

Leistungsbeschreibung

Vergabe-Nr. 1419-0526

Beschaffung: IT-Exchange Archivierungslösung



Kaufmännische Krankenkasse - KKH
Karl-Wiechert-Allee 61
30625 Hannover

Inhalt

| | |
|--|---|
| 1. Zielsetzung & Kontext..... | 3 |
| 2. Leistungsumfang | 3 |
| 2.1 Architektur & Integration | 3 |
| 2.2 Archivierungs- & Retentionsfunktionen | 3 |
| 2.3 Benutzerfreundlichkeit (Endanwender & Admin)..... | 4 |
| 2.4 Sicherheit, Datenschutz & Compliance | 4 |
| 2.5 Betrieb, Service & Wartung | 4 |
| 2.6 Schnittstellen & Integration..... | 5 |
| 2.7 Lizenzierung & Nutzungsrechte..... | 5 |
| 3. Projektdurchführung (Vorgehen, Meilensteine, Deliverables)..... | 6 |
| 4. Rollen & Verantwortlichkeiten | 6 |
| 5. Erfolgs- und Qualitätskriterien (KPIs)..... | 6 |
| 6. Abnahmekriterien | 6 |
| 7. Annahmen, Abgrenzungen & Risiken | 7 |
| 8. Dokumentation, Schulung & Übergabe | 7 |

1. Zielsetzung & Kontext

Die KKH führt eine cloudbasierte E-Mail-Archivierungslösung ein, um eine revisionssichere, rechtskonforme und hochverfügbare Ablage aller ein- und ausgehenden E-Mails aus einer hybriden Exchange-Infrastruktur (Exchange SE On-Premise und Exchange Online) sicherzustellen.

Besonderer Fokus liegt auf:

- Schutz von Sozialdaten gemäß SGB X sowie DSGVO (Art. 6, 9, 28), inkl. strenger Zugriffskontrollen.
- Rechts- und Revisionssicherheit von E-Mails sowie zugehöriger Logs.
- KRITIS-Anforderungen nach BSI-Gesetz (§ 30 Abs. 1 BSIG) und einschlägigen Standards (BSI C5-Typ-2-Testat, C5GleichwV, ISO 27001, B3S-GKV/PV).
- Produktiver Betrieb mit klaren SLAs, Audits und Nachvollziehbarkeit (Audit-Trail).
 - Genauere Informationen zu SLAs sind den Allgemeinen Rahmenbedingungen zum IT-Service-Management zu entnehmen

Zentrale Anforderungen:

- Integration: Nahtlose Anbindung an die bestehende hybride Exchange-Infrastruktur (On-Premise & Online).
- Postfach-Entlastung: Die Lösung muss sicherstellen, dass archivierte E-Mails für den Endanwender nahtlos und ohne Medienbruch zugreifbar bleiben, auch nachdem diese aus dem primären Postfach ausgelagert wurden. (Technische Umsetzung z. B. via Link, Shortcut oder transparentem Zugriff per Add-On / Browseranbindung ist dem Bieter überlassen).
- Benutzerfreundlichkeit: Intuitive Nutzung in Outlook und webbasierten Clients, schlanke Administration.
- Rechtskonformität & Sicherheit: DSGVO, SGB X, GoBD, BSI-KritisV/§ 30 Abs. 1 BSIG.

2. Leistungsumfang

2.1 Architektur & Integration

- Bereitstellungsmodell: Die Lösung wird als Cloud-Service (SaaS) bereitgestellt. Der Anbieter übernimmt den Betrieb der Infrastruktur.
- Hybrid-Unterstützung: Native Unterstützung für die Archivierung von E-Mails aus Exchange Online und Exchange On-Premise Umgebungen.
- Ingestion: Automatisierte, kontinuierliche Erfassung aller relevanten E-Mails inkl. Anhänge. Der Bieter beschreibt das vorgesehene Verfahren (z. B. Journaling, Transport-Regeln, API-basierte Ingestion, MX Redirect) und garantiert die Vollständigkeit der Zustellung.
- Authentifizierung: Unterstützung moderner Authentifizierungsmethoden (OAuth2/Modern Auth) und sichere Kommunikation (TLS).
- Migration: Unterstützung bei der Migration bestehender historischer E-Mail-Bestände (inkl. PST/Archivpostfächer) in das revisionssichere Ziel.
- Skalierbarkeit: Die Lösung muss horizontale Skalierung für große Mail-Volumina gewährleisten.
- Netzanforderungen: Der Anbieter stellt sicher, dass alle erforderlichen betrieblichen und netzwerkseitigen Voraussetzungen (Ports, DNS, Proxy, Bandbreite) für den zuverlässigen Betrieb der Cloud-Lösung erfüllt sind.

2.2 Archivierungs- & Retentionsfunktionen

- Regelbasierte Archivierung: Automatisierte Archivierung aller ein-/ausgehenden und internen E-Mails basierend auf Policies pro z.B. Organisationseinheit, Abteilung oder Rolle.

- Revisionssicherheit: Speicherung in einem unveränderbaren Format (WORM-Prinzip oder gleichwertig). Sicherstellung von Integrität, Versionierung und Chain-of-Custody.
- Aufbewahrungsfristen: Konfigurierbare Fristen gemäß GoBD/HGB/AO sowie fachlichen Vorgaben der KKH. Differenzierung nach z.B. Inhalt, Metadaten oder pro Postfach/Usergruppe.
- Zugriff & Entlastung: Sicherstellung, dass archivierte Nachrichten für den Anwender transparent und performant abrufbar sind, auch nach Entfernung aus dem Primärpostfach.
- Suche & Wiederherstellung: Volltextindex über Betreff, Body & Anhänge. Self-Service-Restore (zurück ins Postfach/als EML/PST) und Massen-Export.
- Optional: Compliance-Funktionen: Unterstützung von Legal Hold und eDiscovery-Funktionen.
- Optimierung: Deduplizierung & Komprimierung zur Speicheroptimierung (sofern bei der angebotenen Lösung anwendbar und/oder herstellerseitig empfohlen).

2.3 Benutzerfreundlichkeit (Endanwender & Admin)

Endanwender:

- Nahtloser Zugriff über den primären E-Mail-Client (Outlook) und/oder webbasierte Clients (OWA).
- Keine zwingende Client-Installation erforderlich (Add-In optional).
- Schnelle Suche (inkl. Vorschau), deutschsprachige UI.
- Self-Service-Funktionen: Wiederherstellung, Export, Suche.

Administratoren/Revision/Datenschutz:

- Zentrale Web-Konsole für Richtlinien, Monitoring, Reporting und Verwaltung.
- Rollen- & Rechteverwaltung (RBAC) mit Anbindung an das Active Directory der KKH.
- Gegebenenfalls Vier-Augen-Prinzip für sensible Aktionen (z. B. eDiscovery-Zugriffe).
- Reporting & KPIs in Absprache mit der KKH: z.B. Archivierungsquote, Ingestion-Latenz, Speicherauslastung, Audit-Einsichten.

2.4 Sicherheit, Datenschutz & Compliance

- Gesetzliche Vorgaben: Einhaltung von DSGVO, SGB X, GoBD, § 30 Abs. 1 BSIg, BSI-KritisV.
- Hosting: Ausschließlich in EU-Rechenzentren (ISO 27001-Zertifizierung, BSI C5-Typ2-Testat oder Meilensteinplan gemäß C5-Gleichwertigkeitsverordnung).
- Kryptografie: Transportverschlüsselung (TLS) und Verschlüsselung ruhender Daten gemäß aktuellem Stand der Technik (BSI TR-02102).
- Schlüsselmanagement: Unterstützung für Customer-Managed Keys (CMK/BYOK) bevorzugt.
 - Auch anbieterspezifische Keyverwaltung möglich.
- Datenschutz: Datensparsamkeit, strikte Trennung von Sozialdaten und Telemetriedaten.
- Zugriffsschutz: MFA, bedingter Zugriff, Privileged Access Management für Administratoren, Session-Timeouts.
- Protokollierung: Fälschungssichere Audit-Logs
 - Export an SIEM wünschenswert
- Meldepflichten: Einhaltung der behördlichen Meldepflichten (§ 30 BSIg).

2.5 Betrieb, Service & Wartung

- Verfügbarkeit: Cloudbetrieb mit SLA $\geq 99,9$ % (Monatsbasis).
- Support:
 - Deutsche Sprache.

- Zentralisierter Single Point of Contact für die gesamte Lösung.
- 24/7-Support für kritische Störungen (Priorität P1).
- Unterstützung bei Updates/Upgrades und Kompatibilitätsproblemen.
- Weitere Informationen sind den Allgemeinen Rahmenbedingungen IT-Service-Management zu entnehmen.
- Wartung: Hersteller führt Patches/Upgrades kontrolliert durch (Change-Fenster, Vorab-Info).
- Monitoring: End-to-End-Überwachung der Lösung. Die Lösung muss Schnittstellen zur Anbindung an externe Monitoring-Systeme bieten.
- Sicherheit: Mehrzonen-Redundanz, Immutability-Konzepte, regelmäßige Restore-Tests.
- Notfallmanagement: Vorhandenes Konzept für Backup, Restore, Failover, RTO/RPO, welches mindestens folgende Punkte erfüllt:
 - Rollen und Verantwortlichkeiten
 - Klassifizierung von Notfällen und festgelegte Reaktionswege
 - Kommunikationsplan
 - Angaben zu RTO und RPO
 - Vorgehen zur Eindämmung und Schadensbegrenzung
 - Backup Strategie
 - Monitoring und Früherkennung

Wiederherstellungszeiträume können dem Dokument Allgemeine Rahmenbedingungen IT Service Management unter Punkt 2.6.1 entnommen werden.

2.6 Schnittstellen & Integration

- Identity: Anbindung an Azure AD / Entra ID und On-Premise Active Directory (Hybrid) via SSO (SAML/OAuth2/OIDC).
- Export von Audit- und Betriebslogs (z. B. Syslog, CEF)
- ITSM: Möglichkeit zur Integration in das bestehende Ticketing-System (aktuell Ivanti) für Incident/Change-Prozesse.
- Exit-Strategie: Vollständiger Export aller Daten in offenen, marktüblichen Formaten (z. B. EML, MBOX, CSV/XML) bei Vertragsende. Nachweis der Integrität (Hash-Werte).

Weitere Informationen zur Integration des KKH-Ivanti und den Change-Prozessen sind den Allgemeinen Rahmenbedingungen IT-Service-Management zu entnehmen.

2.7 Lizenzierung & Nutzungsrechte

- Modell: Die Leistung erfolgt auf Basis eines Service-Abonnements (SaaS). Es werden keine separaten Client-Lizenzen erworben.
- Basis:
 - Nutzerbasierte Abrechnung (Anzahl User)
 - oder Nutzerbasierte Abrechnung (Anzahl Postfächer)
 - oder Abrechnung nach verwendetem Speicherkontingent
- Inhalt: Die Lizenz umfasst Nutzung, Betrieb, Updates und Patches.
- Flexibilität: Anpassung der Nutzeranzahl bzw. des Speicherplatzes während der Laufzeit (monatlich/ quartalsweise) möglich.
- Bei Nutzerbasierter Abrechnung ist ein Prozess für den Umgang mit ausgeschiedenen Benutzern bzw. deren Daten in der Archivierung zu deklarieren.

3. Projektdurchführung (Vorgehen, Meilensteine, Deliverables)

1. Planung & Konzeption: Ist-Aufnahme, Zielbild, Security/Privacy-by-Design, Policy-Design.
Deliverables: Fach- & IT-Konzept, Architekturdiagramm, Migrationskonzept.
2. Implementierung & Integration: Einrichtung, Connectoren, Journaling, Auth-Flows.
Deliverables: Konfigurationsdokumentation, Betriebs-/Sicherheitskonzept, Runbooks.
3. Migration historischer Bestände: Ca. 12 TB, revisionssichere Übernahme.
Gegebenenfalls einfache Erstarchivierung der Postfächer.
Deliverables: Migrationsberichte, Integritätsnachweise.
4. Test & Abnahme: Funktion (Zugriff/Entlastung, Suche, Restore), Sicherheit, Leistung.
Deliverables: Testprotokolle, Abnahmeempfehlung.
5. Schulung & Go-Live: Admin-/Power-User-Training, Endanwender-Guides, Rollout.
Deliverables: Schulungsunterlagen, Betriebsfreigabe, Go-Live-Report.

Der initial geschätzte Projektaufwand beträgt 30PT.

Die Abrechnung erfolgt auf Basis nachvollziehbarer Leistungsnachweise nach tatsächlichem Aufwand.

4. Rollen & Verantwortlichkeiten

KKH (Auftraggeber): Budget, Priorisierung, Abnahme, Benennung Fach-Owner, Bereitstellung von Testumgebungen und Ansprechpartnern (Datenschutz, Sicherheit).

Anbieter: Lieferung der Lösung, Betrieb (SLA), Security-Nachweise, Support, Durchführung von Schulungen.

KKH (IT/Security): Konfiguration der Connectoren, Transportregeln, SIEM-Anbindung, Auditierung.

5. Erfolgs- und Qualitätskriterien (KPIs)

- Integration: Ingestion-Fehlerquote < 0,1 % (Monat), Zustelllatenz im Zielkorridor.
- Compliance: Nachweis DSGVO/SGb X/GoBD; vollständige Audit-Trails.
- KRITIS: § 8a-relevante Kontrollen nachweislich implementiert; SIEM-Feeds / Automatische Reports aktiv.

Weitere KPI und Report-Anforderungen sind den Allgemeinen Rahmenbedingungen IT-Service-Management zu entnehmen.

6. Abnahmekriterien

- Funktionalität: Erfolgreicher Test der Postfach-Entlastung und des nahtlosen Archivzugriffs (inkl. Restore).
- Rechtskonformität: Nachweise DSGVO/SGb X/GoBD (AVV, TOMs, DSFA, Löschkonzept).
- Sicherheit: MFA/RBAC aktiv, Audit-Logs vollständig, SIEM-Anbindung / Reporting verifiziert.
- Betrieb: SLA/Monitoring aktiv, Runbooks übergeben, Supportprozesse getestet.
- Dokumentation: Vollständige technische und operative Dokumentation übergeben.

7. Annahmen, Abgrenzungen & Risiken

Annahmen:

- Erforderliche Lizenzen/Connector-Rechte für Exchange (Online/On-Prem) sind bei der KKH verfügbar.
- Ausreichende Netz-/Bandbreiten-Ressourcen und Zertifikate vorhanden.
- KKH stellt Test-/Pilotgruppen und Ansprechpartner für Datenschutz/Revision.

Abgrenzungen (Out-of-Scope):

- Änderung fachlicher E-Mail-Prozesse außerhalb der Archivierung.
- Drittsystem-Customizing jenseits dokumentierter Schnittstellen.
- Migration defekter/inkonsistenter Quellen ohne vorherige Bereinigung.

Risiken & Gegenmaßnahmen:

- Verschlüsselte Mails (S/MIME): Definition von Schlüsselmanagement/Decryption-Prozessen erforderlich.
- Große historische Bestände: Phasen-Migration, Deduplizierung, Throttling.
- Change-Fatigue: Kommunikations- & Schulungspaket, Pilot/Hyper-Care.

8. Dokumentation, Schulung & Übergabe

- Dokumentation, Schulung und Übergabe haben in deutscher Sprache vorzuliegen / durchgeführt zu werden
- Technische Dokumentation: Architektur, Konfiguration, Security-/Betriebskonzepte, Schnittstellen, Datenflüsse.
- Betriebsunterlagen: Runbooks (Störungsbehebung, Restore, Notfallverfahren), Wartungspläne, KPI-Reports.
- Schulungen: Admin/Support (Hands-on), Endanwender-Guides.
- Verfahrensdokumentation: Der Anbieter erstellt und übergibt eine GoBD-konforme Verfahrensdokumentation, die mindestens technische Architektur, Archivierungs-/Löschkonzepte, Rollenkonzepte und Notfallpläne umfasst.