Centric Cloud Solutions GmbH

„Servicebeschreibung“

Stand: Juli 2023, Version 3

Inhalt

1 Begriffsbestimmungen

Anbieter = Centric Cloud Solutions GmbH
Kunde = Nutzer/Empfänger der von Centric zur Verfügung gestellten Services

2 Einleitung

Die Centric Document Processes beschreiben ein Produktportfolio bestehend aus unterschiedlichen Applikationen mit dem Ziel die Erstellung und Verwaltung von Dokumenten aus dem Personalwesen zu vereinfachen. Dabei handelt es sich um Cloud-basierte Add-ons zur Erweiterung und Integration in SAP-Produkte. Im Folgenden beschreiben wir Ihnen die relevanten Services der Centric Document Processes.
Zusätzlich zu dieser Servicebeschreibung erhalten Sie ein Angebot zur Subscription, ein Angebot über Implementierungsdienstleistungen, die Produktübersicht der jeweiligen Applikation, welche alle Produktfunktionen zusammenfassend aufführt und ein Dokument mit den Vertragsbedingungen (namentlich „Servicebedingungen“).

3 Zweck des Dokuments

Dieses Dokument dient der Beschreibung des von dem Anbieter angebotenen Cloud Services. Dazu werden relevante Informationen über die Architektur der Centric-Produkte, Betrieb, Sicherheit und Datenschutz, Compliance, Support, Mitwirkungspflichten, System- und Nutzungsvoraussetzungen, etc. übersichtlich zusammengefasst bereitgestellt.
Der Kunde und der Anbieter sind sich einig, dass der Service in dem hier beschriebenen Umfang offeriert wird.

Die Servicebeschreibung ist Angebots- und folgerichtig Vertragsbestandteil. Mündliche Nebenabreden bestehen nicht. Abweichungen von dem hier beschriebenen Service oder den in der Produktübersicht aufgeführten Produktfunktionen müssen im Angebot schriftlich definiert sein, um Vertragsbestandteil zu werden. Abweichungen vom hier beschriebenen Service können eine kundenindividuelle Preisgestaltung notwendig werden lassen, sodass die Preise aus der Produktübersicht keine Anwendung mehr finden.

4 Übersicht Portfolio

Das Portfolio der Centric Cloud Solutions **“Centric Document Processes“**, umfasst diverse Produkte bzw. Applikationen zur Erstellung und Verwaltung von Dokumenten aus dem Personalwesen.
Der Grundgedanke des Portfolios ist die Erweiterung des Funktionsumfangs von SAP HCM und SAP SuccessFactors. Dies wird durch Integration der Centric Produkte in die beim Kunden bestehende Personalmanagement- bzw. Payroll-Lösung erreicht.

Centric nutzt die SAP Business Technology Platform, um auf dieser Basis die Produkte zu entwickeln und dem Kunden bereitzustellen. Es handelt sich um bei der SAP Business Technology Platform um eine reine Cloud-Anwendung. Weiterhin wird zur Entwicklung des Frontends SAP UI5 verwendet, sodass die Oberflächen einem einheitlichen Klickverhalten und einer einheitlichen Optik im Vergleich zu den SAP-Produkten folgen. Centric hält in Bezug auf die aufgeführten Produkte den SAP Build-Partnerstatus.

Das Portfolio der Centric Document Processes ist modular aufgebaut. Produkte können sowohl eigenständig als auch Bundle verwendet werden. Darüber hinaus werden teilweise Add-ons angeboten, welche den regulären Produktnutzungsumfang erweitern. Die Add-ons werden unter anderem von

Technologie-Partnern entwickelt und bereitgestellt. Daher kann (muss aber nicht) die technologische Basis der Add-ons von dem Centric Produkt abweichen.

Centric kommuniziert die Release-aktuellen Produktübersichten mit einer Auflistung aller zugesicherten Funktionen zur Transparenz auf der Homepage des jeweiligen Produkts. Die Produktübersichten werden Vertragsbestandteil. Funktionserweiterungen basieren sehr häufig, allerdings nicht ausschließlich, auf dem Input von Kunden. Somit profitieren stets alle Kunden von der Standardisierung und gelebten Best Practices. Wir sind für Input dankbar.

4.1 Centric Employee File

Die Centric Employee File ermöglicht die Speicherung von Dokumenten aus dem Personalwesen mit der direkten Verknüpfung zum jeweiligen Mitarbeiter / zur jeweiligen Mitarbeiterin. Zur Wiederauffindbarkeit steht sowohl eine akteninterne und aktenübergreifende Volltextsuche als auch eine einheitliche und transparente Ordnerstruktur zur Verfügung. Darüber hinaus stehen zahlreiche Funktionen zur Verwaltung und Administration der Dokumente zur Verfügung. Viele davon beziehen sich entweder auf das einfache Handling aus Nutzersicht, Reporting oder die Compliance mit internen und gesetzlichen Vorgaben (bspw. DSGVO). Die Integration in SAP HCM oder SAP SuccessFactors ermöglicht unter anderem die automatisierte Anlage der Personalakten auf Basis der Personalstammdaten und die Übernahme von Rechten und Rollen.

Centric Employee File wurde speziell für die Integration in SuccessFactors® und SAP HCM entwickelt. Der vollständige Funktionsumfang ist zusammenfassend beschrieben in der Produktübersicht.

4.2 Centric Document Builder

Der Centric Document Builder ermöglicht die Erstellung von Dokumenten aus dem Personalwesen mit Hilfe von Dokumentvorlagen, Daten aus einem Quellsystem (bspw. Personalmanagement, Recruiting, etc.) und Textbausteinen. Dabei können Dokumente im Einzelverfahren oder im Serienverfahren erstellt werden. Darüber hinaus sind ebenfalls Workflows zur Dokumentenerstellung und -freigabe möglich.

Mit dem Centric Document Builder lassen sich diverse Dokumenttypen (bspw. Arbeitsverträge, Mitarbeiteranschreiben, Bescheinigungen, etc.) erzeugen. Demnach ist der Centric Document Builder ein generisches Produkt, welches technische und funktionale Möglichkeiten zur Dokumentenerstellung bietet. Die Inhalte (bspw. Vorlagen, Textbausteine, etc.) sind durch den Kunden einzurichten. Sollte Centric beauftragt werden, bei der Einrichtung der Inhalte zu unterstützen, sind die benötigten Informationen durch den Kunden zur Verfügung zu stellen. Auch die fortlaufende Pflege und Verwaltung der Inhalte ist durch den Kunden vorzunehmen.

Centric Document Builder wurde speziell für die Integration in SuccessFactors® und SAP HCM entwickelt. Der vollständige Funktionsumfang ist zusammenfassend beschrieben in der Produktübersicht.

4.3 Centric Reference Letter

Centric Reference Letter ermöglicht die Erstellung von Arbeitszeugnissen mit Hilfe von Zeugnisvorlagen, Daten aus einem Quellsystem (bspw. Personalmanagement oder Payroll) und Textbausteinen gemäß einem Notensystem. Darüber hinaus kann die Zeugniserstellung auch über einen Workflow erfolgen, bei dem Mitarbeiter*innen und Führungskräfte zur Zeugniserstellung und -freigabe eingebunden werden.

Mit Centric Reference Letter lassen sich diverse Zeugnisarten (bspw. Abschlusszeugnis oder Zwischenzeugnis) erzeugen. Demnach ist der Centric Reference Letter ein generisches Produkt, welches technische und funktionale Möglichkeiten zur Zeugniserstellung bietet. Darüber hinaus wird im Produktstandard allerdings bereits Business-Content mitgeliefert. Dieser umfasst unter anderen Vorlagen für diverse Zeugnisarten und juristisch geprüfte und aktuell gehaltene Textbausteine vom renommierten Boorberg Verlag gemäß einem Notensystem. Weiterhin umfasst der Produktstandard ebenfalls einen vorkonfigurierten Zeugnisprozess mit webbasierten Formularen zur Bewertung.

Centric Reference Letter wurde speziell für die Integration in SuccessFactors® und SAP HCM entwickelt. Der vollständige Funktionsumfang ist zusammenfassend beschrieben in der Produktübersicht.

4.4 Centric Payslip Box

Die Centric Payslip Box ermöglicht die Speicherung bzw. Bereitstellung von entgeltrelevanten Dokumenten für bzw. an Mitarbeiter*innen. Zur Wiederauffindbarkeit steht sowohl eine Volltextsuche als auch eine einheitliche und transparente Ordnerstruktur zur Verfügung. Darüber hinaus stehen ausgewählte Funktionen zur Verwaltung der Dokumente zur Verfügung. Die Integration in SAP HCM oder SAP SuccessFactors ermöglicht unter anderem die automatisierte Anlage der Payslip Boxen auf Basis der Personalstammdaten und die automatisierte Übernahme von Entgeltnachweisen, Lohnsteuer-bescheinigungen und DEÜV-Meldungen.

Centric Payslip Box wurde speziell für die Integration in SuccessFactors® und SAP HCM entwickelt. Der vollständige Funktionsumfang ist zusammenfassend beschrieben in der Produktübersicht.

4.5 Sprachpakete

Die Standard-Produktausstattung der Centric Document Processes umfasst die Sprachen Deutsch und Englisch. Sollten weitere Sprachen benötigt werden, bietet Centric weitere Sprachpakte an, welche kostenpflichtig hinzugebucht werden können. Die Verfügbarkeit der vom Kunden gewünschten Sprache ist vorab anzufragen und von Centric schriftlich zu bestätigen. Die Verfügbarkeit von Sprachen der Add-ons, welche durch Partner bereitgestellt werden, ist gesondert zu prüfen.

Werden Produktfunktionen hinzugefügt, aktualisiert Centric die bei Kunden im Einsatz befindlichen Sprachpakete laufend. Unser Angebot umfasst standardmäßig die Übersetzung nach ISO 17100.
Der Umfang der Sprachpakete bezieht sich auf die Oberflächen zur Nutzung der Applikationen. Die Inhalte der Produkte ist stets kundenindividuell (vgl. Vorlagen zur Dokumentenerstellung, Textbausteine, Dokumenttypen und Dokument in der Personalakte). Von daher ist der Kunden in der Verantwortung die benötigten Sprachen für kundenindividuelle Inhalte im Customizing zu pflegen.

4.6 Erweiterungen zu den Produkten

4.6.1 Scan2Employee File

Scan2Employee File ist eine Erweiterung zur digitalen Personalakte mit dem Ziel gescannte Dokumente direkt in der Personalakte abzulegen. Es handelt sich um eine Scan-Software für Multifunktionsgeräte, welche es ermöglicht individuelle Scanprozesse zu etablieren. Die Lösung unterstützt sowohl die Erkennung von Barcodes, die Trennung von Dokumenten auf Basis von Barcodes als auch eine OCR-Erkennung damit später Dokumente im Volltext durchsucht werden können.

Es handelt sich um eine On-Premises Software (Weitere Informationen zur Technik unter Architektur).

Abbildung 1: Integration MFP

4.6.2 On-Premises Archivierung

Im Produktstandard der Centric Employee File ist die Archivierung der Dokumente in dem Cloud-Archivservice vorgesehen. Bei Bedarf können die Dokumente jedoch auch innerhalb der kundeneigenen IT-Infrastruktur archiviert werden. Sofern der Kunde bereits ein CMIS-fähiges Archiv im Einsatz hat, kann dieses als Dateispeicherort verwendet werden. Sollte kein geeignetes Archiv vorhanden sein, bietet Centric ein On-Premises Archiv des Partners **KGS Software GmbH** an.

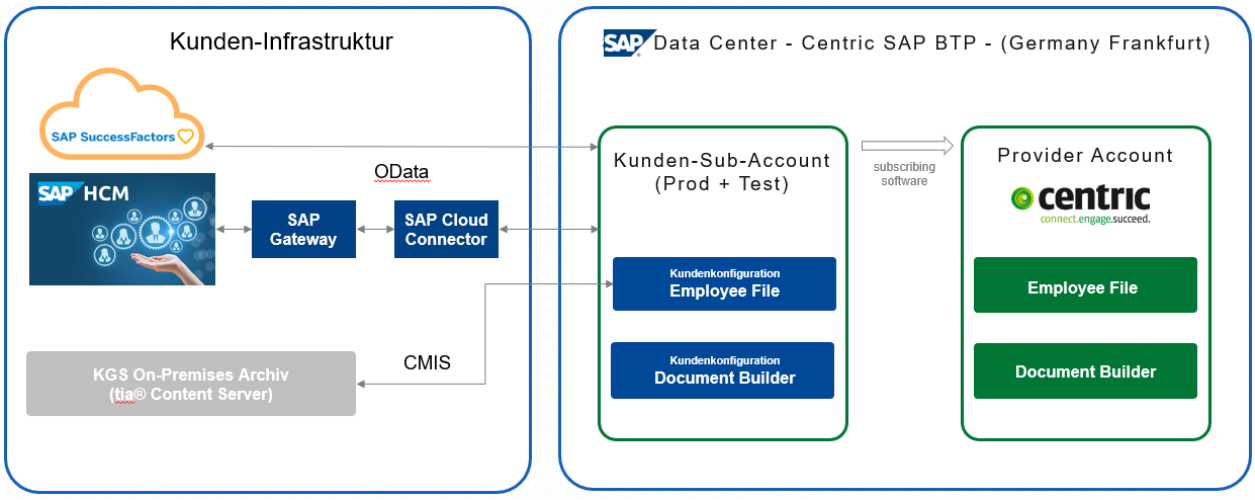


Abbildung 2: OnPremises Archivierung

4.6.3 Elektronische Signatur mit DocuSign

Centric offeriert als DocuSign-ISV-Partner sowohl die elektronische Signatur als auch die vollständige Integration in die Centric-Produkte aus einer Hand.

Die DocuSign Integration beinhaltet die Schnittstelle zu den Centric-Produkten und die notwendigen DocuSign-Umschläge, die zur Abbildung von HR-Prozessen notwendig ist. Die Anzahl der subskribierten DocuSign-Umschläge sind an die Centric-Produkte gebunden und dürfen nicht in einem anderen betreibwirtschaftlichen Kontext verwendet werden. Ein DocuSign-Umschlag ist ein laufender Workflow mit beliebig vielen Dokumenten, Prozessteilnehmer und Unterschriften.

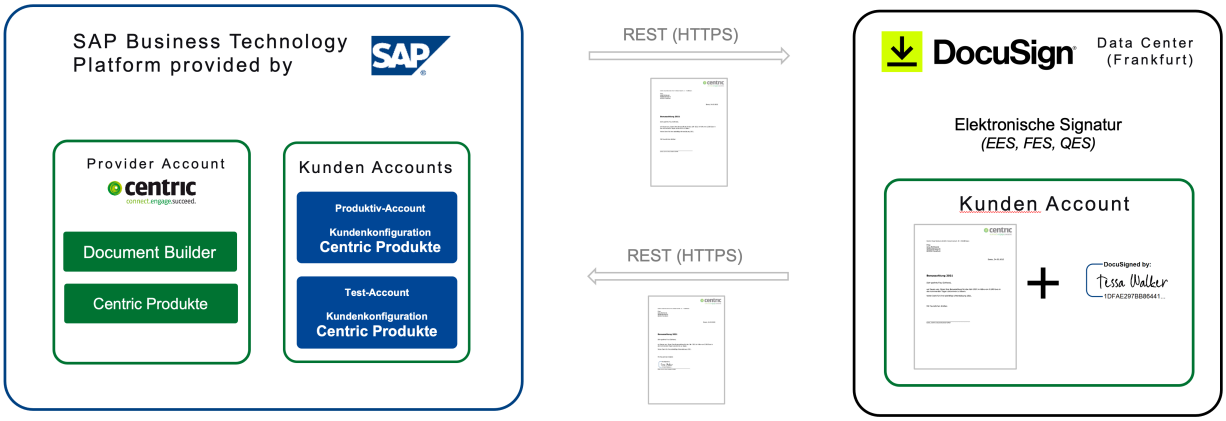


Abbildung 3: DocuSign Anbindung

5 Architektur

Die Centric Produkte basieren auf Services, der SAP Business Technology Platform (SAP BTP). Die Bereitstellung der SAP BTP durch SAP erfolgt je nach genutztem Centric Produkt in einem SAP-Rechenzentrum oder einem von SAP definierten Hyperscaler (AWS Europe). SAP ist verantwortlich für den Betrieb, inkl. Security und BackUp-Funktionalität. (Weitere Informationen unter *Rechenzentrum*)

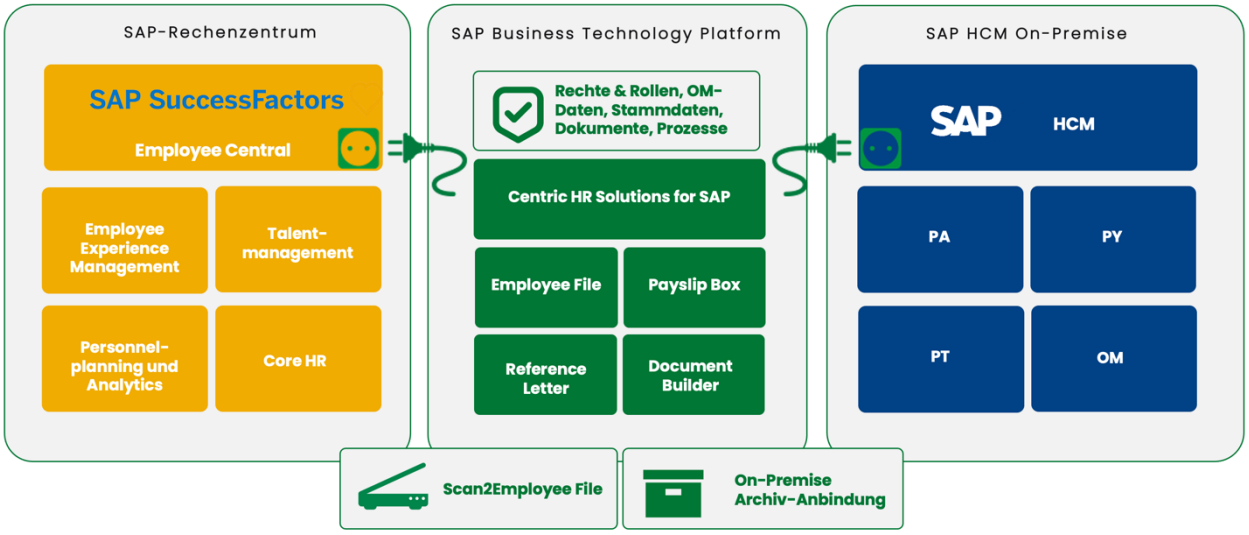


Abbildung 4: Übersicht Centric Architektur

Zusätzliche zu den verwendeten SAP-BTP Services werden weitere 3-Party Service für Centric-Produkt-Erweiterungen genutzt. (Weitere Informationen unter *Verwendete Services und Technologien*)

5.1 Multitenancy

In der SAP-BTP erhält jeder Kunde, in Abhängigkeit von der projektspezifischen Umsetzung, ein oder mehrere Sub-Accounts. Diese Sub-Accounts beinhalten die kundenindividuellen Konfigurationen der Centric Produkte. Kunden Sub-Accounts subskribieren in Abhängigkeit des abgeschlossenen Vertrages die jeweilige Centric Produkte. Jeder Kunden Sub-Account ist ein eigenständiger und unabhängiger Tenant zur Gewährleistung der kundenindividuellen Datenhoheit und Einhaltung der gesetzlichen Datenschutzgrundverordnung. Die Generik der Centric Produkte werden durch den Centric Provider Account zur Verfügung gestellt.

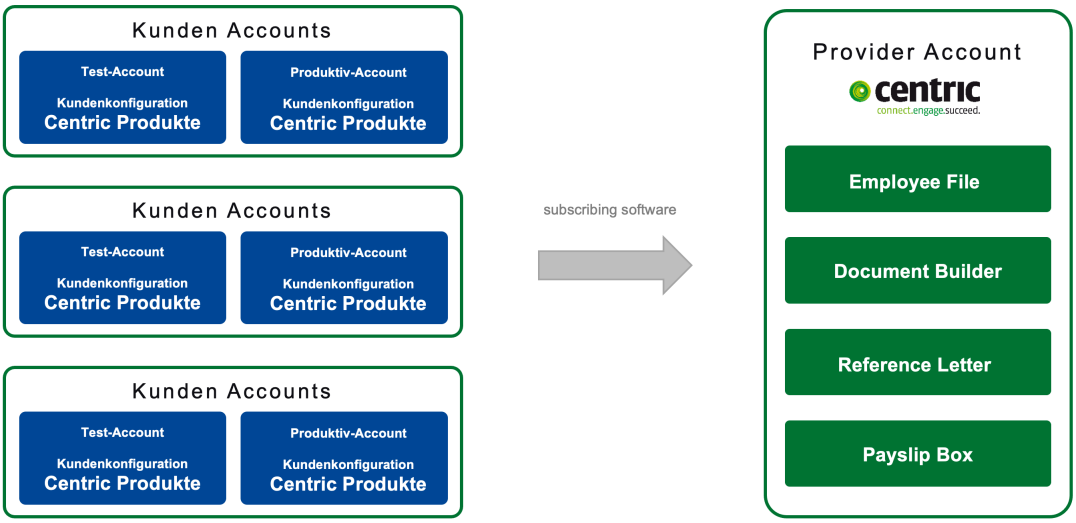


Abbildung 5: Multitenancy und Provider Account

5.2 Authentifizierung und Autorisierung

Centric stellt keinen eigenen Authentifizierungs- und Autorisierung-Service zur Verfügung. Zur Authentifizierung und Autorisierung werden am kundeneigenen Sub-Account die durch Kunden zur Verfügung gestellten Applikationen genutzt.

Folgenden Applikationen werden mit SAML2 (HTTPS) unterstützt:

- Azure AD / On-Premises AD
- SuccessFactors
- SAP Identity Authentication Service (IAS)

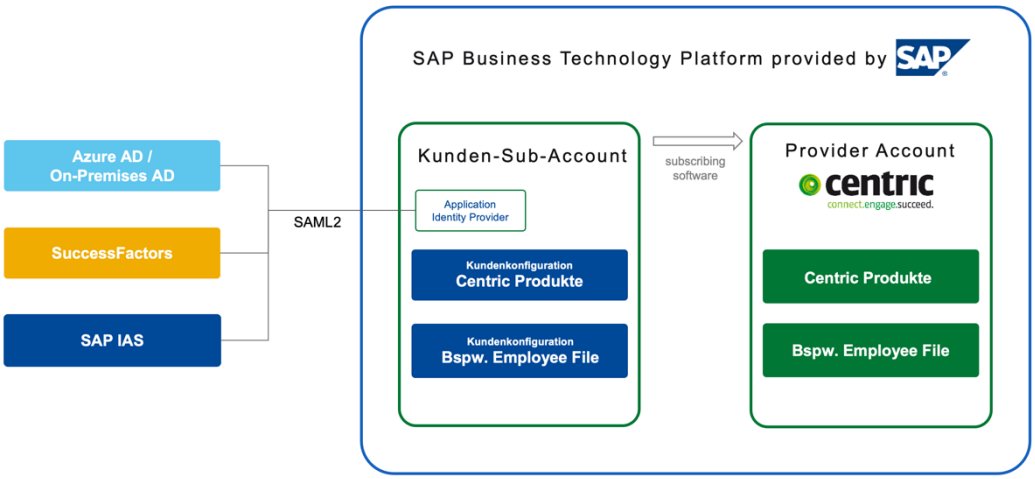


Abbildung 6: Authentifizierung und Autorisierung

5.3 Verwendete Services und Technologie

Das Portfolio der Centric Cloud Solutions GmbH basiert auf technologischen Services die extern bezogen werden. Eine Übersicht der eingesetzten Services ist in der nachfolgenden Tabelle aufgelistet.

(Employee File = EF, Reference Letter = RL, Payslip Box = PB, Document Builder = DB, Scan2Employee File = S2EF)

Service und Technologie	EF	RL	PB	DB	S2EF	Model
SAP UI5 (Fiori Design)	X	X	X	X		SaaS
SAP Cloud Platform Java Server (Neo)	X	X	X			SaaS
SAP HANA Cloud	X	X	X	X		SaaS
SAP Document Service	X		X			SaaS
SAP Object Store	X		X			SaaS
SAP Cloud Foundry Runtime				X		SaaS
Java Application provided by SAP				X		SaaS
DocuSign				X		SaaS
Kofax Autostore / Unified Client					X	OnPremises

5.4 Schnittstellen

Im Nachfolgenden werden, die im Standard unterstützen Schnittstellen der Centric Produkte basierend auf der SAP BTP, beschrieben.

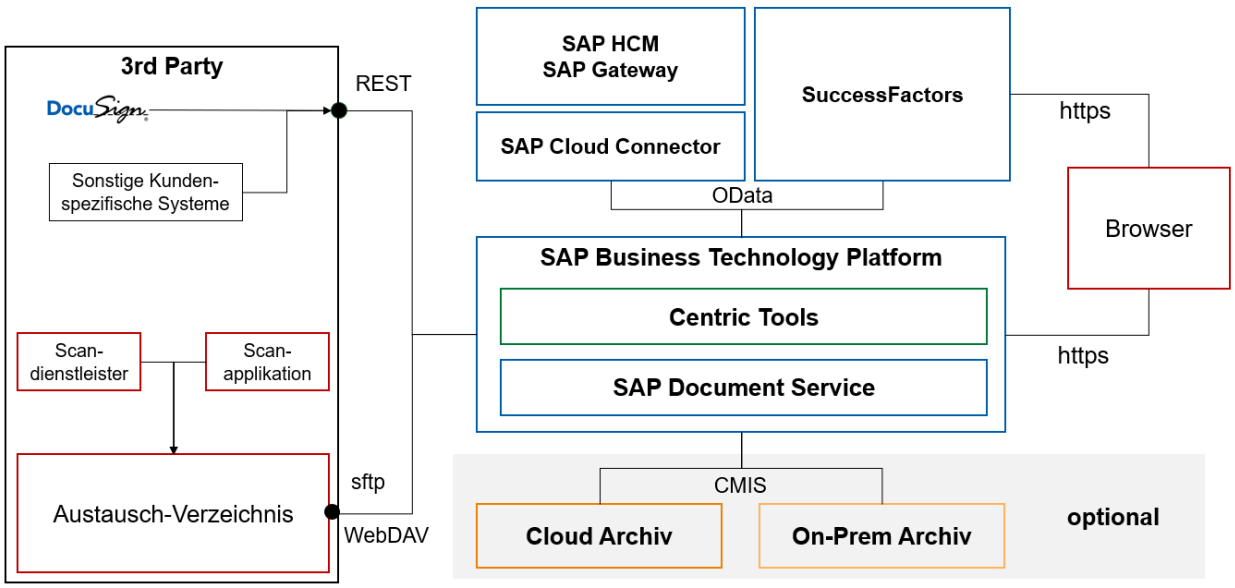


Abbildung 7: Darstellung Schnittstellen

5.4.1 SAP HCM / SuccessFactors

Die Kommunikation zwischen den Centric Produkten in der SAP BTP und SAP OnPremises / SuccessFactors erfolgt über eine HTTPS (Hypertext Transfer Protocol Secure) Verbindung via OData (Open Data Protocol) und REST (Representational State Transfer).

Für die Anbindung eines SAP HCM wird ein SAP Cloud Connector und ein SAP Gateway benötigt. Die Darstellung des UI (User Interface in SAP UI5) erfolgt in den von SAP unterstützen Browsern (Link SAP Help Portal) der via HTTPS mit dem angebunden System (SuccessFactors / SAP BTP) verbunden ist.

5.4.2 Dokumentarchivierung

Werden die Dokumente nicht in den Services der SAP BTP archiviert, können diese in ein OnPremises oder Cloud Archiv abgelegt werden, welches via CMIS (Content Management Interoperability Services) angebunden ist.

5.4.3 Austauschverzeichnis

Die Nutzung von Austauschverzeichnissen zum Dokumentupload in die Centric Produkte (SAP BTP) erfolgt via SFTP (Secure File Transfer Protocol) oder WebDAV (Web-based Distributed Authoring and Versioning).

5.4.4 Scan-Applikationen „Scan2Employe File“

Die Kommunikation zur Dokumentablage zwischen dem On-Premises Scan-Server von „Scan2Employee File“ in die entsprechenden Centric Produkte erfolgt via REST per HTTPS.

5.4.5 DocuSign

Die Einbindung von DocuSign zur Erstellung von elektronischen Signaturen, erfolgt via REST per HTTPS. Dabei ist es unabhängig davon, ob es sich um die kundeneigene oder die von Centric zur Verfügung gestellten Envelope handelt.

5.4.6 E-Mail / Microsoft Outlook

Die Integration und Nutzung von E-Mail-Funktionalitäten werden auf zwei unterschiedliche Möglichkeiten unterstützt.

Microsoft Outlook 365 Add-In

- Funktionalität = Ablage von Dokumenten in Centric Produkte.
- Anbindung = Die Kommunikation zwischen dem Add-In und dem entsprechenden Centric Produkt erfolgt per HTTPS.

SMPT-Postfach Integration

- Funktionalität = Versendung von Benachrichtigungen zu Aktivitäten und Ereignissen in Centric Produkten.
- Anbindung = Szenario 1 - kundeneigenes Postfach
  Der Kunde stellt ein Postfach zum Versenden von E-Mails bereit, das via SMTP angebunden ist. STARTTLS Unterstützung ist vorhanden.

  Szenario 2 - bereitgestelltes Postfach

Centric stellt ein Postfach zum Versenden von E-Mails bereit, das via SMTP angebunden ist. STARTTLS Unterstützung ist vorhanden.

5.4.7 3rd-Party

Die Anbindung von weiteren Services zur Kommunikation mit den auf der SAP BTP basierenden Centric Produkte erfolgt via REST und wird kundenindividuell durch Centric vorgenommen.

6 Betrieb

6.1 Rechenzentrum

Sämtliche in den Centric Produkte verwendeten Services werden direkt vom Hersteller zur Verfügung gestellt und in einem vom Hersteller definierten Rechenzentrum gehostet. Centric nutzt diese Service als Basis für das Portfolio und betreibt keine eigenen Rechenzentren.

6.2 SAP

Die genutzten SAP BPT Services werden durch SAP in einem SAP eigenen Rechenzentrum und einem von SAP definiertem Hyperscaler (AWS Europe) zur Verfügung zur Verfügung gestellt.

Die Verantwortlichkeiten und Zuständigkeiten zwischen SAP, Hyperscaler und Centric hinsichtlich des Betriebes der SAP BTP sind nachfolgend dargestellt. (Weitere Informationen im SAP Trust Center).

Hyperscaler	SAP	Centric
• Sicherheit des Rechenzentrums, einschließlich des benötigten Personals für den Rechenzentrumsbetrieb • Bereitstellung der Hardware • Netzwerkverfügbarkeit	• Implementierung einer robusten Architektur • Sicherung und Wiederherstellung von Tenants • Konfiguration der virtuellen Maschinen, zur Bereitstellung der verwendeten Services • Sicherung der Infrastruktur, Betriebssysteme und/oder Container-Images, Netzwerke und Anwendungen • Betriebs- und Sicherheitsüberwachung • Managen von Sicherheitsvorfällen • Betrieb von Cloud-Ressourcen • Bereitstellung von Patches und Lösungssupport	• Konfiguration der zur Verfügung gestellten Services • Verwaltung von tenantspezifischen Einstellungen und Konfigurationen

Betreibt SAP das Rechenzentrum, werden die aufgeführten Verantwortlichkeiten und Zuständigkeiten des Hyperscalers von SAP übernommen.

6.3 DocuSign

Der verwendete DocuSign Service zur Erstellung von elektronischen Signaturen wird in den DocuSign Rechenzentren (Equinix) in Deutschland gehostet und von DocuSign über eine API zur Verfügung gestellt.

Equinix	DocuSign	Centric
• Sicherheit des Rechenzentrums, einschließlich des benötigten Personals für den Rechenzentrumsbetrieb • Bereitstellung der Hardware • Netzwerkverfügbarkeit	• Implementierung einer robusten Architektur • Erstellung, Sicherung und Wiederherstellung von Envelopes • Konfiguration der virtuellen Maschinen, zur Bereitstellung der verwendeten Services • Sicherung der Infrastruktur, Betriebssysteme und/oder Container-Images, Netzwerke und Anwendungen • Betriebs- und Sicherheitsüberwachung • Managen von Sicherheitsvorfällen • Betrieb von Cloud-Ressourcen • Bereitstellung von Patches und Lösungssupport • Bereitstellung von Services	• Konfiguration und Anbindung der zur Verfügung gestellten Services • Verwaltung von Envelope-spezifischen Einstellungen und Konfigurationen

6.4 Standort

Der Betrieb der Centric Produkte erfolgt in Deutschland lokalisierten Rechenzentren. Zur Einhaltung der von SAP zugesicherten Vereinbarungen können in Europa lokalisierte Ersatz-Rechenzentren durch SAP hinzugefügt werden.

Centric Produkt	Standort „Betrieb“	Standort „Backup RZ“
Centric Employee File	Deutschland, Frankfurt	Europäische Union
Centric Documet Builder	Deutschland, Frankfurt	Europäische Union
Centric Reference Letter	Deutschland, Frankfurt	Europäische Union
Centric Payslip Box	Deutschland, Frankfurt	Europäische Union
Erweiterung: DocuSign	Deutschland, Frankfurt	Europäische Union

6.5 Systemverfügbarkeit

6.5.1 SAP

- Die monatliche Systemverfügbarkeit der SAP BTP basierenden Centric Produkte beträgt 99,7 %
- Ausgenommen sind Zeitfenster für Wartung und Upgrades durch SAP sowie Wartungsarbeiten und Release-Deployments durch Centric. (Weitere Informationen unter Wartung und Weiterentwicklung)

Die aktuelle Verfügbarkeit der genutzten SAP Services kann jederzeit im SAP Trust Center unter Cloud Status eingesehen werden.

6.5.2 DocuSign

- Die Systemverfügbarkeit der Services für elektronischen Signaturen beträgt 99,9 %
- Ausgenommen sind Zeitfenster für Wartung und Upgrades durch DocuSign sowie Wartungsarbeiten und Release-Deployments durch Centric. (Weitere Informationen unter Wartung und Weiterentwicklung)

Die aktuelle Verfügbarkeit des genutzten DocuSign Services kann jederzeit im DocuSign Trust Center eingesehen werden.

6.6 Wartung und Weiterentwicklung

Durch den Abschluss eines Vertrages zwischen dem Kunden und Centric obliegt die Wartung und Weiterentwicklung, der durch Centric zur Verfügung gestellten Services, bei Centric. Die Unterscheidung zwischen der Wartung und Weiterentwicklung liegt in dem Erhalt der Funktionsfähigkeit des Services (Wartung, Technisches Release) und der Weiterentwicklung des Services (Weiterentwicklung, Feature Release).

6.6.1 Wartung

Zum Erhalt der Funktionsfähigkeit der Centric Produkte gehört die regelmäßige Überprüfung der Kompatibilität mit den von SAP zur Verfügung gestellten SAP BTP Services & Technologien (Weitere Informationen unter Services & Technologien), sowie die stetige Überprüfung hinschlicht Softwarefehler und Sicherheitsanpassungen in den Centric Produkten. Sind Anpassungen in den von Centric genutzten Services notwendig, werden diese in einem technischen Release veröffentlicht und automatisch auf das Kundensystem eingespielt.

6.6.2 Weiterentwicklung

Centric veröffentlich 3 Feature Release pro Jahr mit der Bezeichnung „Spring, Summer, Autumn“ und der jeweiligen Jahreszahl. Die Release-Ankündigung erfolgt via E-Mail an die vom Kunden genannten Ansprechpartner in folgendem Zeitintervall:

- 14 Tage vor Release – „Save the Date, Zeitfenster geplanter Downtime “
- 3 Tage vor dem Release – „Informationen zu neuen Funktionen“

Die in dem Release bereitgestellten Weiterentwicklungen unterscheiden sich in Funktionen die *automatisiert zur Verfügung* stehen und Funktionen, die eine *Anpassung in der Konfiguration* benötigen.

7 Sicherheit und Datenschutz

7.1 Rechenzentren

Die Sicherheit der Rechenzentren liegt im Verantwortungsbereich der Servicebetreiber (Weitere Informationen unter Betrieb). Alle genutzten Rechenzentren sind nach den höchsten Sicherheitsstandards zertifiziert. (Weitere Informationen unter Zertifizierung)

7.2 Daten

Je nach genutztem Centric Produkt werden Daten in dem vom Anbieter genutzten Service für unterschiedliche Verwendungszwecke gespeichert und in definierten Zyklen aktualisiert. Das datenführende System ist das an die Centric Produkte angebundene System – Centric Produkte erhalten lediglich einen lesenden Zugriff auf die verwendeten Daten.

Centric Produkt	Gespeicherte Daten
Centric Employee File	• Stammdaten zur Darstellung im Aktenkopf (kundenindividuell) und zum Mapping Identity Provider (Architekturabhängig) • Rolle zur Berechtigungsprüfung in der Akte
Centric Documet Builder	• Stammdaten zum Mapping Identity Provider (kundenindividuell und architekturabhängig) und zur User-Zuweisung (SAP Principal Propagation)
Centric Reference Letter	• Stammdaten zur Zeugniszuweisung (kundenindividuell) und zum Mapping Identity Provider (architekturabhängig) • Rolle zur Berechtigungsprüfung im Workflow
Centric Payslip Box	• Stammdaten zur Darstellung in Payslip Box (kundenindividuell) und zum Mapping Identity Provider (architekturabhängig) • Rolle zur Berechtigungsprüfung in der Payslip Box
Erweiterung: DocuSign	• Stammdaten Unterzeichner (kundenindividuell)

7.2.1 SAP BTP

Durch die Multitenancy-Architektur (Weitere Informationen unter Multitenancy) ist die Datenintegrität jedes einzelnen Kunden sichergestellt. Die Datenspeicherung in der SAP BTP erfolgt schemabasiert in der SAP HANA Cloud (Link SAP HANA Cloud). Alle Daten und Backups werden automatisiert durch die SAP in einer AES-256 Bit Verschlüsselung abgelegt.

7.2.2 DocuSign

Jeder Kunde hat einen eigenen, unabhängigen Account bei DocuSign zur Durchführung von elektronischen Signaturen. Die Datenspeicherung im DocuSign Account erfolgt für dokumentrelevante Informationen in verschlüsselten (AES 256) BLOB (Binary Large Objects) Objekten und Envelope Metadaten in einer SQL-Datenbank (Link DocuSign Trust Center).

7.3 Kommunikation

Die Kommunikation zwischen den Centric Produkten und der Kundenumgebung erfolgt über Standardschnittstellen via HTTPS. (Weitere Informationen unter Schnittstellen)

7.4 Archivierung

Wird in einem Centric Produkt die Funktion der Dokumentarchivierung zur Verfügung gestellt, werden diese im Produktstandard, in dem zugehörigen SAP BTP Service, SAP Document Service / SAP Object Store, mit einer AES 256 Bit Verschlüsselung abgelegt. (Weitere Informationen unter Verwendete Services & Technologien). Alternativ ist kann ein externes Archiv zur Dokumentarchivierung via CMIS angebunden werden.

7.5 Rollen & Berechtigungen

Das vom Kunden zur Verfügung gestellte Rollen & Berechtigungskonzept dient als Basis für die Berechtigungsausprägungen in:

- Centric Employee File
- Centric Document Builder
- Centric Reference Letter
- Centric Payslip Box

Die ankommende Rolle wird auf eine im Produkt vorhandene Rolle gemappt und interne Rolle beinhaltet die funktionale Produktausprägung. Zusätzlich wird durch die ankommende Rolle sichergestellt, dass die in SAP HCM / SuccessFactors vorhandene Mitarbeiter*inn-Berechtigung für die jeweilige Produktnutzung eingehalten wird.

Produkt	Berechtigung via „externe Rolle“
Centric Employee File	• Berechtigung Mitarbeiter SAP HCM / SF = Berechtigung Personalakte • Führungskraft SAP HCM / SF = Berechtigung Personalakte Verantwortungsbereich
Centric Document Builder	• SAP Principal Propagation (Berechtigung Daten SAP-User = Berechtigung Datennutzung Dokumenterstellung)
Centric Reference Letter	• Berechtigung Mitarbeiter SAP HCM / SF = Berechtigung Zeugniserstellung • Führungskraft SAP HCM / SF = Berechtigung Mitarbeiterbewertung Verantwortungsbereich
Centric Payslip Box	• Berechtigung Mitarbeiter HCM / SF = Berechtigung Payslip Box

7.5.1 Rollen

Die nachfolgenden Quellsysteme werden für ein Rollen-Mapping unterstützt:

Quellsystem	Rollen-Mapping
Azure AD / On Premises AD	AD-Gruppe
SAP HCM	HCM-Rolle
SuccessFactors	SuccessFactors-Rolle

7.5.2 Berechtigung

Die in den Centric Produkten konfigurierten Berechtigungen betreffen ausschließlich die in den Centric Produkten zur Verfügung stehenden Produktfunktionen.

Centric Employee File

Die Berechtigungen in Centric Employee File basieren auf Dokumenttypen, Akten- und Dokumentaktionen. Somit ist es möglich, dass für jede extern ankommende Rolle eine individuelle Berechtigungskonfiguration hinsichtlich der Dokumenttypen, Akten- und Dokumentfunktionen vorgenommen werden kann.

(Weitere Informationen zu Akten- und Dokumentfunktionen in unserer Produktübersicht unter Centric.eu)

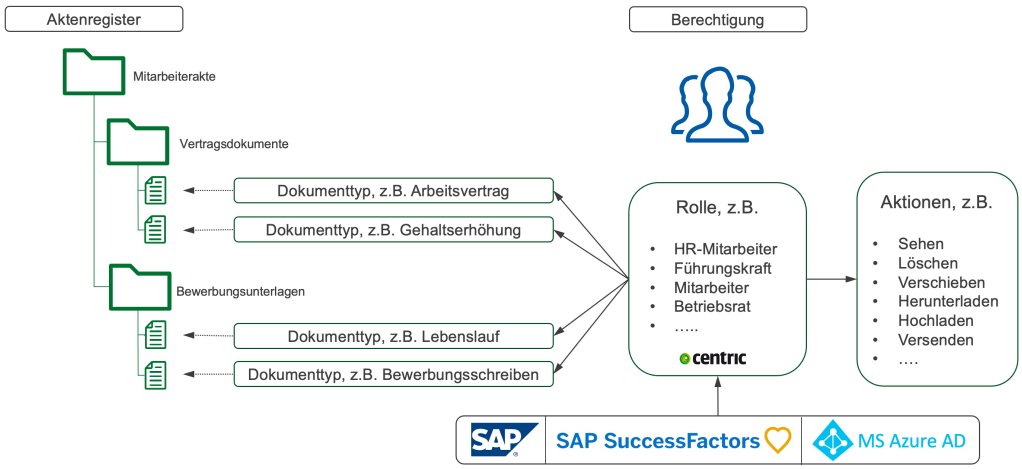


Abbildung 8: Berechtigung Employee File

Centric Payslip Box

Die Berechtigungsausprägung der Payslip Box bezieht sich auf zwei unterschiedliche Bereiche. Für Angestellte der HR-Abteilung steht als Konfigurationsgrundlage der volle Funktionsumfang zur Verfügung während Mitarbeiter*innen ausschließlich Dokumente sehen und herunterladen können.

(Weitere Informationen zur Payslip Box - und Dokumentfunktionen in unserer Produktübersicht unter Centric.eu)

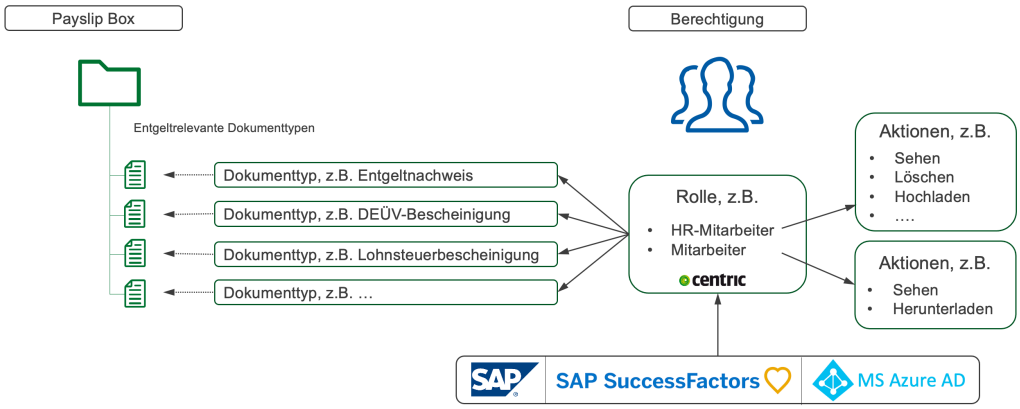


Abbildung 9: Berechtigung Payslip Box

Centric Document Builder

Zur Steuerung der Berechtigungen hinsichtlich der Nutzung und Verwaltung von Dokumentvorlagen werden im Centric Document Builder „Security-Tags“ verwendet. Diese „Security-Tags“ werden einer oder mehreren Dokumentvorlagen zugeordnet und im Rollenmapping des Centric Document Builder der jeweiligen Rolle zugewiesen.

Darüber hinaus wird die „SAP Principal Propagation“ bei der Erstellung von Dokument genutzt. Somit ist sichergestellt, dass die im SAP eingestellte Stammdaten-User-Berechtigung auch für die Verwendung der Stammdaten bei der Dokumenterstellung aktiv ist.

(Weitere Informationen zu Akten- und Dokumentfunktionen in unserer Produktübersicht unter Centric.eu)

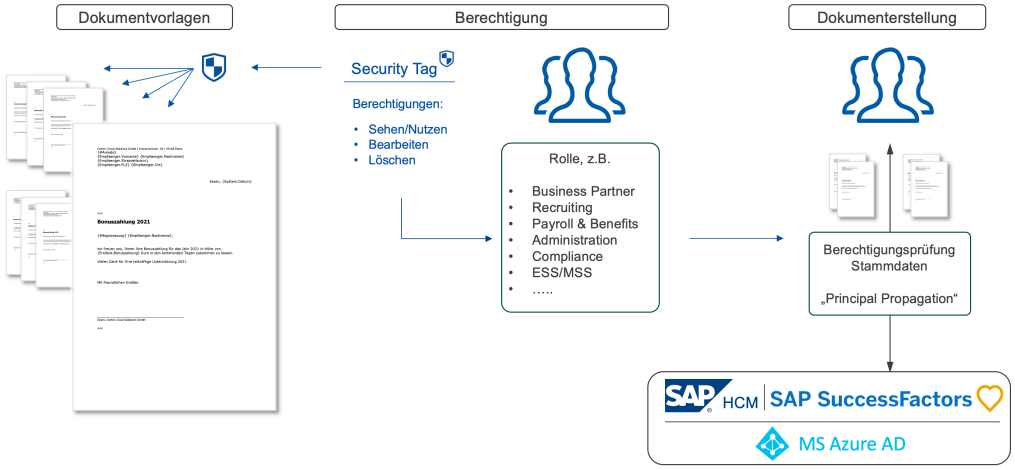


Abbildung 10: Berechtigung Document Builder

Centric Reference Letter

Die Berechtigungen in Centric Employee File basieren auf dem Berechtigungskonzept des angebundenen SAP-Systems (SAP HCM / SuccessFactors).

Die jeweiligen Rollen können auf die Verwaltung der Zeugnisvorlagen und Tätigkeiten im Erstellungsprozess berechtigt werden.

Die Auswahl der Führungskraft im Erstellungsprozess zur Bewertung des Mitarbeiters / der Mitarbeiterin, kann automatisiert auf Basis des angebunden SAP HCM / SuccessFactors oder manuell im Prozess erfolgen.

(Weitere Informationen zu Akten- und Dokumentfunktionen in unserer Produktübersicht unter Centric.eu)

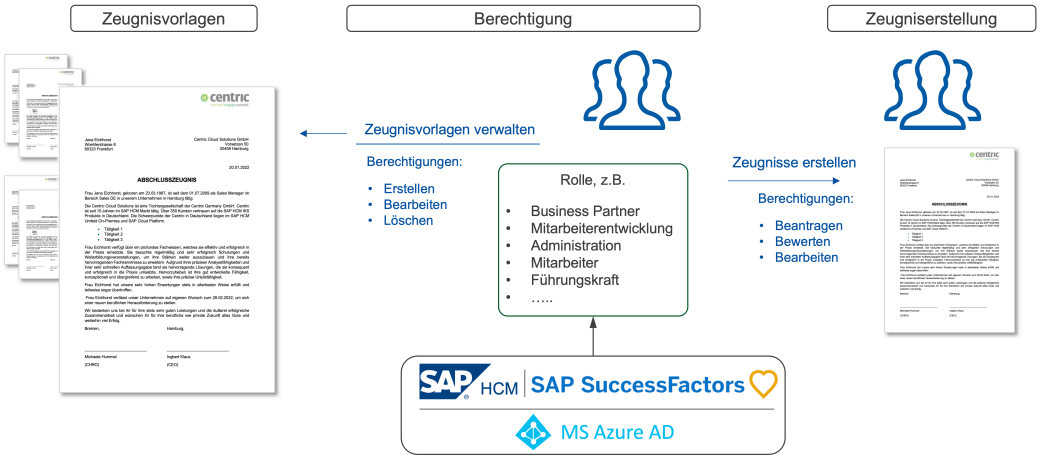


Abbildung 11: Berechtigung Reference Letter

7.6 BackUp & Recovery

Durch die Nutzung der von SAP auf der SAP Business Technology Platform zur Verfügung gestellten Services, werden sämtliche BackUp & Recovery Funktionalitäten durch die SAP abgedeckt.

Die BackUps werden in einem EU-only Rechenzentrum 15 Tage vorgehallten und im nachfolgendem Zeitintervall erstellt:

- Vollständiges BackUp – täglich
- Inkrementelles BackUp – alle 15 Minuten

Zusätzlich sind die Services der SAP Business Technology Platform für den Katastrophenfall mit einem „Disaster Discovery“ in einem Rechenzentrum EU-only abgesichert.

Das BackUp umfasst die Daten in der Datenbank (SAP HANA Cloud) und die Document im Archiv Service (SAP Document Service, Object Store)

8 Compliance

Bei Centric betrachten wir die Informationssicherheit und den Schutz personenbezogener Daten als einen wichtigen Teil unserer Geschäftsabläufe und Dienstleistungen.

Deshalb gelten die folgenden Grundsätze:

- Informationssicherheit ist ein Prozess, nicht ein Projekt.
- Informationssicherheit ist umfassender als IT.
- Der Zweck der Informationssicherheit ist es, einen angemessenen Schutz der Informationen zu gewährleisten.
- Das Bewusstsein aller für die Informationssicherheit ist wesentlich.

In diesem Kapitel möchten wir Ihnen die wichtigsten Inhalte zu dem Thema zusammenfassen.

8.1 Centric-interne Guidelines & Policies

Die Datenintegrität in der Centric-Organisation wird sichergestellt durch vordefinierte Guidelines und Policies.

8.1.1 Centric Information Security Policy

Die Information Security Policy enthält grundlegende Prinzipien und Steuerungsmechanismen für eine angemessene Informationssicherheit. Das Hauptziel der Policy ist es, die Zuverlässigkeit der Informationsbereitstellung innerhalb unseres Unternehmens zu gewährleisten und auf der Grundlage einer Risikobewertung jeglichen Schaden für Kunden und die Centric-Organisation zu vermeiden oder zu begrenzen.
Um ein standardisiertes Vorgehen bei der Risikoanalyse der verfügbaren Informationen und der damit verbundenen Dienste zu ermöglichen, orientieren wir uns an der *CIA-Triade*:

- **Vertraulichkeit:** Informationen müssen vor unberechtigtem Zugriff geschützt werden.
- **Integrität:** Richtigkeit und Vollständigkeit der Informationen müssen gewährleistet sein. Integrität bedeutet, dass die Konssicistenz, Richtigkeit und Vertrauenswürdigkeit der Daten gewahrt bleibt.
- **Verfügbarkeit:** Informationen und wichtige Dienste müssen zu den gewünschten Zeiten verfügbar sein.

Die ordnungsgemäße Einbettung der Policy wird durch ein Informationssicherheitsmanagementsystem (ISMS) gewährleistet. Dieses ist als Prozess zu sehen und folgt dem *PDCA-Zyklus von Deming* (Plan-Do-Check-Act) und ist in der Norm ISO/IEC 27001:2013 beschrieben. Durch die Anwendung dieser Verbesserungsmethodik ist die Centric Organisation stets in der Lage, die Informationssicherheit auf einem hohen Niveau zu halten.

Zur Aufrechterhaltung und regelmäßigen Kontrolle hat der Centric Vorstand einen Corporate Information Security Officer ernannt, welcher wiederum je Geschäftsbereich einen Information Security Officer ernennt.

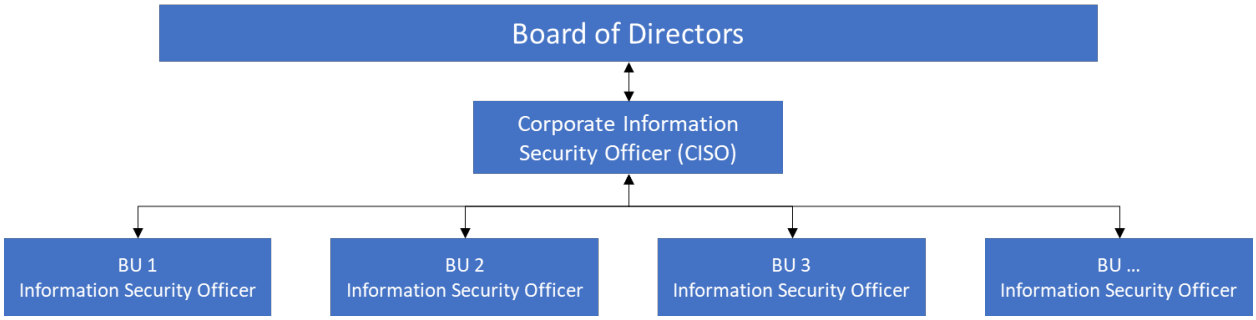


Abbildung 12: Organisation Informationssicherheit

Darüber hinaus dient eine eigene Intranet-Seite Mitarbeiter*innen als zentraler Anlaufpunkt zum Thema Informationssicherheit, zum Beispiel zum Start von internen Prozessen, wie das Reporting von Datenschutzvorfällen (Incidents).

8.1.2 Centric Baseline Information Security (V3)

Die Centric Baseline Information Security ist in dieselben Abschnitte unterteilt, wie die Norm ISO 27002:2013. Sie stellt die Basis für Entscheidungen, Verfahren, Maßnahmen, Verhaltenskodizes und Arbeitsanweisungen in Bezug auf die Informationssicherheit dar.

Ein maßgeblicher Abschnitt der Baseline Information Security beschreibt die Klassifizierung und Verwaltung von Unternehmensressourcen (primär Informationen) mit dem Ziel alle Informationen zu registrieren und mit dem Eigentümer zu verknüpfen. Demnach sind Centric-intern alle Träger von Informationen, wie bspw. Dokumente, E-Mails oder andere Formate in drei Kategorien zu klassifizieren (V1 = public, V2 = restricted, V3 = confidential).

Aufgrund der Sensibilität der Inhalte gilt für die Baseline Information Security selbst ebenfalls eine V3 Klassifizierung, sodass das Dokument nicht extern geteilt werden darf. Dennoch möchten wir Ihnen einen groben Überblick über die Inhalte der Baseline Information Security geben. Folgende Themenabschnitte werden im Rahmen der Centric Baseline Information Security behandelt, die jeweiligen Inhalte definiert und über Maßnahmen in den Betriebsalltag integriert.

1. Interne Organisation
2. Mobile Endgeräte & Telearbeit:
    - Mobile-Device-Management (MDM) und zentrale Verwaltung durch die Centric-IT.
    - Zugriff auf Informationen über gesicherte Netzwerke.
    - Home-Office Maßnahmen zur Sicherung der Verbindung (VPN).
3. Human Resources Security, durch
    - Screening im Recruiting-Prozess
    - Vertraglichen Vereinbarungen zum Datenschutz / Sanktionen bei Zuwiderhandlung.
    - Mitarbeiterhandbuch und Code of Conduct
    - Aufgabentrennung bei Verantwortlichkeiten / Ausübung vs. Freigabe der Tätigkeiten / Freigabeprozesse
    - Unterweisungen, Schulungen, etc.
    - Reporting-Prozesse
    - Beendigung und Änderungen in Bezug auf das Arbeitsverhältnis
4. Assetmanagement
    - Verantwortlichkeit und Eigentümerschaft
    - Klassifizierung von Daten / Informationen.
    - Datenspeicherung, Datenhandling, Zugriffsberechtigungen und Vernichtung
    - Mobile Speichermedien und Drucken
5. Zugriffskontrolle
    - Zugriffsmetrik
    - Benutzerverwaltung und Benutzerverantwortung
    - Authentifizierung, sicheres Login, Kontrolle / Multifaktor-Authentifizierung
    - Autorisierungen / Berechtigungen
    - Passwortrichtlinie
    - Externer Zugriff
6. Verschlüsselung
    - Vorgaben gemäß Klassifizierung
    - Notebooks, externe Speichermedien, Schnittstellen
    - Dokumente, E-Mails
    - Datenbanken
7. Physische Sicherheit
    - Zutrittsregelungen (Mitarbeiter und Besucher)
    - Sichere Räume und Sicherheitszonen
    - Externe Risiken
    - *Clean Desk und Clean Screen*
8. Operationale Sicherheit
    - Operationale Prozesse und Change-Management
    - Teilung von Systemen (Entwicklung / Test / Produktion)
    - Virenschutzmaßnahmen und Firewall
    - Logging von Benutzern und Administratoren
    - Vulnerability Management
    - Backups
9. Sichere Kommunikation
    - Netzwerksicherheit und -teilung
    - Kommunikation, Informationsübermittlung und E-Mails
    - Verbale Kommunikation
10. Sicherer Kauf von Software und sichere Softwareentwicklung (SSD)

- Prüfprozess bei der Beschaffung von interner Software
- Grip-on-SSD Methodik: Erstellt vom Kompetenzzentrum für Informationssicherheit und Schutz der Privatsphäre von, für und durch niederländische Regierungsorganisationen.
- Sicherer Code & Escrow

11. Lieferantenbeziehungen
    - Vertragliche Vereinbarungen
    - Vorgaben an die Informationssicherheit
    - Vorgaben an ethische Compliance-Maßnahmen
12. Informationssicherheit - Incident Management
    - Definition *Security Incident* und *Data Leak*
    - „Incident Management Procedure“
    - Registrierung, Bewertung und Abwicklung von *Incidents*
    - Reporting-Prozesse (intern, Betroffene, staatl. Institutionen)
13. Business Continuity
    - Impact-Analyse
    - Continuity Plan
    - Maßnahmen
    - Pläne in Bezug auf Pandemien, Evakuierung, Notfälle, etc.
14. Compliance
    - Gesetze, Vorschriften, Normen, bewährte Verfahren und Leitlinien
    - Compliance der Centric Mitarbeiter*innen
    - Compliance von Drittanbietern, Lieferanten und sonstigen Partnern
    - Überprüfung der Wirksamkeit der Sicherheitskontrollen
    - Audits
15. Appendix
    - Matrix zur Informationsklassifizierung

8.1.3 Centric Privacy Policy (V2)

Die Privacy Policy stellt sicher, dass die Datenverarbeitung compliant mit der EU-DSGVO und der nationalen Gesetzgebung erfolgt. Sie umfasst die Verarbeitung von Mitarbeiterdaten, Kundendaten, Lieferantendaten und daten weiterer Parteien und erstreckt sich auf alle Business Units der Centric – unabhängig davon, ob die Verarbeitung elektronisch oder nicht-elektronisch erfolgt. Die Richtlinie schreibt die Überwachung des gesamten Lebenszyklus‘ der personenbezogenen Daten innerhalb von Centric vor, von der Erhebung und der Speicherung bis zur täglichen Nutzung, Aufbewahrung und Vernichtung. Dabei werden folgende Prinzipien vorgegeben:

- Rechtmäßigkeit, Fairness und Transparenz
- Beschränkung auf den Grund der Verarbeitung
- Datenminimierung
- Richtigkeit
- Speicherlimitation
- Integrität und Vertraulichkeit
- *Privacy by Default* / Datenschutz-freundliche Grundeinstellungen

Der zweite Abschnitt regelt die interne Organisation zur Umsetzung der Vorgaben. Dazu wird eine Ämterstruktur etabliert. Analog zur oben aufgeführten Grafik liegt die Gesamtverantwortung für den Datenschutz im Centric Vorstand. Weiterhin werden die Rollen *Privacy Officer* und *Privacy Coordinator*

eingeführt und sowohl der Verantwortungsbereich der Ämter, des Managements der Business Unit als auch der Centric Mitarbeiter geregelt.

Darüber hinaus gibt die Privacy Policy Aufschluss über die Rechtmäßigkeit der Datenverarbeitung, die *Centric Privacy Services* und etabliert ein *Privacy Programm*, welches sowohl regelmäßige Schulungen und Sensibilisierungsmaßnahmen vorsieht als auch Arbeitsanweisungen und Abläufe beschreibt.

Jegliche Datenschutzvorfälle werden den örtlichen Behörden umgehend gemeldet.

Weitere Informationen finden sich im jährlichen *Privacy Report*.

8.1.4 Centric Trust Center

Generelle Informationen zu den Themen *Information Security, Privacy und Corporate Social Responsibility* finden Sie online im Centric Trust Centric.

1. Centric Privacy Notice
2. Centric Information Security

Weitere Kontaktmöglichkeiten:

1. Ihr Sales Manager
2. Privacy@centric.eu für Rückfragen zum Datenschutz
3. Security@centric.eu für Rückfragen zum Informationssicherheit

8.2 DSGVO / EU-GDPR

Die DSGVO definiert grundlegende Vorgaben zum Datenschutz und zur Verarbeitung von Daten. Somit dürfen lediglich Daten verarbeitet werden, wenn ein legitimer Grund dazu besteht. In Artikel 88 wird die Datenverarbeitung im Beschäftigungskontext explizit als “besondere Verarbeitungssituation” aufgeführt, sodass die Datenverarbeitung legitimiert wird, aber auch besondere Vorschriften definiert werden. Diese Vorgaben müssen selbstverständlich durch IT-Systeme (wie bspw. eine digitale Personalakte) erfüllt werden. Der dabei wohl wichtigste Punkt ist, dass das System mindestens genauso sicher sein muss, wie die nicht-technische Lösung (bspw. die digitale Personalakte genauso sicher, wie die Papierakte). Im Folgenden gehen wir auf die wichtigsten Artikel ein.

8.2.1 Schutz vor unbefugtem Zugriff (Art. 5f)

Zum Thema „Sicherheit“ spielen eine Vielzahl von Faktoren eine Rolle. Zunächst einmal ist durch den Anwender einer Software sicherzustellen, dass keine unbefugte Person Zugang zu dem PC erhält. Versetzten Sie deshalb stets bei Verlassen des Arbeitsplatzes Ihren PC in Standby-Mode, sodass Sie sich neu authentifizieren müssen. Die Authentifizierung funktioniert klassisch über Ihren Benutzernamen des eingesetzten *Application Identity Providers* (bspw. SuccessFactors User und Passwort oder Active Directory User und Passwort). Auf diese Weise ist der unbefugte Zugriff erst einmal ausgeschlossen. Darüber hinaus erhält jeder Mitarbeiter vordefinierte Berechtigungen. In der Regel werden diese aus Ihrem SAP HCM-System oder SuccessFactors übernommen, können aber noch granularer im Customizing der Centric Produkte angepasst werden. So ist stets gewährleistet, dass ausschließlich Daten und Dokumente einsehbar sind, an denen der User ein berechtigtes Interesse hat. Dies gilt selbstverständlich für alle Möglichkeiten der Einsicht (Suchfunktion, Analysen, Gesamtübersichten, etc.). Zudem können auch Funktionen, wie z.B. der Export einer Akte oder das Drucken eines in der Personalakte befindlichen Dokumentes nur ausgewählten Mitarbeitern ermöglicht werden, um auch hier unbefugten Zugriffen vorzubeugen.

8.2.2 Auskunftsrecht der betroffenen Person (Art. 15)

Nach der DSGVO hat eine betroffene Person das Recht, binnen weniger Stunden Auskunft über Art und Umfang der sie betreffenden Datenverarbeitung zu erhalten. Mit Centric Employee File haben Sie die Möglichkeit Mitarbeitern temporären oder auch dauerhaften Zugriff auf die eigene Akte zu gewähren. Der auskunftsberechtigten Person kann also das Recht erteilt werden, die gespeicherten Daten und Dokumente selbstständig einzusehen.

8.2.3 Recht auf Löschung ("Recht auf Vergessenwerden") (Art. 17)

Mit der DSGVO erhalten so genannte natürliche Personen das Recht, die sie betreffenden Daten unverzüglich löschen zu lassen, sofern z. B. der berechtigende Zweck der Datenerhebung weggefallen ist. In Centric Produkten werden keine Daten führend gespeichert, sondern ausschließlich aus den Stammdaten Ihres führenden Personalmanagementsystems (PMS) angezeigt. Daher sind bei Löschung der Stammdaten im PMS auch Daten in den Centric-Produkten gelöscht. Gespeicherte Dokumente lassen sich darüber hinaus manuell oder automatisiert löschen. Es lässt sich bspw. konfigurieren, dass Dokumente rückstandslos nach einer vordefinierten Zeitspanne gelöscht werden.

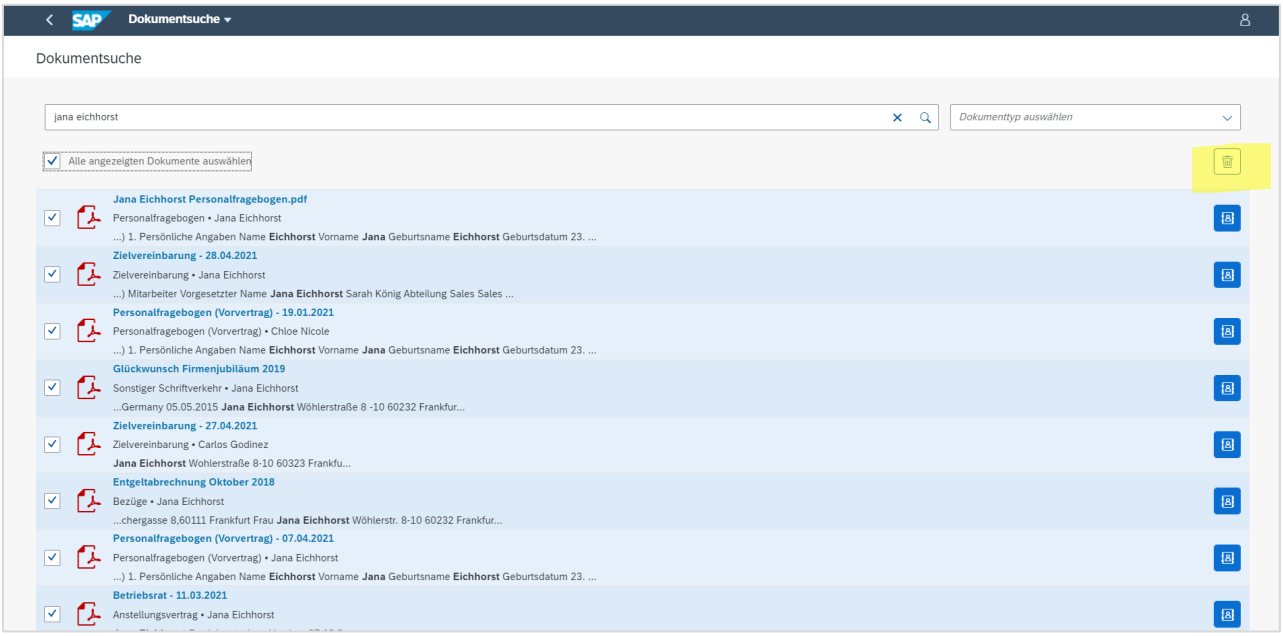


Abbildung 13: Manuelle Löschung von personenbezogenen Dokumenten (auch Mehrfachauswahl)

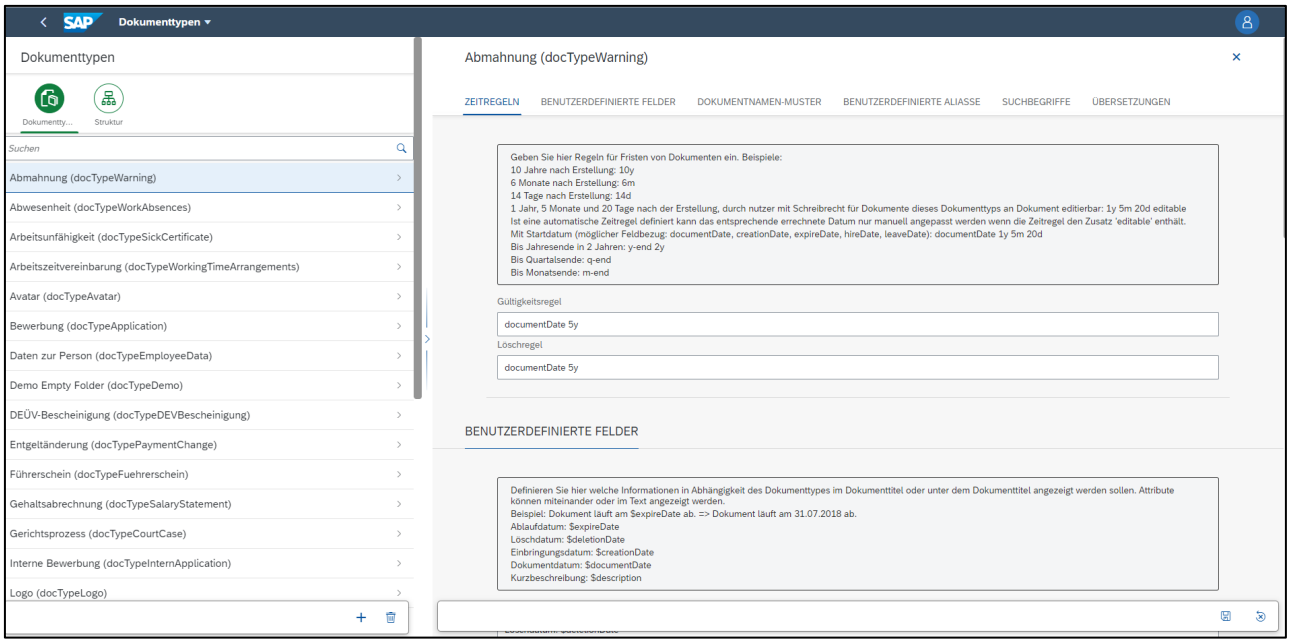


Abbildung 14: Konfiguration von Löschregeln zur automatisierten Löschung

8.2.4 Recht auf Datenübertragbarkeit (Art. 20)

Centric Produkte unterstützen über die integrierten Exportmöglichkeiten das Recht auf Datenübertragbarkeit. Die Daten / Dokumente können in einem für andere Systeme bzw. Menschen lesbaren Format systematisch, auch auszugsweise, bereitgestellt werden.

8.2.5 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Art. 22)

Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Mithilfe der Centric Produkte werden keine Profile gebildet oder automatisierten Entscheidungen getroffen, die zulasten von Personen gehen können.

8.2.6 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (“Privacy by Default”) (Art. 25)

Eine wesentliche Forderung der DSGVO betrifft Sicherheit des Zugriffs auf personenbezogene Daten. Laut Artikel 25 der DSGVO gilt es mit der Datenverarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen durch geeignete technische und organisatorische Maßnahmenden und dem Einsatz geeigneter Mittel zu vermeiden. Dies soll sowohl bei der Implementierung und Konfiguration (Privacy by Design) als auch durch eine entsprechende Voreinstellung der Software (Privacy by Default) erreicht werden. Die Centric Produkte sind auf Basis einer modernen Architektur mit höchsten Sicherheitsstandards entwickelt. Zudem folgen alle Produkte strickt nach dem “Privacy by Default” Prinzip entwickelt, sodass Rechte zur Nutzung der Funktionen oder Einsicht der Inhalte aktiv zugeordnet werden müssen. Sehr gerne sprechen wir in einem gesonderten Termin mit Ihnen über die Maßnahmen zur Datensicherheit.

8.2.7 Verantwortlicher und Auftragsverarbeiter (Art. 28)

Der Kunde bleibt Verantwortlicher im Sinne Art. 28. Centric verarbeitet die Daten nicht in eigener Sache, sondern lediglich im Auftrag des Kunden. Zur Transparenz über betroffene Personen und verarbeitete Daten wird eine gesonderte Auftragsdatenvereinbarung (AVV) geschlossen. Weitere mögliche Subunternehmer zur Auftragserfüllung sind in der AVV aufzuführen und durch den Kunden zu genehmigen.

8.2.8 Sicherheit der Verarbeitung (Art. 32)

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen sind in den *Centric technisch-organisatorischen Maßnahmen* als Anlage zur AVV aufgeführt.

8.2.9 Stellung des Datenschutzbeauftragten (Art. 38)

Herr Jens Langguth (TÜV) ist als externer Datenschutzbeauftragter der Centric Cloud Solutions GmbH eingesetzt. Die Mitarbeiter werden regelmäßig in Bezug auf Datensicherheit, Datenschutz und dem Umgang mit personenbezogenen Daten geschult. Außerdem sind die Mitarbeiter der Centric Cloud Solutions durch Unterzeichnung einer Verpflichtungserklärung zur Wahrung des Datengeheimnisses gemäß Bundesdatenschutzgesetz (DSGVO) verpflichtet.

8.2.10 Zertifizierung (Art. 42)

Zertifizierungsverfahren können dabei helfen die Einhaltung von Sicherheitsstandard in Bezug auf den Datenschutz sicherzustellen. Gerne geben wir Ihnen im nachfolgenden Kapitel 8.3 einen Überblick über relevante Zertifizierungen.

8.3 Zertifizierungen

Zertifizierungen unterstützen mithilfe standardisierter Prüfkataloge die Qualität und Sicherheit von Software-Applikationen. Gerne fassen wir Ihnen die relevanten Zertifizierungen zusammen.

8.3.1 Information Security Management System

KPMG

Certificate

KPMG Cert GmbH
Umweltgutachterorganisation
Barbarossaplatz 1a, 50674 Cologne, Germany

certifies that

SAP SE
Dietmar-Hopp-Allee 16
69190 Walldorf, Germany

with the locations and organizational units as listed in the annex

has established and applies an **information security management system** for the scope

„Operations of **SAP Business Technology Platform** and the services as provided on the Annex of the certificate".
This is in accordance with the Statement of Applicability (SoA) dated 04-03-2021.

A certification audit conducted by KPMG, documented in a report, has verified that the management system complies with the requirements of the following standard:

DIN EN ISO/IEC 27001:2017

In addition to this certification, the organization uses the norms **ISO/IEC 27017:2015** and **ISO/IEC 27018:2019** as sources for the control set as defined in the SoA.

Certification number	11860521
Certification date	31st May 2021
Certificate valid from	1st June 2021
Certification valid until	31st May 2024

DAkkS Deutsche Akkreditierungsstelle D-ZM-16103-01-00

Wilhelm Dolle
Managing Director

Georg Hartmann
Certification body

ISO 27001 der SAP BTP

Die Norm definiert Anforderungen an die Implementierung, Weiterentwicklung und laufende Kontrolle eines *ISMS*. Das Informationssicherheits-Managementsystem dient dazu, die übergeordneten Schutzziele der Verfügbarkeit, Vertraulichkeit und Integrität von Informationen zu gewährleisten.

Das Zertifikat umfasst sowohl die technische Platform der SAP Business Technology Platform als auch den Betrieb im SAP Rechenzentrum.

Nachweise bzw. die aktuell gültige Fassung des Zertifikats können im SAP Trust Center eingesehen werden.

8.3.2 Business Continuity Management System

KPMG

Certificate

KPMG Cert GmbH
Umweltgutachterorganisation
Barbarossaplatz 1a, 50674 Cologne, Germany

certifies that

SAP SE
Dietmar-Hopp-Allee 16
69190 Walldorf, Germany

with the locations and organizational units as listed in the annex

has established and applies a **business continuity management system** for the scope

„Operations of **SAP Business Technology Platform** and the services as provided on the Annex of the certificate".

A certification audit conducted by KPMG, documented in a report, has verified that the management system complies with the requirements of the following standard:

DIN EN ISO 22301:2020-06

Certification number	12090621
Certification date	31st May 2021
Certificate valid from	1st June 2021
Certification valid until	31st May 2024

DAkkS Deutsche Akkreditierungsstelle D-ZM-16103-01-00

Wilhelm Dolle
Managing Director

Georg Hartmann
Certification body

ISO 22301 der SAP BTP

Die Norm definiert Anforderungen an Prozesse zur Sicherstellung der Geschäftskontinuität. Dies dient dazu, dass Maßnahmen ergriffen werden, um eine Unterbrechung der Leistungserbringung auszuschließen oder auf ein Minimum zu reduzieren. Sollte dennoch ein Vorfall auftreten, welcher die Lieferung der Services unterbricht, sind Mechanismen zu etablieren, sodass die Leistungserbringung auf vordefinierten und akzeptablen Ebenen fortgesetzt werden kann. Darüber hinaus ist sicherzustellen, dass die volle Leistungsfähigkeit in kürzester Zeit wiederhergestellt werden kann.

Das Zertifikat umfasst sowohl die technische Platform der SAP Business Technology Platform als auch den Betrieb im SAP Rechenzentrum.

Nachweise bzw. die aktuell gültige Fassung des Zertifikats können im SAP Trust Center eingesehen werden.

8.3.3 CSA Star

KPMG

Certificate

KPMG Cert GmbH
Umweltgutachterorganisation
Barbarossaplatz 1a, 50674 Cologne, Germany

certifies that

SAP SE
Dietmar-Hopp-Allee 16
69190 Walldorf, Germany

with the locations, organizational units and services as listed in the annex of the ISO/IEC 27001 certificate with the certification number 11860521

has established and applies an **information security management system** for the scope

„Operations of **SAP Business Technology Platform** and the services as provided on the Annex of the ISO/IEC 27001 certificate".

A certification audit conducted by KPMG, documented in a report, has verified that the management system complies with the requirements of the following standard:

CSA STAR, CCM version 3.0.1

Certification number	11860521(1)[1]
Certification date	31st May 2021
Certificate valid from	1st June 2021
Certification valid until	31st May 2024

Wilhelm Dolle
Managing Director

Georg Hartmann
Certification body

[1] Valid only with certificate No. 11860521 provided for SAP SE.

CSA STAR Zertifizierung der SAP BTP

Die CSA STAR-Zertifizierung ist eine strenge, unabhängige Bewertung der Sicherheit eines Cloud-Service-Anbieters durch Dritte. Diese technologieneutrale Zertifizierung nutzt die Anforderungen der Managementsystemnorm ISO/IEC 27001:2013 zusammen mit der CSA Cloud Controls Matrix.

Nachweise bzw. die aktuell gültige Fassung des Zertifikats können im SAP Trust Center eingesehen werden

8.3.4 SAP Produkt Zertifizierung

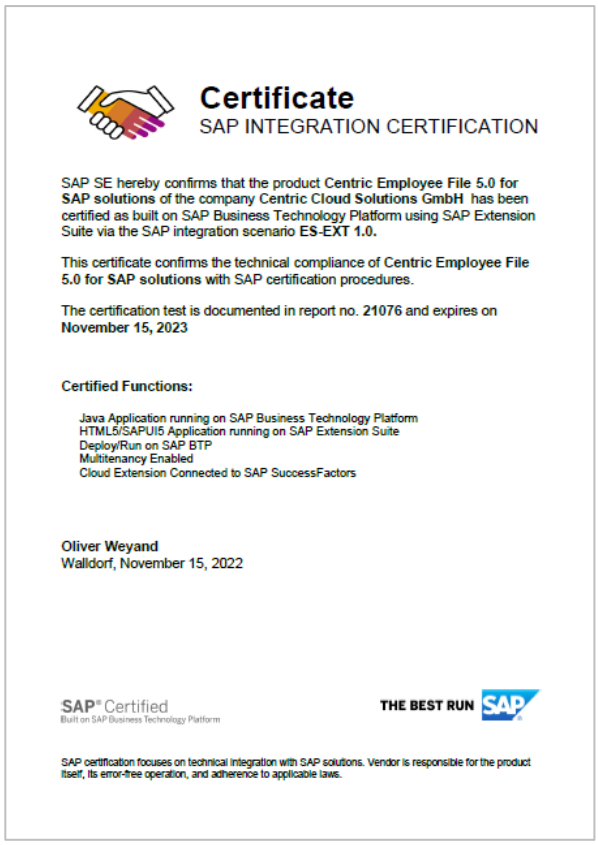
Centric legt Wert auf einen hohen Qualitätsstandard der Produkte. Qualität lässt sich dabei aus unterschiedlichen Perspektiven bemessen. Anwender*innen bewerten die Qualität anhand von Produktfunktionen und dem Oberflächenergonomie. Techniker*innen bewerten die Qualität anhand der Architektur und den Sicherheitsmechanismen. Darüber hinaus hat SAP weitere Qualitätsstandards für Partnerprodukte definiert und bietet ein Zertifizierungsverfahren an. Um die Zertifizierung zu erhalten, prüft SAP auf Antrag des Partners unter anderem die SAP-Integration, die Architektur, die Nähe zur SAP Roadmap und sicherheitsrelevante Inhalte, wie bspw. die Multitenancy, welche den Datenschutz durch strikte Trennung von Kundendaten sicherstellt.

Centric lässt die Produkte jährlich durch SAP zertifizieren.

Available on **SAP Store**

SAP® Certified
Built on SAP Business Technology Platform

Centric Employee File



Certificate
SAP INTEGRATION CERTIFICATION

SAP SE hereby confirms that the product **Centric Employee File 5.0 for SAP solutions** of the company **Centric Cloud Solutions GmbH** has been certified as built on SAP Business Technology Platform using SAP Extension Suite via the SAP integration scenario **ES-EXT 1.0.**

This certificate confirms the technical compliance of **Centric Employee File 5.0 for SAP solutions** with SAP certification procedures.

The certification test is documented in report no. **21076** and expires on **November 15, 2023**

Certified Functions:

Java Application running on SAP Business Technology Platform
HTML5/SAPUI5 Application running on SAP Extension Suite
Deploy/Run on SAP BTP
Multitenancy Enabled
Cloud Extension Connected to SAP SuccessFactors

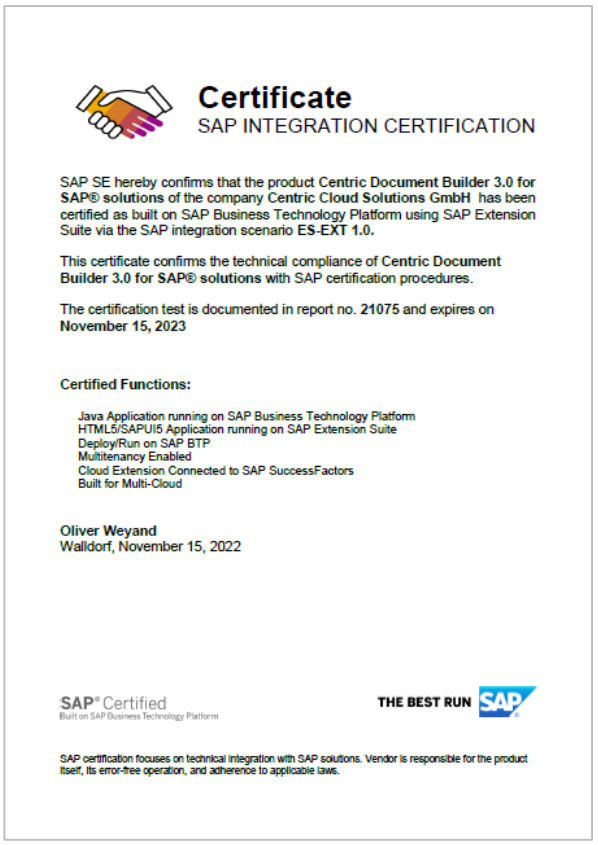
Oliver Weyand
Walldorf, November 15, 2022

SAP® Certified
Built on SAP Business Technology Platform

THE BEST RUN SAP

SAP certification focuses on technical integration with SAP solutions. Vendor is responsible for the product itself, its error-free operation, and adherence to applicable laws.

Centric Document Builder



Certificate
SAP INTEGRATION CERTIFICATION

SAP SE hereby confirms that the product **Centric Document Builder 3.0 for SAP® solutions** of the company **Centric Cloud Solutions GmbH** has been certified as built on SAP Business Technology Platform using SAP Extension Suite via the SAP integration scenario **ES-EXT 1.0.**

This certificate confirms the technical compliance of **Centric Document Builder 3.0 for SAP® solutions** with SAP certification procedures.

The certification test is documented in report no. **21075** and expires on **November 15, 2023**

Certified Functions:

Java Application running on SAP Business Technology Platform
HTML5/SAPUI5 Application running on SAP Extension Suite
Deploy/Run on SAP BTP
Multitenancy Enabled
Cloud Extension Connected to SAP SuccessFactors
Built for Multi-Cloud

Oliver Weyand
Walldorf, November 15, 2022

SAP® Certified
Built on SAP Business Technology Platform

THE BEST RUN SAP

SAP certification focuses on technical integration with SAP solutions. Vendor is responsible for the product itself, its error-free operation, and adherence to applicable laws.

(Weitere Informationen zu der Zertifizierung erhalten Sie unter https://www.sap.com/germany/partners/partner-program/certify-my-solution/software.html)

8.3.5 Penetrationstest

Centric legt großen Wert auf die Sicherheit der Daten und Dokumente aller Kunden. Aus diesem Grund lässt Centric jährlich durch einen externen und spezialisierten Anbieter einen Penetrationstest durchführen. Der Umfang des Tests umfasst:

- Blackbox Pen-Test zur Überprüfung der Cloud-/Infrastruktursicherheit durch Simulation externer/realer Angriffe
- Greybox Pen-Test mit Anmeldung auf Benutzerebene (reine Anwendungsautorisierung) zur Testung der Anwendung auf Basis der Anwendungsnutzer.

Das zusammenfassende Urteil wurde wie folgt beschrieben:

„Die Analyse der Centric-Umgebung zeigt ein gut abgesichertes System in einer professionellen Multi-Tenant-Umgebung eines Hyperscalers. Alle klassischen Anforderungen an eine sichere Umgebung sind im Sinne des BSI-Konzepts des "Stand der Technik" erfüllt. Da die SAP-Cloud auch dem BSI-Kriterienkatalog C5 (Cloud Computing Compliance) entspricht, gilt diese Konformität somit auch für die gesamte Centric-Anwendung. Es konnten keine signifikanten Angriffspunkte identifiziert werden (höher als CVSS Score 3). Alle potenziellen Angriffspunkte (Ports, Zugänge, Webseiten) wurden entsprechend abgesichert. Die Sicherheit ist aus Sicht des Pen-Tests solide und gut.“

Auf Anfrage stellen wir den detaillierten Report gerne zur Verfügung.

BSI-Grundschutz

Der BSI-Grundschutz sieht die sachgerechte Anwendung bewährter technischer, organisatorischer, personeller und infrastruktureller Sicherheitsvorkehrungen vor mit dem Ziel ein Sicherheitsniveau zu erreichen, das geeignet und angemessen ist, geschäftsrelevante Informationen mit durchschnittlichem Schutzbedürfnis zu schützen. Dabei definiert der BSI-Grundschutz den "Stand der Technik" für Sicherheit und entspricht sowohl der EU-DSGVO als auch den Kriterien der Norm ISO 27701.

➔ Der BSI-Grundschutz ist gegeben.

C5-Kriterien

Der C5-Kriterienkatalog (Cloud Computing Compliance Criteria Catalogue) legt Mindestanforderungen für sicheres Cloud Computing fest und richtet sich vor allem an professionelle Cloud-Anbieter, deren Auditoren und Kunden.
Der C5-Kriterienkatalog wurde erstmals 2016 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht und zwischenzeitlich erfolgreich am Markt etabliert.

➔ Die Centric Produkte entsprechen den C5-Kriterien.

OWASP 10

Das Open Web Application Security Project (OWASP) ist eine Non-Profit-Organisation mit dem Ziel, die Sicherheit von Anwendungen und Diensten im World Wide Web zu verbessern. Durch die Schaffung von Transparenz sollen Endbenutzer und Organisationen in die Lage versetzt werden, fundierte Entscheidungen über tatsächliche Sicherheitsrisiken in Software zu treffen. Jeder Pen-Test von Webanwendungen sollte diese Kategorien abdecken.

Zu diesem Zweck werden jedes Jahr die Top-10-Kategorien der aktuellen Bedrohungen für Webanwendungen aufgelistet. Hier finden Sie die aktuelle Liste

➔ Alle 10 Kriterien wurden geprüft und keine Risiken festgestellt.

9 Supportservices

9.1 Ansprechpartner beim Kunden

Im Rahmen des Onboarding-Prozesses benennt der Kunde autorisierte Personen in seiner Organisation, die gegenüber der Centric berechtigt sind, kostenpflichtige Zusatzoptionen zu bestellen sowie kostenpflichtige und / oder sicherheitsrelevante Dienstleistungen zu beauftragen. Derartige Bestellungen oder Beauftragungen müssen in Textform erfolgen, z.B. per Brief, per Fax oder per E-Mail. Dabei muss der Aussteller der Vollmacht berechtigt und eindeutig erkennbar sein.

Die Meldung von Fehlern und Störungen können von autorisierten Personen beim Kunden vorgenommen werden.

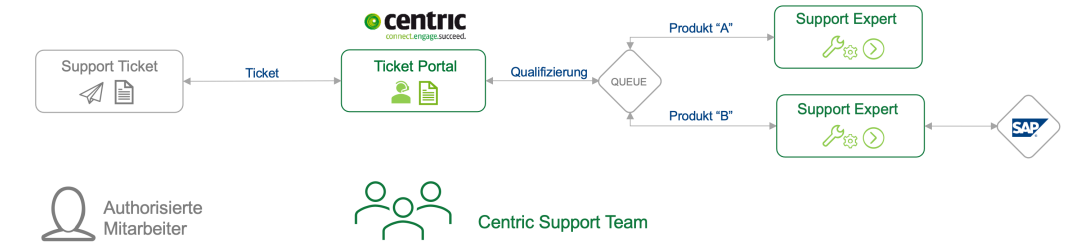
9.2 Centric Service Desk

Der Centric Service Desk ist die zentrale Anlaufstelle für die Kunden (Single Point of Contact).

Die Mitarbeiter des Service Desk nehmen Serviceaufträge und Störungsmeldungen (Incident Management) an. Die Serviceaufträge und Störungsmeldungen werden als *Tickets* dokumentiert, kategorisiert und priorisiert. Die Durchführung der Serviceaufträge oder die Beseitigung der Störungen erfolgen gemäß dem vereinbartem Service Level.

Störungen sind per E-Mail über Ticketsystem an support@centric.managed-otrs.com zu melden.

Dabei liefert er soweit möglich alle zur Entstörung benötigten Informationen zur Behebung der Störung (wie z. B. betroffene Standorte, Auswirkung der Störung und Dringlichkeit).



support@centric.managed-otrs.com

Ticket:
- Produkt
- Beschreibung
- Zusätzliche Informationen
- Ausmaß / Dringlichkeit

Level	Definition	Reaktionszeit	Service-Zeiten	Hinweis
P1	Totaler Ausfall des gesamten Systems (Totalausfall)	2h	24h / 5d	Eskalation an SAP
P2	Arbeiten ist möglich, aber nur unter massiven Einschränkungen	4h	9-18h / 5d	
P3	Arbeiten ist mit einigen Einschränkungen möglich	8h	9-18h / 5d	
P4	Arbeit ist unter kaum bemerkbaren Einschränkungen möglich	16 h	9-18h / 5d	

Abbildung 15: Supportprozess

9.3 Servicezeiten des Service Desk

Der Centric Service Desk ist von montags bis freitags zwischen 09:00 Uhr und 17:00 Uhr erreichbar. Ausgenommen sind die gesetzlichen Feiertage sowie Heiligabend und Silvester; an diesen Tagen ist der Support nicht erreichbar.

9.4 Reaktionszeiten für Supportfälle

Beim Eingang einer Störungsmeldung wird ein Ticket angelegt. Die Reaktionszeiten sind abhängig von der jeweiligen Priorität des Tickets. Die Priorität nimmt Werte zwischen 1 (höchste Priorität) und 4 (niedrigste Priorität) an. Der Wert ergibt sich aus den beiden Faktoren Auswirkung und Dringlichkeit.
Die Auswirkung hat die Ausprägungen „Hoch“, „Mittel“ und „Niedrig“. Sie beschreibt, wie wichtig der Centric Service für die Geschäftsprozesse des Kunden ist und welche Beeinträchtigungen durch die vorhandene Störung entsteht. Die Werte für Dringlichkeit und Auswirkung werden bei der Anlage des Tickets vom Kunden erfragt und mit ihm abgestimmt.

Als Reaktionszeit wird die Zeit definiert, die zwischen der Eröffnung eines Tickets und dem Beginn einer qualifizierten Bearbeitung vergeht. Die Berechnung der Zeit wird nur innerhalb der Servicezeiten des Service Desk vorgenommen. Geht eine Störungsmeldung außerhalb dieser Servicezeiten ein, so beginnt die zugesicherte Reaktionszeit mit dem darauffolgenden Arbeitstag.

Priorität	Definition	Maximale Reaktionszeit
P1	Sehr hoch Totaler Ausfall des gesamten Systems (Totalausfall).	2 Arbeitsstunden
P2	Hoch Arbeiten ist möglich, aber nur unter massiven Einschränkungen.	4 Arbeitsstunden
P3	Mittel Arbeiten ist mit einigen Einschränkungen möglich.	1 Arbeitstag
P4	Niedrig Arbeit ist unter kaum bemerkbaren Einschränkungen möglich.	2 Arbeitstage

9.5 Wartungsfenster

Wartungsfenster, in denen Wartungsarbeiten durchgeführt werden, sind jeweils täglich 00:00 – 08:00 Uhr (MEZ/MESZ).

Eventuelle Wartungsarbeiten außerhalb dieser Zeit werden Ihnen rechtzeitig auf geeignete Art und Weise angezeigt. Darüber hinaus gelten die Wartungsfenster, die sich SAP für die SAP Cloud Plattform selbst ausbedingt: Diese Wartungszeiten sind von der Centric nicht beeinflussbar und somit ebenfalls zur Kenntnis zu nehmen und zu akzeptieren.

SAP Link:
https://www.sap.com/about/agreements/cloud-Services.html?search=service%20level%20agreement&sort=latest_asc&tag=language:german#pdf-asset=6ca1b648-fd7c-0010-87a3-c30de2ffd8ff&page=1

10 Mitwirkungspflichten

Um den Auftrag durchführen zu können, ist Centric auf bestimmte Mitwirkungsleistungen des Kunden angewiesen. Sie werden daher im erforderlichen Umfang mitwirken und dafür Sorge tragen, dass die jeweiligen Mitwirkungsleistungen in Übereinstimmung mit dem vereinbarten Zeitplan rechtzeitig, vollständig und für Centric kostenfrei erbracht werden. Werden Mitwirkungsleistungen nicht, nicht ordnungsgemäß oder nicht zu den vereinbarten Terminen erfüllt, sind die sich daraus ergebenden Entgelterhöhungen und Terminverschiebungen vom Kunden selbst zu tragen bzw. zu vertreten.

Folgende Leistungen sind durch den Kunden (als Auftraggeber) zu erbringen:

10.1 Produkt-übergreifende Mitwirkungspflichten:

- Der Kunde stellt mindestens eine interne Projektleitleitung für technische und fachliche Themen zu Verfügung, welche Deutsch oder Englisch spricht.
- Projektbegleitung durch und Verfügbarkeit von geeignetem Fachpersonal (Fachabteilung HR, technisches Personal, Security Officer, repräsentative Key User, etc.)
- Ausfüllen des Fachkonzepts, welches als Konfigurationsvorlage dient.
- Die Abnahme der jeweiligen Projektphasen erfolgt durch den Kunden (Abnahme des Fachkonzepts, Abnahme Test- bzw. Produktivumgebung nach Implementierung, finale Projektabnahme)
- Lizenzrechtliche Nutzung von SAP HCM oder SuccessFactors
- Der Kunde hat dafür Sorge zu tragen, dass bei beauftragten Entwicklungstätigkeiten Centric eine Testumgebung erhält, auf die ohne Whitelisting zugegriffen werden kann.
- Etwaige Authentifizierungsinfrastruktur (inkl. ausreichende Lizenzen) ist so durch den Kunden bereitzustellen, sodass eine Integration per SAML2 implementiert werden kann.
- **HCM-Projekte**
    - Stellung eines Systemadministrators für HCM (internes o. externes Consulting / SAP Basis)
    - Installierter und konfigurierter SAP Cloud Connector / SAP Gateway Server
    - HCM-User mit Customizing- bzw. Entwickler Berechtigungen für Centric Consultants
    - Technischer HCM-User für die Datensynchronisation über eine Destination. Der technische User sollte eine Rolle in HCM mit Zugriff auf die entsprechenden Infotypen und Zugriff auf die OData API haben (z.B. Name, Adresse, Titel, etc.)
    - Pflege und Anlage der User im Application Identity Provider (Microsoft Active Directory / SAP IAS / etc.)
- **SuccessFactors-Projekte**
    - Stellung eines Systemadministrators für SuccessFactors
    - SuccessFactors User mit Customizing-Berechtigungen für Centric Consultants
    - Technischer SuccessFactors User (inkl. OData API) für die Datensynchronisation über eine Destination. Der technische User sollte eine Rolle in SuccessFactors mit Zugriff auf die entsprechenden Felder und Zugriff auf die OData API haben (z.B. Name, Adresse, Titel, etc.)

10.2 Mitwirkungspflichten Employee File:

- Bereitstellung eines WebDAV oder S-FTP Verzeichnisses, sofern Dokumente über ein Austauschverzeichnis in die Akte hochgeladen werden sollen. Sofern nicht ausdrücklich ein anderes Vorgehen beschrieben wird, ist dies ist im Rahmen einer Migration einer bestehenden Software-Lösung stets der Fall.

- Installation des Outlook Office365 Addins bei den Anwender*innen
- Sollte ein On-Premises Archivsystem durch den Kunden gewünscht werden, ist die Hardware durch den Kunden bereitzustellen
- Die Prüfung des Importprotokolls im Rahmen des Massen-Uploads erfolgt durch den Auftraggeber.
- Im Falle einer Einbringung von Dokumenten über einen initialen Massenupload: Die Bereitstellung der Meta-Daten und Dokumente entspricht den Anforderungen der Centric Cloud Solutions.

10.3 Mitwirkungspflichten Scan2Employee File:

- Bereitstellung von Scan-Hardware. Bei bestehenden MFP-Geräten ist die Kompatibilität sicherzustellen. Centric stellt dazu gerne eine Liste kompatibler Geräte zur Verfügung.
- Bereitstellung eines (virtuellen) Servers zur Installation der Scansoftware gemäß Systemvoraussetzungen (Kapitel 11)
- Ausfüllen der von Centric bereitgestellten Checkliste

10.4 Mitwirkungspflichten Document Builder:

Grundsätzlich gilt:

- Das Anlegen der Dokumenterstellungsvorlagen erfolgt durch den Kunden
- Das Anlegen der Textbausteine erfolgt durch den Kunden

Sollte Centric für die Implementierung der Use-Cases zur Dokumentenerstellung beauftragt werden, fallen folgende Mitwirkungsleistungen des Kunden an:

- Bereitstellung einer Beschreibung zu den umzusetzenden Use-Cases zur Dokumentenerstellung.
    - Bereitstellung der Dokumentenvorlage in MS Word (.docx)
    - Definition der pro Vorlage enthaltenen Daten (Platzhalter)
    - Definition des Quellsystems für die jeweiligen Daten (Platzhalter)
    - Definition des Datenfeldes (technische Feldbezeichnung inkl. OData-Pfad) aus denen der jeweilige Platzhalter in der Dokumentvorlage gespeist werden soll
    - Definition und Erläuterung des jeweiligen Ereignisses (Trigger-Events) zur Dokumentenerstellung
    - Definition und grafische Darstellung des jeweiligen Prozesses
- Priorisierung der Business-Cases zur Dokumentenerstellung nach Häufigkeit und Zeitaufwand pro Dokumenterstellung
- Der Kunde hat dafür Sorge zu tragen, dass auf Seite der Quellsysteme über eine REST-Schnittstelle auf die definierten Daten zugegriffen werden kann.
- Der Kunde hat eine technische Dokumentation zur Nutzung der anzubindenden Schnittstellen bereitzustellen.

10.5 Mitwirkungspflichten Reference Letter:

Grundsätzlich gilt:

- Das Anlegen weiterer Zeugnisvorlagen erfolgt durch den Kunden

Allerdings kann es dazu kommen, dass Zeugnisse per Workflows erstellt und/oder freigegeben werden sollen. In diesem Fall unterstützt Centric nach Beauftragung gerne. Folgende Mitwirkungsleistungen des Kunden fallen an:

- Bereitstellung der Zeugnisvorlage in MS Word (.docx)
- Definition der pro Vorlage enthaltenen Daten (Platzhalter)

- Definition des Quellsystems für die jeweiligen Daten (Platzhalter)
- Definition des Datenfeldes (technische Feldbezeichnung inkl. OData-Pfad) aus denen der jeweilige Platzhalter in der Zeugnisvorlage gespeist werden soll
- Definition und Erläuterung des jeweiligen Ereignisses (Trigger-Events) zur Zeugniserstellung
- Definition und grafische Darstellung des jeweiligen Zeugnisprozesses

10.6 Mitwirkungspflichten Payslip Box:

- Bereitstellung eines WebDAV oder S-FTP Verzeichnis für den Dokumentupload sofern die Dokumente nicht direkt aus HCM kommen.
- Pflege der E-Mail-Adressen (beruflich oder privat) aller Mitarbeiter*innen im HCM oder SuccessFactors.
- Definition der entgeltbezogenen Dokumentarten, welche in die Payslip Box einfließen sollen.
- Aufzeigen, wie die jeweiligen Dokumente im HCM erzeugt werden, sodass die Möglichkeiten zum „Abgreifen“ der Dokumente ersichtlich werden.
- Pflege der Übersicht zur digitalen vs. postalischen Zustellung

11 System- bzw. Nutzungsvoraussetzungen

11.1 Allgemeine System- bzw. Nutzungsvoraussetzungen

Um die Funktionalitäten der Centric SAP Cloud Produkte nutzen zu können, müssen folgende kaufmännischen und technischen Voraussetzungen erfüllt sein:

- Gültiger Vertrag zur Nutzung
- Aktueller Internetbrowser, welcher durch SAP unterstützt wird
- Internetanbindung mit ausreichender Connectivity / Bandbreite
- Im Falle einer Anbindung von SAP HCM/SuccessFactors: Bereitstellung der notwendigen Lizenzen.

11.2 System- bzw. Nutzungsvoraussetzungen bei Integration in SAP HCM

- Installierter und funktionsfähiger SAP Cloud Connector / SAP Gateway
- NetWeaver Release mind. Version 7.31

11.3 System- bzw. Nutzungsvoraussetzungen Scan2Employee File

- Bereitstellung eines (virtuellen) Servers mit mindestens:
  - 2 GHz Prozessor
  - 2 GB RAM, wobei 4 oder mehr GB empfohlen werden
  - 10 GB Speicherplatz (NIC Card)
- Bereitstellung Microsoft® Windows® Lizenzen:
  - Windows Server 2012 R2: Standard and Datacenter
  - Windows 8.1 (32\64 bit): Pro and Enterprise
  - Windows 7 (32\64 bit): Professional, Ultimate, and Enterprise with the latest service pack
  - Windows 10
- Bereitstellung zusätzlicher Software:
  - Microsoft® .NET Framework 3.5
    - Microsoft® .NET Framework 4.0
- Microsoft® .NET Framework 4.5
-

11.4 System- bzw. Nutzungsvoraussetzungen Outlook Addin

- Office365 Service und Outlook Client.

12 Partner und Subunternehmer

Zur Bereitstellung der Produkte, Erweiterung der Produkte, Lieferung von Consulting-Services im Rahmen der Einführungsprojekte oder zur Erfüllung kundenindividueller Anforderungen arbeiten wir mit unterschiedlichen Partnern oder Subunternehmern zusammen. Dabei unterscheiden wir in Technologie- oder Dienstleistungspartner.

Die nachfolgende Liste gibt eine Übersicht möglicher Subunternehmer bzw. Partner.

Technologiepartner:

Unternehmen	Adresse	Leistung
SAP Deutschland SE & Co. KG	Hasso-Plattner-Ring 7 69190 Walldorf	Bereitstellung der SAP BTP als technologische Basis und Bereitstellung des Rechenzentrums.
Beconex GmbH	Bretonischer Ring 18 85630 Grasbrunn	Entwicklung, Installation und Konfiguration der optionalen Scanner-Integration “Scan2Employee File”
DocuSign Germany GmbH	Maximiliansplatz 22 80333 München	Bereitstellung von elektronischen Signaturen und Bereitstellung Rechenzentrum.
KGS Software GmbH	Gutenbergstraße 8 63263 Neu-Isenburg	Entwicklung, Installation und Konfiguration des optionalen On-Archivs.

Dienstleistungspartner:

Unternehmen	Adresse	Leistung
Rhenus Docs to Data GmbH	Rhenus-Platz 1 59439 Holzwickede	Transport, Digitalisierung und Klassifizierung der papierbasierten Personalakten und Bereitstellung der Digitalisate zum Import in die Centric Personalakte.
sensatus GmbH	Hermannstraße 11 32756 Detmold	Consulting-Services bei ausgewählten Implementierungs-projekten. Zertifiziert und erfolgreich.
Xayambe GmbH	Moltkeplatz 1 45138 Essen	Consulting-Services bei ausgewählten Implementierungs-projekten. Zertifiziert und erfolgreich.
TÜV Rheinland Group	Am Grauen Stein 51105 Köln	Stellung des Datenschutzbeauftragten für die Centric Cloud Solutions GmbH

13 Vertragsende

Centric erhebt keinen Anspruch auf die kundeneigenen Inhalte, welche in den Centric-Produkten gepflegt und verwaltet werden. Centric verpflichtet sich den Export der Aktenstruktur inkl. Dokumente und Dokumentmetadaten zu ermöglichen.

Dies geschieht im Produktstandard wie folgt:

- Anfrage der „Exit Routine“ durch autorisierte Ansprechpartner des Kunden im Centric Support Portal
- Bereitstellung des benötigten Security-Tokens zum Start der „Exit Routine“ durch das Centric Support Team
- Download der kundeneigenen Inhalte (Aktenstruktur inkl. Dokumente und Dokumentmetadaten) auf einem vom Kunden zu definierendem Laufwerk
- Restlose Löschung der kundeneignen Inhalte nach definierter Sicherheitsfrist.

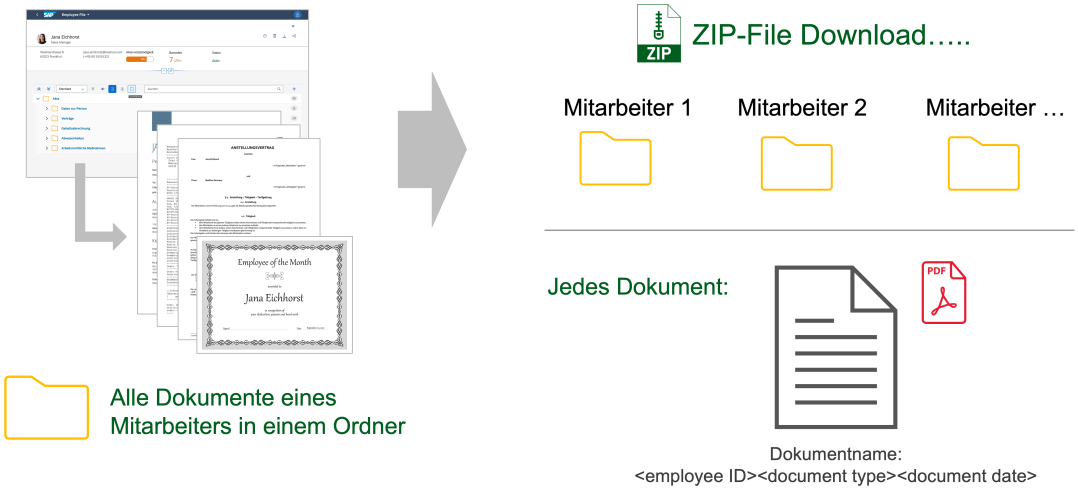


Abbildung 16: Exit-Routine