

Anlage TA10

Mindestanforderung an das Angebot

Diese Anforderungen verstehen sich ergänzend zur Leistungsbeschreibung des Kapitel 2 des Informationsmemorandums.

A. Cloudleistungen

1. Art der Cloud

Die angebotene Softwarelösung muss als Public-Cloud-Lösung (Ressourcen werden für eine Vielzahl nicht näher bestimmter Kunden bereitgestellt) verfügbar sein und im Auftragsfall in einer Public-Cloud-Umgebung bereitgestellt werden.

2. Leistungsort

Personenbezogene Daten des Auftraggebers dürfen ausschließlich innerhalb der EU/des EWR oder in Staaten mit einem Angemessenheitsbeschluss gemäß Art. 45 DSGVO verarbeitet werden. Für nicht-personenbezogene Daten besteht keine geografische Beschränkung.

3. Georedundanz

Der Cloud-Dienst wird abweichend vom C5-Basiskriterium PS-02 aus mindestens drei georedundanten Standorten bereitgestellt. Beim gleichzeitigen Ausfall zweier Standorte bleibt mindestens ein weiterer verfügbar. Die vereinbarte Verfügbarkeit ist einzuhalten; die Funktionsfähigkeit der Redundanz ist mindestens jährlich durch Tests und Übungen gemäß BCM-04 zu überprüfen.

4. Identitäts- und Berechtigungsmanagement (IDM)

Gemäß C5-Zusatzkriterium IDM-02 erhält der Auftraggeber einen Self-Service zur eigenständigen Vergabe und Änderung von Zugangs- und Zugriffsberechtigungen. Technische Maßnahmen verhindern die Beauftragung von Leistungen außerhalb des vertraglichen Leistungsumfangs durch Nutzer.

5. Sonstiger Nutzungsumfang/Lizenzmetrik

Der Nutzungsumfang kann jederzeit erweitert oder reduziert werden.

6. Endgeräte/Zugang

Der Zugang erfolgt webbasiert, für mobile Endgeräte optimiert und ohne Plug-ins oder Add-ons. API-Schnittstellen müssen unter Berücksichtigung des REST-Konzepts umgesetzt werden. Native Zugriffssoftware ist für PCs und Notebooks ab Windows 11 sowie als App für mobile Geräte ab iOS 16 und Android 12 vorgesehen.

Gemäß §30 Abs. 2 BSIg/NIS2 ist das zur Verfügung stellen einer Multifaktor Authentifizierung (MFA) in der angefragten Lösung für den Auftraggeber Pflicht.

7. Speicher-Größe (für Speicherung von Auftraggeberdaten)

Die Daten werden beim Auftragnehmer ohne Begrenzung des Speicherumfangs gespeichert.

8. Art der Anbindung

Die Verbindungen zum System sollen mit IPSec, TLS (mindestens in Version 1.2, vorzugsweise 1.3) und redundanten Anbindungen umgesetzt werden.

9. Datensicherung

- a. Der Auftragnehmer ist verpflichtet, in angemessener Frist auf Anforderung des Auftraggebers Daten sicher und entsprechend der zum Zeitpunkt der Löschung geltenden Standards zu löschen oder dem Auftraggeber eine entsprechende Löschmöglichkeit einzuräumen. Bei personenbezogenen Daten gelten zudem die Regelungen eines noch zu vereinbarenden Auftragsverarbeitungsvertrages (AVV). Dies gilt nicht, soweit der Auftragnehmer zur Aufbewahrung von bestimmten Daten nach dem Recht der EU oder eines Mitgliedstaats verpflichtet ist. Für den Fall einer solchen Aufbewahrungspflicht, ist der potenzielle Auftragnehmer verpflichtet, den Auftraggeber unverzüglich darüber zu informieren, die Daten sicher vor dem Zugriff Dritter zu schützen und soweit im Rahmen der gesetzlichen Aufbewahrungspflicht zulässig, nach dem jeweils aktuellen Stand der Technik verschlüsselt aufzubewahren.
- b. Soweit die Erstellung von Backups der Daten des Auftraggebers vereinbart ist, ist der Auftragnehmer verpflichtet, auf Anforderung des Auftraggebers in angemessener Frist eine Wiederherstellung von Dateien aus einem Backup auf den vom Auftraggeber gewünschten vorhandenen Stand vorzunehmen.
- c. Die Leistung ist so auszugestalten, dass die Daten des Auftraggebers entweder zu jeder Zeit selbstständig durch den Auftraggeber oder, soweit dies aus technischen Gründen nicht möglich ist, mit Unterstützung durch den Auftragnehmer aus der Cloudinfrastruktur in einem marktüblichen Austauschformat exportiert werden können. Damit muss auch der Export von vom Auftraggeber bestimmten Teilen der Daten möglich sein. Soweit die Daten verschlüsselt sind, ist diese Pflicht nur dann erfüllt, wenn der Auftraggeber über den Schlüssel verfügt. Für den Export der Daten und deren Sicherung bei dem Export ist der Auftraggeber verantwortlich. Der Auftragnehmer erstellt Backups sämtlicher Konfigurationen, Anwendungsdaten und sonstiger zur Leistungserbringung erforderlicher Daten in

einem mindestens fünf Kilometer entfernten Rechenzentrum. Backups dürfen frühestens nach einem Monat gelöscht werden. Wiederherstellungstests sind in das Notfallmanagement einzubetten; über ihre Ergebnisse ist der Auftraggeber auf Anforderung zusätzlich zum C5-Basiskriterium OPS-08 zu informieren.

10. IT-Sicherheit

Der Auftragnehmer erbringt die Leistungen unter Einhaltung des bei Vertragsschluss jeweils aktuellen Cloud Computing Compliance Criteria Catalogue - C5 (Basiskriterien). Zudem beachtet der Auftragnehmer die durch den Auftraggeber zum Vertragsinhalt gemachten Sicherheitsanforderungen, z.B. aus seiner Sicherheitsrichtlinie im Sinne des Mindeststandard(s) des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Nutzung externer Cloud-Dienste. Sofern sich der Anforderungskatalog C5 (Basiskriterien) während der Laufzeit des Vertrages ändert, wird sich der Auftragnehmer bemühen, auch die neuen bzw. geänderten Anforderungen innerhalb angemessener Frist zu erfüllen. Sollte der Auftragnehmer nicht innerhalb von zwölf Monaten (vorbehaltlich einer anderen vom Gesetzgeber vorgegebenen Umsetzungsfrist, die in jedem Fall einzuhalten ist) ab der Veröffentlichung des Nachfolgedokumentes gegenüber dem Auftraggeber auf Anforderung erklären, dass er die neuen und die geänderten Anforderungen erfüllt, hat der Auftraggeber ein mit einer Frist von einem Monat auszuübendes Sonderkündigungsrecht bezogen auf die betroffenen Leistungen. Der Auftraggeber verliert das Sonderkündigungsrecht nicht dadurch, dass er es nicht unverzüglich ausübt. Die Erneuerung eines etwaigen Testats erfolgt im üblichen Prüfungsturnus.

Folgende C5-Zusatzkriterien sind einzuhalten:

- **CRY-03:** Die privaten Verschlüsselungsschlüssel sind ausschließlich und ausnahmslos dem Auftraggeber gemäß den geltenden rechtlichen und regulatorischen Anforderungen bekannt.
- **AM-05:** Physische Assets interner und externer Mitarbeiter werden zentral verwaltet. Die Verwaltung ermöglicht die Verteilung von Software, Daten und Richtlinien sowie die Deaktivierung, Löschung oder Sperrung aus der Ferne.
- **OPS-22:** Sicherheitspatches werden ab dem Zeitpunkt ihrer Verfügbarkeit in Abhängigkeit des nach der jüngsten Version des Common Vulnerability Scoring Systems (CVSS) eingeordneten Schweregrades der dadurch adressierten Schwachstellen eingespielt:
 - Kritisch (CVSS = 9.0 - 10.0): 3 Stunden
 - Hoch (CVSS = 7.0 - 8.9): 3 Tage
 - Mittel (CVSS = 4.0 - 6.9): 1 Monat
 - Niedrig (CVSS = 0.1 - 3.9): 3 Monate

Der Auftragnehmer verfügt für die Bereitstellung der Leistung (inklusive der dazu notwendigen infrastrukturellen, organisatorischen, personellen und technischen Komponenten) über ein angemessenes, dokumentiertes und implementiertes Sicherheitskonzept und ein Informationssicherheits-Managementsystem (ISMS) jeweils gemäß ISO 27001 einschließlich eines Notfall-Managements. Das Sicherheitskonzept hat sich an ISO 27017 auszurichten. Sofern personenbezogene Daten verarbeitet werden, hat es sich zudem an ISO 27018 auszurichten.

Soweit vereinbart, weist der Auftragnehmer dies durch gültige Zertifikate oder gleichwertige Nachweise nach. Sicherheitskonzept, ISMS und Zertifikate müssen, soweit auf die zu erbringende Leistung anwendbar, diese vollumfänglich abdecken und sind entsprechend des festgelegten Prüfungsturnus im relevanten Standard zu erneuern.

Der Auftragnehmer verfügt über einen IT-Sicherheitsbeauftragten mit der erforderlichen Fachkunde und teilt dem Auftraggeber dessen Kontaktdaten auf Anforderung mit. Sicherheitsvorfälle sind unverzüglich (innerhalb von 24 Std.) dem Auftraggeber mitzuteilen. Der Auftraggeber ist registriert als besonders wichtige Einrichtung und gemäß BSIG/NIS2 §32 meldepflichtig. Dafür ist eine gesonderte Vereinbarung zur Meldepflicht bei Sicherheitsvorfällen mit dem Auftragnehmer zu schließen.

Sicherheitskonzept und Informationssicherheits-Managementsystem basieren auf ISO 27001 und BSI IT-Grundschutz in der jeweils geltenden Fassung. Das Notfallmanagement erfolgt gemäß ISO 22301. Die Umsetzung der IT-Sicherheitsvorgaben ist durch entsprechende Zertifikate nach ISO 27001 oder gleichwertige Zertifizierung nachzuweisen. Verwendete Verschlüsselungs- und Authentifikationsmechanismen sind auf Anforderung des Auftraggebers offenzulegen.

Der Auftragnehmer garantiert, dass sämtliche im Rahmen der Leistungserbringung verarbeiteten, gespeicherten oder übermittelten Daten (insbesondere KRITIS-relevante Daten) uneingeschränkt und ausschließlich dem Recht der Europäischen Union (EU) sowie dem Recht der Bundesrepublik Deutschland unterliegen. Ein Zugriff von Behörden, Gerichten oder sonstigen staatlichen Stellen aus Drittstaaten (außerhalb des EWR) auf diese Daten ist sowohl rechtlich als auch technisch lückenlos auszuschließen.

11. Protokollierung

Zu protokollieren sind:

- Zugriffe auf die genutzten Leistungen einschließlich Daten und Datensicherungen mit Angaben zu zugreifender Person, Zeitpunkt, Zugriffsart und Dauer.
- Sämtliche Zugriffe auf Infrastrukturkomponenten, insbesondere An- und Abmeldungen, Installation, Deinstallation und Änderung von Anwendungen sowie Änderungen an Berechtigungen und Benutzerverwaltung. Weitere Daten einschließlich Metadaten werden im vertraglich vereinbarten Umfang erfasst.

- Der Sicherheitsstatus des Cloud-Managementsystems hinsichtlich Vollständigkeit, Verfügbarkeit, Integrität und Vertraulichkeit der verarbeiteten Daten.
- Art und Zeitpunkt von Datensicherungen und Rücksicherungen.

Die Protokolle sind mindestens sechs Monate und revisionssicher aufzubewahren.

12. Aktualisierung

Der Auftragnehmer stellt allgemein verfügbare, vom Hersteller regulär unterstützte Programmstände bereit. Updates sowie neue Releases und Versionen sind bei Verfügbarkeit zu installieren und zu integrieren.

13. Reporting

Das Reporting umfasst sämtliche leistungsrelevanten Sicherheitsvorfälle mit Zeitpunkt, Art, Umfang und den ergriffenen Beseitigungsmaßnahmen sowie durchgeführte Backups und Datenexporte einschließlich ihrer erfolgreichen Verifikation.

Gemäß der zugehörigen Erläuterung sind Sicherheitsvorfälle unverzüglich, spätestens innerhalb von 24 Stunden, dem Auftraggeber mitzuteilen. Hierzu ist eine gesonderte Vereinbarung zur Meldepflicht bei Sicherheitsvorfällen mit dem Auftragnehmer zu schließen.

B. Weitere Leistungen

1. SAP-Schnittstelle

Die angebotene WFM-Lösung muss über eine Schnittstelle an das SAP-S/4HANA-System des Auftraggebers angebunden werden. Die Schnittstelle muss die durchgängige Bearbeitung der in der Leistungsbeschreibung festgelegten Geschäftsprozesse sowie den hierfür erforderlichen bidirektionalen Datenaustausch ermöglichen. Maßgeblich sind die in den Vergabeunterlagen beschriebene SAP-Systemlandschaft und die festgelegten Integrationsanforderungen.

2. Deutschsprachiger Support und deutschsprachige Software

Der Support für Anwender und Anwendungsadministratoren ist in deutscher Sprache zu erbringen. Die hierfür eingesetzten Personen mit unmittelbarem Kontakt zum Auftraggeber müssen über Deutschkenntnisse in Wort und Schrift mindestens auf dem Niveau C1 des Gemeinsamen Europäischen Referenzrahmens für Sprachen (GER) verfügen. Dies umfasst insbesondere die verständliche und präzise Kommunikation komplexer fachlicher und technischer Sachverhalte.

Alle für Anwender und Anwendungsadministratoren vorgesehenen Bedienoberflächen der angebotenen WFM-Lösung müssen vollständig in deutscher Sprache verfügbar sein.

Dies umfasst insbesondere Menüs, Dialoge, Bedienhinweise, nutzergerichtete System- und Fehlermeldungen sowie die für Bedienung und Anwendungsadministration bereitgestellten Hilfetexte und WFM-Handbücher.

Technische Bezeichnungen, Programmierschnittstellen sowie ausschließlich zur technischen Diagnose bestimmte Protokoll- und Fehlermeldungen dürfen in englischer Sprache vorliegen, sofern dadurch die deutschsprachige Bedienung und Anwendungsadministration nicht beeinträchtigt wird.

3. Benutzer- und Rollenverwaltung / Performance

Die angebotene Lösung muss mindestens 300 namentlich angelegte Benutzer verwalten können, einschließlich interner Mitarbeiter und Benutzer externer Dienstleister. Jedem Benutzer müssen gleichzeitig mehrere Rollen zugeordnet werden können. Die Berechtigungen ergeben sich aus der Gesamtheit der zugeordneten Rollen. Es gibt keine Beschränkung der Anzahl zuordenbarer Rollen je Benutzer

Die Lösung muss bei dieser Benutzeranzahl und bei gleichzeitiger Nutzung über alle Zugriffsebenen (Desktop, mobile App, Portal) einen performanten, unterbrechungsfreien Arbeitsablauf gewährleisten. Die Arbeitsfähigkeit der Anwender darf durch Antwortzeiten nicht wesentlich beeinträchtigt werden.

4. Mandantenfähigkeit

Die angebotene Lösung muss mandantenfähig aufgebaut sein. Innerhalb eines IT-Systems (einer Instanz der Cloud-Lösung) müssen mindestens drei organisatorische Einheiten als eigenständige Mandanten betrieben werden können, z. B. DVV, Netze Duisburg und [weitere Gesellschaft]. Die Anzahl der Mandanten muss später erweiterbar sein, ohne dass eine weitere Instanz nötig wird.