Migration der Daten aus dem bisher genutzten System der AG gem. den Anforderungen in Kap. 3.3.4 der Leistungsbeschreibung, sofern nicht in Preisblattposition 4.1 enthalten.
4.4	Einrichtung von Workflows gem. den Anforderungen in Kap. 3.3.6 der Leistungsbeschreibung, sofern nicht in Preisblattposition 4.1 enthalten.
4.5	Schnittstellenanbindung zu ARIS gem. den Anforderungen in Kap. 3.3.5 der Leistungsbeschreibung, sofern für die Datenmigration in Kap. 3.3.4 der Leistungsbeschreibung erforderlich.
5	Angrenzende Dienstleistungen

5.1	Unterstützungsleistungen bei der Erstellung eines Betriebshandbuchs nach den Vorgaben der GIZ gem. den Anforderungen in Kap. 3.2.6.1 der Leistungsbeschreibung. Das Inhaltsverzeichnis ist als Anhang in Kap. 5.1 aufgeführt.
5.2	Initiale Erstellung eines Benutzerhandbuchs für die Fachseite gem. den Anforderungen in Kap. 3.2.6.2 der Leistungsbeschreibung.
6	Schulungen und Schulungsunterlagen
6.1.	Schulungen inklusive aller Schulungsunterlagen entsprechend des aktuellen Funktionsumfangs der SaaS-Lösung für die Rolle der Administrator*in gem. den Anforderungen in Kap. 1.4 und 3.4 der Leistungsbeschreibung.
6.2	Schulungen inklusive aller Schulungsunterlagen entsprechend des aktuellen Funktionsumfangs der SaaS-Lösung für die Rolle der Schreibenden gem. den Anforderungen in Kap. 1.4 und 3.4 der Leistungsbeschreibung.
6.3	Schulungsunterlagen entsprechend des aktuellen Funktionsumfangs der SaaS-Lösung für die Rolle der Endnutzenden (Lesende) gem. den Anforderungen in Kap. 1.4 und 3.4 der Leistungsbeschreibung.
7	Optionale Leistungen
7.1	Optionale Schnittstellenanbindung an ein zukünftiges BPM-Tool gemäß Kap. 3.1.6 inkl. zugehöriger Beratungsleistungen gem. den Anforderungen in Kap. 3.2.12 der Leistungsbeschreibung.
7.2	Optionale Schnittstellenanbindung an Third-Party Application gemäß Kap. 3.1.6 inkl. zugehöriger Beratungsleistungen gem. den Anforderungen in Kap. 3.2.12 der Leistungsbeschreibung.
7.3	Optionale Schulungen inklusive aller Schulungsmaterialien entsprechend dem aktuellen Funktionsumfang der SaaS-Lösung für die Rolle der Administrator*in gem. den Anforderungen in den Kap. 1.4 und 3.4. der Leistungsbeschreibung.
7.4	Optionale Schulungen inklusive aller Schulungsmaterialien entsprechend dem aktuellen Funktionsumfang der SaaS-Lösung für die Rolle der Schreibenden gem. den Anforderungen in den Kap. 1.4 und 3.4 der Leistungsbeschreibung.

7.5	Optionale Beratungs- und Programmierleistungen gem. den Anforderungen in Kap. 3.6 der Leistungsbeschreibung.
-----	--

5. Anhang

5.1 Inhaltsverzeichnis des Betriebshandbuchs

Inhaltsverzeichnis

1	Übersicht	9
1.1	Geltungsbereich	9
1.2	Zielsetzung	9
2	Systembeschreibung	10
2.1	Steckbrief	10
2.2	Schutzbedarfsfeststellung und Modellierung	11
2.2.1	Ergebnis der Schutzbedarfsfeststellung	11
2.2.2	Sicherheitsanforderungen und Modellierung	11
2.3	Datenschutz	12
2.4	Verträge, Anforderungen und Vereinbarungen	12
2.5	Lizenzmanagement	13
2.6	Rollen und Verantwortlichkeiten	13
2.7	Betriebs-, Service- und Wartungszeiten	13
2.7.1	Regelbetrieb	13
2.7.2	Besondere Vereinbarungen zu Servicezeiten	14
2.8	Technische Beschreibung	14
2.8.1	Systemkomponenten	14
2.8.2	Systemarchitektur	16
2.8.3	Datenflüsse und Schnittstellen	17
2.8.4	Weiterführende Dokumentation	17
3	Betriebsprozesse und Administration	19
3.1	Operative Aufgaben	19
3.2	Service Request Management	19
3.3	Incident- und Problem Management	19
3.4	Change Management	20
3.5	Patch Management	20
3.5.1	Meldungen und Patches der Hersteller	20
3.5.2	Patchplanung	20
3.6	Test Management	21
3.7	Monitoring und Troubleshooting	21
3.7.1	Monitoring	21
3.7.2	Ressourcen für das Troubleshooting	21
4	Systemsicherheit	23
4.1	Physische und umgebungsbezogene Sicherheit	23
4.2	Systemhärtung	23
4.3	Firewall-Regelwerk	23
4.4	Schutz vor Schadprogrammen	23
4.5	Administrativer Fernzugriff	24
4.6	Rollen und Berechtigungen	24
4.6.1	Berechtigungsrollen	25
4.6.2	Authentisierung und Autorisierung	25
4.6.3	Benutzerkonten- und Zugriffsvergabe	25
4.6.4	Service User (technische Benutzerkennungen)	26
4.7	Protokollierung	26
4.8	Datensicherung und Wiederherstellung	27
4.9	Löschen und Vernichten	28
5	IT-Notfallplanung	29
5.1	Notfallkonzept	29
5.2	Zeitkritische Ressourcen und Verfahren	29
5.3	Prüfen der Funktionsfähigkeit	29
6	Abkürzungsverzeichnis	30
7	Glossar	31
8	Anhänge	32