

B. Leistungsbeschreibung

Inhaltsverzeichnis

I.	Vertragspartner	1
II.	Gegenstand der Beschaffung	1
III.	Beschreibung des Anwendungs- / Einsatzbereiches	1
IV.	Rahmenbedingungen	2
1	Zeitplanungen	2
2	Allgemeine Anforderungen	2
3	Datenschutz	5
4	Lizenzierung & Kosten	5

I. Vertragspartner

Der Deutsche Gesetzliche Unfallversicherung e. V. (AN, im Folgenden: AG) ist der Spitzenverband der gewerblichen Berufsgenossenschaften und der Unfallversicherungsträger der öffentlichen Hand. Die neun gewerblichen Berufsgenossenschaften sind nach Branchen orientiert. Die Unfallversicherungsträger der öffentlichen Hand gliedern sich in 16 Unfallkassen, drei Gemeindeunfallversicherungsverbände, vier Feuerwehr-Unfallkassen sowie die Unfallversicherung Bund und Bahn.

Der Verband nimmt die gemeinsamen Interessen seiner Mitglieder wahr und fördert deren Aufgaben zum Wohl der Versicherten und Unternehmen. Er vertritt die gesetzliche Unfallversicherung gegenüber Politik, Bundes-, Landes-, europäischen und sonstigen nationalen und internationalen Institutionen sowie Sozialpartnern.

II. Gegenstand der Beschaffung

Der AG beabsichtigt den Erwerb einer cloudbasierte Backup- und Wiederherstellungslösung (SaaS) für Jira, Confluence und Microsoft 365 (Office 365) sowie Entra ID. Ziel ist die Bereitstellung einer sicheren, skalierbaren, revisionssicheren und gesetzeskonformen Datensicherung.

III. Beschreibung des Anwendungs- / Einsatzbereiches

Der AG nutzt verschiedene Cloud-Lösungen wie Microsoft Teams, SharePoint Online und OneDrive for Business. Zusätzlich kommen die Sicherheit- und Compliance-Dienste der Microsoft-365-Plattform zum Einsatz. Diese ermöglichen den Schutz, die Überwachung und die gesetzeskonforme Aufbewahrung von Benutzeridentitäten, Dateien, Teams-Inhalten sowie Geräten und Anwendungen.

Vorhaben: Backup Cloud to Cloud (26_EU_031), Version 1

Darüber hinaus werden Jira und Confluence zur strukturierten Projektsteuerung, Dokumentation und Zusammenarbeit eingesetzt.

Exchange Online ist als zukünftige Lösung vorgesehen, um die bestehenden E-Mail-Strukturen in die Microsoft-365-Umgebung zu integrieren und eine zentrale sowie effiziente Verwaltung sicherzustellen.

IV. Rahmenbedingungen

1 Zeitplanungen

Die technische Aktivierung des SaaS-Service müssen spätestens innerhalb von 4 Wochen nach Zuschlag erfolgen.

Der AG versteht unter technische Aktivierung die vollständige Implementierung der Backup- und Wiederherstellungslösung für die genannten Cloud-Services in den Betrieb.

2 Allgemeine Anforderungen

Dieses Kapitel beschreibt in den folgenden Abschnitten die zu erfüllenden Anforderungen, die an die zu beschaffende SaaS Lösung gestellt werden.

2.1 Grundsätzliche Anforderungen

Der AN hat eine cloudbasierte, zentrale Verwaltungsplattform bereitzustellen, die die Sicherung und Wiederherstellung von Daten aus mehreren SaaS-Anwendungen ermöglicht. Die Lösung muss eine einheitliche, integrierte Managementoberfläche bieten, über die sämtliche Backup- und Restore-Prozesse für folgende Systeme zentral gesteuert werden können: Jira, Confluence und Microsoft 365 (Office 365) sowie Entra ID.

Die Lösung muss automatisierte Backups, vollständige und granulare Restores, unabhängige und unveränderbare Datenspeicherung, sowie Funktionen zur Sicherstellung von Datenschutz, Integrität und Nachweisführung bereitstellen.

- Automatisierte vollständige Sicherung aller Daten und Metadaten aus Jira, Confluence und Microsoft 365 (inkl. Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams, Planner/Groups sowie Entra ID).
- AG versteht unter granulare Wiederherstellung einzelner Elemente, Tickets/Issues, Seiten/Spaces, einzelne E-Mails, Ordner, Dateien, Kalendereinträge in Outlook, Teams Chats, M365 Gruppen, Planner sowie vollständige Mandanten-/Site-/Space-Restores die komplett wiederhergestellt werden.
- Such- und Filterfunktionen über alle gesicherten Daten hinweg mit Vorschau/Metadatenansicht.

2.2 Technische Anforderungen

Die Lösung muss über folgende Funktionen verfügen:

Vorhaben: Backup Cloud to Cloud (26_EU_031), Version 1

- Automatisierte Sicherungen müssen mindestens einmal täglich erfolgen. Zusätzlich müssen manuelle Sicherungen durch den AG auslösbar sein.
- Zeitpunktgenaue Wiederherstellung (Point-in-Time Restore) im Rahmen der verfügbaren Sicherungspunkte (Hot Storage).
- Granulare sowie vollständige Wiederherstellungen; Wiederherstellung in ursprüngliche Ziele, sofern fachlich zulässig.
- Der AN muss die Durchführung von Wiederherstellungstests ermöglichen. Für Wiederherstellungstests dürfen keine zusätzlichen Kosten anfallen.
- Für die Datensicherung muss unbegrenzter Speicherplatz pro User zur Verfügung stehen.
- Die Lösung muss Überwachungs- und Benachrichtigungsfunktionen bereitstellen, um sicherungsrelevante Auffälligkeiten frühzeitig zu erkennen. Hierzu gehören mindestens:
 - o Überwachung des Erfolgs- und Fehlerstatus von Sicherungs- und Wiederherstellungsprozessen.
 - o Benachrichtigungen bei fehlgeschlagenen oder unvollständigen Sicherungen,
 - o Erkennung und Meldung außergewöhnlicher Änderungen im Sicherungsumfang (z. B. ungewöhnlich hohe Lösch-, Änderungs- oder Verschlüsselungsraten).
 - o Protokollierung sicherungsrelevanter Ereignisse.
 - o Konfigurierbare Alarmierungen per E-Mail oder über vergleichbare Benachrichtigungsmechanismen.

2.3 Datenverschlüsselung und Sicherheit

Der AN hat sicherzustellen, dass sämtliche im Rahmen des Cloud-Backup-Dienstes verarbeiteten Daten nach dem Stand der Technik wirksam verschlüsselt werden. Dies umfasst mindestens folgende Anforderungen:

Verschlüsselung während der Übertragung (In-Transit)

- Alle Daten müssen während der Übertragung zwischen Kundenumgebung, Plattform und Speicherorten durch Transportverschlüsselung geschützt werden.
- Es ist mindestens ein aktuelles und sicheres Protokoll wie TLS 1.2 oder höher einzusetzen.

Verschlüsselung bei Speicherung (At-Rest)

- Alle gespeicherten Daten des AG müssen mittels eines symmetrischen AES-256 geschützt werden.
- Die Lösung muss sämtliche Daten während der Übertragung und im Ruhezustand verschlüsseln. Das eingesetzte Verschlüsselungs- und Schlüsselmanagementverfahren ist vom Anbieter zu beschreiben (deutsch oder englisch) und mit dem Angebot einzureichen.

Vorhaben: Backup Cloud to Cloud (26_EU_031), Version 1

- Der Dienstleister hat sicherzustellen, dass weder administrative Benutzer noch Systemprozesse des Dienstleisters unautorisierten Zugriff auf die Schlüsselinformationen erhalten. Die Schlüsselverwaltung muss nach dem Stand der Technik erfolgen und den Einsatz etablierter Key-Management-Systeme mit rollenbasierter Zugriffskontrolle, Auditierung und Schlüsselrotation unterstützen.

Die Datensicherung muss wirksam gegen Ransomware geschützt sein. Eine Veränderung oder Löschung der Sicherungsdaten im Regelbetrieb muss ausgeschlossen sein.

Der Wiederherstellungsservice muss gem. den SLA für alle Daten zu jederzeit möglich sein. Dies gilt insb. auch während einer laufenden Ransomware-Attacke gegen den AG.

Es muss eine vollständig revisionssichere, unveränderbare und nicht löschbare Protokollierung aller sicherungsrelevanten Aktionen gewährleistet sein.

2.4 Administrative Zugänge

Für sämtliche administrativen Konten ist die Nutzung einer MFA (Multi-Factor-Authentifizierung) verpflichtend.

2.5 Support und Instandsetzung

Der AN ist für die Aufrechterhaltung der Betriebsbereitschaft entsprechend der vereinbarten Verfügbarkeit bzw. Instandsetzungszeiten während der Vertragslaufzeit verantwortlich. Die Backuplösung muss eine **hohe Verfügbarkeit von 99,9% im Jahresmittel (VK 2)** gewährleisten.

Der AN muss über ein Störungsmanagementsystem (Ticket-System) zur Unterstützung der Serviceprozesse verfügen. In dem eingesetzten Verfahren müssen alle Abläufe von der Annahme von Störungsmeldungen, deren Bestätigung gegenüber dem Melder sowie die Abläufe bis hin zur Behebung der Störung und dessen Dokumentation erfasst werden. Für alle Meldewege ist anzugeben auf welchem Wege diese zu welchen Zeiten und unter welchen Kontaktdaten zu erreichen sind.

Der AN stellt einen deutsch- oder englischsprachigen 24/7-Support und einen deutschsprachigen Support mindestens zu Geschäftszeiten zur Verfügung.

3 Datenschutz

Der AN verpflichtet sich bei der Datenverarbeitung iSd Art. 4 Nr. 2 DSGVO auf die Einhaltung des Daten- und des Sozialdatenschutzes. Die Parteien schließen einen Auftragsverarbeitungsvertrag gemäß Artikel 28 DSGVO und § 80 SGB X. Verantwortliche Stelle für die Datenverarbeitung iSd Art. 4 Nr. 7 DSGVO ist der AG. Der AN fungiert als Auftragsverarbeiter iSd Art. 4 Nr. 8 DSGVO. Der AN verpflichtet sich die Einhaltung der sozial-/datenschutzrechtlichen Bestimmungen nachzuweisen und gibt Auskunft über deren Umsetzung (siehe Anlage 1 zum Auftragsverarbeitungsvertrag).

4 Lizenzierung & Kosten

Der AN hat ein nutzer- bzw. objektbasiertes Lizenzmodell bereitzustellen, bei dem die Anzahl der zu lizenzierenden Einheiten klar und transparent nachvollziehbar ist.

Für die Datenspeicherung inaktiver Nutzerkonten, insbesondere ehemaliger Mitarbeitender, dürfen keine zusätzlichen Kosten anfallen; eine zusätzliche Lizenzierung darf hierfür nicht erforderlich sein.

Eine Limitierung, Kontingentierung oder mengenabhängige Kostenmodelle für Speicherplatz sind nicht zulässig.

Die Positionen O im Preisblatt sind optionale Leistungen ohne Abrufverpflichtungen (C EVB-IT Cloud Nr. 3.3). Der Abruf erfolgt in Textform, der AN bestätigt dem AG den Abruf innerhalb von 2 Werktagen und muss die Bereitstellung der O Lizenzen innerhalb von 7 Werktagen nach Abruf bereitstellen. Die Abrechnung der O Lizenzen erfolgt anteilig für die verbleibende Vertragslaufzeit in Bezug auf Basis der vereinbarten Einheitspreise in Dok. H.

5 Vertragsende, Aufbewahrung & Exit

Ein Exit aus dem Dienst muss jederzeit möglich sein. Der AG muss seine Daten vollständig, ohne Zusatzkosten und ohne Anbieterabhängigkeit exportieren können. Es gelten Ziff 7 EVB-IT AGB.