Informationen zur EU-DSGVO

Inhaltsverzeichnis

1. Informationen zur EU-DSGVO

Hier erhalten Sie allgemeine Hinweise im Hinblick auf Sicherheit und Datenschutz.

1.1. Allgemeines

Die auf die Einhaltung und Umsetzung datenschutzrechtlicher Vorgaben (insbesondere solcher der DSGVO) bezogenen Informationen und Angaben in dieser Dokumentation stellen keine rechtliche Beratung im Einzelfall dar und ersetzen eine solche daher ausdrücklich nicht. Sie sollen lediglich für aktuelle und datenschutzrechtlich relevante Themen sensibilisieren und rechtlich unverbindliche allgemeine Informationen zur Verfügung stellen. Für die Umsetzung datenschutzrechtlicher Vorgaben in Ihrem Unternehmen empfehlen wir Ihnen ausdrücklich, fachkundige Beratung in Anspruch zu nehmen.

Das neue EU-Datenschutzrecht (insbesondere durch die DSGVO) gestaltet die Betroffenenrechte neu (siehe Art. 12 ff. DSGVO). Hieraus geht hervor, dass die für die Verarbeitung von personenbezogenen Daten verantwortliche Stelle (der "Verantwortliche") insbesondere alle Rechte und Pflichten im Hinblick auf die Betroffenenrechte (u.a. Auskunft über Art, Zweck und Ausmaß der Datenerhebung, Anspruch auf Berichtigung der Datenverarbeitung durch den Betroffenen, Löschung personenbezogener Daten unter gewissen Umständen oder Datenübertragung) ständig beachten und entsprechend handeln muss. Die Einstellungen im d.3ecm-System ermöglichen – bei richtiger Anwendung – ein DSGVO-konformes Arbeiten, insbesondere durch die Beachtung der Betroffenenrechte. Bei entsprechender Implementierung/Einstellung ist es möglich, den Grundsätzen der DSGVO (u.a. Datenminimierung, Vertraulichkeit, Integrität, Verfügbarkeit der Datenverarbeitung sowie der Belastbarkeit der Systeme) gerecht zu werden.

1.2. Datenkommunikation

1.2.1. Datenkommunikation d.3 content crawler

Über den d.3 content crawler können E-Mails aus verschiedenen Quellen ausgelesen werden und in das d.3-Repository importiert werden. Hierbei können Journal-, Benutzer-, Gruppen- und Funktionspostfächer überwacht werden.

Der d.3 content crawler setzt sich aus folgenden Modulen zusammen:

- d.3 content crawler Service
- d.ecs content crawler
- d.ecs groupware

d.3 content crawler Service

Der d.3 content crawler Service ist ein Windows-Dienst, der die Konfiguration über den d.ecs content crawler (6.1.3) ausliest und die entsprechenden Postfächer verarbeitet. Anhand der Konfiguration wird ermittelt, welche E-Mails verarbeitet werden sollen. Für jede zu verarbeitende E-Mail wird eine Job im d.ecs content crawler angelegt.

d.ecs content crawler

Der d.ecs content crawler ist eine Selfhosted-App (Backend-Service), über den die E-Mail-Archivierung konfiguriert wird. Zusätzlich werden die Archivierungsjobs zentral verwaltet.

Konfiguration

Die Persistierung der Konfiguration findet im d.ecs jstore statt. Der d.ecs content crawler stellt zum Verwalten der Konfiguration die entsprechenden Oberflächen zur Verfügung.

Job-Verwaltung

Die Archivierungsjobs werden durch den d.3 content crawler Service (6.1.2) erstellt. Über den d.ecs content crawler werden diese verwaltet. Wird eine E-Mail erfolgreich im d.3-Repository gespeichert, wird der entsprechende Archivierungsjob aus dem System gelöscht. Kommt es bei der Verarbeitung einer E-Mail zu einem Fehler, kann der berechtigte Administrator über die Oberfläche des d.ecs content crawler die Ursache einsehen und mittelbar beheben. Jobs, die aufgrund der Ursachenbereinigung vom System nicht gelöscht wurden, können über die Oberfläche manuell gelöscht werden.

d.ecs groupware

Die d.ecs groupware ist eine Selfhosted-App (Backend-Service), welche die E-Mail-Objekte direkt verarbeitet und diese zur weiteren Verarbeitung der d.ecs dms übergibt.

Zur Verarbeitung der E-Mails speichert die d.ecs groupware die zu verarbeitenden E-Mails zwischen. Dieses Cacheverzeichnis wird nach der erfolgreichen Verarbeitung der E-Mail direkt bereinigt.

Anbindung Microsoft Exchange

Die d.ecs groupware greift über das Exchange Web Service (EWS) Protokoll auf Microsoft Exchange zu.

Anbindung IBM Domino

Damit die d.ecs groupware auf IBM Domino Ressourcen zugreifen kann, ist auf einem der IBM Domino Server der Service d.ecs domino installiert. Dieser ist als Servlet in IBM Domino integriert.

Zur Verarbeitung der E-Mails speichert d.ecs domino die zu verarbeitenden E-Mails zwischen. Dieses Cacheverzeichnis wird nach der erfolgreichen Verarbeitung der E-Mail direkt bereinigt.

Der Zugriff auf die Mailsysteme erfolgt über eine verschlüsselte Verbindung.

1.2.2. Datenkommunikation d.3 core components

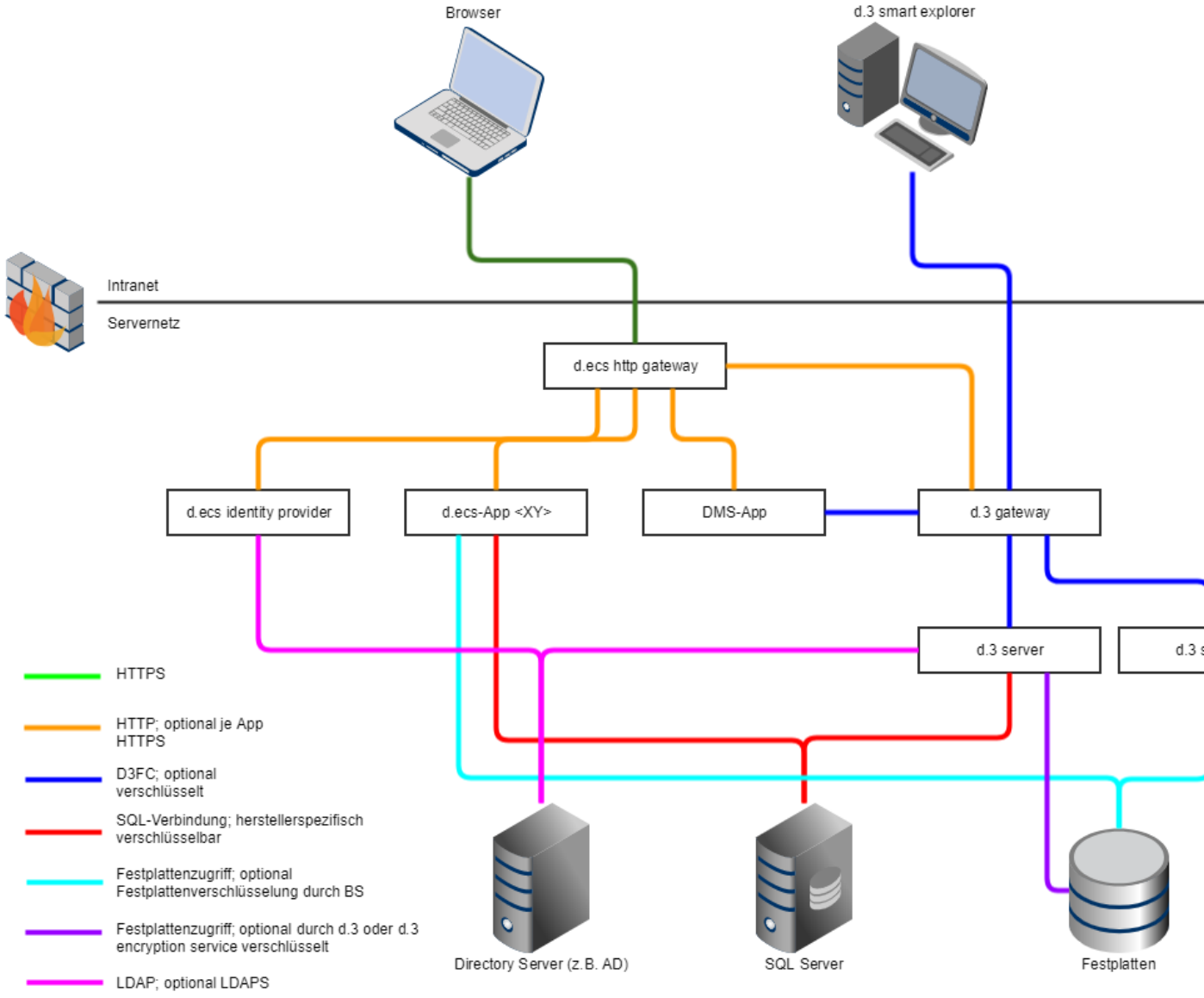
Darstellung des Datenflusses d.3 core components

Ist es aufgrund der Daten erforderlich, dass innerhalb des Servernetzes verschlüsselt wird, wird eine erhöhte Sicherheit nur dann erreicht, wenn mit der Aktivierung organisatorische Maßnahmen verbunden sind.

Ferner sind SQL Server und d.3 search gesondert zu betrachten. Bei beiden kann zwar die Datenhaltung/Festplatte verschlüsselt werden, dennoch sind die Daten transparent zugreifbar. Kritische Daten sollten daher ggf. hier nicht gespeichert werden. Bei d.3 search gibt es zudem eine Sonderoption, so dass hier nur die Worte zum jeweiligen Dokument ohne Zusammenhang zueinander gespeichert werden können.

Die d.velop d.3-Client-Komponenten kommunizieren hauptsächlich über d.3 gateway mit dem Servernetz. Ist es aufgrund der Daten erforderlich, innerhalb des Servernetzes zu verschlüsseln, wird eine erhöhte Sicherheit nur mit der Aktivierung organisatorische Maßnahmen erreicht. Zum Beispiel könnte hier die Kommunikation zwischen d.3 gateway und d.3 client core components die Net-Crypt-Verschlüsselung via public.key-Datei aktivieren werden. Für weitere Informationen lesen Sie bitte im entsprechendem Handbuch nach.

Im nachfolgenden Datenflussdiagramm ist das Kernprodukt der d.velop d.3-Client-Komponenten, d.3 smart explorer und dessen Vernetzung im kompletten d.3ecm-System skizziert.



1.2.3. Datenkommunikation d.3 document render service

Der Dienst d.3 document render service bereitet Nutzdaten eines d.3-Repositorys auf, sodass seitenweise auf den Inhalt der Dateien zugegriffen werden kann.

Die Kommunikation zwischen d.3 document render service und d.3 mobile connector wird mittels HTTP-Protokoll hergestellt.

d.3 document render service verwendet das D3FC-Protokoll um Daten von d.3 server/d.3 gateway abzufragen.

Zudem verwendet d.3 document render service eine SQL-Verbindung zu einer Datenbank, die herstellerspezifisch verschlüsselt werden kann.

1.2.4. Datenkommunikation d.3 mobile

Darstellung des Datenflusses der zugehörigen d.3-Produkte

d.3 mobile ist eine mobile App zum Arbeiten mit Dokumenten, Akten und zur Teilnahme an Workflows.

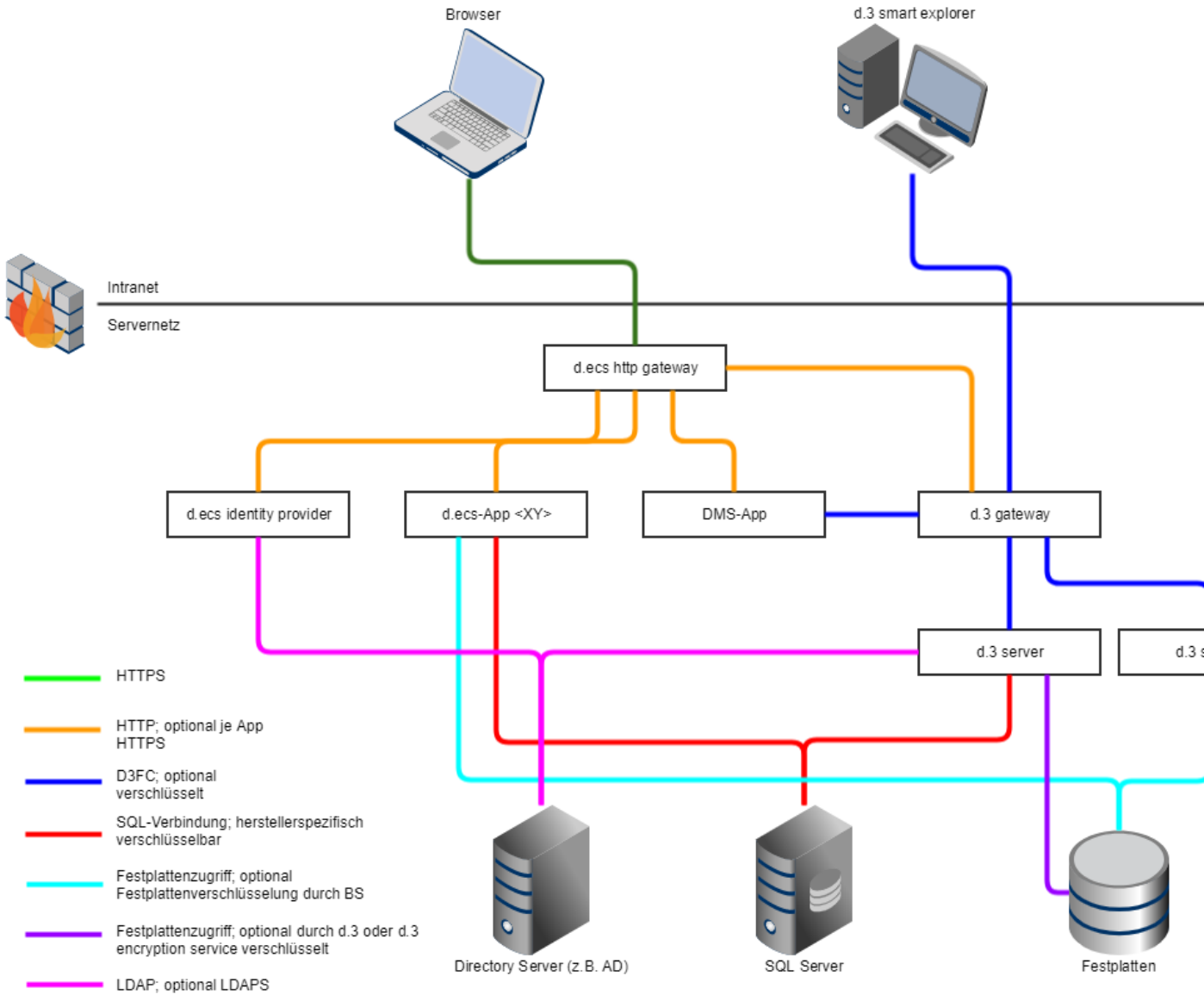
Die Speicherung und Verarbeitung von Daten wird über den d.3-Server und andere Server-Dienste, wie d.ecs forms oder d.ecs storage manager durchgeführt.

d.3 mobile besteht im Backend aus einer WebApp, der d.3 mobile App und d.3 mobile connector.

Die Kommunikation zwischen der d.3 mobile App und d.3 mobile connector wird mittels dem HTTP-Protokoll über d.3 presentation server gateway oder d.ecs http gateway hergestellt.

d.3 mobile connector verwendet das D3FC-Protokoll um Daten vom d.3-Server/d.3 gateway abzufragen, bereitzustellen oder Verarbeitungsprozesse zu starten.

Um ein Dokument in einer Dokumentansicht anzeigen zu können, wird im Backend d.3 document render service benötigt. Mittels HTTP-Protokoll kommuniziert d.3 mobile connector mit d.3 document render service.



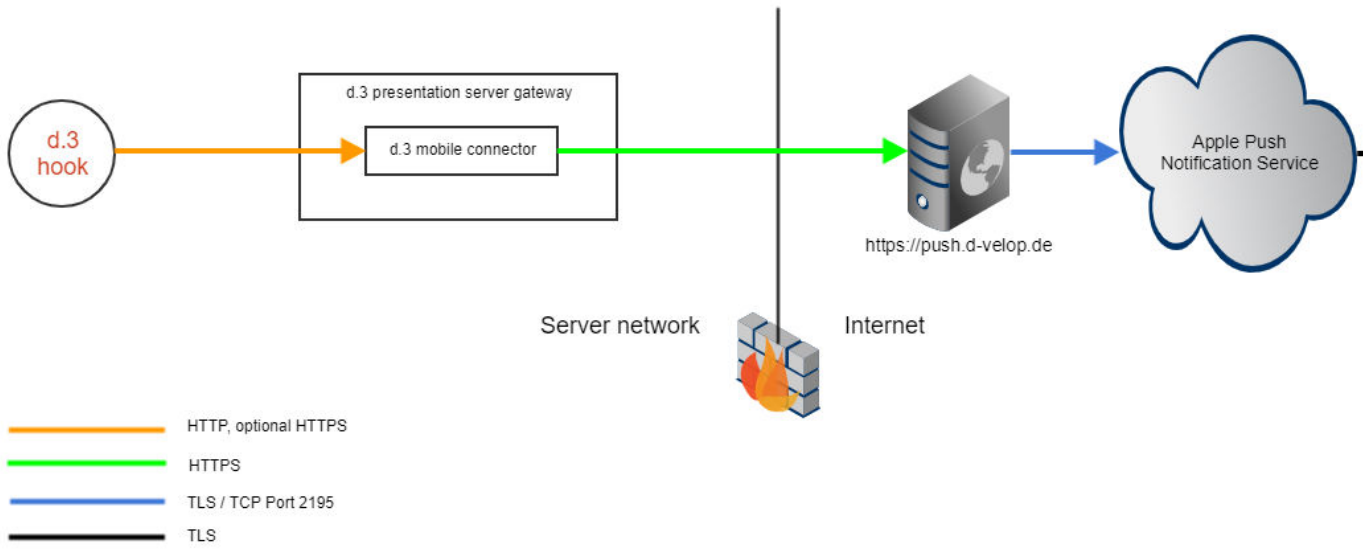
d.3 mobile mit Push-Mitteilungen

Bei einem neuen Postkorbeingang für einen d.3-Benutzer wird mittels eines d.3-Hooks über das HTTP-Protokoll der interne d.3 mobile connector aufgerufen.

d.3 mobile connector sendet per HTTPS an den Push-Server der d.velop AG, den Betreff und die Anzahl ungelesener Einträge.

Der Push-Server bei der d.velop AG verschlüsselt diese Daten und sendet sie TLS-verschlüsselt an den APNS (Apple Push Notification Service).

Sobald die mobilen Geräte des jeweiligen d.3-Benutzers online sind, wird die Push-Mitteilung vom APNS an das mobile Gerät übertragen.



1.2.5. Datenkommunikation d.3one

Mit d.3one werden dem Endanwender ausschließlich Benutzeroberflächen zum Arbeiten mit Dokumenten und Akten bereitgestellt. Die Datenhaltung und Verarbeitung ist Aufgabe von d.3 server.

d.3one besteht aus einzelnen Microservices (Apps), deren Kommunikation untereinander mithilfe des HTTP- oder HTTPS-Protokolls stattfindet.

Folgende Apps sind Bestandteil des Produktes d.3one:

- DMSApp
- PdfApp
- ImageApp
- TunnelApp
- ProcessportalApp
- FileContainerApp
- InboxApp
- RepoApp

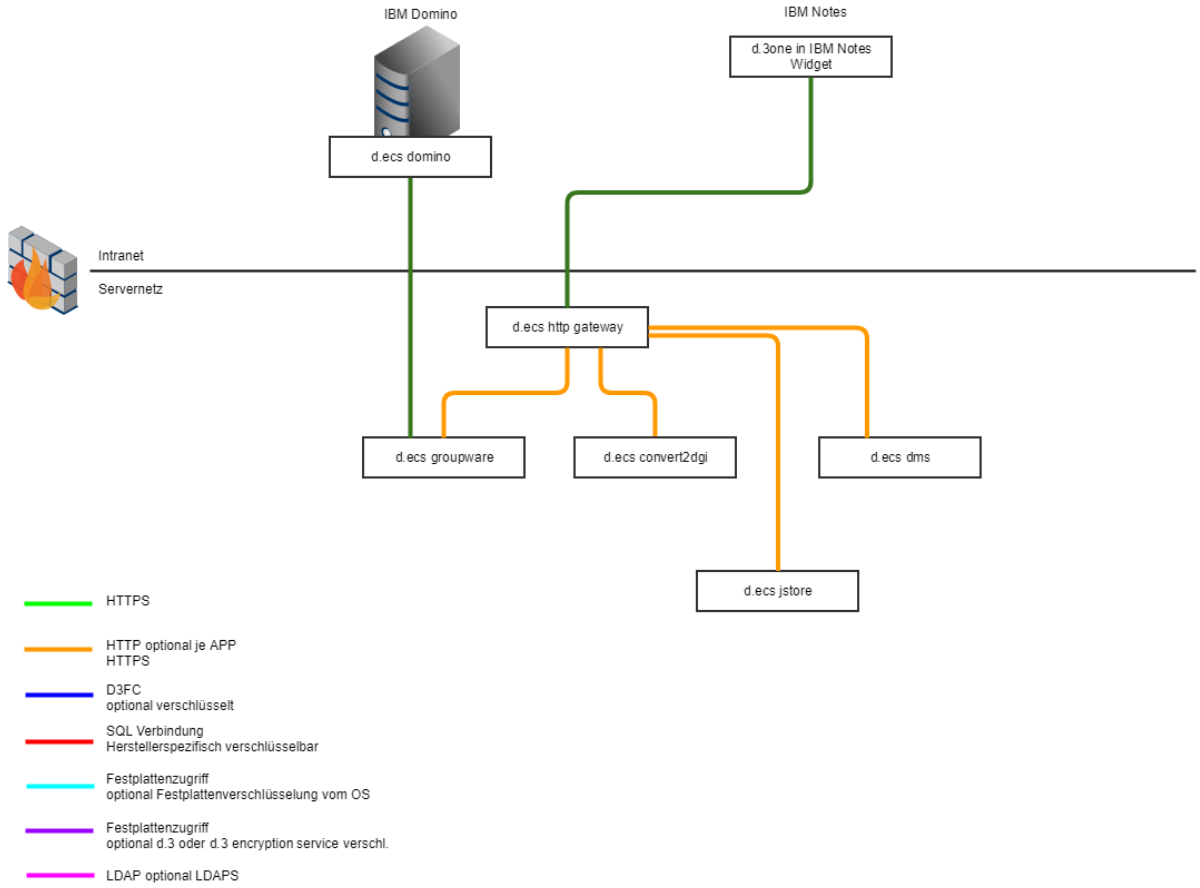
Grundsätzlich wird die Kommunikation der Microservices über d.ecs http gateway geführt. Darüber hinaus werden zentrale Infrastrukturkomponenten verwendet, wie z.B. d.ecs jstore, d.ecs home und d.ecs identity provider. Apps, die mit d.3 server direkt kommunizieren, verwenden das D3FC-Protokoll und das HTTP-Protokoll, um Daten bereitzustellen, abzufragen oder Verarbeitungsprozesse auf dem d.3-Server zu starten.

Ein autorisierter Benutzer interagiert mit d.3one ebenfalls mithilfe des HTTP-Protokolls im Browser. Die Kommunikation zwischen Mensch und Software wird ebenfalls über d.ecs http gateway geführt.

Für Anwendungen von Drittanbietern wird eine REST-HTTP-Schnittstelle verwendet, deren Weg auch über d.ecs http gateway führt, um mit d.3one zu interagieren.

1.2.6. Datenkommunikation d.3one in IBM Notes

Über d.3one in IBM Notes können E-Mails aus der Benutzermaildatenbank in das d.3-Repository importiert werden.



d.3one in IBM Notes setzt sich aus folgenden Modulen zusammen:

- d.3one in IBM Notes Widget
- d.ecs groupware

d.3one in IBM Notes Widget

d.3one in IBM Notes Widget ist ein Plug-In, das die d.3one Oberfläche in IBM Notes integriert und weitere Funktionen im E-Mail-Client bereitstellt. Über das Widget wird u.a. der Ablagedialog von d.3one (d.ecs dms) aufgerufen.

Konfiguration

Die Persistierung der Konfiguration findet im d.ecs jstore statt. Der d.ecs content crawler stellt zum Verwalten der Konfiguration die entsprechenden Oberflächen zur Verfügung.

d.ecs groupware

Die d.ecs groupware ist eine Selfhosted-App (Backend-Service), welche die E-Mail-Objekte direkt verarbeitet, und diese zur weiteren Verarbeitung der d.ecs dms übergibt.

Zur Verarbeitung der E-Mails speichert die d.ecs groupware die zu verarbeitenden E-Mails zwischen. Dieses Cacheverzeichnis wird nach der erfolgreichen Verarbeitung der E-Mail direkt bereinigt.

Anbindung IBM Domino

Die d.ecs groupware greift via https auf den d.ecs domino Service auf IBM Domino zu. Der Service ist als Servlet umgesetzt.

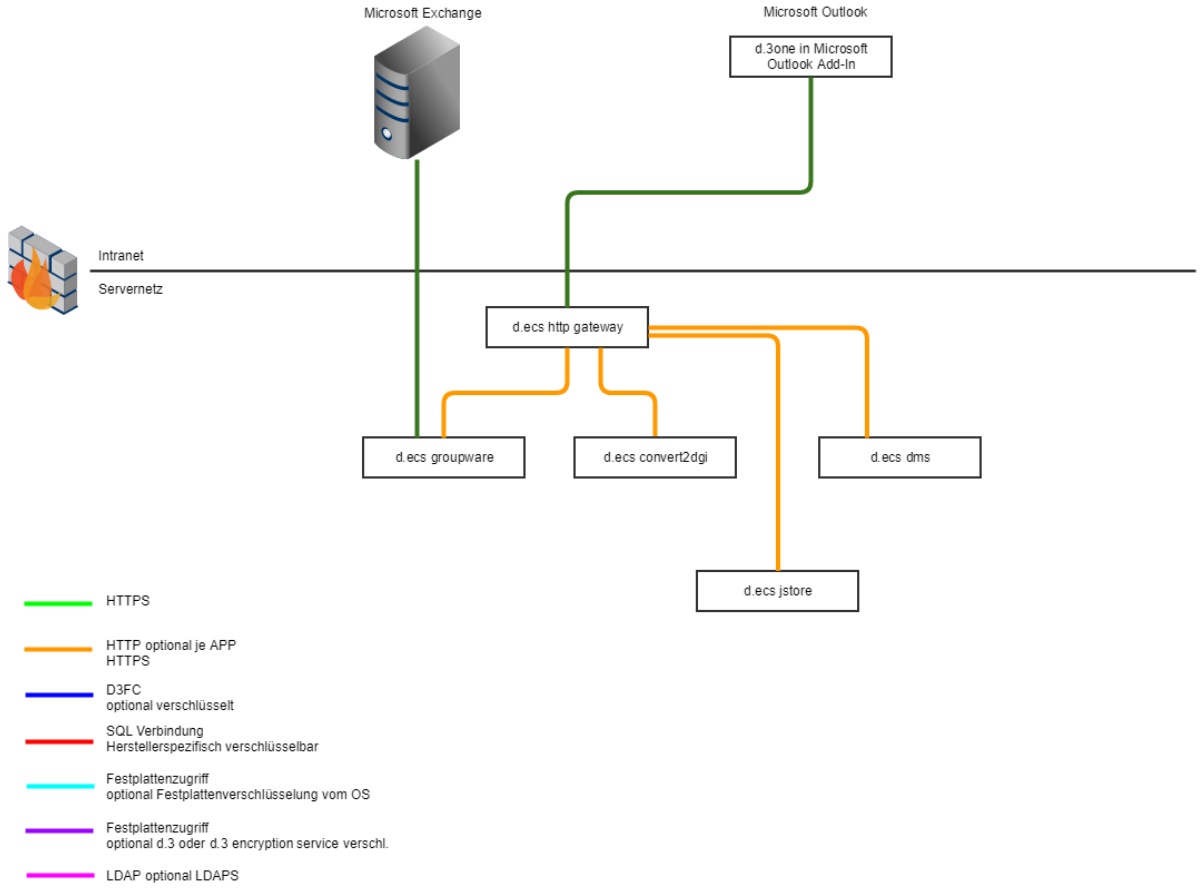
Die Kommunikation der einzelnen Services und Apps erfolgt ausschließlich über d.ecs http gateway. Lesen Sie für weitere Informationen das entsprechende Handbuch.

Um auf die E-Mail-Systeme zuzugreifen, kommuniziert die d.ecs groupware über eine verschlüsselte Verbindung direkt mit IBM Domino bzw. dem d.ecs domino. Der Zugriff auf die Mailsysteme erfolgt über eine verschlüsselte Verbindung.

Ist es erforderlich, dass bestimmte Daten nicht ins technische Log geschrieben werden, finden Sie im d.3one in Microsoft Outlook Handbuch Informationen, wie Sie den Loglevel konfigurieren und welche Umfang die verschiedenen Loglevel haben.

1.2.7. Datenkommunikation d.3one in Microsoft Outlook

Über d.3one in Microsoft Outlook können E-Mails aus dem Benutzerpostfach und in das d.3-Repository importiert werden.



d.3one in Microsoft Outlook setzt sich aus folgenden Modulen zusammen:

- d.3one in Microsoft Outlook Add-In
- d.ecs groupware

d.3one in Microsoft Outlook Add-In

d.3one in Microsoft Outlook Add-In ist ein Add-In, dass die d.3one Oberfläche in Microsoft Outlook integriert und weitere Funktionen in dem Mail-Client bereitstellt. Über das Addin wird u.a. der Ablagedialog von d.3one (d.ecs dms) aufgerufen.

Konfiguration

Die Persistierung der Konfiguration findet im d.ecs jstore statt. Der d.ecs content crawler stellt zum Verwalten der Konfiguration die entsprechenden Oberflächen zur Verfügung.

d.ecs groupware

Die d.ecs groupware ist eine Selfhosted-App (Backend-Service), welche die E-Mail-Objekte direkt verarbeitet, und diese zur weiteren Verarbeitung der d.ecs dms übergibt.

Zur Verarbeitung der E-Mails speichert die d.ecs groupware die zu verarbeitenden E-Mails zwischen. Dieses Cacheverzeichnis wird nach der erfolgreichen Verarbeitung der E-Mail direkt bereinigt.

Anbindung Microsoft Exchange

Die d.ecs groupware greift über das Exchange Web Service (EWS) Protokoll auf Microsoft Exchange zu.

Die Kommunikation der einzelnen Services und Apps erfolgt ausschließlich über d.ecs http gateway. Lesen Sie für weitere Informationen das entsprechende Handbuch.

Um auf die E-Mail-Systeme zuzugreifen kommuniziert die d.ecs groupware über eine verschlüsselte Verbindung direkt mit Microsoft Exchange bzw. dem d.ecs domino. Der Zugriff auf die Mailsysteme erfolgt über eine verschlüsselte Verbindung.

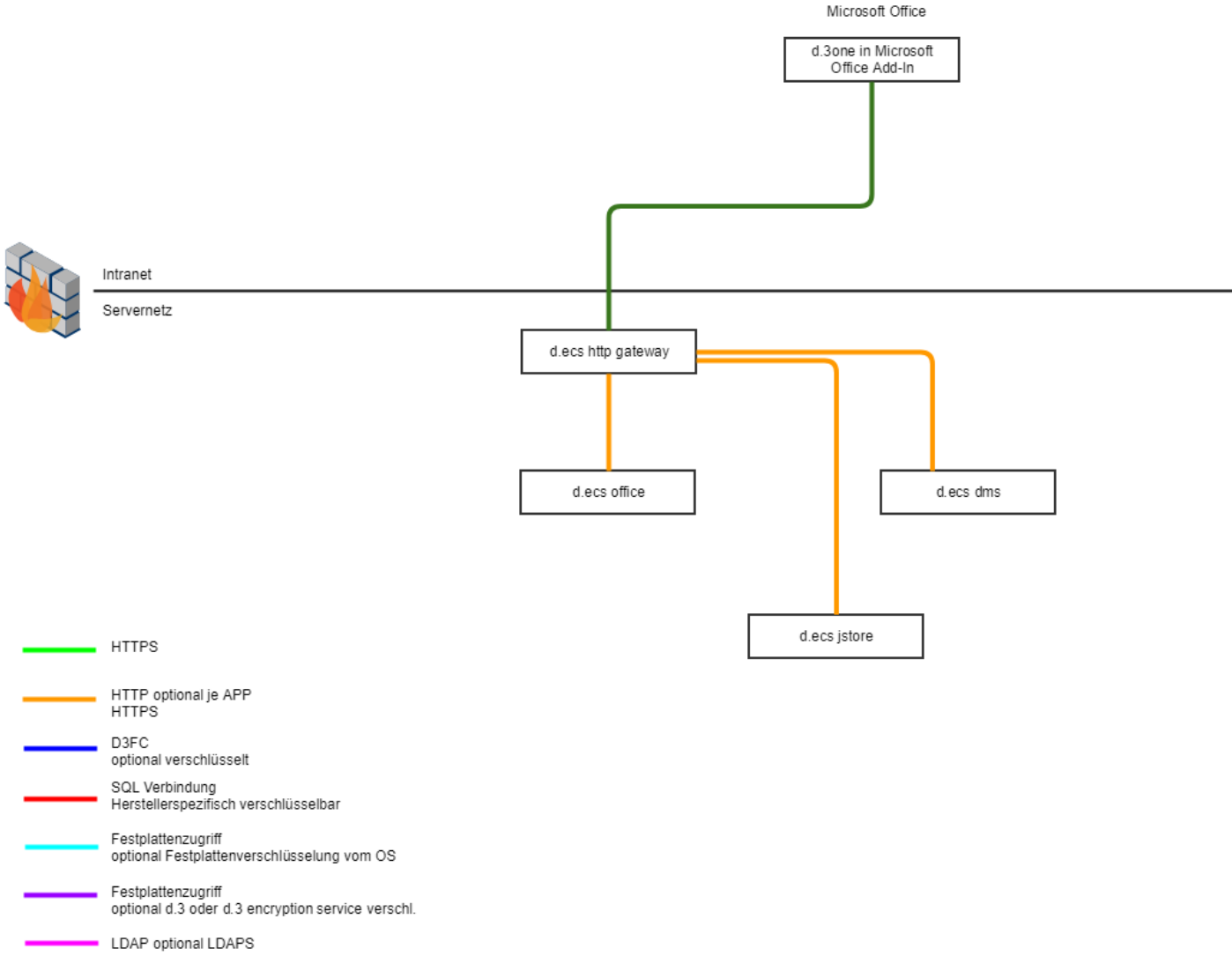
Ist es erforderlich, dass bestimmte Daten nicht ins technische Log geschrieben werden, finden sie im d.3one in Microsoft Outlook Handbuch Informationen, wie Sie den Loglevel konfigurieren und welche Umfang die verschiedenen Loglevel haben.

1.2.8. Datenkommunikation d.3one in Office

Darstellung des Datenflusses von d.3one in Microsoft Office

Die Kommunikation zwischen dem Microsoft Office Add-In und d.ecs office erfolgt ausschließlich über https. Die d.ecs Office Anwendung kommuniziert innerhalb des Servers über http mit den anderen Infrastrukturanwendungen. Diese können optional verschlüsselt werden.

Eine Absicherung kann aber auch über andere geeignete organisatorische Maßnahmen erfolgen.



1.2.9. Datenkommunikation d.3one in SAP ERP

Die d.3one-Integration in SAP erfolgt über konfigurierbare Suchlinks. Diese werden entweder in einem HTML-Viewer in SAP oder in einem Webbrowser außerhalb des SAP-Systems geöffnet. Ein Datenaustausch zwischen d.3one und SAP findet nicht statt.

1.2.10. Datenkommunikation d.3 search

Die Kommunikation zwischen dem d.3-System (d.3 gateway) und dem Storagemanager erfolgt über das d.3fc-Protokoll. Dieses kann wahlweise auch verschlüsselt werden. Die Datenhaltung von d.3 search erfolgt auf einer lokalen Festplatte des Rechners, auf dem d.3 search installiert ist.

1.2.11. Datenkommunikation d.3 sync

d.3 sync stellt dem Endanwender Benutzeroberflächen zum lokalen Arbeiten mit Dokumenten und Akten bereit. Synchronisierte Dokumente und die Verwaltungsdatenbanken werden lokal gespeichert.

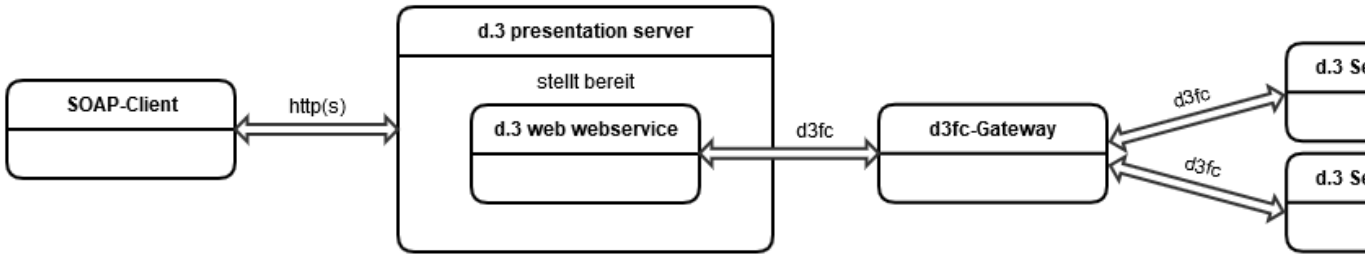
d.3 sync kommuniziert ausschließlich mit d.3 server, um Daten bereitzustellen und abzufragen. Generell können Sie die Kommunikation zwischen d.3 sync und d.3 server verschlüsseln. Für diese Verschlüsselung wird das D3FC-Protokoll verwendet. Sie benötigen die Datei PUBLIC.KEY. Diese Datei wird automatisch in d.3 gateway erstellt und befindet sich dort im Verzeichnis dlink. Kopieren Sie die Datei PUBLIC.KEY in das Installationsverzeichnis des d.3 sync-Dienstes, um die Verschlüsselung zu aktivieren. Standardmäßig ist das Installationsverzeichnis C:\Program Files (x86)\d.velop\d.3 sync\service.

Weitere Informationen zur Verschlüsselung mit dem D3FC-Protokoll finden Sie im Handbuch zu d.3 gateway.

1.2.12. Datenkommunikation d.3 web webservice

Wird eine SOAP-Anfrage von Ihrer Anwendung gesendet, sind mehrere d.velop-Komponenten zur Bearbeitung dieser involviert.

Das folgende Schaubild veranschaulicht, welche Komponenten eingesetzt werden und welches Protokoll diese verwenden:



Damit die komplette Kommunikationsstrecke verschlüsselt erfolgt, müssen sowohl die Verbindungen auf http-, als auch d3fc-Basis verschlüsselt werden.

Damit die Kommunikation zwischen Ihrer SOAP-Anwendung und d.3 presentation server verschlüsselt erfolgt, muss d.3 presentation server eine gesicherte https-Verbindung anbieten.

Weiterhin ist es wichtig, dass neben der Verschlüsselung auf https-Basis, auch die Kommunikation zwischen d.3 web webservice und d3fc-Gateway bzw. d.3-Serverprozessen, verschlüsselt erfolgt.

Wie eine gesicherte http- und d3fc-Kommunikation eingerichtet werden kann, ist im Handbuch von d.3 presentation server beschrieben.

Eine erfolgreich gesicherte http-Verbindung kann dabei an der Verbindungsart https erkannt werden.

Sobald die Verschlüsselung auf d3fc-Seite aktiv ist, wird beim Start von d.3 web webservice "Found public.key" protokolliert.

1.2.13. Datenkommunikation d.capture batch

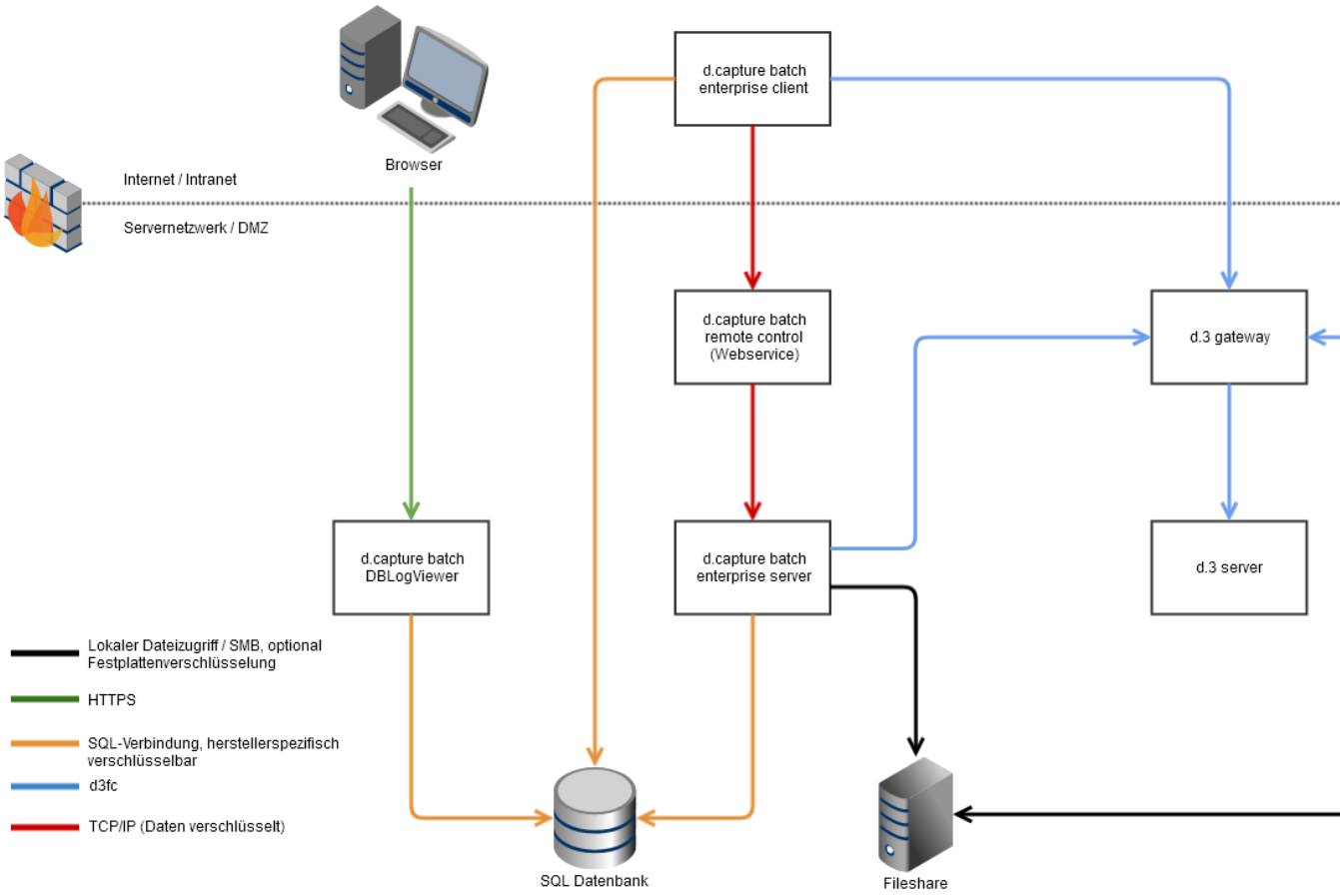
Darstellung des Datenflusses von d.capture batch

d.capture batch kommuniziert über d.3 gateway mit d.3 server. Die Kommunikation zwischen d.3 server, d.3 gateway und d.capture batch erfolgt unverschlüsselt über das d3fc-Protokoll.

Alle d.capture batch-Instanzen kommunizieren mit einem SQL-Server, sofern eine Benutzerverwaltung oder das Stapel-Logging in Verwendung sind. Die Verbindung zum SQL-Server - sowohl von d.capture batch als auch von d.capture batch DBLogViewer - erfolgt über ODBC und kann ggf. herstellerspezifisch verschlüsselt werden. Der Abruf des Stapel-Loggings geschieht über eine verschlüsselte HTTPS-Verbindung.

Die Kommunikation von d.capture batch enterprise server und client geschieht per TCP/IP über den d.capture batch remote control Webservice. Die übertragenen Daten sind verschlüsselt.

Unter Umständen greifen d.capture batch-Instanzen auf ein gemeinsames Verzeichnis zum Dateiaustausch zu. In diesem Verzeichnis befinden sich unverschlüsselte Binär- und Metadaten der Stapel. Diese können optional über das Betriebs- oder Storagesystem verschlüsselt werden. Hierzu befolgen Sie bitte die Hinweise des entsprechenden Herstellers.

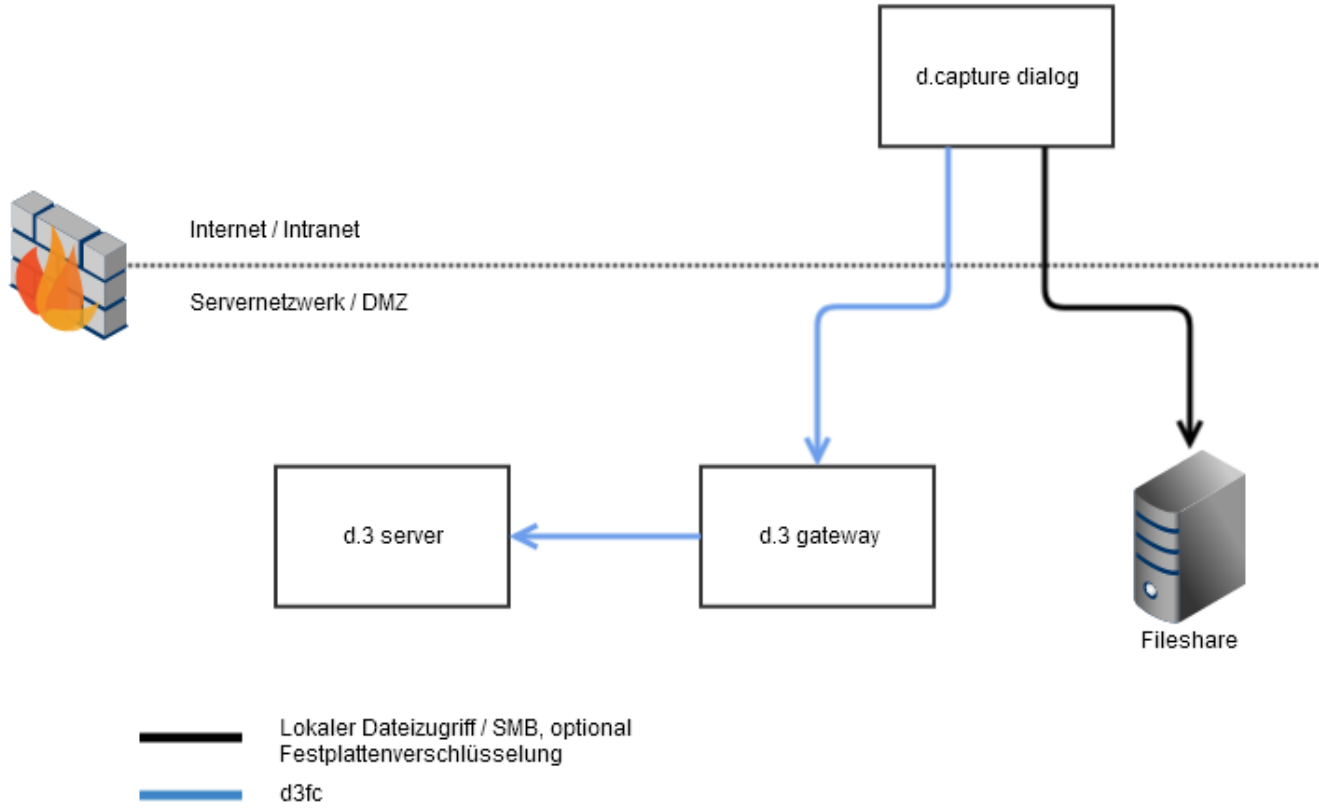


1.2.14. Datenkommunikation d.capture dialog

Darstellung des Datenflusses von d.capture dialog

d.capture dialog kommuniziert über d.3 gateway mit d.3 server. Die Kommunikation zwischen d.3 server, d.3 gateway und d.capture dialog erfolgt unverschlüsselt über das d3fc-Protokoll.

Gegebenenfalls greift d.capture dialog auf ein geteiltes Arbeitsverzeichnis zu. In diesem Verzeichnis befinden sich unter Umständen unverschlüsselte Binärdaten. Diese können optional über das Betriebs- oder Storagesystem verschlüsselt werden. Hierzu befolgen Sie bitte die Hinweise des entsprechenden Herstellers.



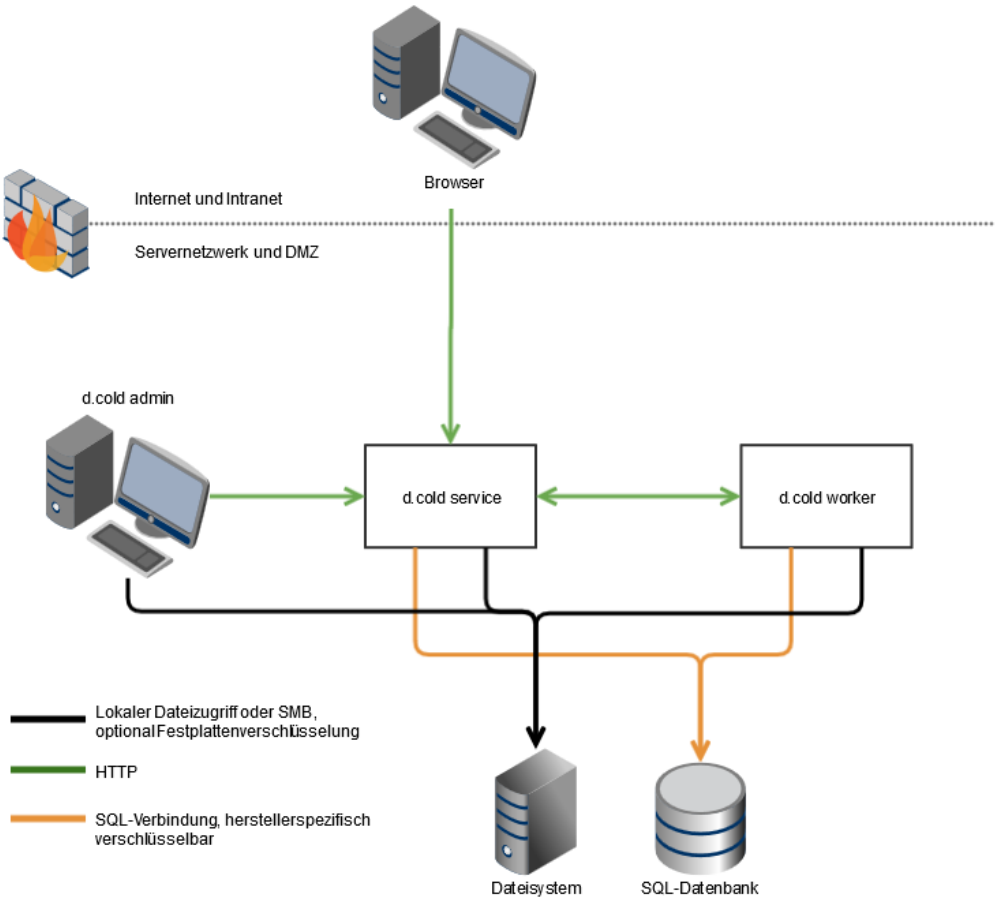
1.2.15. Datenkommunikation d.cold

Darstellung des Datenflusses von d.cold

Die Komponente d.cold admin kommuniziert mit d.cold service über HTTP und ebenso kommuniziert d.cold service mit den d.cold worker-Prozessen, die auf demselben Server ausgeführt werden, über HTTP. Bei einer Installation auf mehreren Servern kommunizieren die d.cold service-Instanzen auch über das HTTP-Protokoll und leiten die Anfragen ggf. an die lokalen d.cold worker-Prozesse weiter.

Mit Blick auf die Datenhaltung von d.cold beachten Sie Folgendes: Alle d.cold worker- und d.cold service-Instanzen kommunizieren zur Jobverwaltung mit einem SQL-Server. Die Verbindung zum SQL-Server erfolgt über ODBC und kann ggf. herstellerspezifisch verschlüsselt werden. Darüber hinaus greifen auch alle d.cold-Prozesse auf ein gemeinsames Verzeichnis zu. In diesem Verzeichnis befinden sich Konfigurations- und Logdateien.

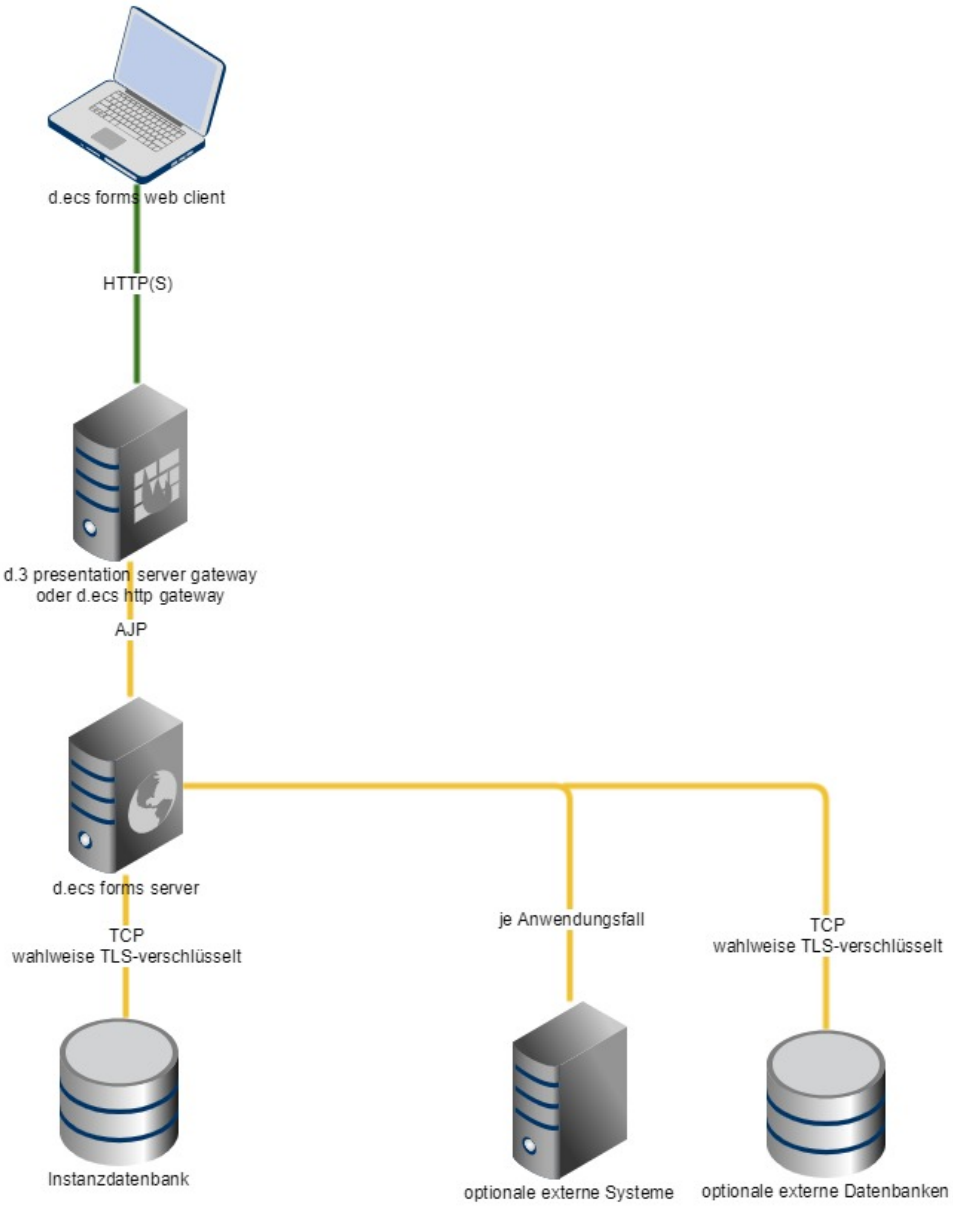
Zusätzlich findet die d.cold-Verarbeitung im Dateisystem statt. Je nach Konfiguration der d.cold-Prozessketten kann die d.cold-Verarbeitung lokal oder auf einem im Netzwerk erreichbaren Verzeichnis stattfinden. Zwar können die Datenhaltung und die Festplatte verschlüsselt werden, dennoch sind die Daten transparent zugreifbar. Kritische Daten sollten daher ggf. nicht mit d.cold verarbeitet werden.



1.2.16. Datenkommunikation d.ecs forms

Darstellung des Datenflusses von d.ecs forms

Der d.ecs forms web client wird aus einem Web-Browser heraus bedient. Dieser kommuniziert per HTTP(S) mit dem d.3 presentation server gateway oder dem d.ecs http gateway. Diese wiederum dienen als Proxy, die per AJP die Anfragen des d.ecs forms web clients an den d.ecs forms server weiterreichen. Der d.ecs forms server lädt Daten und Formulare aus der Instanzdatenbank. Diese wird per TCP angesprochen. Je nach Anwendungsfall können zusätzliche externe Systeme und Datenbanken an den d.ecs forms server angebunden werden.



1.2.17. Datenkommunikation d.ecs monitor

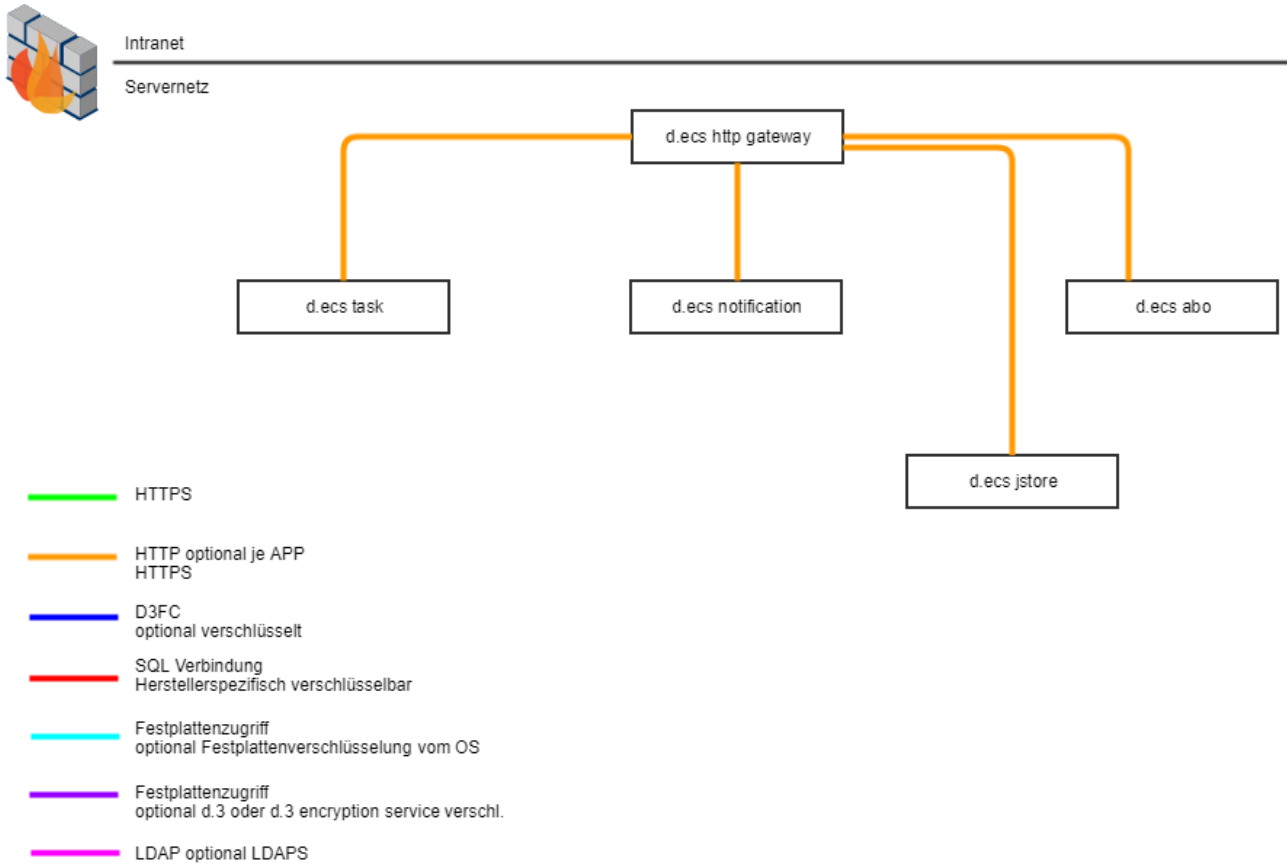
Der d.ecs monitor selber erfasst und verarbeitet weder DSGVO relevante Daten, noch stellt er diese Daten dar. Einzelne Wrapper können hiervon abweichen. Bitte achten Sie hier auf die einzelne Wrapper Dokumentation.

1.2.18. Datenkommunikation d.ecs monitor for d.3 hostimp

Soll verhindert werden, dass die Administratoren Zugriff auf Daten bekommen, die bei der Verarbeitung durch den d.3 server host import auf Fehler gelaufen sind, so müssen Sie darauf geachten, dass das entsprechende Feature deaktiviert ist. Die Informationen hierzu finden Sie in der Dokumentation von d.ecs monitor for d.3 hostimp im Unterkapitel **Grundlegendes.**

1.2.19. Datenkommunikation d.ecs notification

Die Kommunikation mit d.ecs notification erfolgt über https. Der Service kann von beliebigen Services der d.velop AG genutzt werden. Die konkrete Datenkommunikation wird in den Handbüchern der aufrufenden Services beschrieben.

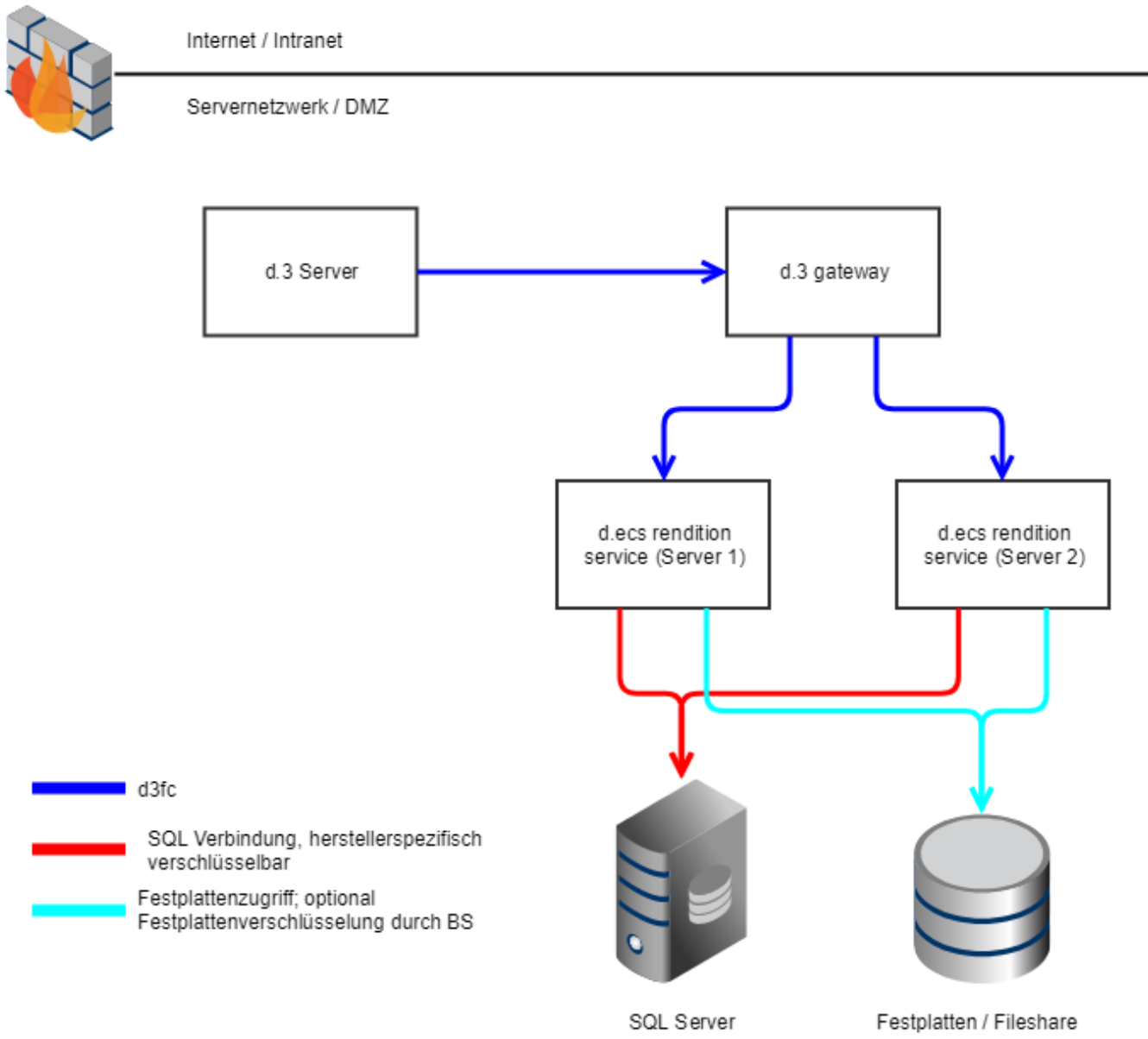


1.2.20. Datenkommunikation d.ecs rendition service

Darstellung des Datenflusses von d.ecs rendition service

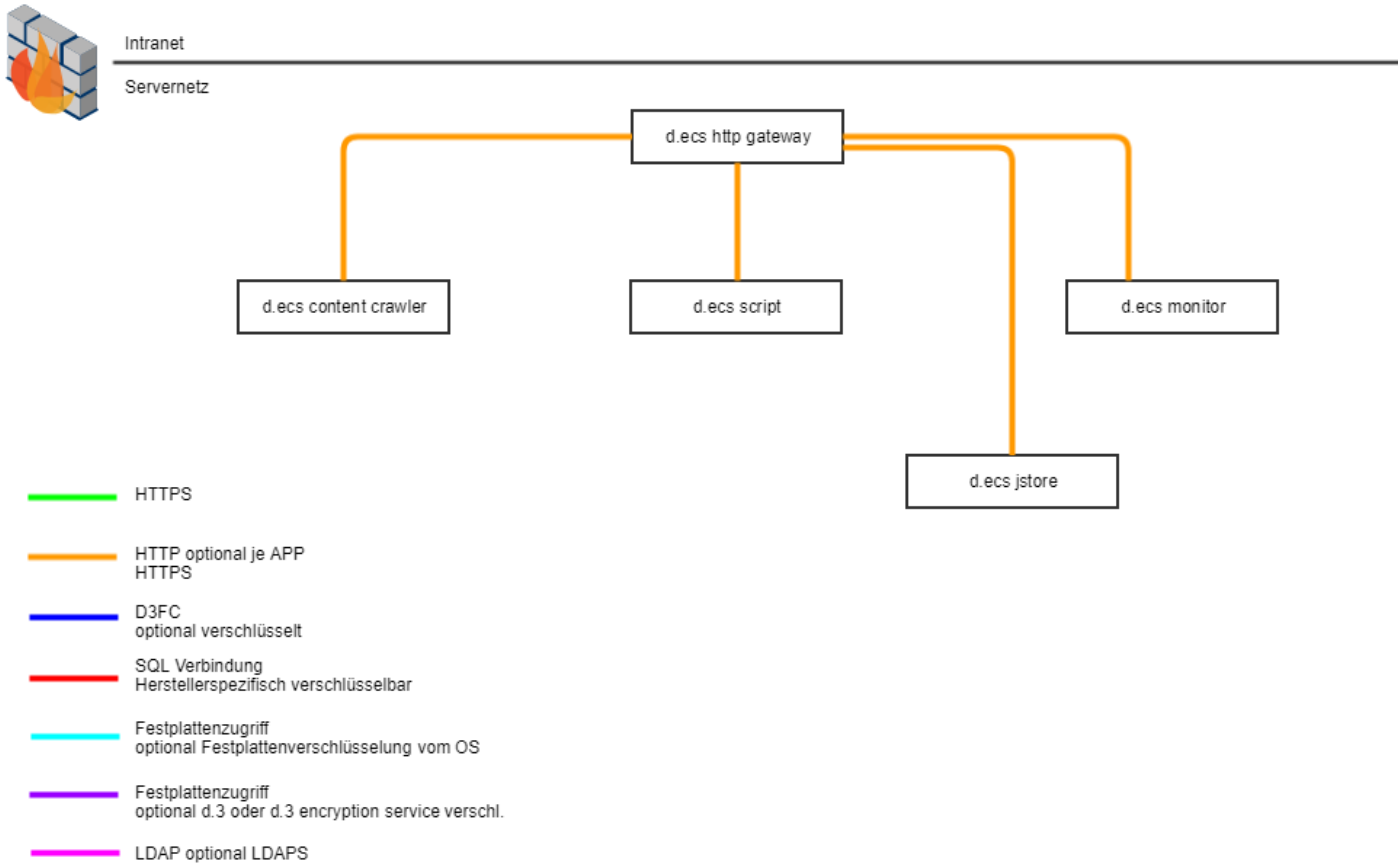
Der d.3-Server (d.3 async) kommuniziert mit d.ecs rendition service über d.3 gateway. d.3 gateway verteilt die Anfragen an die verfügbaren d.ecs rendition service-Instanzen. Die Kommunikation zwischen d.3 server, d.3 gateway und d.ecs rendition service erfolgt unverschlüsselt über das d3fc-Protokoll.

Darüber hinaus ist die Datenhaltung von d.ecs rendition service zu betrachten. Alle d.ecs rendition service-Instanzen kommunizieren zur Jobverwaltung mit einem SQL-Server. Die Verbindung zum SQL-Server erfolgt über ODBC und kann ggf. herstellerspezifisch verschlüsselt werden. Daneben greifen auch alle d.ecs rendition service-Instanzen auf ein gemeinsames Verzeichnis zum Dateiaustausch zu. In diesem Verzeichnis befinden sich alle erhaltenen oder erstellten Dateien zu aktiven Jobs. Zwar kann die Datenhaltung/Festplatte verschlüsselt werden, dennoch sind die Daten transparent zugreifbar. Kritische Daten sollten daher ggf. nicht an den d.ecs rendition service gesendet werden.



1.2.21. Datenkommunikation d.ecs script

d.ecs script verwaltet PowerShell-Skripte die von weiteren Services aufgerufen werden und innerhalb d.ecs script ausgeführt werden.



1.2.22. Datenkommunikation d.ecs storage manager

Die Kommunikation zwischen den führenden Systemen und dem d.ecs storage manager erfolgt

- bei d.3 über Filesysteme (Verzeichnisstruktur) und Datenbanktabellen bzw.
- bei SharePoint über die d.ecs storage manager API

In beiden Fällen werden Dokumente von der führenden Applikation an den d.ecs storage manager übergeben. Die Dokumente werden dabei vom führenden System (d.3) direkt in Verzeichnissen abgelegt, die auch im d.ecs storage manager konfiguriert sind, oder die Übergabe erfolgt per API (SharePoint) und werden dabei temporär vom d.ecs storage manager in den konfigurierten Verzeichnissen abgelegt. Die betroffenen Verzeichnisse werden über die d.ecs storage manager Administration im Abschnitt **Allgemein** konfiguriert.

Dabei dienen der **Public-Pfad** und der **Archiv-Pfad** (inklusive der Unterverzeichnisse) zur Übergabe bzw. temporären Ablage von Dokumenten, die vom d.ecs storage manager auf das konfigurierte Storagesystem ausgelagert werden sollen. Der **Jukebox-Pfad** wird vom d.ecs storage manager verwendet um angeforderte Dokumente der führenden Applikation in diesem Pfad zur Verfügung zu stellen bzw. temporär zu speichern sie dann per API an SharePoint weiterzuleiten.

Warnung

Rechte auf die Verzeichnisse/Dateien benötigen die d.3 Prozesse (d.3 hostimp/d.3 async/d.3 gateway,...) und d.ecs storage manager selbst. In der Regel werden alle genannten Prozesse (bis auf d.3 gateway) durch d.3 process manager gestartet (Windows Dienst). Somit reicht es in der Regel dem User, unter dem der Dienst läuft, die entsprechenden Rechte zu geben. d.3 gateway ist auch ein Windows Dienst und sollte damit unter dem selben User ausgeführt werden wie d.3 process manager.

1.2.23. Datenkommunikation d.velop archivelink for SAP Solutions

Die Kommunikation zwischen den führenden SAP Systemen und der Schnittstelle d.velop archivelink for SAP Solutions (Content-Server) erfolgt über das HTTP/HTTPS Protokoll. Abhängig vom angeschlossenen Ablagesystem d.3ecm, ecspand for SharePoint oder d.ecs Storage Manager erfolgt die Kommunikation dann je nach Ablagemodi über Filesysteme oder API-Import und Datenbanktabellen.

Die Ablagemodi synchrone oder asynchrone Ablage, API-Import sowie die Datei-Verzeichnisse (sogenanntes "Export Verzeichnis") werden über die Administrationsoberflächen von d.velop archivelink for SAP Solutions in der Konfiguration der Content-Repositories im Bereich "Archiving Mode" eingestellt. In dem Modus API-Import "Off" werden die Dokumente und auch zugehörige Metadaten-Dateien in das Export Verzeichnis abgelegt. Durch die Nutzung von externen Betriebssystemmitteln können diese Dateien zudem zusätzlich geschützt werden. Nach dem erfolgreichen Import in das angebundene d.3ecm, SharePoint, SharePoint Online oder d.ecs Storage Manager werden diese Daten gelöscht.

Wichtig: Rechte auf die Verzeichnisse/Dateien benötigen die d.3ecm-/SharePoint-Prozesse (Hostimp/Async/d.3 Gateway,ecspand Importservice,...) und der d.ecs storage manager selbst. In der Regel werden alle genannten d.3ecm Prozesse (bis auf den d.3 gateway) durch den d.3 process manager gestartet (Windows Dienst). Somit reicht es in der Regel aus, dem User, unter dem der Dienst läuft, die entsprechenden Rechte zu geben. Der d.3 Gateway ist auch ein Windows Dienst und sollte damit unter dem selben User ausgeführt werden wie der d.3 process manager.

Für die Archivelink-Ablage von eingehenden Dokumenten werden die gescannten Imagedateien inklusive JPL-Dateien mit den Barcode-/Workflowtyp-Informationen direkt in Dateiverzeichnisse für die weitere Verarbeitung abgelegt. Die Dateiverzeichnisse werden in der Konfiguration des sogenannten "HTTP-Scripts" unter "Barcode-" und "Workflow-Directory" definiert. Nach der erfolgreichen Ablage und Verknüpfung der Dokumente werden diese Dateien gelöscht. Durch die Nutzung von externen Betriebssystemmitteln können diese Dateien zudem zusätzlich geschützt werden.

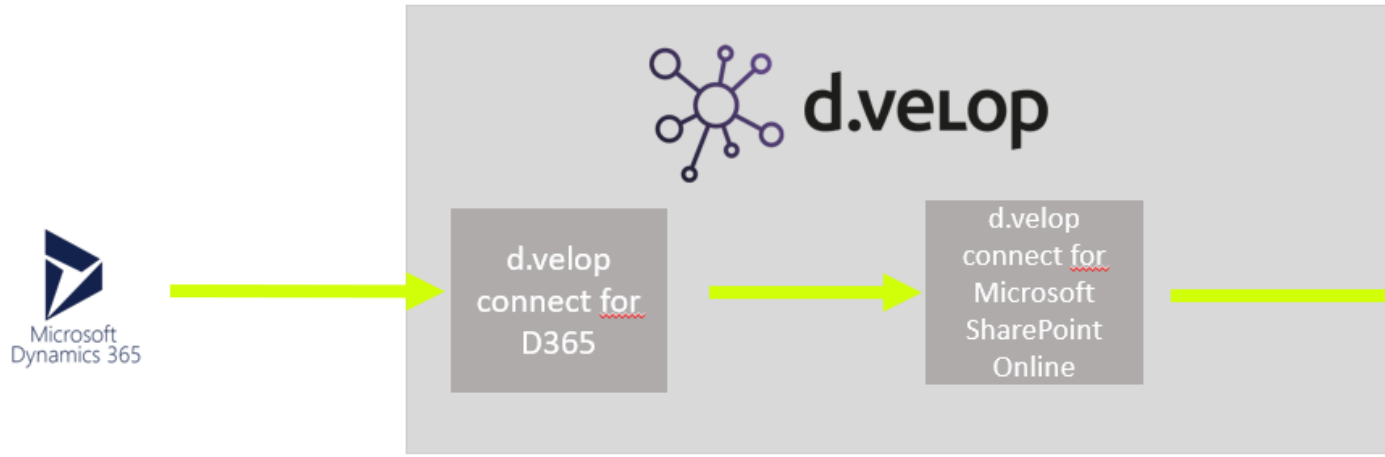
1.2.24. Datenkommunikation d.velop connect for Microsoft Dynamics 365

Um grundsätzlich zu verstehen, wo im Kontext der DSGVO bei einer Installation von d.velop connect for Microsoft Dynamics 365 angesetzt werden kann, muss kurz erläutert werden, welche Daten und Dienste es grundsätzlich gibt, und wie diese Daten vorgehalten werden oder miteinander kommunizieren.

Typische Topologie

Der Adapter d.velop connect for Microsoft Dynamics 365 ist eine App in der d.velop cloud-Plattform, die Konfigurationsmöglichkeiten und Dienste bereitstellt, um eine weitere Applikation eines Drittanbieters oder der d.velop AG an die d.velop cloud-Plattform anzubinden.

Bei der Konfiguration der Applikation werden Informationen über zu exportierende Dokumentarten gespeichert. Diese Informationen sind nicht personenbezogenen und nur von Personen mit entsprechenden Administrationsrechten konfigurier- und einsehbar. Die zur Verfügung gestellten Dienste reichen Informationsobjekte im Speicher zum Ziel weiter und speichern diese Informationen nicht. Ein typischer Datenfluss sieht wie folgt aus.



Neben der dauerhaften Speicherung von Konfigurations- und Verbindungsdaten wird die Nutzung auf technischer Ebene ohne personenbezogene Daten für einen Zeit von weniger als vier Wochen protokolliert.

Optional kann ein Upload-Dienst genutzt werden, um Dokumente temporär abzulegen und eine vorsignierte URL für die weitere Verarbeitung zu erzeugen. Diese Dateien werden nach 15 Minuten automatisch gelöscht.

Im Sinne der Topologie wenden Sie daher bitte die Grundsätze der DSGVO auf die Drittsysteme oder auch die d.velop Infrastrukturkomponente an, wie in den jeweiligen Handbüchern beschrieben.

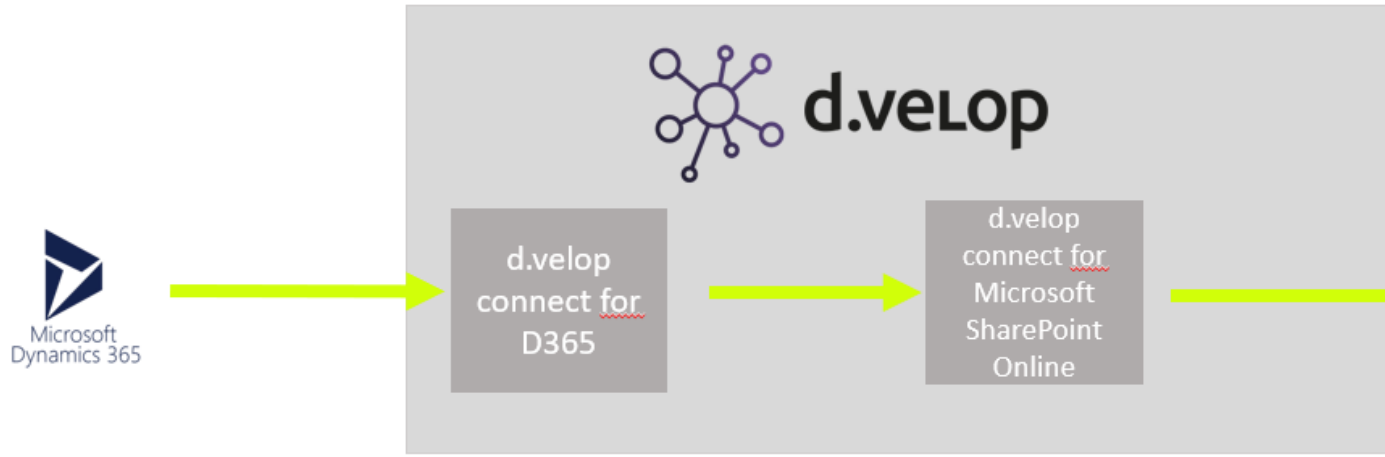
1.2.25. Datenkommunikation d.velop connect for Microsoft SharePoint

Um grundsätzlich zu verstehen, wo im Kontext der DSGVO bei einer Installation von d.velop connect for Microsoft SharePoint angesetzt werden kann, muss kurz erläutert werden, welche Daten und Dienste es grundsätzlich gibt, und wie diese Daten vorgehalten werden oder miteinander kommunizieren.

Typische Topologie

Der Adapter d.velop connect for Microsoft SharePoint ist eine App in der d.velop-Plattform, die Konfigurationsmöglichkeiten und Dienste bereitstellt, um eine weitere Applikation eines Drittanbieters oder der d.velop AG an eine Microsoft SharePoint-Installation anzubinden.

Bei der Konfiguration der Applikation werden Informationen für die Verbindung zum Microsoft SharePoint-Server, sowie Zuordnungen von Feldern, zwischen dem Quell- und dem Zielsystem Microsoft SharePoint gespeichert. Diese Informationen sind nicht personenbezogenen und nur von Personen mit entsprechenden Administrationsrechten konfigurier- und einsehbar. Die zur Verfügung gestellten Dienste geben Informationsobjekte im Speicher zum Ziel weiter und speichern diese nicht. Ein typischer Datenfluss sieht wie folgt aus.



Neben der dauerhaften Speicherung von Konfigurations- und Verbindungsdaten wird die Nutzung auf technischer Ebene ohne personenbezogene Daten für einen Zeit von <4 Wochen protokolliert.

Im Sinne der Topologie wenden Sie daher bitte die Grundsätze der DSGVO auf die Drittsysteme oder auch die d.ecs infrastructure-Komponenten an, wie in den jeweiligen Handbüchern beschrieben.

1.2.26. Datenkommunikation d.velop customizing for SAP Solutions

d.velop customizing for SAP Solutions wird von den d.velop-SAP-Produkten im Rahmen der Lizenzprüfung aufgerufen. Des Weiteren werden mit d.velop customizing zentrale Servicefunktionalitäten zur Verfügung gestellt, die von den Produkten aufgerufen werden. Hierbei werden keine Informationen zu den Aufrufen in SAP-Tabellen protokolliert. Die Funktionen werden über einen Klasse- oder Funktionsbaustein-Aufruf angesprochen. Es findet keine Datenkommunikation zu externen Systemen aus d.velop customizing statt.

1.2.27. Datenkommunikation d.velop data connector

d.velop data connector bietet die Möglichkeit, dass externe Datenquellen mit SharePoint verbunden werden.

Über die Konfiguration des Produktes können verschiedenste Datenquellen angebunden werden. Ist es aufgrund der Daten erforderlich, dass innerhalb des Servernetzes verschlüsselt wird, sollten die Konfiguration entsprechend vorgenommen werden. In Richtung SharePoint wird die SharePoint API verwendet. Hier sind HTTP und HTTPS als Übertragsweg möglich. Falls die Daten es erfordern, sollte auch hier HTTPS als Übertragsungsweg über die Konfiguration hinterlegt werden.

1.2.28. Datenkommunikation d.velop data module for SAP ERP

d.velop data module for SAP ERP kann über den RFC-fähigen Funktionsbaustein /DVELOP/ATR_GET_DATA angesprochen werden. Der Funktionsbaustein liefert die Daten zu einer vorher konfigurierten Selektion-ID. Des weiteren kann d.velop data module for SAP ERP Dateien auf einen lokalen PC oder dem Applikationsserver bzw. einem angebundenen Netzwerkpfad ablegen.

1.2.29. Datenkommunikation d.velop ilm archiving for SAP Solutions

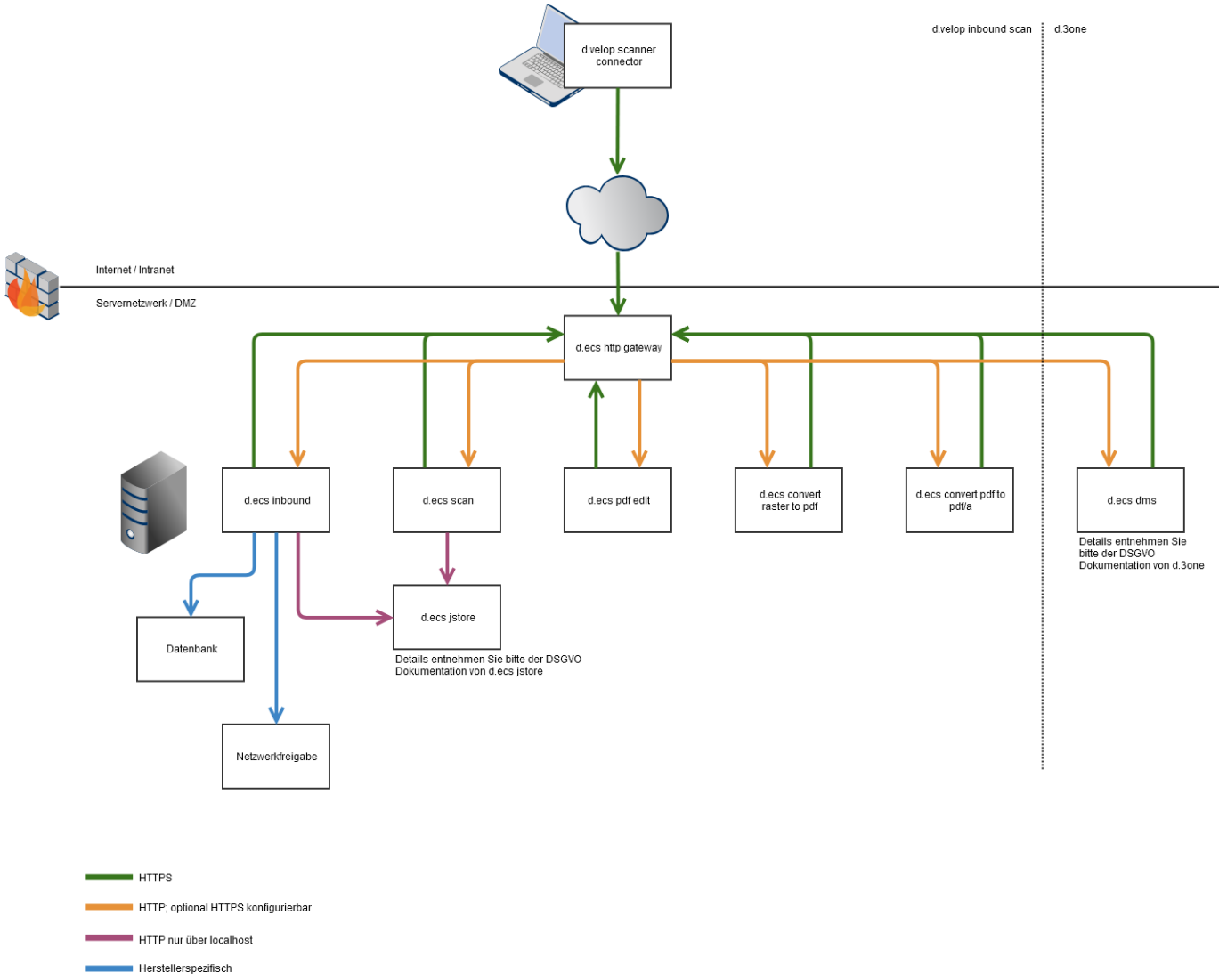
Die Kommunikation zwischen den führenden SAP Systemen und der Schnittstelle d.velop ilm archiving for SAP Solutions (WebDAV-Server) erfolgt über das WebDAV-Protokoll (RFC4918), das um ILM-spezifische Funktionen erweitert wurde. Die Kommunikation erfolgt dabei über das HTTP/HTTPS-Protokoll, konfigurierbar in den SAP RFC-Destinationen (Transaktionscode SM59). SAP Information Lifecycle Management (ILM) ist das führende System und verwaltet und steuert die, an die ILM-Ablage übergebenen, Daten.

1.2.30. Datenkommunikation d.velop inbound scan

Die einzelnen Komponenten der d.velop inbound suite kommunizieren miteinander ausschließlich mit dem verschlüsselten HTTPS-Protokoll über das d.ecs http gateway. Anfragen werden vom d.ecs http gateway an die einzelnen Backend-Komponenten im Server-Netzwerk mittels unverschlüsseltem HTTP-Protokoll weitergeleitet. Diese Kommunikation kann optional verschlüsselt werden.

Mit dem d.ecs jstore wird über ein unverschlüsseltes HTTP-Protokoll kommuniziert. Die Kommunikation findet jedoch ausschließlich über das lokale Netzwerkgerät statt und kann nicht im Netzwerk abgefangen werden.

Die Kommunikation mit Infrastrukturkomponenten ist teilweise nur unverschlüsselt möglich oder eine Verschlüsselung ist, abhängig vom jeweiligen Hersteller, optional möglich.



1.2.31. Datenkommunikation d.velop personnel file for SAP ERP

Im d.velop personnel file for SAP ERP werden die Dokumente über die SAP-Standardschnittstelle Archivelink abgelegt und gelesen.

d.velop personnel file for SAP ERP besitzt eine Schnittstelle zur Kommunikation mit dem personnel file Fiori Add-On. Über die Schnittstelle werden die für die Fiori-Anzeige benötigten Informationen bereitgestellt. Für die Verwendung der Schnittstelle sind zusätzliche Berechtigungen notwendig.

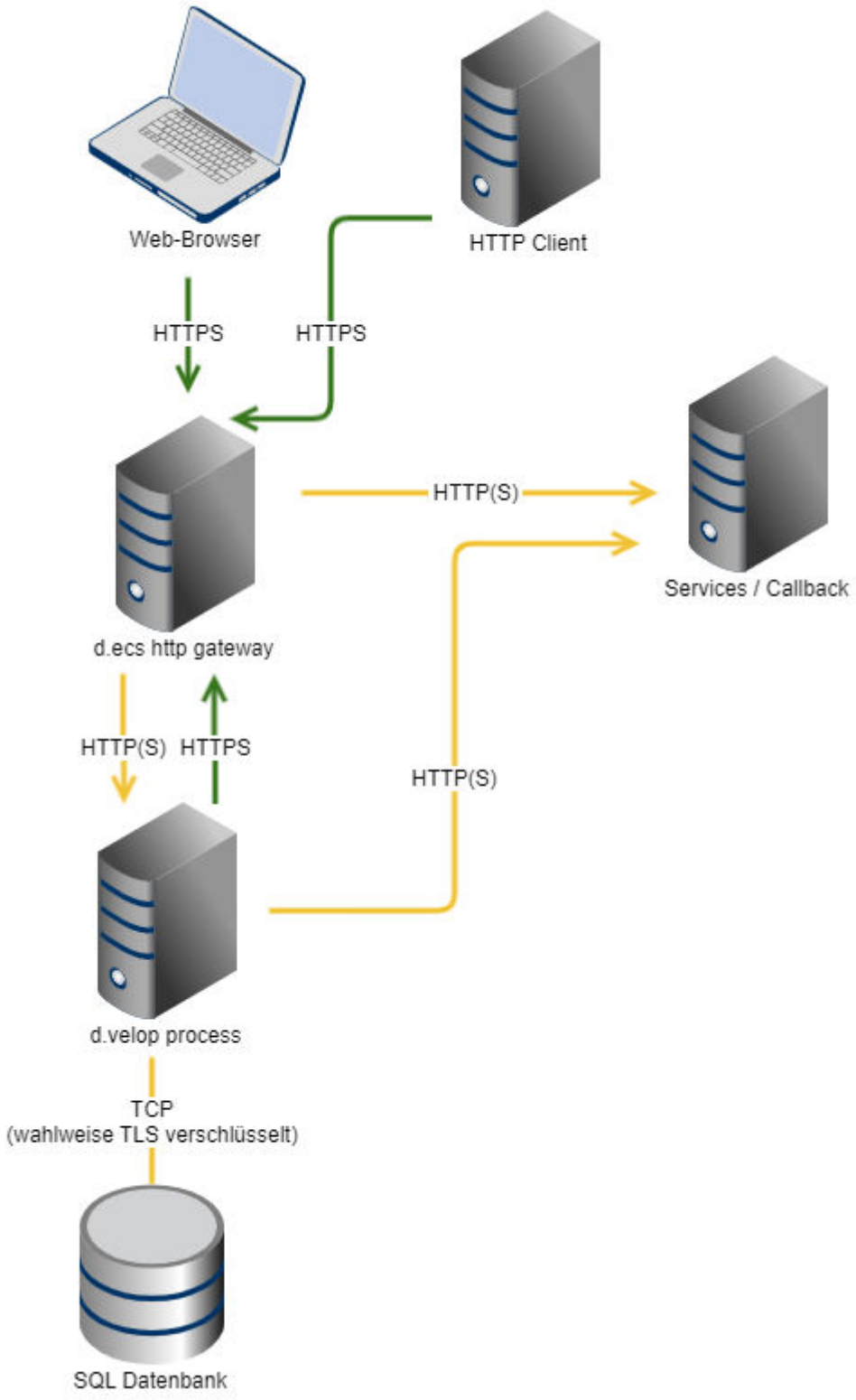
Nähere Informationen finden Sie in der Produktdokumentation.

1.2.32. Datenkommunikation d.velop process

Darstellung des Datenflusses von d.velop process

d.velop process kann sowohl in einem Webbrowser als auch per HTTP-API verwendet werden. Die Kommunikation findet immer per HTTPS via d.ecs http gateway statt. d.ecs http gateway dient als Proxy, der per HTTP(S) die Anfragen an d.velop process weiterreicht. d.velop process speichert Laufzeitdaten und Verlaufsdaten in einer SQL-Datenbank. Diese Datenbank wird per TCP angesprochen.

d.velop process kann je nach Anwendungsfall während einer Prozessausführung Callback- und Service-Schnittstellen externer Apps aufrufen. d.velop process kommuniziert mit den externen Apps ebenfalls per HTTP(S). Die Kommunikation mit Services findet auch über d.ecs http gateway statt. Callbacks können auch direkt aufgerufen werden. Beim direkten Aufrufen werden Laufzeitdaten der konkreten Prozessinstanz an die externe App übertragen.



1.2.33. Datenkommunikation d.velop task processor

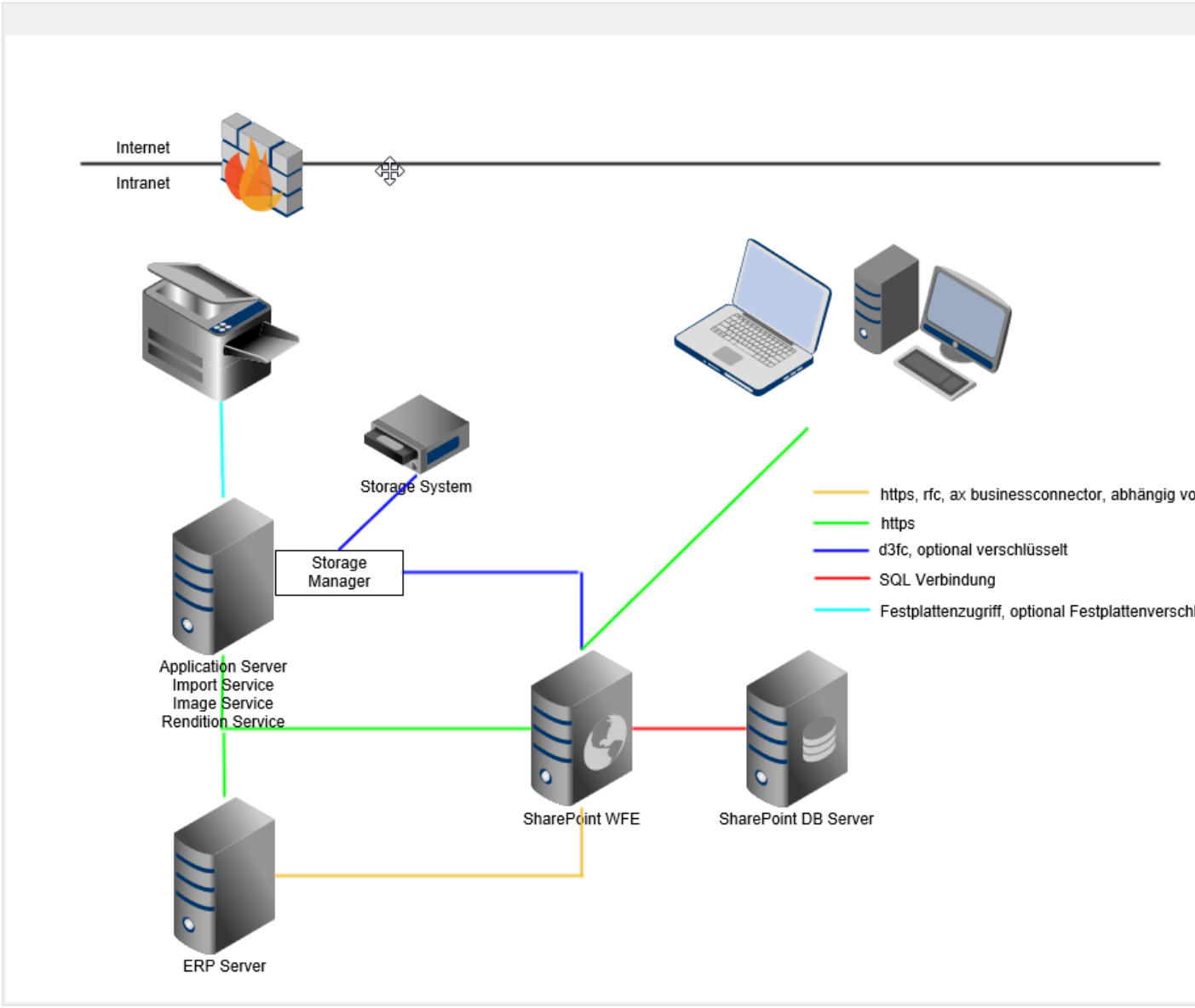
Typische Topologie

Betrachten wir eine typische Topologie beim Einsatz von ecspand, so finden wir den d.velop task processor in der Regel auf dem Application Server.

Der d.velop task processor verfügt dabei über einen generischen Charakter. Seine konkrete Ausprägung wird durch seine Konfiguration festgelegt. Mit PowerShell oder auch eigenen Assemblies wird konkret eingerichtet, wie der d.velop task processor arbeitet.

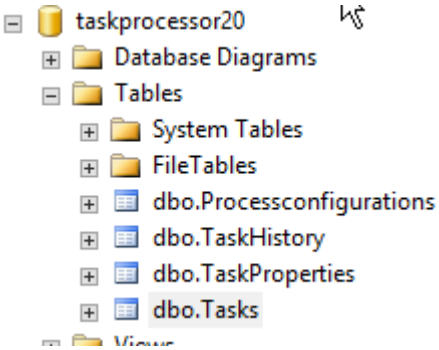
Ein Beispiel für eine Nutzung finden Sie in ecspand invoice processing.

d.velop task processor arbeitet als Windows Dienst, verfügt über eine eigene Datenhaltung in einer Microsoft SQL Datenbank, sowie über eine Konfigurationsoberfläche.



Datenhaltung

Der d.velop task processor verfügt über eine eigene Datenhaltung in einer Microsoft SQL Datenbank. Ihr Aufbau ist wie folgt:



Die Datenbank hat rein technischen Charakter und stellt ausschließlich die Funktionsweise des d.velop task processor sicher.

Abhängig von Ihrer konkreten projektspezifischen Implementation ist es theoretisch möglich, das personenbezogene Daten als TaskProperty hereingereicht und verarbeitet wird. Stellen Sie dann bitte selbstständig sicher, das diese Daten geschützt sind und auch wieder abgeräumt werden.

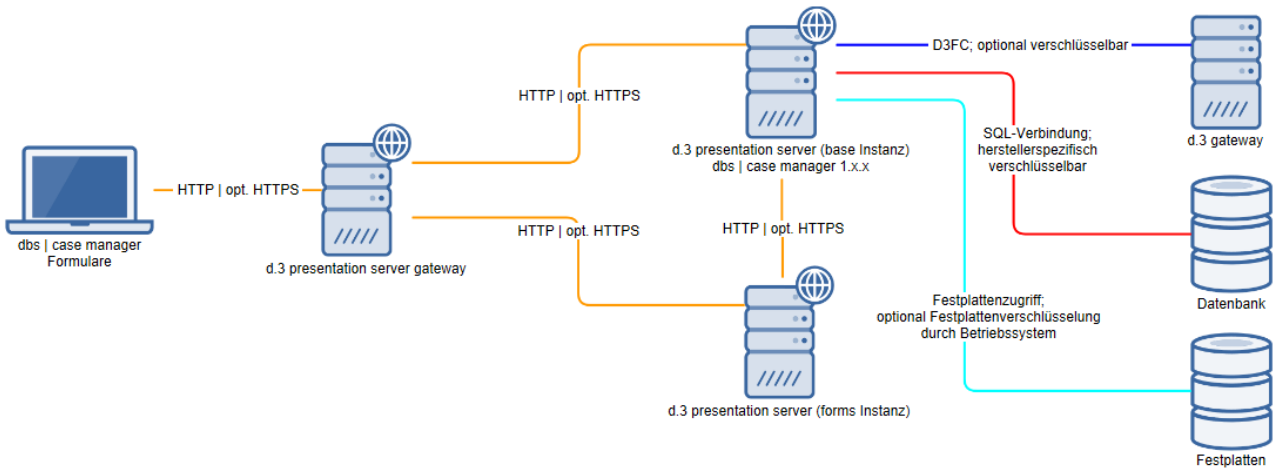
Der d.velop task processor verfügt von sich aus über Mechanismen, die die Daten nach Ihrer Abarbeitung entfernt und im Sinne des Grundsatzes der Datenminimierung arbeitet.

Datenkommunikation

Die tatsächliche Kommunikation mit weiteren Systemen ist abhängig von Ihrer konkreten projektspezifischen Implementierung. Im Falle von ecspand invoice processing kommunizieren PowerShell Skripte über das Client Side Object Model mit Ihrem Microsoft SharePoint. Wenn Ihr Microsoft SharePoint mit SSL aufgesetzt wurde, findet die Kommunikation mit dem System ebenfalls mit SSL, also gesichert, statt. Die Skripte werden im Kontext des Dienst Accounts ausgeführt, mit dem der Windows Dienst des d.velop task processor installiert wurde.

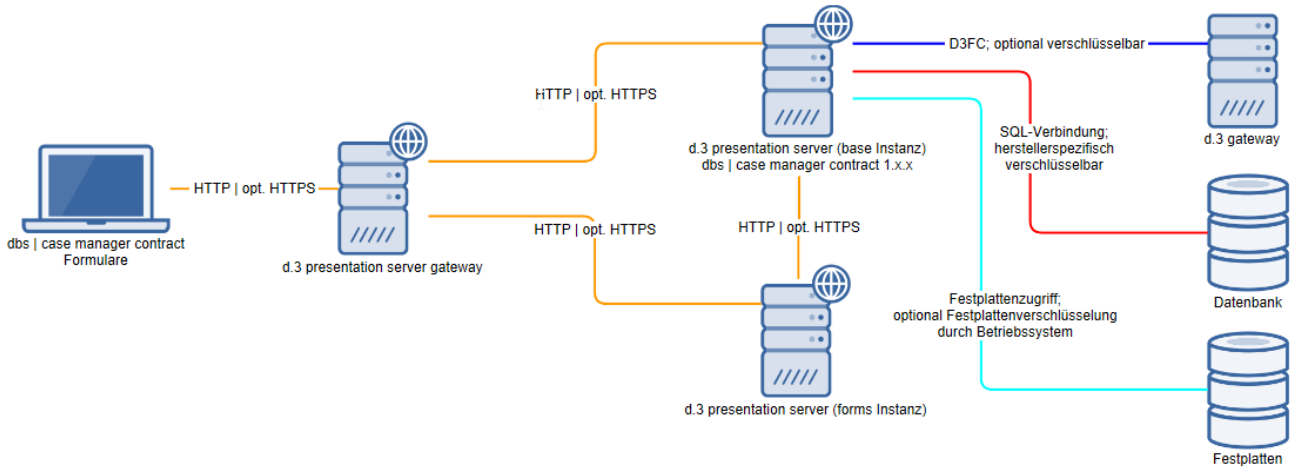
1.2.34. Datenkommunikation dbs | case manager

dbs | case manager wird innerhalb d.3 presentation server betrieben. Daraus ergibt sich folgende ergänzende Darstellung des Datenflusses:



1.2.35. Datenkommunikation dbs | case manager contract

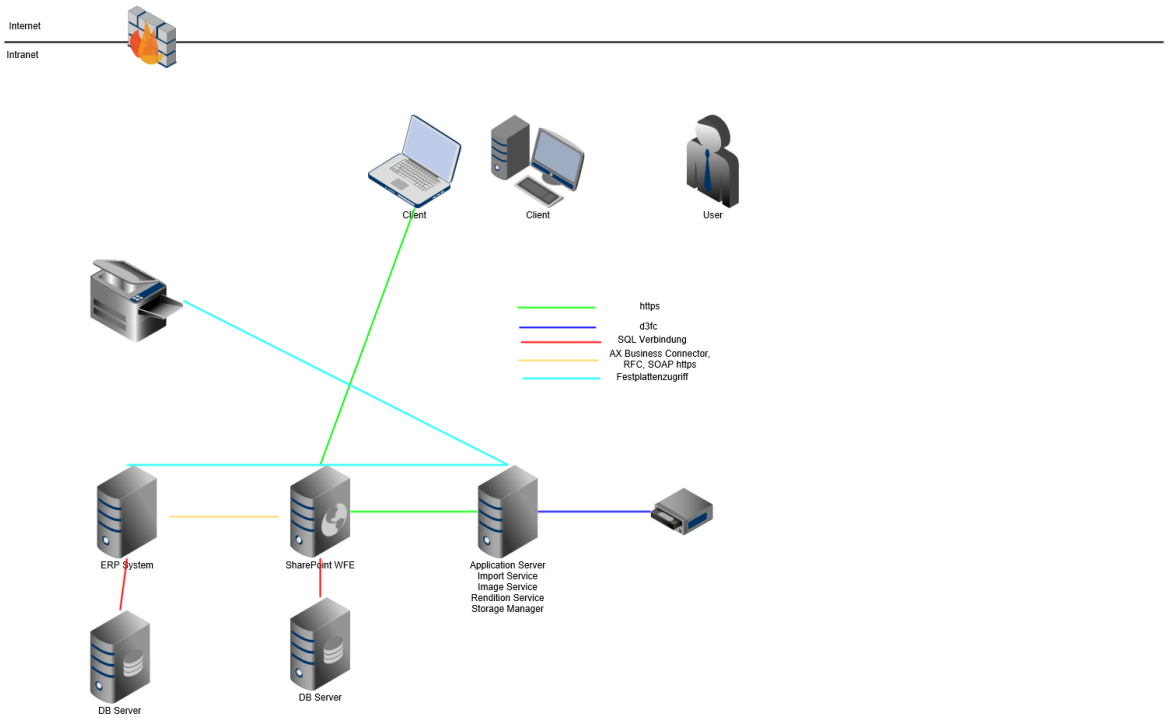
dbs | case manager contract wird innerhalb d.3 presentation server betrieben. Daraus ergibt sich folgende ergänzende Darstellung des Datenflusses:



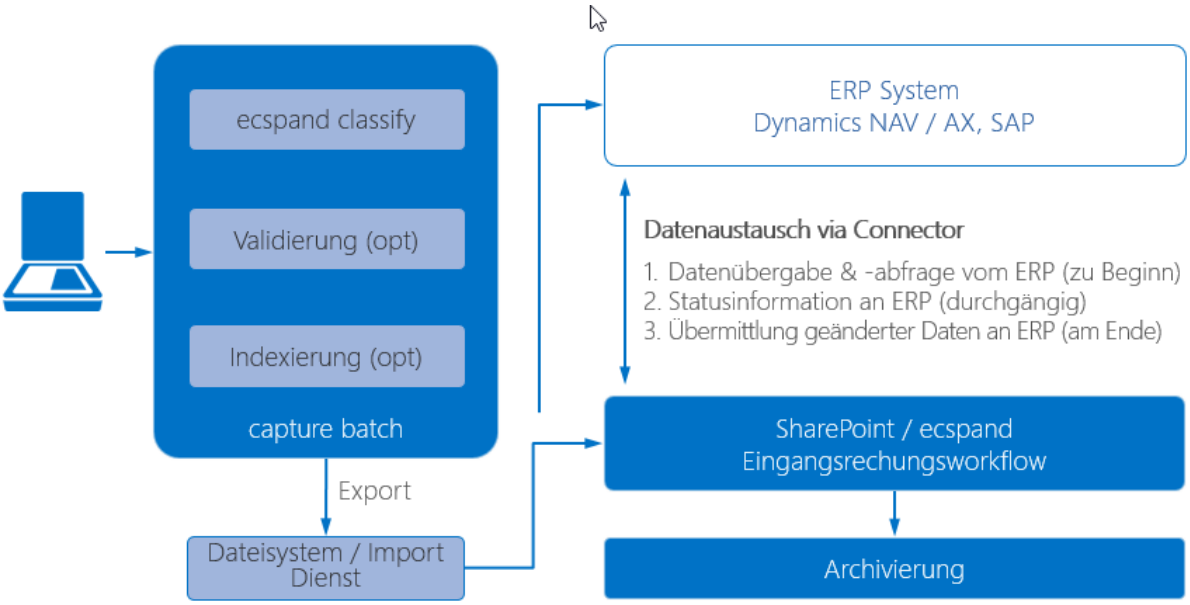
1.2.36. Datenkommunikation ecspand invoice processing

Um grundsätzlich zu verstehen, wo im Kontext der DSGVO bei ecspand invoice processing angesetzt werden kann, muss kurz erläutert werden, welche Daten und Dienste es grundsätzlich gibt und wie diese Daten vorgehalten werden oder mit einander kommunizieren. Da es sich bei ecspand invoice processing in der Regel um einen Prozess mit einer Vielzahl an eingesetzten Komponenten handelt, betrachten wir in diesem Kapitel ausschließlich die Datenhaltung des Produktes escpand invoice processing.

Darstellung des Datenflusses einer typischen ecspand invoice processing Installation



.



In einem typischen Aufbau einer Eingangsrechnungsverarbeitungsprozesskette sind in der Regel folgende Komponenten involviert.

- eine Scanstrecke zur Digitalisierung der Rechnungen
- ein ImportService zur Überführung der Daten in den SharePoint
- ein ArchiveConnect Modul für einen Import in das ERP System (SAP, Dynamics NAV, Dynamics AX)
- ecspand invoice processing im Microsoft SharePoint
- ein d.ecs storage manager mit einer Anbindung an ein Archivsystem
- der d.velop task processor

Wie bereits erwähnt, betrachten wir in diesem Kapitel lediglich die Datenhaltung und Datenkommunikationswege der ecspand invoice processing im Microsoft SharePoint und gehen zusätzlich auf direkte Übergabewege ein.

Allgemeines

Bei Eingangsrechnungen handelt es sich um Dokumente, die neben der DSGVO dem übergeordneten Recht der GOBD unterliegen.

Die Pflicht, diese Dokumente aufzubewahren, wird dabei als höher angesehen, als die Berücksichtigung eines Antrages auf Löschung einer natürlichen Person. Die Objekte stammen von Lieferanten oder Kreditoren und liegen somit in der Regel auch bei diesen vor.

Übergabe von Scanstrecke an ecspand Import Service

Abhängig von der konkret bei Ihnen vorliegenden Installation des ecspand Import Services wird es vermutlich einen oder mehrere Ordner geben, in denen die eingescannten Rechnungen für einen Import in den Microsoft SharePoint abgelegt werden.

Sofern der Import Service aktiv ist und die dort abgelegten Objekte fehlerfrei sind, werden diese nach wenigen Augenblicken asynchron verarbeitet.

Das bedeutet im Umkehrschluss, dass es durchaus vorkommen kann, dass Rechnungen in diesen Ordnern liegen bleiben, sofern diese fehlerhaft sind und nicht verarbeitet werden können, oder der Import Service gar nicht aktiv ist, um diese Rechnungen zu verarbeiten.

Sofern Sie für sich identifiziert haben, dass die eingescannten Rechnungen besonders schützenswert sind, achten Sie bitte darauf, dass der Ordner, obwohl er in der Regel nicht auf öffentlich zugänglichen Servern liegt, nicht von Jedermann eingesehen werden kann.

Setzen Sie eine Berechtigung bspw. des Dienstkontos des Import Service auf den Ordner. Somit sind die Rechnungen nicht direkt einsehbar. Richten Sie ggf. ein Monitoring mit dem d.ecs montitor ein, das Sie proaktiv darauf hinweist, dass es in diesem Ordner Objekte gibt, die dort länger als gewünscht verbleiben.

Überlegen Sie sich auch, ob Sie die Rechnungen in Papierform in dieser Betrachtung berücksichtigen müssen und wie Sie mit den physikalischen Objekten in der Folge des Prozesses umgehen.

Nach Import in den Microsoft SharePoint, wird dem Import des ERP Systems eine so genannte Quittungsdatei bereitgestellt, die das ERP System importiert und entsprechende Objekte erzeugt. Auch für diesen Ordner gelten obige Überlegungen.

Betrachten Sie ansonsten die Dokumentation zu dem eingesetzten Scanprodukt und allgemeine Vorgehensweisen zum physikalischen Zugang und Schutz der eingesetzten Festplatten.

Datenhaltung im ERP System

Betrachten Sie die Datenhaltung im ERP System bitte gesondert unter dem Blickwinkel der DSGVO und nutzen Sie dazu Informationen des Herstellers. Eine Kommunikation mit dem ERP System findet systemabhängig statt:

- SAP - RFC
- Microsoft Dynamics AX - AX BusinessConnector
- Microsoft Dynamics NAV - Standard SOAP

Datenhaltung in Microsoft SharePoint

Nach Übergabe der Rechnung und Import in Microsoft SharePoint bewegen Sie sich aus Security Perspektive im Microsoft SharePoint Standard. Prüfen Sie dabei die Sicherheitskonzepte aus der Produktdokumentation oder Ihre konkrete individuelle Umsetzung.

Personenbezug finden Sie dabei im SharePoint mindestens immer dann, wenn ein UserFeld eingesetzt wird. Im Kontext der ERV, abhängig von der ausgewählten Installation, finden Sie in der Regel an folgenden Stellen einen Personenbezug.

- In der Verantwortlichkeitenliste im Kontext von Kostenstellen-Verantwortlichen und -Vertretern.
- In der Verteilergruppenliste als Mitglied einer Gruppe.
- In der Workflowtypenliste als Empfänger.
- An einer Rechnung selbst in der Bibliothek Eingangsrechungen, als Sachbearbeiter, sachlicher Prüfer, Subprüfer, Freigeber, in den internen Notizen, im Verlauf oder in den Standardfeldern **Erstellt von**, **Geändert von** und **Ausgecheckt von**.
- Im Protokoll zum Workflowverlauf als Teilnehmer des Workflows in der Bibliothek **Workflow-Reporte**.

Sollten Sie für sich identifizieren, das ein Betroffenenrecht in diesen Daten relevant sein könnte, suchen Sie bitte in den oben aufgeführten Listen und Bibliotheken. Berücksichtigen Sie diese Dinge bitte auch in Ihrem Löschkonzept.

Ein Beispiel: Sollte ein Mitarbeiter Ihr Unternehmen verlassen, der an diesem Prozess teilgenommen hat:

- Entfernen Sie den Mitarbeiter aus jeglichen Gruppen in der Verantwortlichkeitenliste.
- Entfernen Sie den Mitarbeiter als Empfänger in der Workflowtypenliste.
- Entfernen Sie den Mitarbeiter aus den Gruppen FiBu, Pruefer oder Verteilergruppen.

Nach GOBD darf eine protokollierte Teilnahme an einem Freigabeprozess oder die Rechnung selbst jedoch nicht fristlos gelöscht werden. Sie müssen somit nicht an den Rechnungen oder in Workflowprotokollen außerordentlich löschend tätig werden.

Orientieren Sie sich dabei an den Fristen aus der GOBD und führen Sie nach Ablauf einer entsprechenden Zurückhaltungszeit reguläre Löschläufe durch. Definieren Sie die Löschläufe bitte in Ihrem individuellen Löschkonzept.

Aufbau und Nutzung von eigenen Tabellen im Kontext der ERV

Bei der Installation der ERV wird eine eigene Datenbank angelegt, die über folgende Daten verfügt.

- IPConfiguration, zum Vorhalten der Konfiguration. Es wird die abspeichernde Person festgehalten.
  - Der LoginName wird dabei abgespeichert, der Datensatz ist jedoch rein technischer Natur.
- IPGOBD, zum Vorhalten der Kommunikation mit dem ERP System.
  - Diese Daten sind für eine Prüfung im Sinne der GOBD erforderlich und sind somit vorrangig zu Rechten der DSGVO zu bewerten.
- ObjectLocks, zum Sperren der parallelen Bearbeitung einer Rechnung durch 2 konkurrierender Benutzer
  - es wird rein technisch festgehalten, ob eine Rechnung gerade durch eine andere Person in Bearbeitung ist. Dabei wird auch der UserName abgespeichert. Diese Tabelle ist rein technischer Natur und beinhaltet keinerlei weiterer personenbezogener Daten. Diese Tabelle wird durch einen automatischen Mechanismus regelmäßig geleert.
- TaskGridSettings, zum Speichern der Sichten in dem Aufgabenwebpart eines Anwenders
  - Neben einem technischen LoginNamen gibt es in dieser Tabelle ausschließlich technische Daten zur Speicherung einer gewünschten persönlichen View eines Aufgabenwebparts.
- TaskGridLastSelectedSettings, zum Speichern der letzten Nutzung einer Sicht im Aufgabenwebpart, beinhaltet den LoginName zur Identifizierung der persönlich verwendeten View.
- WorkflowTaskHistory, zum Abspeichern jeglicher Entscheidungen und Kommentare von Anwendern.

1.2.37. Datenkommunikation ecspand HR management

Generell

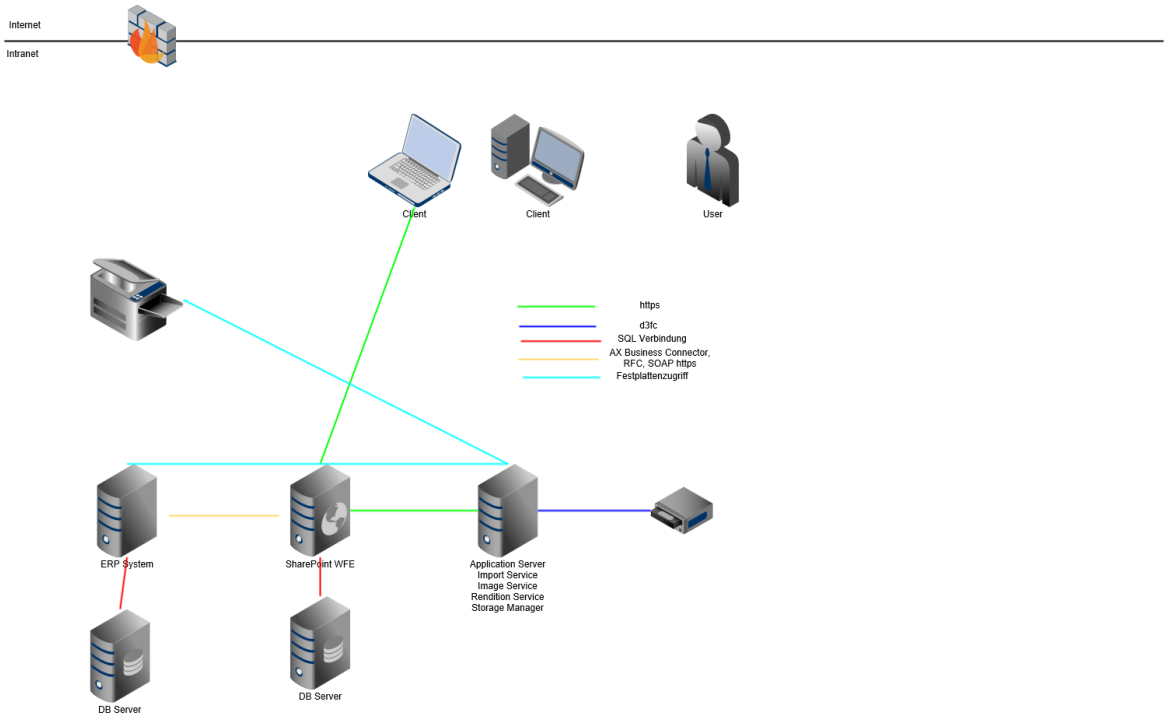
Im Generellen werden alle Daten, sei es vom Benutzer eingegeben oder über automatisierte Mechanismen erzeugte Daten und Dokumente, immer direkt im SharePoint, genauer gesagt in der Inhaltsdatenbank der SharePoint Webseitensammlung gespeichert.

Informationen und Dokumente können dabei über die folgenden Wege in das ecspand HR management gelangen:

- Manuell via Drag and Drop durch einen Benutzer vom Desktop oder einen anderen Ordner im Windows Dateisystem.
- Manuell mit der ecspand Sidebar, auch via Drag and Drop durch einen Benutzer vom Desktop, einen anderen Ordner im Windows Dateisystem oder aus einem Programm der Microsoft Office Suite (Outlook, Word, Excel, PowerPoint).
- Manuell auf Basis einer Vorlage innerhalb einer Personalakte.
- Manuell auf Basis eines Workflows, welches automatisch ein Dokument generiert.

Zu allen Dokumenten können verschiedenste Informationen zu einer Person eingegeben werden. Generell sind nur Informationen hinterlegt, welche Dokumentenbezogen sind. Diese Dokumenteneigenschaften beinhalten im Standard keine Personenbezogene Daten. Es gibt jedoch gerade in einer Personalabteilung viele Daten, welche zu einer Person gespeichert werden. Diese werden grundsätzlich in der Personalakte selbst gepflegt, können aber auch in Dokumente gespeichert werden. Ein Beispiel dabei wäre die Verwendung von Ablaufdaten zu Dokumenten (Zertifikate, Schulungsbestätigungen) oder Gerichtsbezogene Dokumente.

Die folgende Grafik zeigt eine klassische Datenkommunikation im ecspand Umfeld:



(Ident mit ecspand invoice processing)

Nach dem Anlegen einer Personalakte bewegen Sie sich aus Security Perspektive im Microsoft SharePoint Standard.

Anlage und Übernahme von Personaldaten

Über Standard Schnittstellen, welche seitens der d.velop bereitgestellt werden, können Personalakten aus einem führenden System automatisch übernommen werden. Exemplarisch:

- ecspand Import Service
  - Mittels Steuerdateien können Akten und Dokumente aus einem führenden System automatisch übernommen werden. Die Steuerdateien werden über ein Windows Freigabeverzeichnis geteilt. Auf dieses Verzeichnis haben im Standard nur Service Accounts Zugriff, welche als Windows Dienste laufen und diese überwachen.
  - Durch den Einsatz einer Monitoring-Software kann sichergestellt werden, dass der Windows Dienst einwandfrei läuft und die Dokumente nicht auf der Windows Freigabe liegen bleiben.
- d.velop FlowHeater
  - Sind Daten in einer Datenbank verfügbar, so können die Daten ohne Windows Freigabeverzeichnis direkt in den SharePoint synchronisiert werden. Dieser Dienst läuft ebenfalls unter einem Service Account.
- Scan-Strecke
  - Dokumente, welche über einen Scan-Vorgang in die Personalakte übernommen werden sollen, werden hier durch automatische Vorgänge unterstützt. Diese Windows Dienste laufen ebenfalls unter einem Service Account und sorgen für eine Reibungslose und sichere Übernahme der Dokumente in die Persoanlakten. Diese Datenübertragung ist wie von den anderen Produkten bereits mehrfach im Einsatz und können über Monitoring-Software überwacht werden.

Eigene Arbeitstabellen

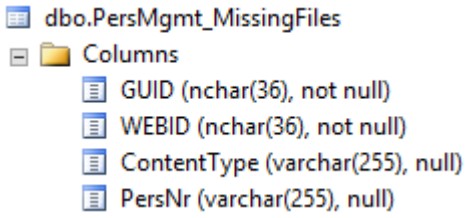
Um im ecspand HR management komplexere Arbeitsprozesse abbilden zu können, gibt es 2 Module, welche auch eigene Arbeitstabellen verwenden:

- Missing Files
- Expiration Files

Missing Files

Mit diesem Modul können fehlende Dokumente gesucht werden. So kann Beispielsweise festgestellt werden, in welcher Personalie der Führerschein noch nicht abgelegt wurde.

In dieser Tabelle, welche sich in der ecspand Inhaltsdatenbank befindet, werden folgende Eigenschaften zu Dokumenten gespeichert:



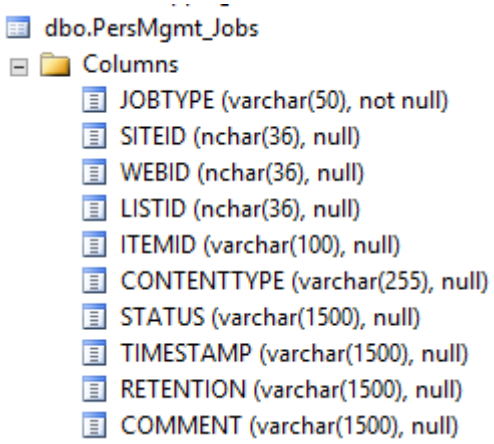
- GUID
  - Technische SharePoint Identifikation eines Dokumentes (kryptische Buchstaben und Zahlenkombination)
- WEBID
  - Technische Identifikation der Dokumentengruppe (kryptische Buchstaben und Zahlenkombination)
- ContentType
  - Technische Identifikation der Dokumentenart (kryptische Buchstaben und Zahlenkombination)
- PersNr
  - Die Personalnummer zum Dokument

Es werden keine weiteren Personenbezogene Daten gespeichert. Mit Hilfe dieser Daten kann solch eine Suchabfrage erstellt werden.

Expiration Files

Mit diesem Modul werden ablaufende Dokumente markiert, welche gesetzlich zur Löschung verpflichtet sind.

In dieser Tabelle, welche sich in der ecspand Inhaltsdatenbank befindet, werden folgende Eigenschaften zu Dokumenten gespeichert:



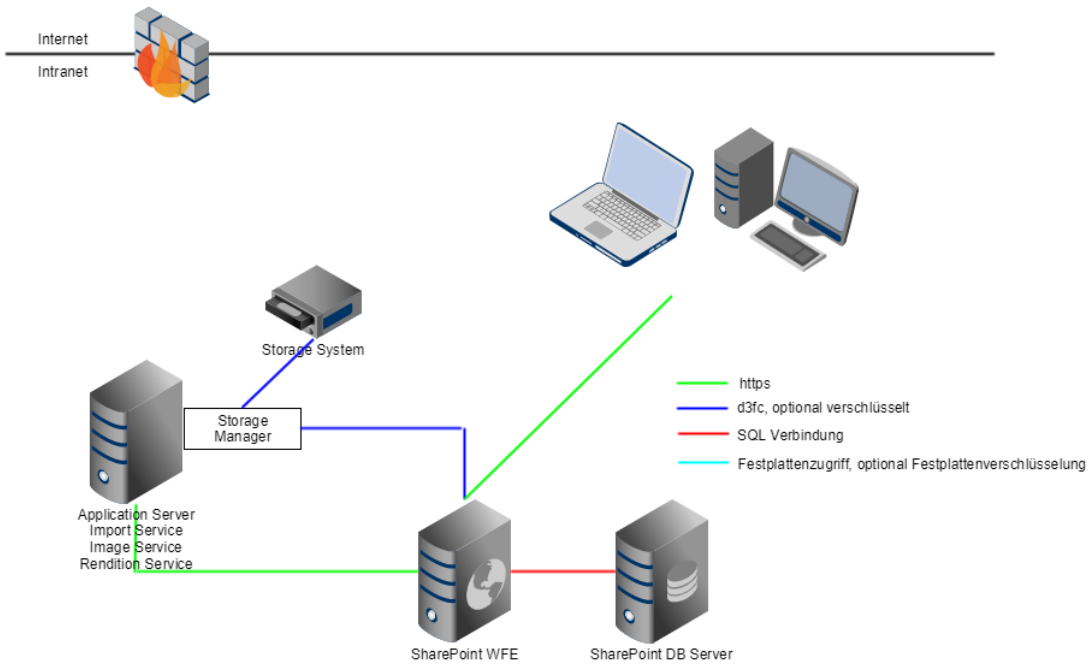
- JOBTYPE
  - Aktuell werden nur ablaufende Dokumente hinterlegt. In späteren Versionen kann dies ausgebaut werden und um weitere Job-Typen ergänzt werden.

- SITEID
  - Technische Identifikation der Webseitensammlung (kryptische Buchstaben und Zahlenkombination)
- WEBID
  - Technische Identifikation der Dokumentengruppe (kryptische Buchstaben und Zahlenkombination)
- LISTID
  - Technische Identifikation des Ablageortes im SharePoint (kryptische Buchstaben und Zahlenkombination)
- ITEMID
  - Technische Identifikation eines Dokumentes zur Dokumentenart (nicht eindeutig) (kryptische Buchstaben und Zahlenkombination)
- CONTENTTYPE
  - Technische Identifikation der Dokumentenart (kryptische Buchstaben und Zahlenkombination)
- STATUS
  - Zahl oder Beschreibung zum Status des Dokumentes
- TIMESTAMP
  - Datum und Uhrzeit zum Job
- RETENTION
  - Anzahl von Monaten, wann das Dokument abläuft
- COMMENT
  - Wird das Dokument verlängert (weil eine Gerichtsverhandlung aktiv läuft), so beinhaltet der Kommentar die Person, welche das Dokument verlängert hat und wann dies gemacht wurde.

1.2.38. Datenkommunikation ecspand quality management

Um grundsätzlich zu verstehen, wo im Kontext der DSGVO bei ecspand quality management angesetzt werden kann, muss kurz erläutert werden, welche Daten und Dienste es grundsätzlich gibt und wie diese Daten vorgehalten werden oder mit einander kommunizieren. Da es sich bei ecspand quality management in der Regel um einen Prozess mit einer Vielzahl an eingesetzten Komponenten handelt, betrachten wir in diesem Kapitel ausschließlich die Datenhaltung des Produktes escpand quality management.

Darstellung des Datenflusses einer typischen ecspand quality management Installation



Datenhaltung im SharePoint

Nach dem Anlegen eines Dokumentes über das ecspand quality management, bewegen Sie sich aus Security Perspektive im Microsoft SharePoint Standard. Prüfen Sie dabei die Sicherheitskonzepte aus der Produktdokumentation oder Ihre konkrete individuelle Umsetzung.

Personenbezug finden Sie dabei im SharePoint mindestens immer dann, wenn ein Benutzerfeld eingesetzt wird. Im Kontext des Qualitätsmanagement, abhängig von der ausgewählten Installation, finden Sie in der Regel an folgenden Stellen einen Personenbezug.

- In den Autorisierungsregeln.
- An einem Dokument in der Bibliothek im Arbeitsbereich und Portal als Bearbeitet von, Deaktiviert von, Freigegeben von, Genehmigt von, Geprüft von, Zugewiesen an, Erstellt von, Geändert von, Ausgecheckt von und im Workflow-Kommentar.
- In der Aufgabenliste als "Zugewiesen an".

Sollten Sie für sich identifizieren, das ein Betroffenenrecht in diesen Daten relevant sein könnte, suchen Sie bitte in den oben aufgeführten Listen und Bibliotheken. Berücksichtigen Sie diese Dinge bitte auch in Ihrem Löschkonzept.

> **Anmerkung**
> Sollte ein Mitarbeiter Ihr Unternehmen verlassen, der an diesem Prozess teilgenommen hat:
>
> - Entfernen Sie den Mitarbeiter aus jeglichen Gruppen im Qualitätsmanagement.
> - Entfernen Sie den Mitarbeiter aus den Autorisierungsregeln.

1.2.39. Datenkommunikation ecspand services

Um grundsätzlich zu verstehen, wo im Kontext der DSGVO bei einer Installation der ecspand services angesetzt werden kann, muss kurz erläutert werden, welche Daten und Dienste es grundsätzlich gibt und wie diese Daten vorgehalten werden oder mit einander kommunizieren. Da es sich bei ecspand services um eine Vielzahl generisch nutzbarer Komponenten handelt, ist dies eine Beispielverwendung.

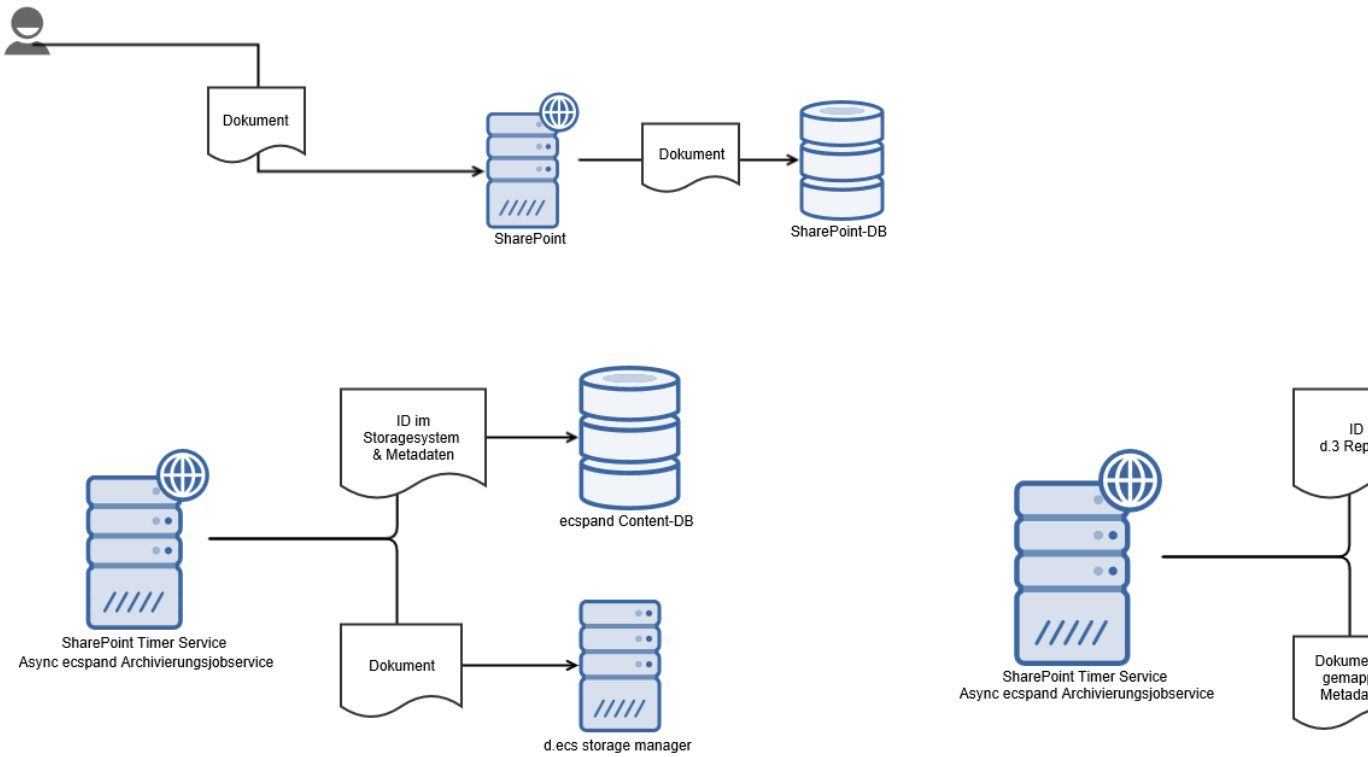
Sie müssen diese Informationen auf Ihre konkrete Ausprägung übertragen.

Typische Topologie

In einer typischen Topologie im ecspand Umfeld finden Sie in der Regel eine Einrichtung folgender Komponenten vor:

- Ein ERP System ist in die Landschaft und Prozesse integriert.
- Dokumente werden gescannt. Ein Import-Service ist im Einsatz.
- Dokumente werden gerendert, also in das PDF Format gebracht. Ein Rendition-Service ist im Einsatz.
- Dokumente werden archiviert. Ein Storage-Manager ist im Einsatz.

Die folgende Grafik visualisiert die zu berücksichtigen technischen Komponenten:



Dies ist exemplarisch und kann in Ihrer konkreten Einrichtung von dieser Topologie abweichen. Es soll lediglich visualisiert werden, welche Datenbanken und Systeme üblicherweise eingesetzt werden.

Entnehmen Sie bitte Ihrer kundenspezifischen Einrichtungsdokumentation, welche konkreten Dienste bei Ihnen eingesetzt werden.

ecspand services - eigene Verwaltungsdaten

ecspand verfügt über eigene Datenbanken zum Verwalten von Konfigurationen und Aufgaben (Archivierung, Rendition, usw.)

Den Aufbau der Datenbanken, sowie die berechtigungstechnische Einrichtung sind in der Dokumentation der ecspand services beschrieben.

Die Tabellen werden nun im Detail erläutert:

Tabellen für den Bereich Compliance:

- dbo.ComplianceListItems
- dbo.ComplianceListItemsDepDocs
- dbo.ComplianceListItemsLock
- dbo.ComplianceListItemsMetaData
- dbo.ecspandJobs
- dbo.LinkItems
- dbo.LinkMappings

Diese Tabellen verfügen, mit einer Ausnahme, über keine personenbezogenen Daten und sind von der DSGVO nicht berührt. Sie haben technischen Charakter.

Die Tabelle **ComplianceListItemsMetaData** ist jedoch so aufgebaut, dass Metadaten von archivierten Objekten in der jeweiligen Version Ihrer Anpassung gespeichert werden.

Somit werden in dieser Tabelle zu allen Objekten, die archiviert werden sollen, Metadateninformationen enthalten sein, sofern Sie an der Regel zur Archivierung festgelegt haben, dass dies auch geschehen soll.

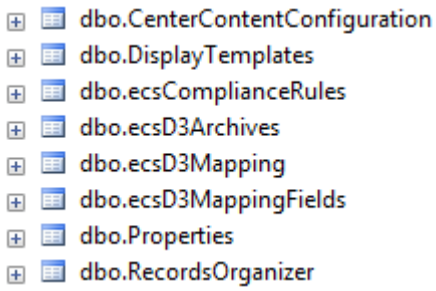
Das reguläre und auch das privilegierte Löschen wird in der Dokumentation der ecspand services gesondert betrachtet und erläutert.

Wenn Sie die Versionsseite des entsprechenden Objektes im SharePoint öffnen, dann werden Ihnen die Informationen aus dieser Tabelle angezeigt.

Die Tabellen **ecspandJobs**, sowie **LinkItems** haben rein technischen Charakter und sind nicht von der DSGVO betroffen.

In der Tabelle **LinkMappings** finden Sie Informationen, welches LinkItem (Verknüpfungen) bei welcher Person angezeigt werden soll. Enthalten ist lediglich der LoginName. Neben dieser User-Information werden in dieser Tabelle keinerlei weitere Informationen zu der Person vorgehalten. Werden die Verknüpfungen über die center Oberfläche gelöscht, so werden diese gleichzeitig aus der Datenbanktabelle entfernt.

Konfigurationstabellen in der Konfigurationsdatenbank:



In denTabellen **CenterContentConfiguration** und **DisplayTemplates** werden Konfigurationen des ecspand centers persistiert. Es wird festgehalten, welche Person diese Konfiguration ablegt, bzw. wird das Konto als Windows Logon Name protokolliert, mit dem die Änderung durchgeführt wurde.

Die Tabelle **ecsComplianceRules** ist nicht von der DSGVO betroffen. Sie enthält keinerlei persönliche Daten.

In der Tabelle **ecsD3Archives** werden d.3-Instanzen mit entsprechenden Dienstkonten (User, Kennwort) festgehalten. Das Kennwort wird doppelt verschlüsselt abgelegt. Die Tabelle hat technischen Charakter und beinhaltet keinerlei weitere Informationen zum dem Dienstkonto.

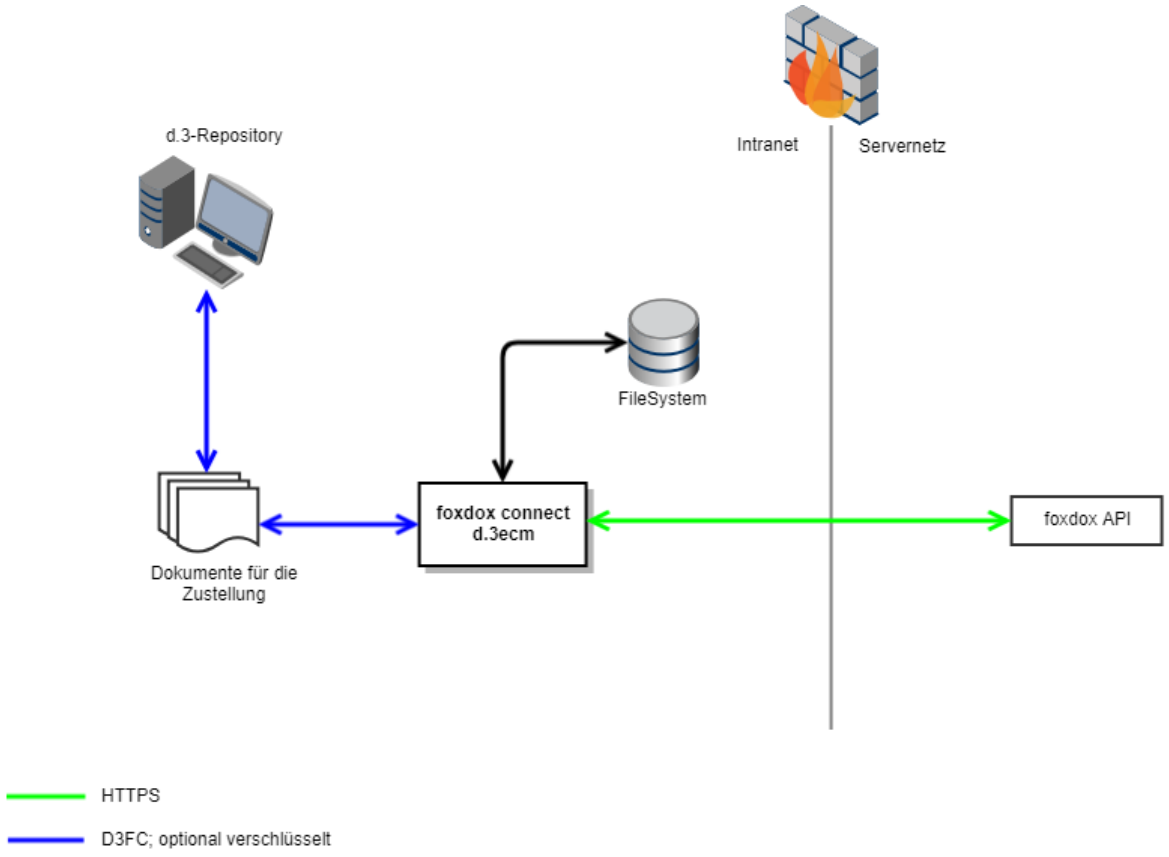
Die Tabellen **ecsD3Mapping**, **ecsD3MappingFields**, **Properties** und **RecordsOrganizer** beinhalten keinerlei personenbezogener Daten und sind somit nicht für die DSGVO relevant.

1.2.40. Datenkommunikation foxdox connect d.3ecm

Darstellung des Datenflusses von foxdox connect d.3ecm

foxdox connect d.3ecm ist eine Softwarekomponente, die dafür zuständig ist, Dokumente zwischen einem beim Kunden installierten d.3 und foxdox auszutauschen. Es handelt sich dabei um eine beim Kunden installierte Software. Es können zum einen Dokumente aus einem d.3-Repository an einen foxdox-Benutzer zugestellt werden und zum anderen wird es ermöglicht, Dokumente eines foxdox-Benutzers in d.3 zu archivieren. Die Zustellung eines Dokuments erfolgt immer im Kontext eines Provider-Dienstes.

Die Kommunikation zur foxdox-API erfolgt über eine verschlüsselte Verbindung.



Anlieferung von Dokumenten für die Zustellung

Der Administrator wählt im d.3-Repository Dokumente aus, die er an den foxdox-Benutzer zustellen möchte. foxdox connect d.3ecm holt sich die ausgewählte Dokumente von dem d.3-Repository, erstellt eine .fdx-Datei und komprimiert die in einem passwortgeschützten Container. Als Verschlüsselung für den Container wird AES-256 verwendet. Das zufallsgenerierte Passwort wird RSA-2048 verschlüsselt und zusammen mit dem Container über https an die foxdox-API gesendet. Für weiterführende Informationen steht die Dokumentation des Zustellungsprozess zur Verfügung.

Empfang von Dokumenten

Der foxdox-Benutzer wählt in foxdox ein Dokument aus, das er an den foxdox-Provider versenden möchte. foxdox connect d.3ecm fragt in einem konfigurierten Intervall die foxdox-API an, ob neue Dokumente zum Empfangen vorliegen. Ist das der Fall, werden diese Dokumente heruntergeladen und in das lokale Dateisystem gespeichert. Im Anschluss lädt foxdox connect d.3ecm die Dokumente ins d.3-Repository hoch und löscht die Dokumente aus dem lokalen Dateisystem.

1.2.41. Datenkommunikation foxdox link

Anlieferung von Dokumenten für die Zustellung

Der Provider legt im Outbox-Ordner eine .fdx-Datei an, in der Zustellungsordner, Empfänger und zu versendende Dokumente definiert sind. Daneben werden die zu versendenden Dateien abgelegt. Durch die Verzeichnisüberwachung bekommt das Programm mit, dass dort Dokumente zum Versenden abgelegt wurden. Der Ordnerinhalt wird durch einen asynchronen Prozess komprimiert und in einem passwortgeschützten Container zusammengefasst. Als Verschlüsselung für den Container wird AES-256 verwendet. Das zufallsgenerierte Passwort wird nach RSA-2048 verschlüsselt und zusammen mit dem Container über HTTPS an die foxdox-API gesendet.

Empfang von Dokumenten

Ein asynchroner Prozess fragt in einem konfigurierten Intervall über die API ab, ob neue Dokumente für den Provider bereit stehen. Ist das der Fall, werden diese heruntergeladen und auf dem lokalen Dateisystem gespeichert.

Initial Konten verwalten

Der Provider kann sogenannte Initialkonten für mehrere Benutzer anlegen. Diese sind bereits mit dem Dienst des Providers verknüpft. Für die Zuweisung von Benutzer und Empfänger von Dokumenten wird eine PSUID verwendet.

Direktschlüssel verwalten

Der Provider kann sogenannte Direktschlüssel anlegen. Diese können von foxdox-Benutzern verwendet werden, um sich mit einem bestimmten Dienst des Providers zu verbinden. Für die Zuweisung von Benutzer und Empfänger von Dokumenten wird eine PSUID verwendet.

Provider konfigurieren

Hier werden keine Personenbezogenen Daten verarbeitet.

Dienste konfigurieren

Hier werden keine Personenbezogenen Daten verarbeitet.

Benutzer konfigurieren

Das sind die Benuzer, die Zugriff auf foxdox.link haben. Es werden keine personenbezogenen Daten verarbeitet.

Stammdaten verwalten

Hier können die Stammdaten für die Datenerfassung eingestellt werden. Es werden keine personenbezogenen Daten verarbeitet.

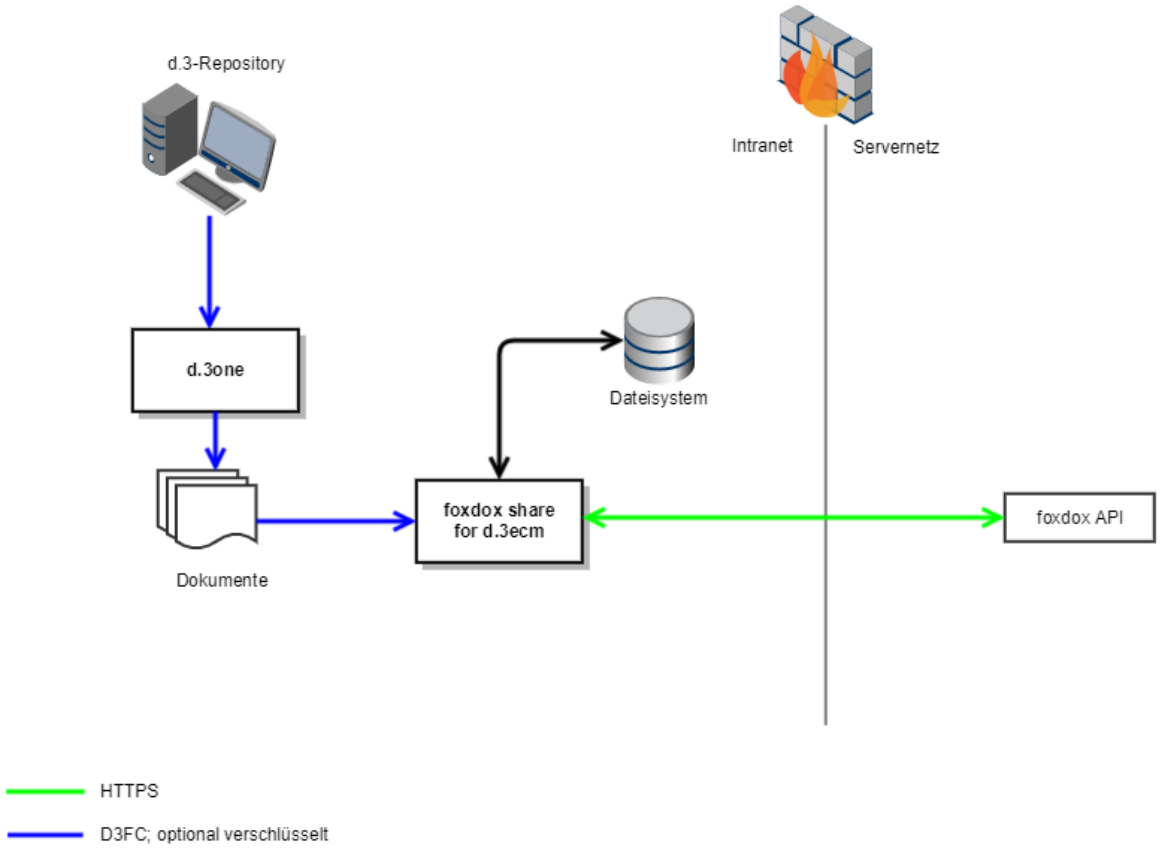
1.2.42. Datenkommunikation foxdox share for d.3ecm

Darstellung des Datenflusses von foxdox share for d.3ecm

foxdox share for d.3ecm ist eine Softwarekomponente, mit der Dokumente aus einem beim Kunden installierten d.3one an foxdox geschickt werden können. Es handelt sich dabei um eine beim Kunden installierte Software.

Hierfür integriert sich die Komponente in d.3one.

Die Kommunikation zur foxdox-API erfolgt über eine verschlüsselte Verbindung.

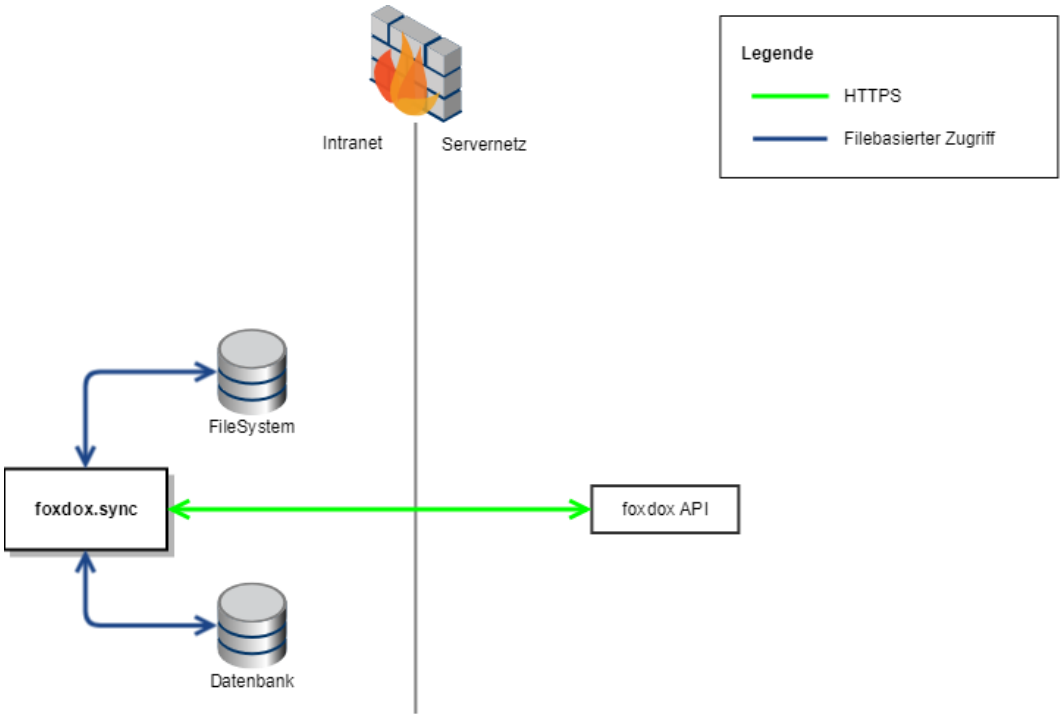


Anlieferung von Dokumenten für die Zustellung

Der d.3one-Benutzer wählt in d.3one Dokumente aus, die er an einen foxdox-Benutzer schicken möchte. Die Dokumente werden temporär auf das lokale Dateisystem geschrieben und dann über die foxdox API hochgeladen.

1.2.43. Datenkommunikation foxdox sync

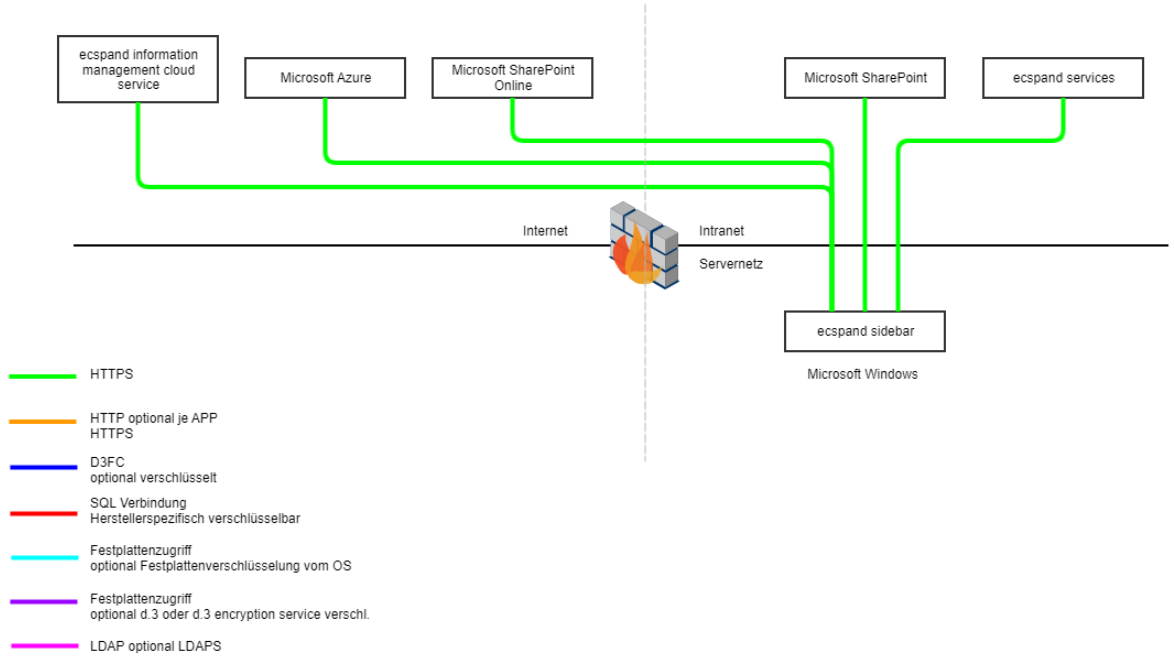
Darstellung des Datenflusses von foxdox sync mit dem foxdox-Backend



Synchronisation der lokalen Daten mit den foxdox-Services

foxdox sync synchronisiert lokale Daten mit den foxdox-Services. Hierfür greift foxdox sync über datei-basierten Zugriff auf lokale Daten zu und speichert für die Synchronisation in einer lokalen Datenbank Dokument- und Ordnerdetails. Änderungen an Dokumenten oder Ordner werden über die foxdox API synchronisiert. Die Kommunikation erfolgt über https.

1.2.44. Datenkommunikiation ecspand sidebar



Die ecspand sidebar greift über das Client Side Object Model, REST-Services und SOAP-Services auf Microsoft SharePoint, Microsoft Azure, ecspand services und d.velop composer (früher: ecspand information management cloud Service) zu. Dies hängt von Ihrer Verbindungskonfiguration ab.

Sollten Sie für sich identifiziert haben, dass die Kommunikation verschlüsselt durchgeführt werden soll, kann in der Verbindungskonfiguration eine https Verbindung mit SSL eingerichtet werden.

1.2.45. Datenverarbeitung bei Integrationen von d.velop documents

In diesem Artikel finden Sie wichtige Informationen zur Datenverarbeitung bei Integrationen von d.velop documents for Microsoft 365, damit Sie die technischen und rechtlichen Aspekte nachvollziehen können. Folgende Fragen werden beantwortet:

- **Technische Voraussetzungen**: Welche technischen Voraussetzungen bestehen, um die Integrationen verwenden zu können?
- **Datenübermittlung**: Wie erfolgt technisch die Übermittlung der Daten an Microsoft?
- **Vertragliche Grundlagen**: Welche vertraglichen Grundlagen gelten?
- **Rechenzentren**: In welchen Rechenzentren werden Microsoft Office-Dokumente verarbeitet?

Technische Voraussetzungen

Um die Integrationen verwenden zu können, benötigen Sie d.velop documents (Cloud- oder Hybridbetrieb) und ein gültiges Microsoft 365-Abonnement.

Datenübermittlung

- d.velop documents stellt eine Web Application Open Platform Interface Protocol (WOPI)-API bereit, die von Microsoft angesprochen wird. Weitere Informationen zum Thema finden Sie unter: Web Application Open Platform Interface Protocol (WOPI)
- Die Kommunikation zwischen d.velop documents und Office für das Web erfolgt verschlüsselt (Transportverschlüsselung) in Kombination mit individuell bereitgestellten Access Tokens je Dokument.

Vertragliche Grundlagen

- d.velop ist dem Office Cloud Storage Partnerprogramm beigetreten. Daher gelten folgende Microsoft-Richtlinien: Microsoft Cloud Storage Partner Program Integration Terms
- Bei Abschluss des Microsoft 365-Abonnements ist der Kunde für den Abschluss entsprechender Verträge mit Microsoft hinsichtlich der Datenverarbeitung verantwortlich.

Rechenzentren

- Microsoft versucht nach eigenen Angaben, Dokumente, die mit Office für das Web bearbeitet werden, im nächstgelegenen Rechenzentrum zu verarbeiten. Jedoch kann Microsoft die Verarbeitung im nächstgelegenen Rechenzentrum nicht garantieren.
- Weitere Informationen zur Verarbeitung finden Sie auf der Seite von Microsoft unter: FAQ - How does Office for the web determine the datacenter to route a given user to?

1.3. Betroffenenrechte

Das neue Datenschutzrecht gestaltet die Betroffenenrechte neu. Wie sich die Neugestaltung der Betroffenenrechte auf Ihr d.velop-Produkt auswirkt, erfahren Sie in diesem Kapitel.

1.3.1. Auskunft

Auskunft d.3 search

Daten, die beauskunftet werden müssen, können über die führende Anwendung d.3 abgerufen und dort im Zusammenhang mit allen anderen gespeicherten Daten dargestellt werden.

Auskunft d.classify

Mit dem **Anonymisierungsassitent** kann in den in d.classify hinterlegten Referenzen nach Dokumente der betroffenen Person gesucht werden.

Auskunft d.ecs forms

Mit der Instanzsuche in d.ecs forms können Formular-Instanzen ermittelt werden, in denen ein vorgegebener Suchbegriff vorkommt. Diese Instanzen können technisch exportiert werden.

Auskunft d.velop GDPR compliance center

Personenbezogene Daten innerhalb von d.velop GDPR compliance center werden lediglich in zwei Kontexten gespeichert:

- Zu jedem Datenschutzgegenstand kann ein Verantwortlicher sowie ein Genehmiger in Form eines Benutzernames bzw. einer Benutzerkennung angegeben werden.
- In der Konfiguration des Verzeichnisses der Verarbeitungstätigkeiten besteht die Möglichkeit, Ansprechpartner mit Name, Vorname, Position, Abteilung sowie Telefonnummer zu hinterlegen.

Eine Auskunft über die Hinterlegung einer Person als Verantwortlicher oder Genehmiger eines Datenschutzgegenstands kann einfach über die Übersicht der Datenschutzgegenstände und Sortierung nach Verantwortlicher und Genehmiger erfolgen.

Eine Auskunft über die Hinterlegung einer Person als Ansprechpartner kann nach Aufruf der Konfiguration des Verzeichnisses der Verarbeitungstätigkeiten erfolgen.

Auskunft d.velop process

Ein automatisiertes Durchsuchen der Laufzeitdaten und Verlaufsdaten ist aktuell nicht möglich.

Bitte beachten Sie, dass DSGVO-relevante Benutzerdaten nicht in den Laufzeitdaten und Verlaufsdaten von Prozessen gespeichert werden sollten, sondern ausschließlich in referenzierten Drittsystem.

Auskunft dbs | case manager

Nachfolgend finden Sie eine Aufstellung der im Standard innerhalb von dbs | case manager contract gespeicherten personenbezogenen Daten. Sofern Sie als Verantwortlicher dem Auskunftsrecht einer betroffenen Person nachkommen müssen, so können Sie die entsprechenden Daten über die entsprechenden Oberflächen recherchieren. Darüber hinaus kann je nach Eigenschaft und Konfiguration auch die Volltextrecherche, die Vertragsübersicht inkl. Facettierung sowie die Standardsuche innerhalb des d.3ecm-Systems für die Suche verwendet werden.

Das Produkt dbs | case manager dient dazu, alle wesentlichen Information im Unternehmen wie Dokumente, Informationen, Aufgaben und Konversationen vorgangsorientiert zusammenzufassen und digital zur Verfügung zu stellen. Anhand von Vorgangstypen, Statusmodellen, erweiterten Stammdaten sowie Aufgabentemplates gelingt es, die jeweils unternehmensindividuellen Geschäftsprozesse flexibel zu modellieren. Der dbs | case manager stellt daher ein generisches Produkt dar, dass für beliebige Prozesse und somit auch innerhalb beliebiger Verarbeitungstätigkeiten im Sinne der DSGVO verwendet werden kann. Die nachfolgenden Erläuterungen können sich daher immer nur auf das Produkt als solches und dessen Standardlieferumfang beziehen. Eine Analyse und Bewertung der datenschutzrelevanten Aspekte von Verarbeitungstätigkeiten, die auf Basis von dbs | case manager realisiert wurden, bedarf daher einer konkreten Betrachtung der kundenspezifisch realisierten Prozesse.

Innerhalb von dbs | case manager können unterschiedliche personenbezogene Daten gespeichert werden. Die folgende Auflistung bezieht sich lediglich auf solche personenbezogene Daten, die aufgrund des Produktstandards gespeichert werden können:

- Name, Vorname:
  Name und Vorname in Form von Freitexteingaben werden im Standard lediglich erfasst, um den Personenkontakt eines Geschäftspartners zu hinterlegen.

Dies erfolgt in der Partnerverwaltung bzw. im Vorgangsformular durch Eingabe eines externen Ansprechpartners.

- Benutzer/d.3-Benutzer:
  Benutzerkennungen bzw. d.3-Benutzer werden immer dann verwendet, wenn im Hinblick auf Prozesssteuerung oder Protokollierung der Benutzer relevant ist.
  Somit werden Benutzerkennungen vorwiegend für die Zuordnung von Verantwortlichkeiten für Vorgänge, Aufgaben sowie als Empfänger von Postkorbeinträgen und Nachrichten sowie zur Protokollierung von Aktivitäten innerhalb des Vorgangsmanagements verwendet. Ebenso kann ein Benutzer im Rahmen dieser Verantwortlichkeiten als Stellvertreter eines anderen Benutzers hinterlegt werden.
  Darüber hinaus werden Benutzerkennungen verwendet, um diesen entsprechende Rechte auf Funktionen im Vorgangsmanagement geben zu können.
- E-Mail-Adressen:
  E-Mail-Adressen werden verwendet, um externe Konversationen versenden zu können. Somit kann eine E-Mail-Adresse als Empfänger einer einzelnen Konversation genutzt werden bzw. in der Partnerverwaltung zum Ansprechpartner hinterlegt werden, um die E-Mail-Adresse einfach in den externen Konversationen auswählen zu können.
- Telefonnummer und Adressdaten:
  Telefonnummer und Adressdaten können optional für Personenkontakt des Geschäftspartners hinterlegt werden

Auskunft dbs | case manager contract

Nachfolgend finden Sie eine Aufstellung der im Standard innerhalb von dbs | case manager contract gespeicherten personenbezogenen Daten. Sofern Sie als Verantwortlicher dem Auskunftsrecht einer betroffenen Person nachkommen müssen, so können Sie die entsprechenden Daten über die entsprechenden Oberflächen recherchieren. Darüber hinaus kann je nach Eigenschaft und Konfiguration auch die Volltextrecherche, die Vorgangsübersicht inkl. Facettierung sowie die Standardsuche innerhalb des d.3ecm-Systems für die Suche verwendet werden.

Das Produkt dbs | case manager contract ist als ganzheitliches Vertragsmanagementsystem konzipiert. Der digitale Vertragsvorgang umfasst alle wesentlichen Informationen wie Dokumente, Stammdaten, Aufgaben und Konversationen. Das integrierte Vorgangsmanagement erlaubt die individuelle Modellierung des Geschäftsprozesses Vertragsmanagement anhand von Vertragstypen, Statusmodellen, erweiterten Stammdaten sowie Aufgabentemplates. Insofern beziehen sich die nachfolgenden Erläuterungen im Kern auf das Standardprodukt sowie auf die damit ausgelieferten Standardprozesse. Wesentliche für ein Verzeichnis der Verarbeitungstätigkeiten relevante Aspekte wie z.B. Zweck oder Betroffenengruppen hängen aber davon ab, für welche Arten von Verträgen dbs | case manager contract verwendet wird bzw. in welchen Verarbeitungstätigkeiten dieses Produkt Einsatz findet.

Innerhalb von dbs | case manager contract können unterschiedliche personenbezogene Daten gespeichert werden. Die folgende Auflistung bezieht sich lediglich auf solche personenbezogene Daten, die aufgrund des Produktstandards gespeichert werden können:

- Name, Vorname:
  Name und Vorname in Form von Freitexteingaben werden im Standard lediglich erfasst, um den Personenkontakt eines Geschäftspartners zu hinterlegen.
  Dies erfolgt in der Partnerverwaltung bzw. im Vertragsformular durch Eingabe eines externen Ansprechpartners bzw. bei der Erfassung einer Kündigung durch den Geschäftspartner.
- Benutzer/d.3-Benutzer:
  Benutzerkennungen bzw. d.3-Benutzer werden immer dann verwendet, wenn im Hinblick auf Prozesssteuerung oder Protokollierung der Benutzer relevant ist.
  Somit werden Benutzerkennungen vorwiegend für die Zuordnung von Verantwortlichkeiten für Verträge, Fristen, Aufgaben sowie als Empfänger von Postkorbeinträgen und Nachrichten sowie zur Protokollierung von Aktivitäten innerhalb des Vertragsmanagements verwendet. Ebenso kann ein Benutzer im Rahmen dieser Verantwortlichkeiten als Stellvertreter eines anderen Benutzers hinterlegt werden.
  Darüber hinaus werden Benutzerkennungen verwendet, um diesen entsprechende Rechte auf Funktionen im Vertragsmanagement geben zu können.

- E-Mail-Adressen:
  E-Mail-Adressen werden verwendet, um externe Konversationen versenden zu können. Somit kann eine E-Mail-Adresse als Empfänger einer einzelnen Konversation genutzt werden bzw. in der Partnerverwaltung zum Ansprechpartner hinterlegt werden, um die E-Mail-Adresse einfach in den externen Konversationen auswählen zu können.
- Telefonnummer und Adressdaten:
  Telefonnummer und Adressdaten können optional für Personenkontakt des Geschäftspartners hinterlegt werden

Auskunft ecspand

In formeller Hinsicht bestimmt Art.12 Abs. 5 DSGVO, dass die Auskunft grundsätzlich unentgeltlich erfolgen muss.

Dazu hat der Verantwortliche ohne unangemessene Verzögerung, spätestens jedoch innerhalb eines Monats zu antworten.

Wenn der Antrag auf Auskunft in elektronischer Form eingegangen ist, sollte auch die Antwort in elektronischer Form erfolgen.

Wenn Sie für sich identifiziert haben, dass Sie diesem Recht nachkommen müssen, identifizieren Sie bitte in der Aufarbeitung Ihres Verarbeitungsverzeichnisses, an welchen Stellen personenbezogene Daten existieren. Nutzen Sie die ecspand Suche, ggf. auch in mehreren Abfragen, um alle identifizierten Objekte in einem jeweiligen Suchresultat aufzulisten.

Von dort aus sind Sie in der Lage, das Ergebnis an sich, nicht die Objekte selbst, als .csv-Datei elektronisch zu exportieren.

Falls Sie für sich herausgabepflichtige Objekte identifiziert haben, so arbeiten Sie ggf. mit eigenen ContentTypes oder Feldern, die diese Herausgabepflicht markieren. Da das Produkt jedoch einen hohen generischen Charakter mit sich bringt und wir nicht wissen, was genau Sie mit dem Produkt umsetzen, können Sie diese Erleichterung im Microsoft SharePoint Standard sehr leicht für sich umsetzen.

Auskunft ecspand invoice processing

In formeller Hinsicht bestimmt Art.12 Abs. 5 DSGVO, dass die Auskunft grundsätzlich unentgeltlich erfolgen muss.

Dazu hat der Verantwortliche ohne unangemessene Verzögerung, spätestens jedoch innerhalb eines Monats zu antworten.

Wenn der Antrag auf Auskunft in elektronischer Form eingegangen ist, sollte auch die Antwort in elektronischer Form erfolgen.

Wenn Sie für sich identifiziert haben, dass Sie diesem Recht nachkommen müssen, identifizieren Sie bitte in Ihrer konkreten Implementierung der ecspand ERV, basierend auf dem Kapitel Datenhaltung Datenkommunikationsflüsse, an welchen Stellen personenbezogene Daten existieren.

Verarbeiten Sie Rechnungen von natürlichen Personen oder ausschließlich von juristischen Personen?

Nutzen Sie die strukturierte ecspand Suche, ggf. auch in mehreren Abfragen, um alle identifizierten Objekte in einem jeweiligen Suchresultat aufzulisten.

Von dort aus sind Sie in der Lage, das Ergebnis an sich, nicht die Objekte selbst, als .csv Datei elektronisch zu exportieren.

Schauen Sie dazu bitte in die Dokumentation der ecspand Services.

Rechnungen sollten in der Regel, da sie weiteren Rechten unterliegen, nicht herausgabepflichtig sein. Im Prozess der ERV sind Sie sogar Empfänger der Rechnung. Ein potentieller Antragsteller sollte somit über das Dokument verfügen.

Bei einem Antrag auf Auskunft durch einen Mitarbeiter oder Prozessteilnehmer, gehen Sie wie oben beschrieben vor. Rechnungen sind in diesem Zusammenhang nicht herausgabepflichtig, da weitere Rechte auf den Dokumenten liegen.

Auskunft ecspand HR management

In formeller Hinsicht bestimmt Art.12 Abs. 5 DSGVO, dass die Auskunft grundsätzlich unentgeltlich erfolgen muss.

Dazu hat der Verantwortliche ohne unangemessene Verzögerung, spätestens jedoch innerhalb eines Monats zu antworten.

Wenn der Antrag auf Auskunft in elektronischer Form eingegangen ist, sollte auch die Antwort in elektronischer Form erfolgen.

Wenn Sie für sich identifiziert haben, dass Sie diesem Recht nachkommen müssen, sind alle Daten zu einer Person in dessen Personalakte gespeichert.

Schauen Sie dazu bitte in die Dokumentation der ecspand HR management.

Sollte der komplette Akt heruntergeladen werden müssen, können die beiden folgenden Module unterstützend wirken:

- ecspand Dokumentenkorb (nur On-Premise) d.velop AG
  - Dokumenten können hier markiert und in den Dokumentenkorb übernommen werden. Dieser Dokumentenkorb kann damit als ZIP Paket heruntergeladen werden.
- ecspand Offline Synchronization (aktuell nur On-Premise) d.velop GmbH Wien
  - Akten können in einem heruntergeladen werden.

Auskunft ecspand quality management

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten.

Basierend auf dem Kapitel **Datenkommunikation** kann identifiziert werden, an welchen Stellen personenbezogene Daten existieren.

Die strukturierte ecspand Suche kann genutzt werden, ggf. auch in mehreren Abfragen, um alle identifizierten Objekte in einem jeweiligen Suchresultat aufzulisten.

Von dort aus kann das Ergebnis, nicht die Objekte selbst, als `csv` Datei exportiert werden. Die Dokumentation der ecspand services enthält nähere Informationen dazu.

Auskunft foxdox connect d.3ecm

Innerhalb von foxdox connect d.3ecm werden keine personenbezogenen Daten gespeichert.

Es kann sein, dass personenbezogene Details in den Logdateien stehen. Deshalb empfehlen wir, dass die Logdateien nach spätestens 30 Tagen gelöscht werden.

Ob personenbezogene Details in den Logdateien stehen, hängt von der Nutzung des Produkts ab. Zum Beispiel können bestimmte schützenswerte personenbezogene Details in Dokumentnamen enthalten sein.

Auskunft foxdox share for d.3ecm

Innerhalb von foxdox share for d.3ecm werden keine personenbezogenen Daten gespeichert.

Es kann sein, dass personenbezogene Details in den Logdateien stehen. Deshalb empfehlen wir, dass die Logdateien nach spätestens 30 Tagen gelöscht werden.

Ob personenbezogene Details in den Logdateien stehen, hängt von der Nutzung des Produkts ab. Zum Beispiel können bestimmte schützenswerte personenbezogene Details in Dokumentnamen enthalten sein.

Auskunft foxdox sync

Auskunft über personenbezogene Daten anderer

Wenn Sie personenbezogene Daten anderer in Dokumenten in Ihrem DMS gespeichert haben, sind Sie nach Art.12 Abs. 5 DSGVO dazu verpflichtet grundsätzlich unentgeltlich über die gespeicherten Daten Auskunft zu erteilen. Dazu hat der Verantwortliche ohne unangemessene Verzögerung, spätestens jedoch innerhalb eines Monats zu antworten. Wenn der Antrag auf Auskunft in elektronischer Form eingegangen ist, sollte auch die Antwort in elektronischer Form erfolgen. Wenn Sie für sich identifiziert haben, dass Sie diesem Recht nachkommen müssen, identifizieren Sie bitte in der Aufarbeitung Ihres Verarbeitungsverzeichnisses, an welchen Stellen personenbezogene Daten existieren. Nutzen Sie die foxdox-Suche, ggf. auch in mehreren Abfragen, um alle identifizierten Objekte in einem jeweiligen Suchresultat aufzulisten. Von dort aus sind Sie in der Lage, das Dokument direkt zu öffnen, oder den Ordner zu öffnen, in dem das Dokument gespeichert ist.

Falls Sie für sich herausgabepflichtige Objekte identifiziert haben, so arbeiten Sie ggf. mit eigenen Dokumentarten, die diese Herausgabepflicht markieren. Da das Produkt jedoch einen hohen generischen Charakter mit sich bringt und wir nicht wissen, was genau Sie mit dem Produkt umsetzen, können Sie diese Erleichterung in foxdox sehr leicht für sich umsetzen. Um eigene Dokumentarten festlegen zu können, benötigen Sie ein kostenpflichtiges foxdox-Konto.

Auskunft über Ihre personenbezogenen Daten

Wenn Sie Auskunft über Ihre personenbezogenen Daten erhalten möchten, können Sie das zum einen direkt in Ihren Konto-Einstellungen einsehen.

Wenn Sie darüberhinaus erfahren möchten, welche weiteren personenbezogenen Daten gespeichert sind, dann schreiben Sie uns eine Mail an datenschutz@foxdox.de. Sie erhalten innerhalb eines Monats eine Auskunft von uns.

1.3.2. Löschung

Löschung d.3 search

Die Löschung erfolgt über das führende System d.3. Daten, die dort gelöscht werden, werden auch in d.3 search entfernt. Dabei werden genutzte Worte nicht direkt aus dem Index gelöscht, sondern nur die Referenzen auf die entsprechenden Dokumente werden entfernt. Bei einer Reindizierung wird dann auch der Index dementsprechend bereinigt, dass nicht mehr genutzte Worte aus dem Index komplett entfernt werden.

Daten in temporären Verzeichnissen werden täglich wieder entfernt.

Löschung d.classify

Mit dem **Anonymisierungsassitenten** in d.classify Admin kann nach Dokumente der betroffenen Person in den hinterlegten Referenzen gesucht werden.

Die gefundenen Dokumente können hier gesichtet und, bei Bedarf, anonymisiert oder gelöscht werden.

Löschung d.ecs forms

Über die Instanzsuche können Formular-Instanzen ermittelt werden, die Daten zu einem definierten Suchbegriff enthalten. Diese können anschließend anhand der Identifier aus der Instanzdatenbank gelöscht werden.

Löschung d.ecs storage manager

d.ecs storage manger gibt die Löschanforderung der aufrufenden Applikation (z.b: d.3 oder ecspand), wenn möglich, an die Storagesysteme weiter. Dabei muss sichergestellt sein, dass diese Systeme auch das privilegierte Löschen unterstützen, um Daten vor Ablauf der Retention-Zeit aus dem Storage entfernen zu können.

Löschung d.velop GDPR compliance center

Die Löschung des Benutzernamens bzw. der Benutzerkennung, die als Verantwortlicher oder Genehmiger eines Datenschutzgegenstands hinterlegt sind, erfolgt durch den Aufruf des Datenschutzgegenstandes und Änderung des jeweiligen Verantwortlichen oder Genehmigers.

Die Löschung von personenbezogenen Daten zu einem für das Verzeichnis der Verarbeitungstätigkeiten hinterlegten Ansprechpartner erfolgt innerhalb der Konfiguration des Verzeichnisses der Verarbeitungstätigkeiten.

Löschung d.velop process

Ein automatisiertes Durchsuchen der Laufzeitdaten und Verlaufsdaten ist aktuell nicht möglich.

Bitte beachten Sie, dass DSGVO-relevante Benutzerdaten nicht in den Laufzeitdaten und Verlaufsdaten von Prozessen gespeichert werden sollten, sondern ausschließlich in referenzierten Drittsystem.

Löschung dbs | case manager + contract

Eine Löschung der personenbezogenen Daten erfolgt über die jeweiligen Oberflächen.

Löschung ecspand

Artikel 17 Abs. 1 DSGVO stellt mit dem Recht auf Löschung personenbezogener Daten zunächst keine wesentlichen Änderungen im Vergleich zum entsprechenden § 35 Abs. 2 BDSG dar. Die wichtigsten Fallgruppen, in denen die Löschung von Daten verlangt werden kann, bleiben dieselben. Nach Art. 17 Abs. 3b DSGVO scheidet eine Löschung dabei auch weiterhin aus, wenn gesetzliche Aufbewahrungsfristen bestehen (siehe § 35 Abs. 3 Nr. 1 BDSG).

Legen Sie in einem Löschkonzept fest, welche Objekte tatsächlich bei Antrag auf Löschung gelöscht werden müssen. Prüfen Sie Rechte Dritter und Aufbewahrungsrechte der Objekte und ob diese tatsächlich gelöscht werden dürfen.

Prüfen Sie, ob zu löschende Objekte ggf. archiviert werden. Sollte dies der Fall sein, prüfen Sie bitte, ob Ihr Archivsystem das privilegierte Löschen unterstützt, oder ob Sie dort konfigurativ und kaufmännisch weitere Maßnahmen durchführen müssen, wie z.B. das Erwerben einer erweiterten Lizenz.

Das Löschen von Dokumenten mit abgelaufener Aufbewahrungszeit sowie das privilegierte Löschen von Dokumenten in den ecspand services ist im Kapitel **DSGVO** beschrieben.

Löschung ecspand invoice processing

Art. 17 Abs. 1 DSGVO bringt mit dem Recht auf Löschung personenbezogener Daten zunächst keine wesentlichen Änderungen im Vergleich zum entsprechenden § 35 Abs. 2 BDSG. Die wichtigsten Fallgruppen, in denen die Löschung von Daten verlangt werden kann, bleiben dieselben. Nach Art. 17 Abs. 3b DSGVO scheidet eine Löschung dabei auch weiterhin aus, wenn gesetzliche Aufbewahrungsfristen bestehen (siehe § 35 Abs. 3 Nr. 1 BDSG).

Im Falle von Eingangsrechnungen ist das der Fall.

Bei einem Antrag durch einen (ehemaligen) Mitarbeiter, bewegen Sie sich im SharePoint Standard. In diesem Fall müssen keine Dokumente gelöscht werden, jedoch muss die Mitgliedschaft in Prozessgruppen angepasst werden. Weitere Informationen dazu finden Sie in dem Kapitel Datenhaltung und Datenkommunikationsflüsse.

Legen Sie in einem Löschkonzept fest, welche Objekte tatsächlich bei Antrag auf Löschung gelöscht werden müssen. Prüfen Sie Rechte Dritter und Aufbewahrungsrechte der Objekte und ob diese tatsächlich gelöscht werden dürfen.

Prüfen Sie, ob zu löschende Objekte ggf. archiviert werden. Sollte dies der Fall sein, so prüfen Sie bitte, ob Ihr Archivsystem das privilegierte Löschen unterstützt, oder ob Sie dort konfigurativ und kaufmännisch weitere Maßnahmen durchführen müssen, wie z.B. das Erwerben einer erweiterten Lizenz. Prüfen Sie ggf. das in der Einleitung erwähnte Dokument im d.velop Service Portal, das Ihnen zu dieser Themenstellung weitere Informationen bereitstellt.

Was muss ich tun, damit ich Daten die ich löschen muss auch löschen kann bzw. wie lösche ich konkret?

Definieren Sie in Ihrem Löschkonzept, welche Objekte konkret gelöscht werden müssen.

Ergänzen Sie den Regelfall dabei um Ihre konkrete Ausprägung der ERV. Berücksichtigen Sie folgende Dokumente:

- die Eingangsrechnung
- abhängige hochgeladene Dokumente
- abhängige hochgeladene fiburelevante Dokumente
- den Workflowreport
- GOBD Daten, zugänglich im Bereich der Konfigurationsseite der ERV
- Workflowverlaufsinformationen, zugänglich im Bereich der Konfigurationsseite der ERV
- weitere in Ihrem Prozess verwendete Dokumente

Löschung ecspand HR management

Ablaufende Dokumente

Einige Dokumentarten sind per Gesetz nach einer geregelten Anzahl von Monaten zur Löschung verpflichtet. Die dafür hinterlegte Person erhält eine Benachrichtigung und muss manuell auf einer eigenen Seite die zur Löschung markierten Dokumente löschen.

Dieses Feature kann auch für nicht gesetzlich zur Löschung verpflichtende verwendet werden. In der Konfiguration sind dafür alle Dokumentarten und Informationstypen hinterlegt.

EU-DSGVO

Um die neue Datenschutz-Grundverordnung der EU (2016/679) – welche mit 25. Mai 2018 in Kraft tritt (Übergangsfrist läuft seit 2016) – zu gewährleisten, sind verschiedene Maßnahmen notwendig. Dazu zählt die Erstellung eines Verfahrensverzeichnisses (Art. 30) auf Basis der Analysierten Daten (Art. 9):

- Definition der Prozesse auf Basis der Daten, welche sich auf Personen beziehen (Gedrucktes und Digitales)
- Welche Kategorisierung besitzen diese Daten
- Welchen Zweck beinhaltet die Speicherung dieser Daten
- Wo werden diese Daten gespeichert, verarbeitet und erhoben

Die Kategorisierung der Daten nach Art. 9 lässt sich in folgende Stufen einteilen:

- Hoch / sehr hoch (vertraulich)
  - Rassische und ethnische Herkunft, Politische Meinung, Gewerkschaftszugehörigkeit, Angabe zu Strafdaten, Daten, die einem Berufsgeheimnis unterliegen, Gesundheitsdaten, Verhaltenskontrolle, Bank- oder Kreditkartendaten, Biometrische Daten (z.B. Foto)
- Mittel
  - Vertragsdaten, Auftragsdaten, Bonitätsprüfung, Personaleinsatzplanung, Private Kontaktdaten von Mitarbeitern, Daten zum Beschäftigungsverhältnis
- Gering

- Daten aus öffentlich zugänglichen Quellen, Adressdaten aus Telefonbuch, Daten, die kein schutzwürdiges Interesse des Betroffenen erforderlich machen

Löschung ecspand quality management

Was muss man tun, damit Daten, die man löschen muss, auch gelöscht werden können, bzw. wie löscht man konkret?

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern die unter Artikel 17 der DSGVO definierten Bedingungen eintreffen.

Bei einem Antrag durch einen (ehemaligen) Mitarbeiter, bewegen Sie sich im SharePoint Standard. In diesem Fall müssen keine Dokumente gelöscht werden, jedoch muss die Mitgliedschaft in Prozessgruppen angepasst werden. Weitere Informationen dazu finden Sie in dem Kapitel Datenhaltung und Datenkommunikationsflüsse.

Legen Sie in einem Löschkonzept fest, welche Objekte tatsächlich bei Antrag auf Löschung gelöscht werden müssen. Prüfen Sie Rechte Dritter und Aufbewahrungsrechte der Objekte und ob diese tatsächlich gelöscht werden dürfen.

Prüfen Sie, ob zu löschende Objekte ggf. archiviert werden. Sollte dies der Fall sein, so prüfen sie bitte, ob Ihr Archivsystem das privilegierte Löschen unterstützt oder ob Sie dort konfigurativ und kaufmännisch weitere Maßnahmen durchführen müssen, wie z.B. das Erwerben einer erweiterten Lizenz.

Was muss ich tun, damit ich Daten die ich löschen muss auch löschen kann bzw. wie lösche ich konkret?

Definieren Sie in Ihrem Löschkonzept, welche Objekte konkret gelöscht werden müssen.

Ergänzen Sie den Regelfall dabei um Ihre konkrete Ausprägung vom escpand quality management. Berücksichtigen Sie folgende Dokumente:

- das Dokument
- abhängige hochgeladene Dokumente
- den Workflowreport
- weitere in Ihrem Prozess verwendete Dokumente

Löschung foxdox connect d.3ecm

Da keine personenbezogenen Daten erfasst werden, ist eine Löschung nicht vorgesehen.

Es kann sein, dass personenbezogene Details in den Logdateien stehen. Deshalb empfehlen wir, dass die Logdateien nach spätestens 30 Tagen gelöscht werden.

Löschung foxdox share for d.3ecm

Da keine personenbezogenen Daten erfasst werden, ist eine Löschung nicht vorgesehen.

Es kann sein, dass personenbezogene Details in den Logdateien stehen. Deshalb empfehlen wir, dass die Logdateien nach spätestens 30 Tagen gelöscht werden.

Löschung foxdox sync

Sie haben das Recht, von uns zu verlangen, dass Sie betreffende personenbezogene Daten unverzüglich gelöscht werden, wenn eines der folgenden Szenarien auf die dann vorliegende Situation zutrifft:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Sie widerrufen Ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Abs. 1 Buchstabe a oder Artikel 9 Abs. 2 Buchstabe a DSGVO stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

- Sie legen gemäß Artikel 21 Abs. 1 DSGVO Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder Sie legen gemäß Artikel 21 Abs. 2 Widerspruch gegen die Verarbeitung ein.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Abs. 1 DSGVO erhoben.

Sollten wir einmal Ihre personenbezogenen Daten öffentlich gemacht haben und nach den oben genannten Punkten zu deren Löschung verpflichtet sein, so treffen wir unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um Dritte für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass Sie von uns die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt haben.

Wir sind nicht zur Löschung oder zur Information Dritter über Ihr Löschungsverlangen verpflichtet, wenn die weitere Verarbeitung Ihrer personenbezogenen Daten erforderlich ist

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
- zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem wir unterliegen, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die uns übertragen wurde;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Abs. 2 Buchstaben h und i sowie Artikel 9 Abs. 3 DSGVO;
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Abs. 1 DSGVO, soweit das in Abs. 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Sie können Ihre in Ihrem foxdox-Konto befindlichen Daten jederzeit aus Ihrem foxdox-Konto löschen.

Zum Löschen Ihrer Daten haben Sie folgende Möglichkeiten:

- Gesamtes foxdox-Konto löschen
- Bestimmte Dokumente in Ihrem Konto suchen und dann löschen.

In formeller Hinsicht bestimmt Art. 12 Abs. 5 DSGVO, dass die Löschung grundsätzlich unentgeltlich erfolgen muss. Dazu haben wir ohne unangemessene Verzögerung, spätestens jedoch innerhalb eines Monats Ihr Löschverlangen zu prüfen und diesem unter den genannten Voraussetzungen nachzukommen.

1.3.3. Betroffenenrechte ecspand sidebar

Die Betroffenenrechte können nicht auf Daten der ecspand sidebar angewandt werden, da diese ausschließlich über einen technischen Charakter, z.B. in der Konfiguration oder in temporären Dateien, verfügen. Alle temporären Dateien werden beim Programmstart gelöscht.

Konfigurationen sind benutzerspezifisch, aber auch nur im Kontext des Anwenders tauglich und durch Mechanismen des Betriebssystems auf den konkreten Endanwender beschränkt. Das betrifft sowohl Zugang (Anmeldung) als auch Ablage (geschütztes lokales User-Verzeichnis) dieser Daten.