
Whitepaper

Rhenus Cloud Archiv



INHALTSVERZEICHNIS

1	Das Wichtigste zuerst	3
2	Warum sich für das Rhenus Cloud Archiv entscheiden?	4
2.1	Vorteile für den Anwender	4
2.2	Key-User-Support	4
2.3	Datenimport	5
2.4	Datensicherung und Datensicherheit	5
2.5	Authentifizierung	7
2.6	Datenbank und Recherche	7
2.7	Löschen	8
2.8	Verfügbarkeit	9
2.9	Export	10

1 Das Wichtigste zuerst

- DS-GVO-konform (privacy-by-design)
- Cloud-basierend (eigene deutsche Rechenzentren Tier 3, ISO 27001-zertifiziert)
- Stets verschlüsselte Kommunikation
- Multi-Mandantenfähig
- Universeller Webclient
- Intuitive, blitzschnelle Volltextsuche
- Versionierung der Dokumente
- Verschiedene Logging Level (Wer hat wann was verändert?)
- User-Anbindung durch eine Vertrauensstellung an Kunden-AD möglich
- Integrierte Dokumentenanzeige für verschiedene Dateiformate
- Indexierung von Volltext, Feldern und Anhängen
- Unabhängig vom ERP-System
- Automatische, dienstbasierte Datei- und Ordner-Archivierung
- Einhängen als virtuelles Laufwerk – der User merkt keinen Unterschied
- Clientbasierte E-Mail-Archivierung
- Serverbasierte E-Mail-Archivierung
- Nahtloser Zugriff auf archivierte E-Mails in MS Outlook
- Verschiedene 2-Faktor-Authentifizierungen möglich

2 Warum sich für das Rhenus Cloud Archiv entscheiden?

Archivlösungen stehen immer wieder auf dem Prüfstand – zumindest sollten sie es.

Fortschreitende Digitalisierung, exponentielles Datenwachstum und neue Technologien auf der einen Seite – Effizienzdruck und Compliance-Anforderungen auf der anderen. Das digitale Unternehmensarchiv muss immer schneller, flexibler, benutzerfreundlicher, performanter, skalierbarer, sicherer und ressourcenschonender werden – und zwar am besten alles gleichzeitig: ohne Aufwand oder Unterbrechungen im laufenden Betrieb.

Die serviceorientierte Cloud-Architektur erlaubt es uns Ihnen stets moderne Technologie bereitzustellen, ohne aufwändige Migrations- und Upgrade Projekte.

2.1 Vorteile für den Anwender

- Universeller Web-Client
- Zugang unabhängig vom ERP-System
- Intuitive Benutzeroberfläche erleichtert die Bedienung
- Viele praktische und intuitive Suchhilfen unterstützen die Arbeit
- Konsequente Volltextsuche (Google-typisch) mit blitzschneller Auto-Complete-Funktion
- Schemafreie Trefferliste
- Client-unabhängiges Rendering für schnelle und exakte Dokumentenansicht
- Preview-Funktion direkt aus der Trefferliste
- Kategorienfilter
- Inhaltsorientierter Aktenbaum
- Möglichkeit flexibler Input-Szenarien (Scan, Web-Scan, Mail, Office, PDF)

2.2 Key-User-Support

Rhenus bietet für alle geschulten Anwender (sogenannte Key-User) System-Support über Telefon und Ticketsystem. So können Sie Ihre Mitarbeiter entlasten und stellen sicher, dass eine stets professionelle Unterstützung der Anwender gegeben ist.

2.3 Datenimport

Zwei Komponenten:

- Datenannahme der Dokumente und Anlagen
- Anreicherung mit Indexwerten (optional)

Entgegengenommen werden praktisch alle Dateiformate, unabhängig davon, ob sie sich im Archiv-internen Client anzeigen lassen oder nicht. So kann man zu Auftragsbestätigungen z.B. die passenden CAD-Pläne mitarchivieren.

Unzählige Wege:

- Physisch per Festplatte oder USB-Stick
- SFTP-Import
- Verzeichnisimport (auch Hotfolder möglich)
- ERP-System-Schnittstellen
- Archiv-Systemschnittstellen
- DMS-Schnittstellen
- Manueller Upload
- Webservice-basiert (REST-API)
- ...

Tipp:

Bei einer Digitalisierung durch Rhenus, erfolgt der Datenimport immer ausschließlich innerhalb der Rhenus-Umgebung. Ihre Daten verlassen diese gesicherte Umgebung zu keiner Zeit und das völlig ohne Schnittstellenkosten, denn alle unsere Digitalisierungssysteme sind bereits an das Rhenus Cloud Archiv angebunden.

2.4 Datensicherung und Datensicherheit

Die Rhenus-eigenen Rechenzentren befindet sich an einer festen deutschen Adresse, sind redundant ausgelegt, nach ISO 27001 zertifiziert und zeichnen sich durch mindestens folgende Merkmale aus:

- 24/7 Managed Service durch Fachpersonal
- Alle Daten werden immer auf mindestens 2 Rechenzentren verteilt und bieten auch bei Extremsituationen maximale Verfügbarkeit
- Volle Hardware-Redundanz und max. 4h Reaktionszeit der Lieferanten
- Sicherung der Daten zusätzlich in täglichem Backup (in jedem Rechenzentrum)
- alle Bereiche durch automatisiertes Monitoring überwacht

Wie funktioniert die Sicherheit meiner Daten im Detail?

Die Archivdaten werden, innerhalb eines manipulationssicheren Datencontainers, auf einem Storage gespeichert. Nur das Archivsystem hat Zugriff auf diese Daten und diese können nur von diesem, mittels eines Schlüssels, abgerufen werden. Einzig vom Kunden gelistete Personen haben Zugriff auf das digitale Archiv und erhalten Einblick in die Inhalte der Dokumente. Von Seiten Rhenus gibt es keine Tätigkeiten (beispielsweise Wartungsarbeiten), für die sich Rhenus-Mitarbeiter auf das digitale Archiv des Kunden einloggen muss. Einzig wenn es zu einem Problem kommt und der Support von Rhenus kontaktiert wird, kann ein gemeinsamer Zugriff auf das digitale Archiv notwendig sein. Mit einer expliziten Supportanfrage gewährt der Kunde zur Problemlösung den Zugriff auf das Archiv durch einen Administrator der Rhenus. Der Kunde kann im Anschluss jegliche, dokumentbezogene Handlung des Administrators im digitalen Archiv nachverfolgen.

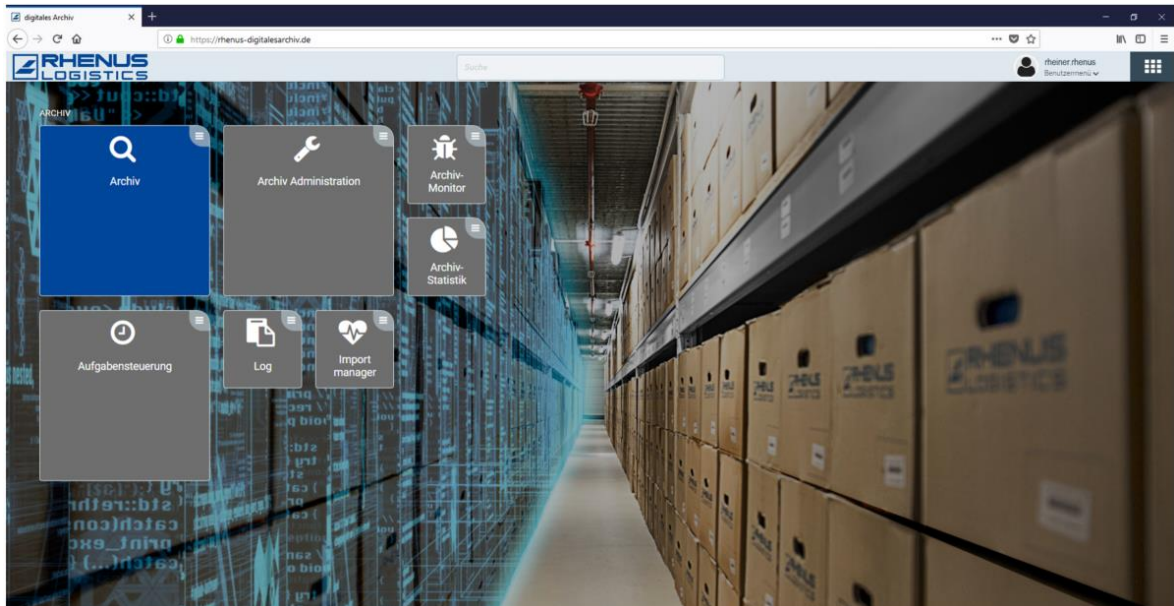
Mitarbeiter der Rhenus erhalten mehrfach im Jahr wiederkehrende Trainings zum Thema Informationssicherheit und Datenschutz, haben bei Unternehmenseintritt als Teil des Arbeitsvertrages eine Vertraulichkeitsverpflichtung sowie eine Datenschutzerklärung unterzeichnet und müssen zusätzlich ein polizeiliches Führungszeugnis vorlegen.

Eine Wirksamkeitskontrolle der Schulungsmaßnahmen findet über regelmäßige interne wie externe Audits statt. Nach Vorbild von BSI-Grundschutz, ISO 9001 und ISO 27001 werden regelmäßig System- als auch Prozessaudits durchgeführt.

Die Unveränderbarkeit der Daten ist weiterhin durch eine digitale Signatur gewährleistet. Jeder Datensatz kann aus dem Archiv heruntergeladen werden, nicht aber verändert werden. Denn wenn eine Veränderung eines Datensatzes geschieht, dann wird dieser veränderte Datensatz getrennt von dem Original-Datensatz behandelt, indem diese eine eigene Signatur erhält und als separate Datei abgelegt wird.

Die Verschlüsselung jedes einzelnen Dokumentes kann gesondert mittels einer AES-256-Verschlüsselung "at-rest" erfolgen.

2.5 Authentifizierung



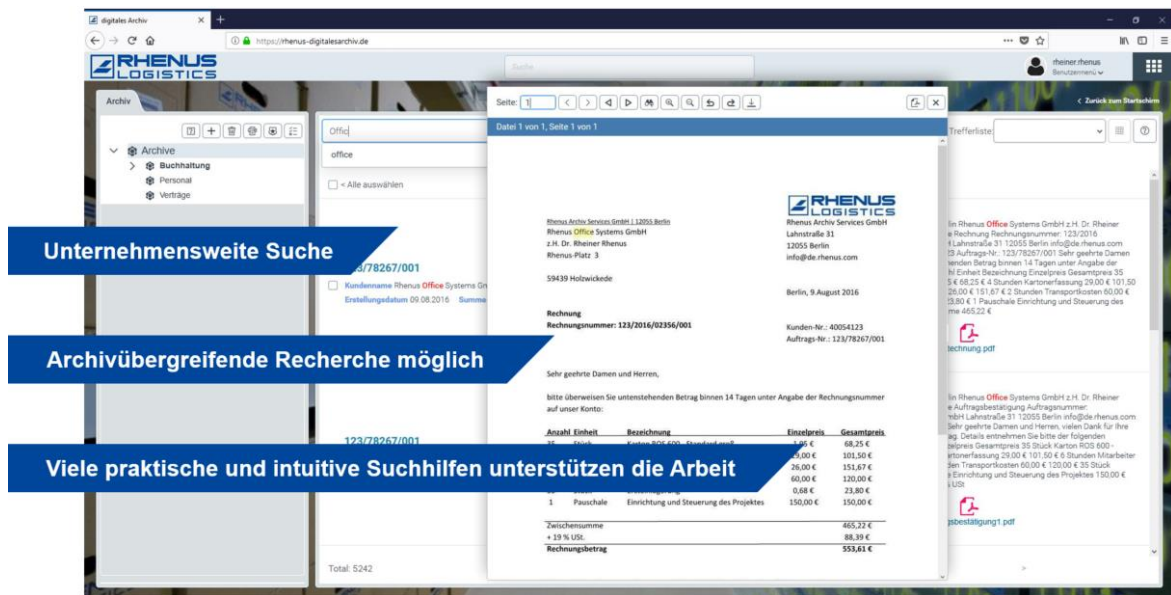
Der Zugriff auf die Dokumente innerhalb des digitalen Archivs wird mittels eines Web-Clients ermöglicht. Die Authentifizierung der User erfolgt über einen Verzeichnisdienst, wo jegliche Personen mit Zugriffsberechtigung gelistet sind und nur diese auch eine Legitimation zur Anmeldung mit Benutzername und Passwort haben. Die Passwörter der Zugriffsberechtigten liegen nur im jeweiligen Authentifizierungssystem, nicht in den Datenbanken des digitalen Archivs.

2.6 Datenbank und Recherche

Die Recherchefunktion ermöglicht es durch schnelles, einfaches Finden und Sichten von archivierten Dateien, Prozesse effizient abzuwickeln. Dies kann zusätzlich durch eine komfortable Volltextsuche abgebildet werden. Innerhalb der Archivierung können Anhänge indiziert als auch in die Volltextsuche inkludiert werden.

Hervorzuheben ist, dass es sich im Archiv um eine ganzheitliche Suche handelt, bei welcher folgende Komponenten gleichzeitig in einem Suchvorgang durchsucht werden:

- Dateiname
- Inhalt der Dateien
- Anhänge
- Indexkriterien



Suchanfragen werden durch praktische und zudem intuitive Suchhilfen unterstützt:

- Suche mit automatischer Vervollständigung
- Hervorheben des Suchbegriffes
- Vorschau auf das jeweilige Dokument (Rendering)
- Kategorienfilter (Möglichkeit der Gruppierung von Dokumenten anhand eines gleichen Indexwertes)
- Inhaltsorientierter Aktenbaum (Möglichkeit der Organisation von Dokumenten in einer Baumstruktur anhand von hierarchisch gegliederten Indexwerten)

2.7 Löschen

Das Löschen eines Dokumentes oder eines Archivs kann auf zwei verschiedene Arten erfolgen; zum einen kann ein berechtigter Benutzer (nicht empfehlenswert) ein Dokument oder Archiv löschen. Für Administratoren ist einsehbar, welcher Benutzer, welche Dokumente oder welches Archiv zu welchem Zeitpunkt gelöscht hat.

Neben diesem manuellen Prozess besteht die Möglichkeit bei Datenimport festzulegen wie lange Dokumente archiviert werden sollen. Diese Eigenschaft nennt sich „Retention“. Es handelt sich dabei um einen Wert, ab dem ein Dokument aus der Datenbank gelöscht wird.

Das automatisierte Löschen bezieht sich lediglich auf das Löschen von Dokumenten und nicht auf ganze Archive.

Aus Datenschutzgründen empfehlen wir das manuelle Löschen nur Rhenus im Vier-Augen-Prinzip mit dem Kunden zu erlauben. Das automatisierte Löschen sollte bei der Einrichtung des Archives eingerichtet und genutzt werden.

2.8 Verfügbarkeit

Die Verfügbarkeit des digitalen Archivs wird durch eine Vielzahl an technisch-organisatorischen Maßnahmen sichergestellt.

Neben Maßnahmen wie der Zutrittskontrolle (dient dazu das Unbefugte nicht in die Rhenus-eigenen Rechenzentren gelangen), der Zugangskontrolle (zum Zwecke, dass nur autorisierte Personen Zugang zum digitalen Archiv haben) und der Zugriffskontrolle (nur berechtigte Benutzer können auf ihre jeweiligen Daten zugreifen), gibt es spezifische Maßnahmen, die die Verfügbarkeit des digitalen Archivs sicherstellen.

Die grundlegendsten Aspekte bilden sowohl die Auftragskontrolle bei Dienstleistungspartnern und Subunternehmen als auch Mitarbeiterprüfungen und Schulungen zum Thema Datenschutz. Darauf aufbauend, ist die Netzwerkverfügbarkeit durch eine redundante Auslegung der Netzwerkanbindung sichergestellt. Darüber hinaus erfolgt die Anbindung der Server an das Netzwerk über Leitungen, die über getrennte Wege in das Gebäude führen und von verschiedenen Providern bereitgestellt werden.

Weitere Aspekte, die der Verfügbarkeit dienen, liegen im Brandschutz, im Wasserschutz und in der Stromversorgung. Der Brandschutz ist durch z.B. eine automatische Löscheinrichtung, die Aufteilung der Gebäude in mehrere Brandabschnitte und Feuerschutztresore gekennzeichnet. Der Wasserschutz zeichnet sich u.a. dadurch aus, dass Serverräume und Datenträgerarchive so untergebracht sind, dass sie nicht von möglichen Überschwemmungskatastrophen bedroht werden können. Auch die Stromversorgung ist redundant ausgelegt, wird durch eine Anlage zur unterbrechungsfreien Stromversorgung (USV) sowie großzügig dimensionierte Notstromaggregate ergänzt und durch eine eigens eingerichtete Klimaversorgung komplettiert.

Ein weiterer wichtiger Aspekt ist der Schutz gegen schadenstiftende Software (Viren, Ransomware etc.), der durch auf den Systemen eingesetzte next generation Cloud-Virens Scanner sowie next generation Firewall-Cluster abgedeckt wird.

Ein Backup-Verfahren zur Vermeidung von Datenverlusten bei Systemausfällen wird eingesetzt und ist ebenfalls redundant ausgelegt. Das Backup wird auf jeweils ortstrennten Servern durchgeführt.

Abschließend zum Thema Verfügbarkeit ist zu erwähnen, dass die Verschlüsselung der Kommunikation und von Daten sich nach den Empfehlungen zur Auswahl geeigneter Krypto-Techniken und kryptographischen Algorithmen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) richtet.

2.9 Export

Unternehmen ändern sich, ihre Ausrichtungen, ihre Strategien, ihre Mitarbeiter. Rhenus kennt diese Herausforderungen und so wissen wir, dass es Situationen gibt, in denen Teile oder gar ganze Archive wieder aus dem Rhenus Cloud Archiv ausgelagert werden müssen.

Vielleicht erfordert aber auch ein Projekt oder eine Zusammenarbeit einen Weitertransport von archivierten Dokumenten.

Ähnlich des Imports gibt es für den Export eine Vielzahl an Möglichkeiten;

- per Festplatte oder USB-Stick
- SFTP-Export
- Verzeichnisexport
- Manueller Download
- Webservice-basiert (REST-API)

Selbstverständlich können auch sämtliche Metadaten zum Dokument exportiert werden.