d.velop

Information regarding the European GDPR (General Data Protection Regulation)

Table of Contents

1. Information regarding the European GDPR (General Data Protection Regulation)

This chapter provides you with a general overview of security and data protection.

1.1. General

The information and data in this documentation relating to the compliance with and implementation of data protection requirements (in particular those stipulated by the GDPR) do not constitute legal advice for any individual case and we explicitly point out that they cannot serve as a substitute for legal advice. They are merely intended to sensitize you to current data protection issues and provide general information which is however not binding in legal respect. For the implementation of data protection law requirements in your company, we explicitly recommend that you avail yourself of professional advice.

The new EU data protection law (in particular the GDPR) provides for a reformation of the rights of the persons concerned by the data processing (the "data subjects") (see Articles 12 et seqq. GDPR). The GDPR stipulates that the body which is responsible for the processing of personal data (the "controller") is in particular obliged at all times to observe all rights and duties regarding the rights of the data subjects (including amongst others the right to information about the nature, purpose and scope of the data collection, the right to rectification of the data processing by the data subject, the right to erasure of personal data under certain circumstances or data transfer) and to act accordingly. The settings of the d.3ecm system, if applied correctly, enable GDPR-compliant approaches and procedures, in particular by observation of the rights of the data subjects. If the implementation/ settings are correct, the principles of the GDPR (including amongst others data minimisation, confidentiality, integrity, availability of the data processing and resilience of the systems) can be satisfied and complied with.

1.2. Data communication

1.2.1. Data communication d.3 content crawler

The d.3 content crawler allows you to read e-mails from various sources and store them in the d.3 repository. In this process, journal, user, group and functional mailboxes can be monitored.

The d.3 content crawler consists of the following modules:

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

d.3 content crawler service

The d.3 content crawler service is a Windows service reading the configuration via the d.ecs content crawler (6.1.3) and processing the respective mailboxes. The service determines which e-mails are to be processed based on the configuration. For each e-mail to be processed, a job is generated in d.ecs content crawler.

d.ecs content crawler

d.ecs content crawler is a self-hosted app (backend service) used to configure e-mail archiving. Additionally, the archiving jobs are centrally managed.

Configuration

The configuration is persistently stored in d.ecs jstore. d.ecs content crawler provides the respective user interfaces to administer the configuration.

Job management

The archiving jobs are generated by d.3 content crawler service (6.1.2). They are managed via d.ecs content crawler. If an e-mail is successfully stored in the d.3 repository, the respective archiving job is deleted from the system. If an error occurs when processing an e-mail, the entitled administrator can view the cause via the d.ecs content crawler interface and resolve it immediately. Jobs which could not be deleted from the system after the cause was resolved can be manually deleted via the user interface.

d.ecs groupware

d.ecs groupware is a self-hosted app (backend service) that directly processes e-mail objects and passes them to d.ecs dms for further processing.

d.ecs groupware temporarily stores the e-mails for processing. This cache directory is cleared immediately after the e-mail has been processed.

Connection to Microsoft Exchange

d.ecs groupware uses the Exchange Web Service (EWS) protocol to access Microsoft Exchange.

Connection to IBM Domino

For d.ecs groupware to access IBM Domino, the d.ecs domino service must be installed on one of the IBM Domino servers. This is integrated into IBM Domino as a servlet.

d.ecs domino temporarily stores the e-mails for processing. This cache directory is cleared immediately after the e-mail has been processed.

The mail systems are accessed via an encrypted connection.

1.2.2. Data communication d.3 core components

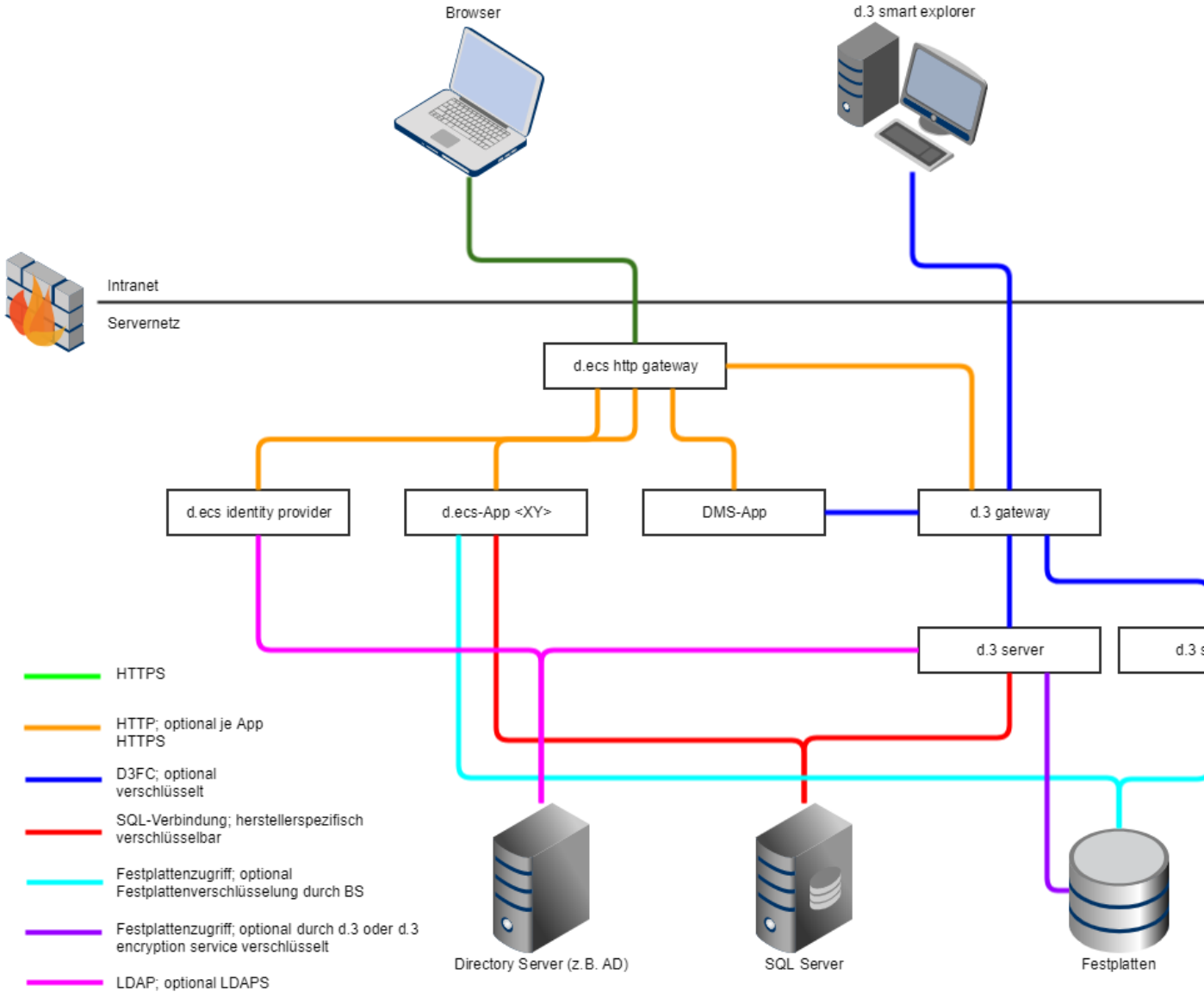
Representation of the data stream of d.3 core components

If the information requires an encryption within the server network, an increased security can only be achieved, if organizational measures are combined with enabling it.

Moreover, SQL Servers and d.3 search must be analyzed separately. For both, the data storage/harddisk can be encrypted, however, the data are still transparently accessible. Critical data should thus not be stored here. For d.3 search, a special option exists so that only the words are stored here without any context.

The d.velop d.3 client components communicate mainly via d.3 gateway with the server network. If the information requires an encryption within the server network, an increased security can only be achieved, if organizational measures are combined with enabling it. For example, the communication between d.3 gateway and d.3 client core components could activate Net-Crypt encryption via public.key file. Please refer to the corresponding manual for further information.

The following data flow diagram outlines the core product of the d.velop d.3 client components, d.3 smart explorer and its networking in the entire d.3ecm system.



1.2.3. Data communication d.3 document render service

The service d.3 document render service prepares user data of a d.3 repository so that the content of the files can be accessed page by page.

The communication between d.3 document render service and d.3 mobile connector is established using the HTTP protocol.

d.3 document render service uses the D3FC protocol to query data from d.3 server/d.3 gateway.

In addition, d.3 document render service uses an SQL connection to a database that can be encrypted manufacturer-specifically.

1.2.4. Data communication d.3 mobile

Representation of the data flow of the associated d.3 products

d.3 mobile is a mobile app to work with documents, dossiers and for the participation in workflows.

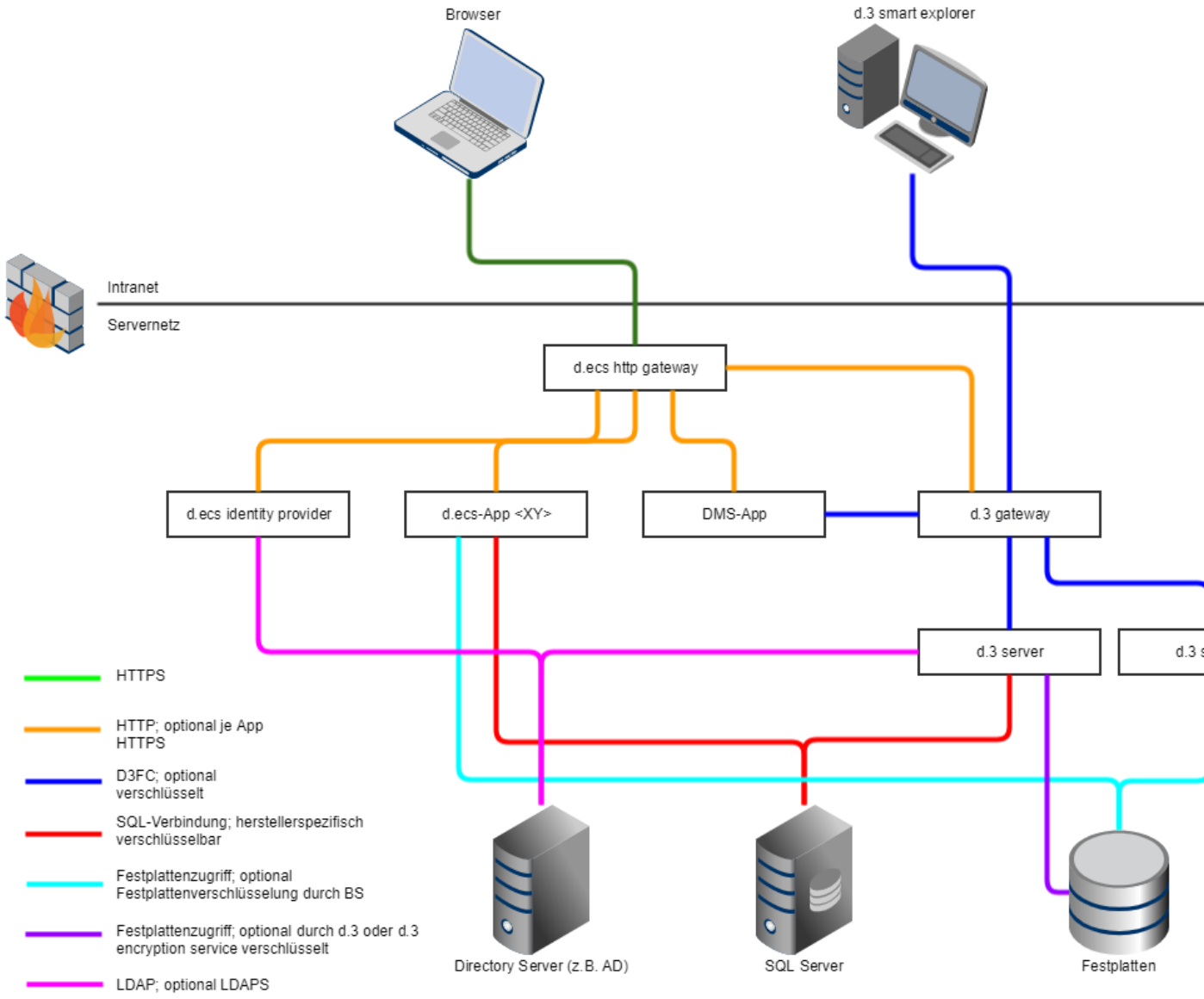
The storage and processing of data is performed via the d.3 server and other server services such as d.ecs forms or d.ecs storage manager.

d.3 mobile consists of a WebApp, the d.3 mobile app and the d.3 mobile connector in the backend.

The communication between the d.3 mobile app and the d.3 mobile connector is established using the HTTP protocol via the d.3 presentation server gateway or the d.ecs http gateway.

d.3 mobile connector uses the D3FC protocol to retrieve data from d.3 server/d.3 gateway, to provide it or to start processing.

To display a document in a document view, d.3 document render service is required in the backend. Using HTTP protocol, d.3 mobile connector communicates with d.3 document render service.



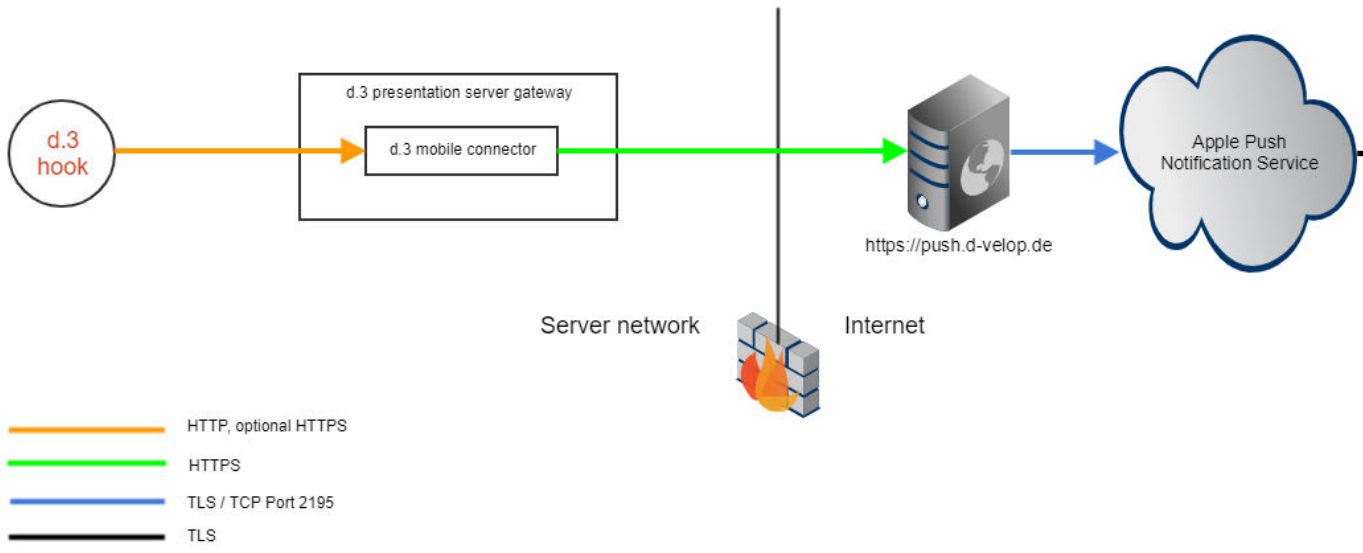
d.3 mobile with push messages

With a new mailbox entry for a d.3 user, the internal d.3 mobile connector is called via the HTTP protocol using a d.3 hook.

d.3 mobile connector sends via HTTPS to the push server of d.velop AG the subject and the number of unread entries.

The push server at d.velop AG encrypts this data and sends it TLS encrypted to the APNS (Apple Push Notification Service).

As soon as the mobile devices of the respective d.3 user are online, the push message is transmitted from the APNS to the mobile device.



1.2.5. Data communication d.3one

With d.3one the end user is exclusively provided with the user interface to work with documents and dossiers. Data retention and processing is part of d.3 server.

d.3one consists of single microservices (apps), which communicate with each other either by using the HTTP or HTTPS protocol.

The following apps are part of d.3one as a product:

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

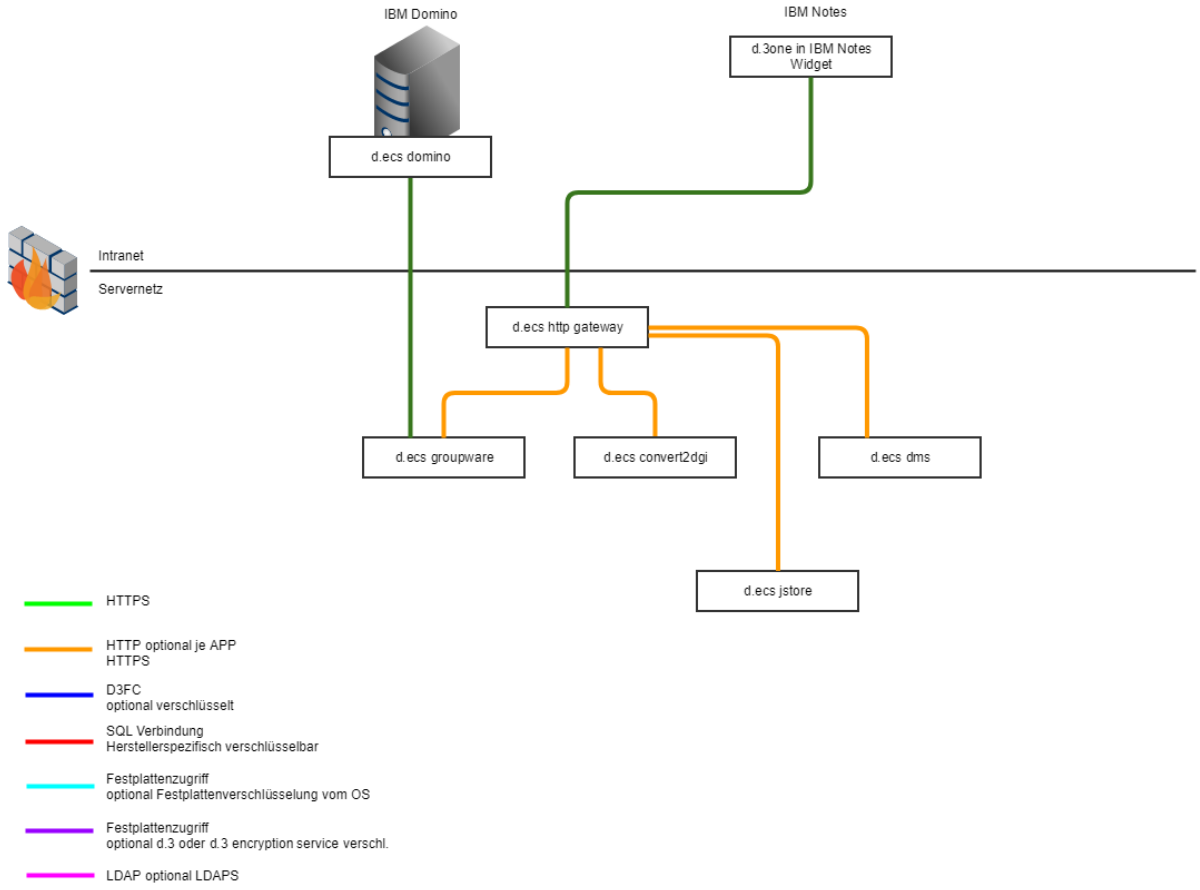
In general, the communication of the microservices is managed by d.ecs http gateway. In addition, core infrastructure components are used, e.g. d.ecs jstore, d.ecs home, and d.ecs identity provider. Apps that communicate with d.3 server directly use the D3FC protocol and HTTP to provide data, send requests or start processing operations on the d.3 server.

An authorized user interacts with d.3one using the HTTP protocol in the browser. The communication between humans and software is also managed by d.ecs http gateway.

For third-party applications interacting with d.3one, a REST HTTP interface is used while the communication is also directed across d.ecs http gateway.

1.2.6. Data communication d.3one in IBM Notes

d.3 one in IBM Notes allows you to read e-mails from the user mail database and store them in the d.3 repository.



d.3one in IBM Notes consists of the following modules:

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

d.3one in IBM Notes widget

d.3one in IBM Notes widget is a plug-in integrating the d.3one interface into IBM Notes thus providing additional functions in the e-mail client. Among other things, the widget allows you to open the storage dialog of d.3one (d.ecs dms).

Configuration

The configuration is persistently stored in d.ecs jstore. d.ecs content crawler provides the respective user interfaces to administer the configuration.

d.ecs groupware

The d.ecs groupware is a self-hosted app (backend service) directly processing e-mail objects and passing them to d.ecs dms for further processing.

d.ecs groupware temporarily stores the e-mails for processing. This cache directory is cleared immediately after the e-mail has been processed.

Connection to IBM Domino

The d.ecs groupware accesses the d.ecs domino service on IBM Domino via https. The service is implemented as a servlet.

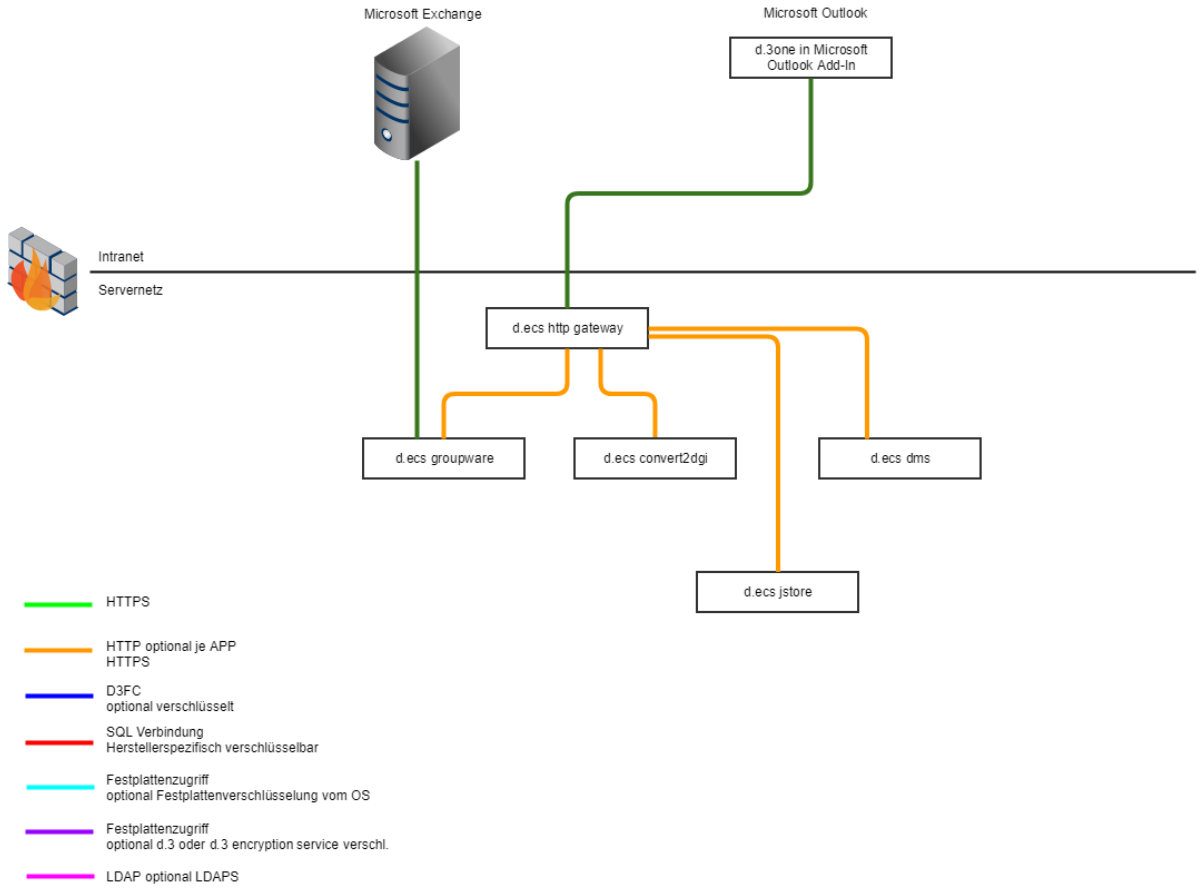
The communication of the individual services and apps is managed by d.ecs http gateway. For further information, read the respective manual.

In order to access the e-mail systems, d.ecs groupware directly communicates with IBM Domino or d.ecs domino via an encrypted connection. The mail systems are accessed via an encrypted connection.

If it is necessary that certain information is not written to the technical log, the manual of the d.3one in Microsoft Outlook contains information on how to configure the log level and on the extent of the different log levels.

1.2.7. Data communication d.3one in Microsoft Outlook

d.3one in Microsoft Outlook allows you to read e-mails from the user mailbox and store them in the d.3 repository.



d.3one in Microsoft Outlook consists of the following modules:

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

d.3one in Microsoft Outlook Add-In

d.3one in Microsoft Outlook Add-In is an add-in integrating the d.3one interface into Microsoft Outlook thus providing additional functions in the e-mail client. Among other things, the add-in allows you to open the storage dialog of d.3one (d.ecs dms).

Configuration

The configuration is persistently stored in d.ecs jstore. d.ecs content crawler provides the respective user interfaces to administer the configuration.

d.ecs groupware

The d.ecs groupware is a self-hosted app (backend service) directly processing e-mail objects and passing them to d.ecs dms for further processing.

d.ecs groupware temporarily stores the e-mails for processing. This cache directory is cleared immediately after the e-mail has been processed.

Connection to Microsoft Exchange

d.ecs groupware uses the Exchange Web Service (EWS) protocol to access Microsoft Exchange.

The communication of the individual services and apps is managed by d.ecs http gateway. For further information, read the respective manual.

In order to access the e-mail systems, d.ecs groupware directly communicates with Microsoft Exchange or d.ecs domino via an encrypted connection. The mail systems are accessed via an encrypted connection.

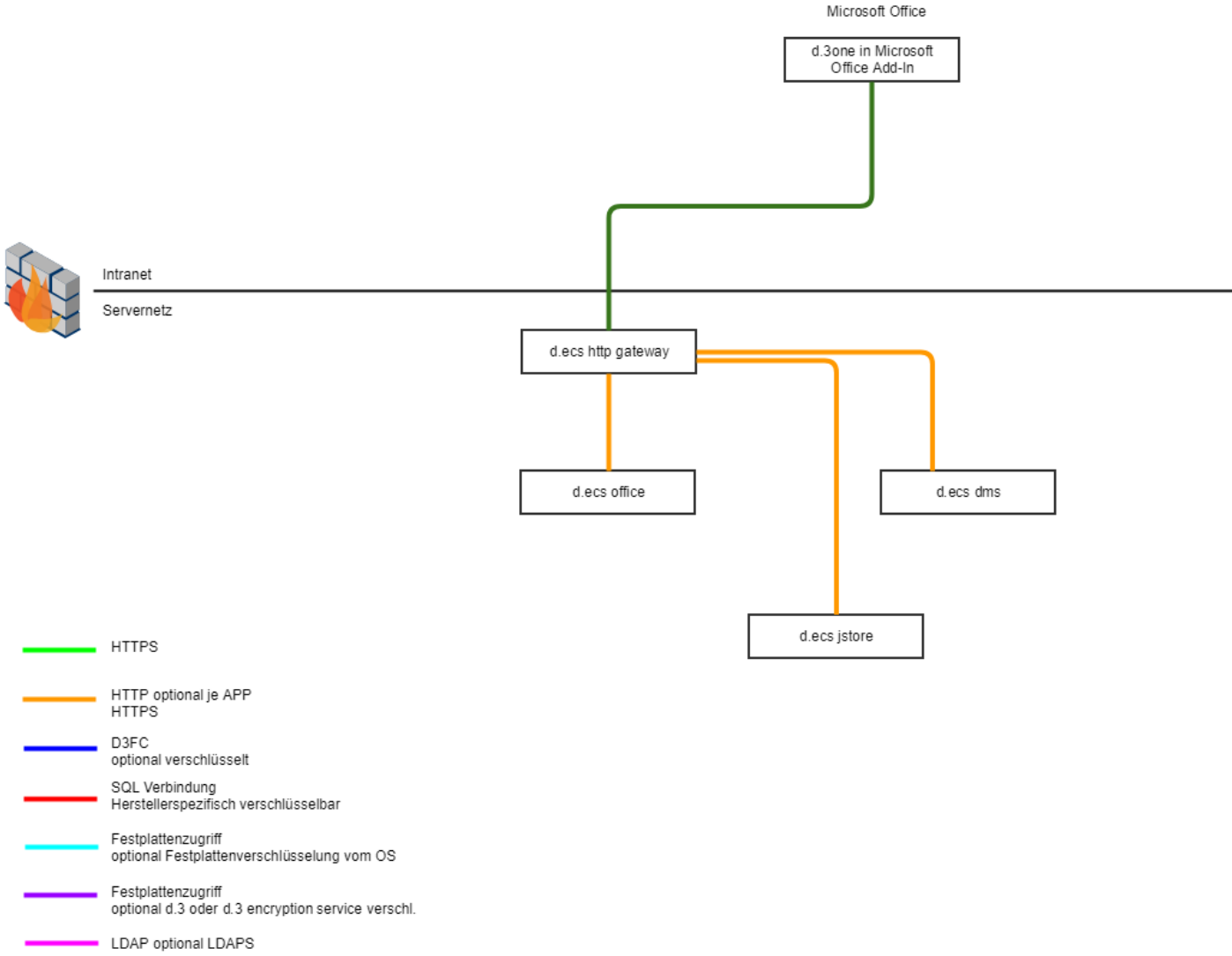
If it is necessary that certain information is not written to the technical log, the manual of the d.3one in Microsoft Outlook contains information on how to configure the log level and on the extent of the different log levels.

1.2.8. Data communication d.3one in Office

Representation of the data stream in d.3one in Microsoft Office

The communication between the Microsoft Office add-in and d.ecs office is exclusively conducted via https. The d.ecs office application communicates with other infrastructure applications via http within the server. This can optionally be encrypted.

It can also be protected using other suitable organizational measures.



1.2.9. Data communication d.3one in SAP ERP

The d.3one integration in SAP takes place via configurable search links. These are opened either in an HTML viewer in SAP or in a web browser outside the SAP system. There is no data exchange between d.3one and SAP.

1.2.10. Data communication d.3 search

Communication between the d.3 system (d.3 gateway) and storage manager takes place via the d.3fc protocol. Optionally, this can also be encrypted. The data of d.3 search is stored on the computer where d.3 search is installed.

1.2.11. Data communication d.3 sync

d.3 sync provides the end user with user interfaces for working locally with documents and dossiers. Synchronized documents and databases are stored locally.

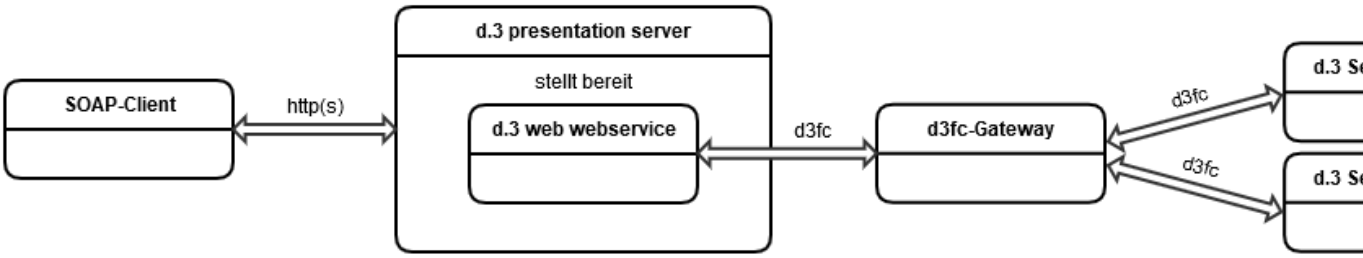
d.3 sync communicates only with d.3 server in order to deploy and request data. You can encrypt the communication between d.3 sync and d.3 server. The D3FC protocol is used for this encryption. You need the PUBLIC.KEY file. This file is automatically generated d.3 gateway and is located in the dlink directory. To enable the encryption, copy the PUBLIC.KEY file into the installation directory of the d.3 sync service. By default the installation directory is C:\Program Files (x86)\d.velop\d.3 sync\service.

For more information about encryption with the D3FC protocol, see the d.3 gateway manual.

1.2.12. Data communication d.3 web webservice

If a SOAP request is sent by your application, several d.velop components are involved for processing it.

The following diagram illustrates which components are used and which protocol they use:



To ensure that the entire communication link is encrypted, the connections must be encrypted on a basis of http and d3fc.

To ensure that communication between your SOAP application and d.3 presentation server is encrypted, d.3 presentation server must provide a secure https connection.

Furthermore, it is important that in addition to encryption based on https, communication between d.3 web webservice and d3fc gateway or d.3 server processes is also encrypted.

How to set up secure http and d3fc communication is described in the manual of d.3 presentation server.

A successfully secured http connection can be recognized by the connection type https.

As soon as the encryption is enabled on the d3fc side, "Found public.key" is logged when d.3 web webservice is started.

1.2.13. Data communication d.capture batch

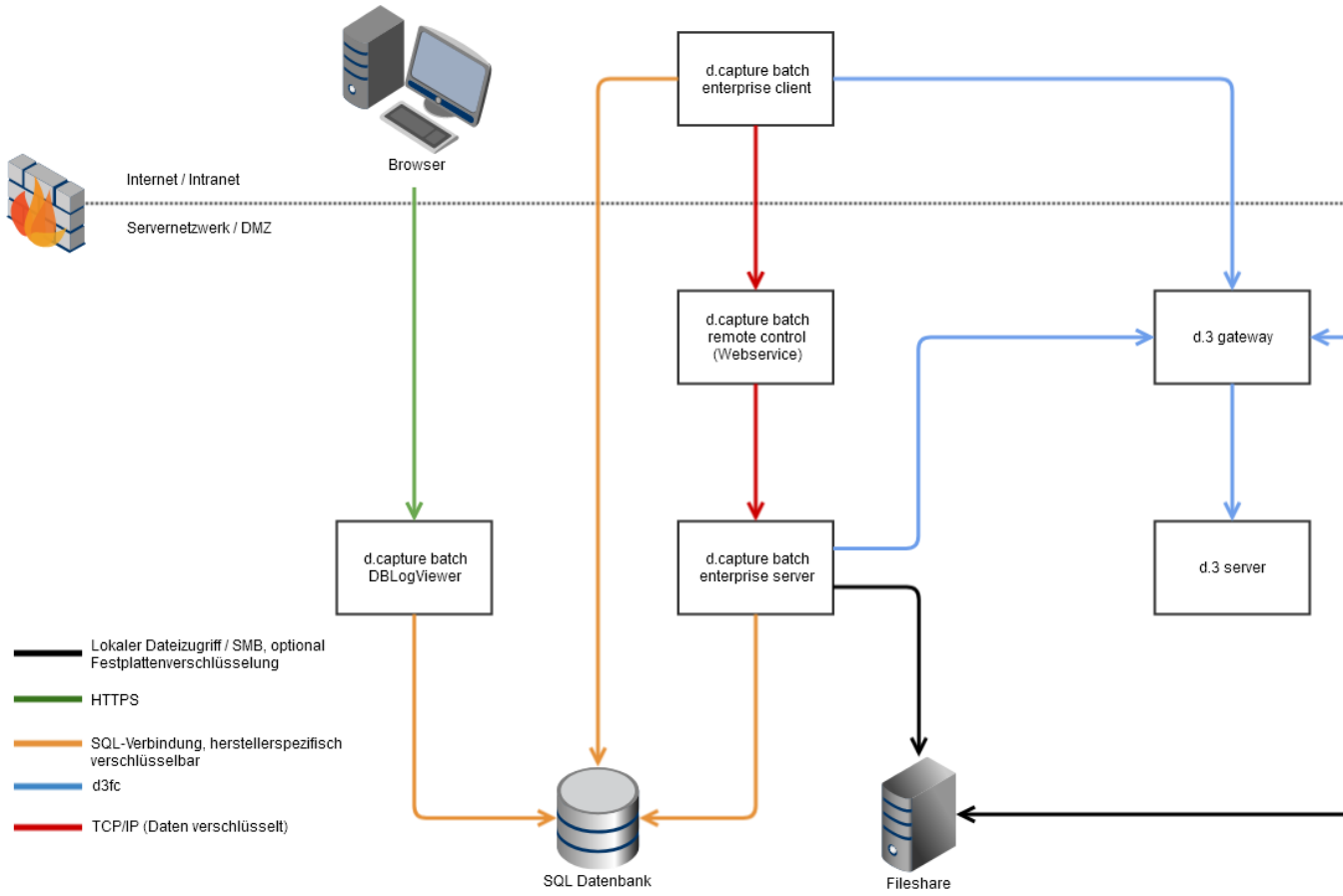
Representation of the data stream in d.capture batch

d.capture batch communicates with the d.3 server via the d.3 gateway. The communication between d.3 server, d.3 gateway and d.capture batch is encrypted via the d3fc protocol.

All d.capture batch instances communicate with an SQL-server, if the user management or the batch logging are used. The connection to the SQL server - by d.capture batch as well as by d.capture batch DBLogViewer - is established using the ODBC and may be encrypted based on vendor functionality. The batch logging is read via an encrypted HTTPS connection.

d.capture batch enterprise server and client communicate with each other via TCP/IP using the den d.capture batch remote control webservice. The transmit information is encrypted.

Under certain conditions, d.capture batch instances access a common shared directory for file exchange. This directory contains unencrypted binary and meta data of the batches. These can be optionally encrypted using functions of the operating system or storage system. For this effect, please follow the instructions by the vendor.

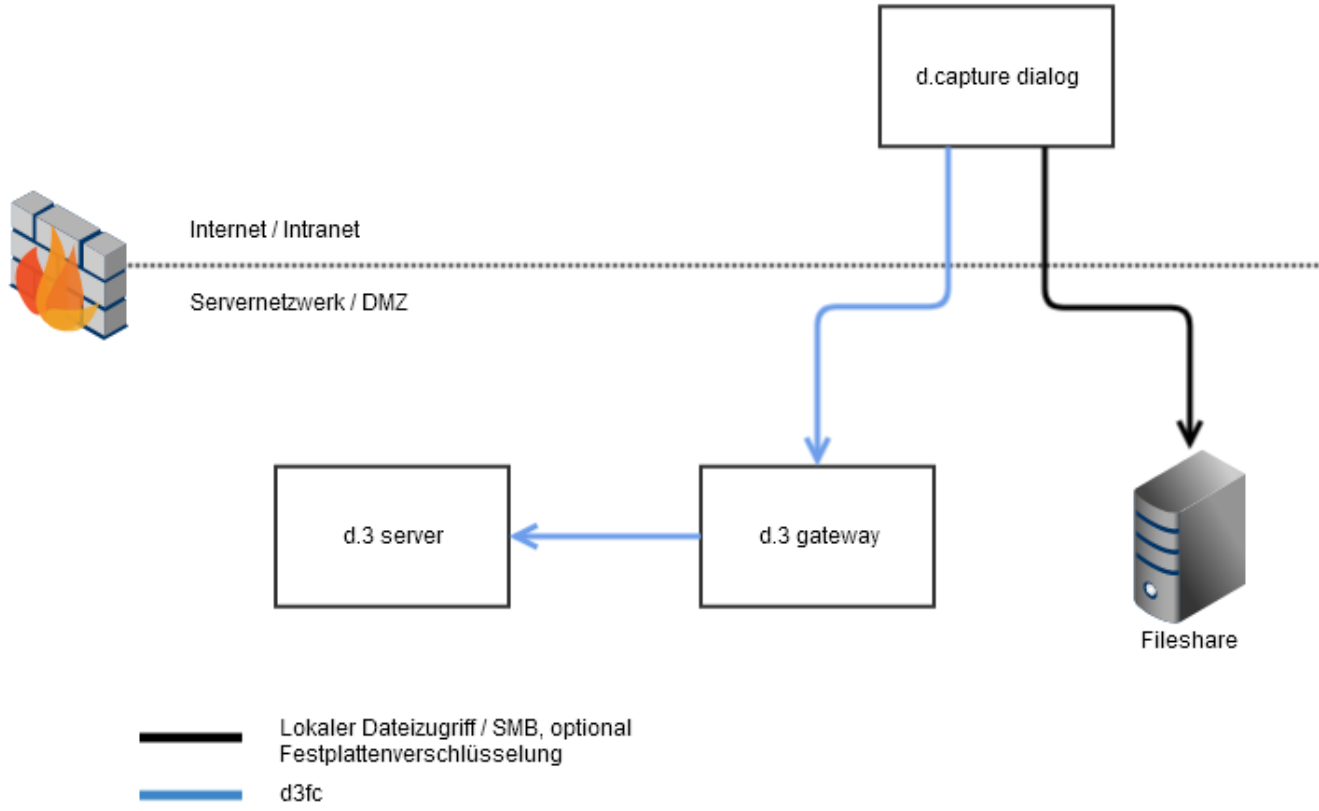


1.2.14. Data communication d.capture dialog

Representation of the data stream in d.capture dialog

d.capture dialog communicates with d.3 server via d.3 gateway. The communication between d.3 server, d.3 gateway and d.capture dialog is encrypted via the d3fc protocol.

If necessary, d.capture dialog accesses a shared working directory. This directory contains unencrypted binary data. These can be optionally encrypted using functions of the operating system or storage system. For this effect, please follow the instructions by the vendor.



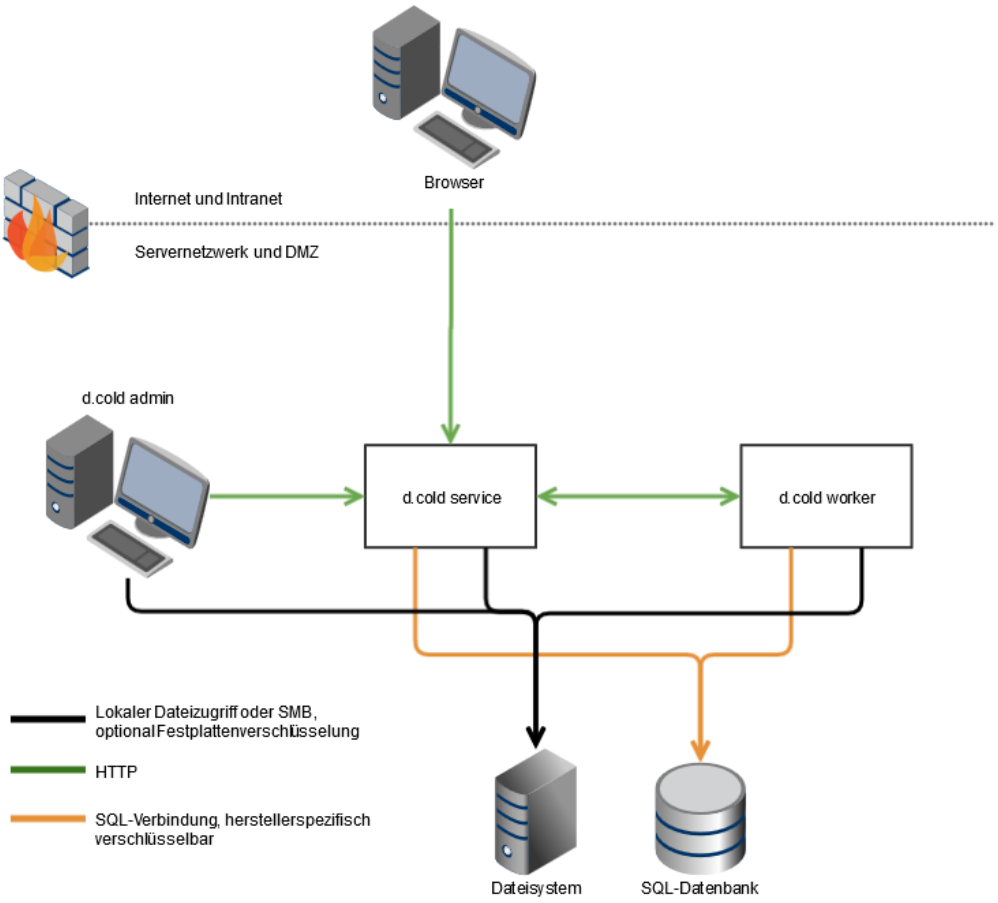
1.2.15. Data communication d.cold

Representation of the data stream of d.cold

The component d.cold admin communicates with d.cold service via HTTP, and d.cold service also communicates with the d.cold worker processes running on the same server via HTTP. When installed on several servers, the d.cold service instances also communicate using the HTTP protocol and route the queries to the local d.cold worker processes.

With regard to the data management of d.cold, please note the following: All d.cold worker and d.cold service instance communicate with an SQL server for job management purposes. The connection to the SQL server is established via ODBC and can optionally be encrypted using vendor-specific functions. Furthermore, all d.cold processes access a shared directory. This directory contains configuration and log files.

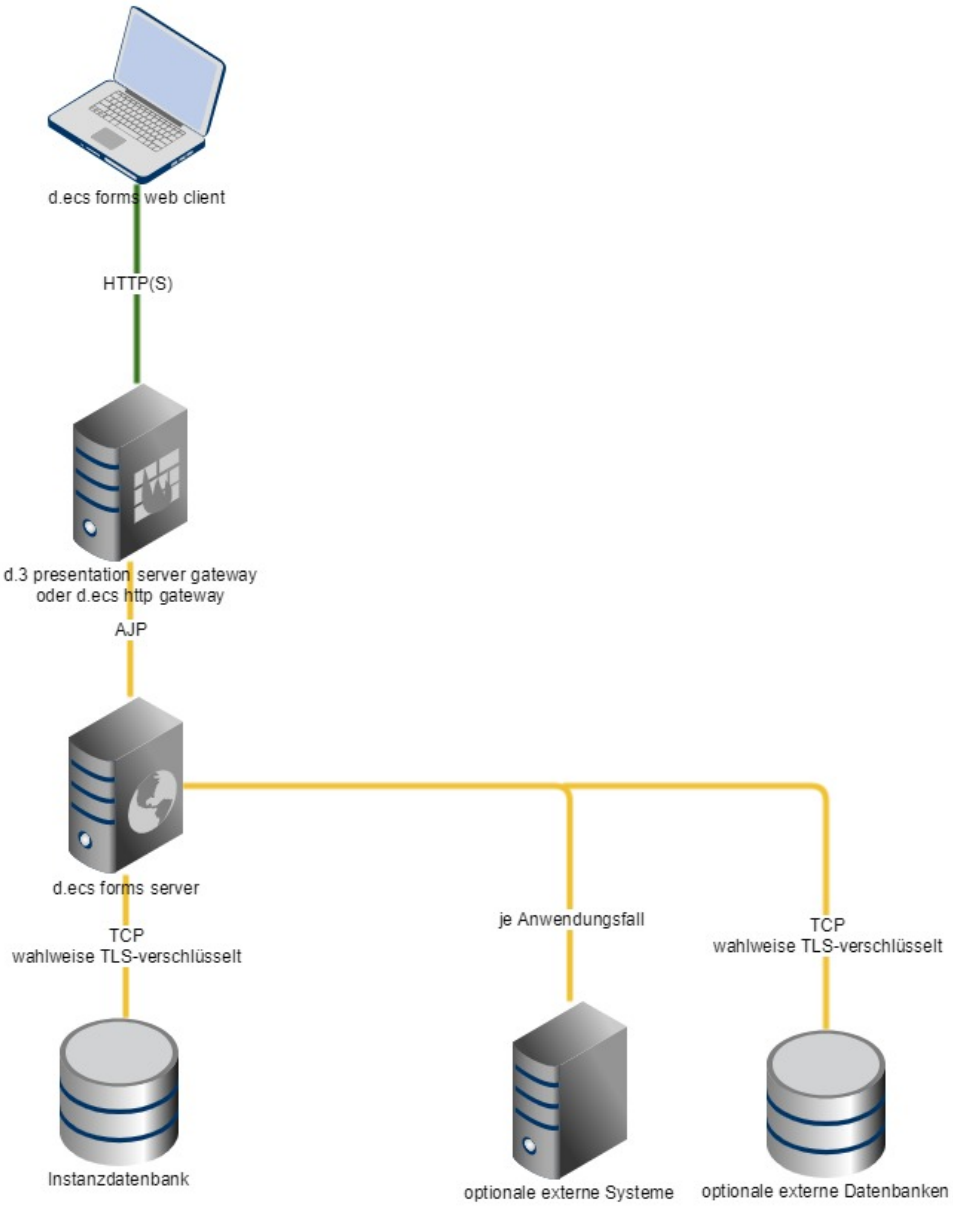
Additionally, the d.cold processing is done in the file system. Depending on the configuration of the d.cold process chains the d.cold processing can be done either locally or in a directory in the network. Although the data storage and the hard disk can be encrypted, the data is still transparently accessible. If applicable, critical data should therefore not be processed by d.cold.



1.2.16. Data communication d.ecs forms

Representation of the data stream of d.ecs forms

The d.ecs forms web client is operated from within a browser. This uses HTTP(S) to communicate with the d.3 presentation server gateway or the d.ecs http gateway. They function as a proxy forwarding AJP requests of the d.ecs forms web clients to the d.ecs forms server. The d.ecs forms server loads data and forms from the instance database. This is addressed by TCP. Depending on the use case, you can connect the d.ecs forms server to external systems and databases.



1.2.17. Data communication d.ecs monitor

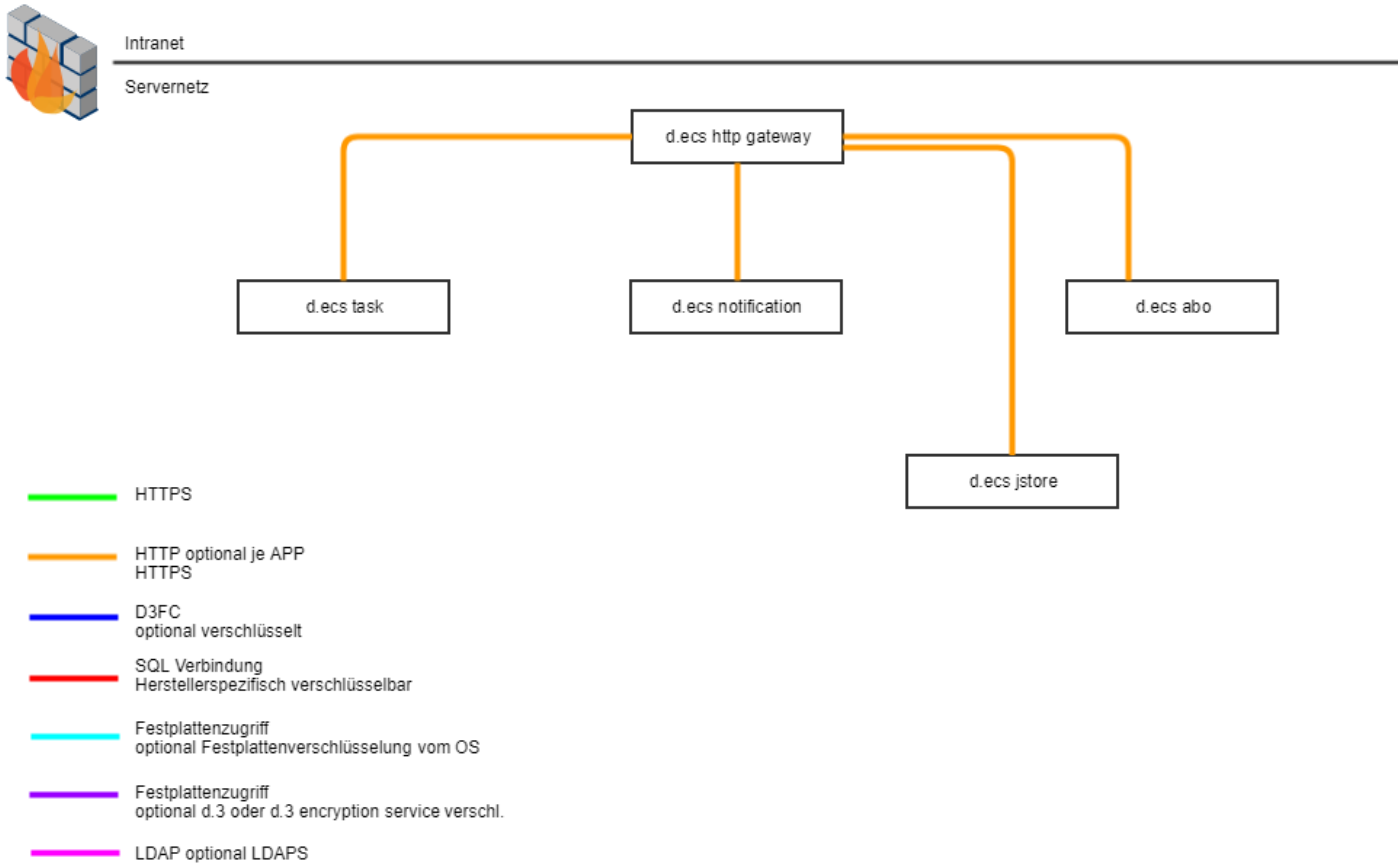
The d.ecs monitor itself does not collect and process DSGVO relevant data, nor does it display this data. Individual wrappers may differ. Please refer to the individual wrapper documentation.

1.2.18. Data communication d.ecs monitor for d.3 hostimp

If you want to prevent administrators from accessing data that has been corrupted during processing by the d.3 server host import, you must make sure that the corresponding feature is deactivated. Additional information can be found in the manual for d.ecs monitor for d.3 hostimp in the subchapter **Basic information.**

1.2.19. Data communication d.ecs notification

The communication with d.ecs notification takes place via https. The service can be used by any services of d.velop AG. The specific data communication is described in the manuals of the calling services.

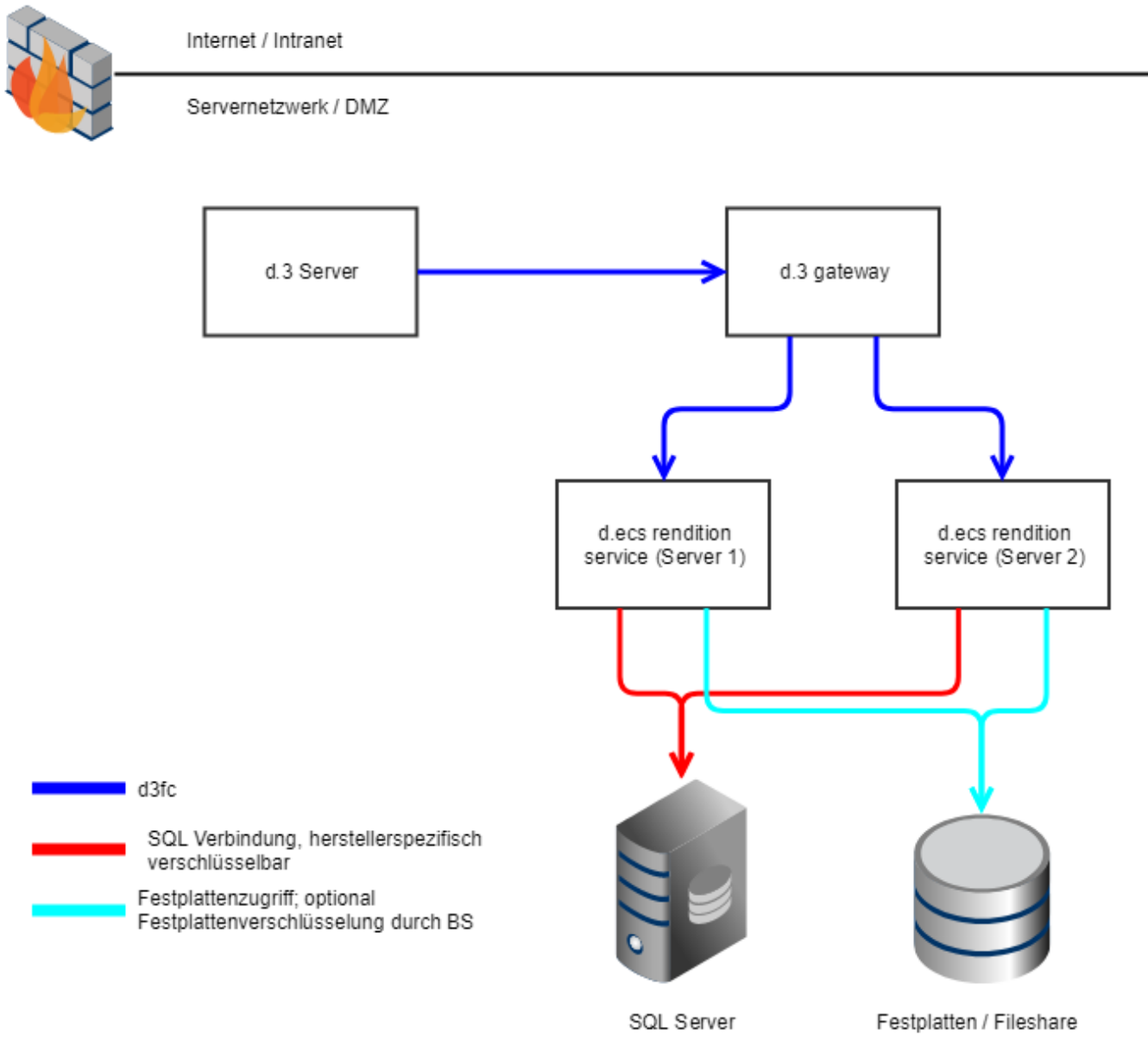


1.2.20. Data communication d.ecs rendition service

Representation of the dataflow in d.ecs rendition service

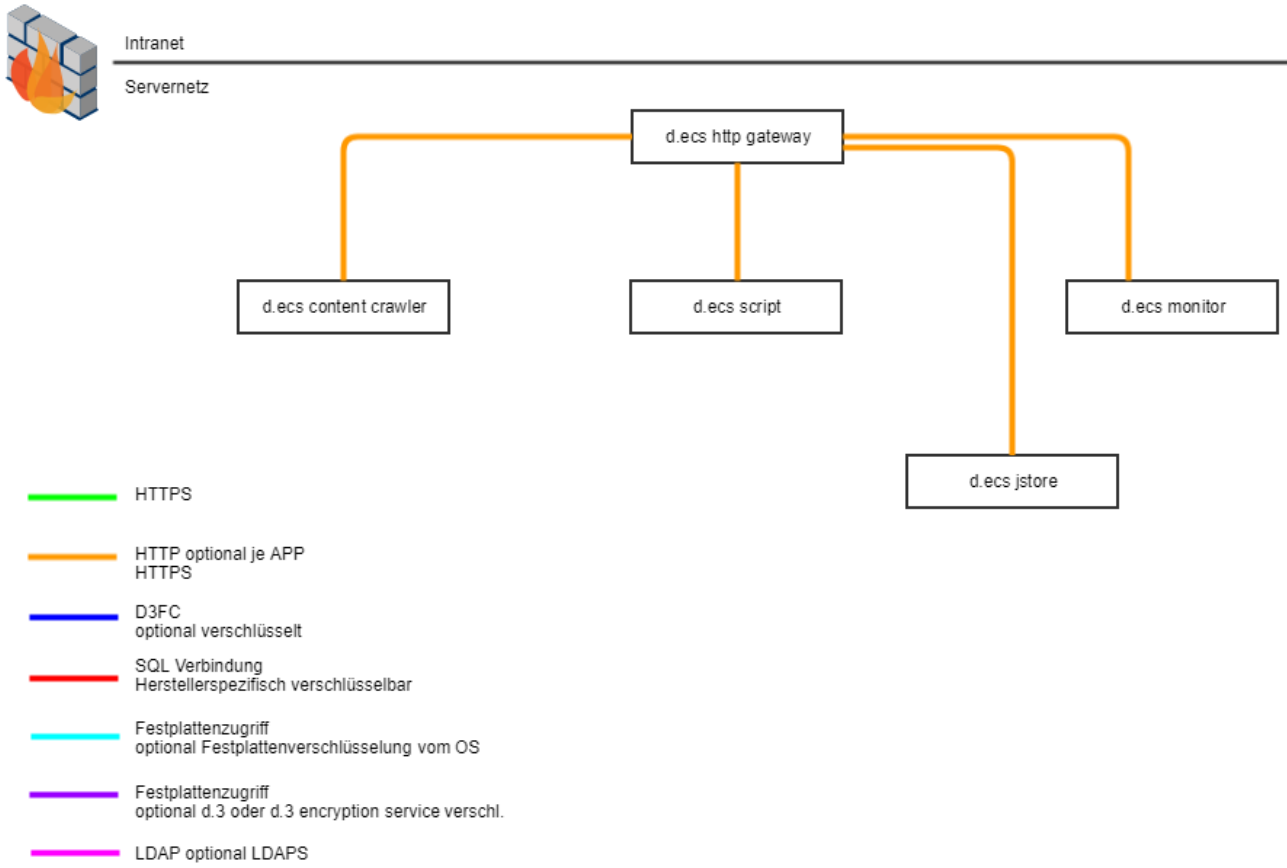
The d.3 server (d.3 async) communicates with d.ecs rendition service via d.3 gateway. d.3 gateway distributes the requests to the available d.ecs rendition service instances. The communication between d.3 server, d.3 gateway and d.ecs rendition service is unencrypted and uses the d3fc protocol.

Moreover, the data storage of d.ecs rendition service must be considered. For the job management, all d.ecs rendition service instances communicate with an SQL-server. The connection to the SQL server is established via ODBC and can optionally be encrypted using vendor-specific functions. Moreover, all d.ecs rendition service instances access a shared directory for file exchange. This directory contains all received and created files for active jobs. The data storage/harddisk can be encrypted but the data is still accessible in clear text. Thus critical files should possibly not be sent to the d.ecs rendition service.



1.2.21. Data communication d.ecs script

d.ecs script manages PowerShell scripts that are called by other services and executed within d.ecs script.



1.2.22. Data communication d.ecs storage manager

The communication between the leading systems and the d.ecs storage manager is handled by

- for d.3 via file systems (directory structure) and database tables or
- at SharePoint via the d.ecs storage manager API

In both cases, documents are passed from the leading application to the d.ecs storage manager. The leading system (d.3) directly stores the documents in the directories which are also configured with the d.ecs storage manager or the documents are transferred via API (SharePoint and are temporarily stored in the directories configured with the d.ecs storage manager. The affected directories are configured via the d.ecs storage manager administration in the section **Common**.

In this process, the **Public path** and the **Archive path** (including the subdirectories) act as the directories for the transfer or temporary storage of documents that should be moved from d.ecs storage manager to the configured storage system. The **Jukebox path** is used by the d.ecs storage manager to provide documents requested by the leading application in this path or to store them temporarily for provision to SharePoint using the API.

Warning

Rights to the directories/files are required by the d.3 processes (d.3 hostimport/d.3 async/d.3 gateway, ...) and by the d.ecs storage manager itself. Typically, all named processes (except for d.3 gateway) are started by d.3 process manager (Windows service). Thus, it is usually sufficient to grant the respective rights to the user under which the service is running. d.3 gateway is also a Windows service and should thus be executed with the same user as d.3 process manager.

1.2.23. Data communication d.velop archivelink for SAP Solutions

The leading SAP systems and the interface d.velop archivelink for SAP Solutions (Content Server) communicate via the HTTP/HTTPS protocol. Depending on the connected storage system d.3ecm, ecspand for SharePoint or d.ecs storage manager and depending on the storage modes, the communication takes place via file systems or API import and database tables.

The storage modes synchronous or asynchronous storage, API import as well as the file directories (so-called “export directory") are configured in the configuration of the content repositories under section "Archive Mode” of the administration of d.velop archivelink for SAP Solutions. In the mode API import “Off”, the documents and related metadata files are stored in the export directory. These files can also be additionally protected by using external operating system tools. Having successfully imported into the connected d.3ecm, SharePoint, SharePoint Online or d.ecs storage manager, this information is deleted.

Important: Rights for the directories/files are required by the d.3ecm/SharePoint processes (hostimport/Async/d.3 gateway,ecspand Importservice,...) and the d.ecs storage manager itself. Typically, all named d.3ecm processes (except for d.3 gateway) are started by the d.3 process manager (Windows service). Thus it is typically sufficient to assign the respective rights to the user under which the service is running. The d.3 gateway is also a Windows service and should thus be executed with the same user as the d.3 process manager.

For the ArchiveLink storage of inbound documents, the scanned image files including their JPL files with the barcode and workflow information are directly stored in the file directories for further processing. The file directories are defined in the configuration of the so-called “HTTP script” under “Barcode” and “Workflow directory”. Having successfully stoired and linked the documents, these files are deleted. These files can also be additionally protected by using external operating system tools.

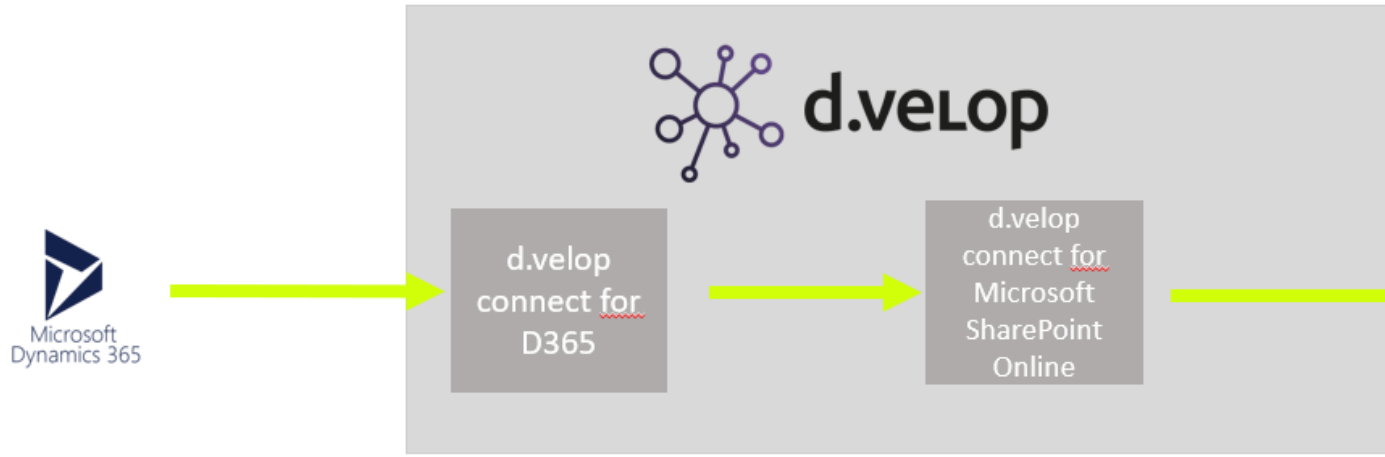
1.2.24. Data communication d.velop connect for Microsoft Dynamics 365

In order to basically understand where in the context of the GDPR an installation of d.velop connect for Microsoft Dynamics 365 can be approached, it is necessary to briefly explain which data and services exist in principle and how these data are stored or communicate with each other.

Typical topology

The adapter d.velop connect for Microsoft Dynamics 365 is an app in the d.velop cloud platform that provides configuration options and services to connect another third-party application or d.velop AG application to a d.velop cloud platform.

When configuring the application, information about the document types to be exported is saved. This information is not personal and can only be configured and viewed by persons with appropriate administration rights. The services provided pass on information objects in the memory to the destination and do not store this information. A typical data flow looks like this.



In addition to the permanent storage of configuration and connection data, use on a technical level without personal data is logged for a period of less than four weeks.

Optionally, an upload service can be used to temporarily store documents and generate a pre-signed URL for further processing. These files are automatically deleted after 15 minutes.

In terms of topology, please apply the principles of the GDPR to the third-party systems or the d.velop infrastructure components as described in the respective manuals.

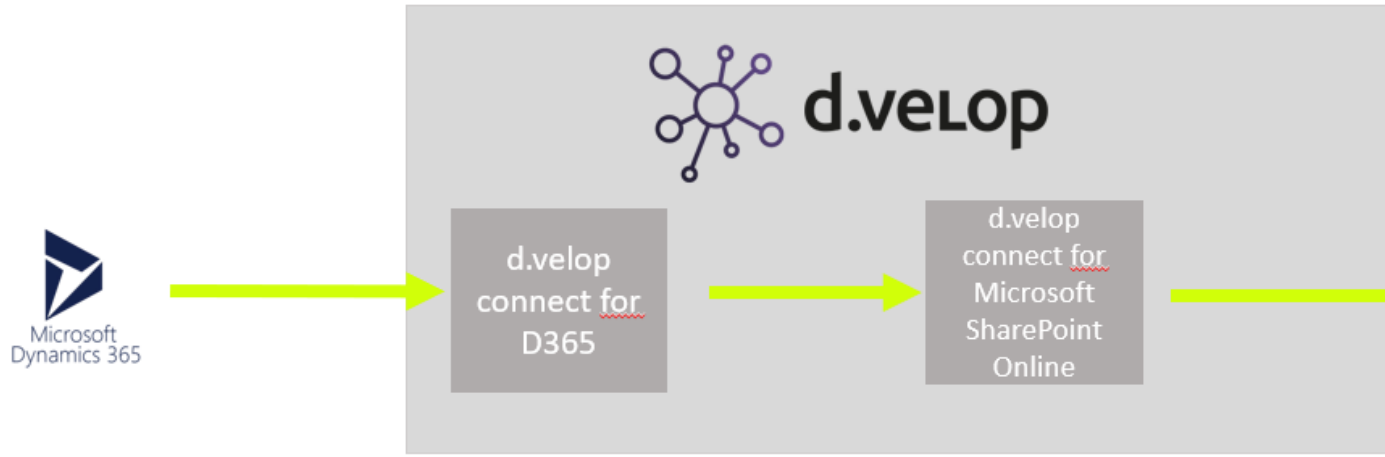
1.2.25. Data communication d.velop connect for Microsoft SharePoint

In order to basically understand where in the context of the GDPR an installation of d.velop connect for Microsoft SharePoint can be approached, it is necessary to briefly explain which data and services exist in principle and how these data are stored or communicate with each other.

Typical topology

The adapter d.velop connect for Microsoft SharePoint is an app in the d.velop platform that provides configuration options and services to connect another third-party application or d.velop AG application to a Microsoft SharePoint installation.

When configuring the application, information for the connection to the Microsoft SharePoint server as well as assignments of fields between the source and destination systems Microsoft SharePoint are stored. This information is not personal and can only be configured and viewed by persons with appropriate administration rights. The services provided pass on information objects in the memory to the destination and do not store them. A typical data flow looks like this.



In addition to the permanent storage of configuration and connection data, use on a technical level without personal data is logged for a period of <4 weeks.

In terms of topology, please apply the principles of the GDPR to the third-party systems or the d.ecs infrastructure components as described in the respective manuals.

1.2.26. Data communication d.velop customizing for SAP Solutions

d.velop customizing for SAP Solutions is called by the d.velop SAP products as part of the license check. Furthermore, d.velop customizing provides central service functionalities that are called up by the products. No information on the calls is logged in SAP tables. The functions are addressed via a class or function module call. There is no data communication to external systems from d.velop customizing.

1.2.27. Data communication d.velop data connector

d.velop data connector offers the possibility to connect external data sources with SharePoint.

The configuration of the product can be used to connect various data sources. If the data requires encryption within the server network, the configuration should be carried out accordingly. The SharePoint API is used towards SharePoint. HTTP and HTTPS are possible as transport options here. If the data requires it, HTTPS should also be stored here as a transport option via the configuration.

1.2.28. Data communication d.velop data module for SAP ERP

d.velop data module for SAP ERP can be addressed via the RFC-enabled function module /DVELOP/ATR_GET_DATA. The function module returns the data for a previously configured selection ID. Furthermore, d.velop data module for SAP ERP can store files on a local PC or the application server or a connected network location.

1.2.29. Data communication d.velop ilm archiving for SAP Solutions

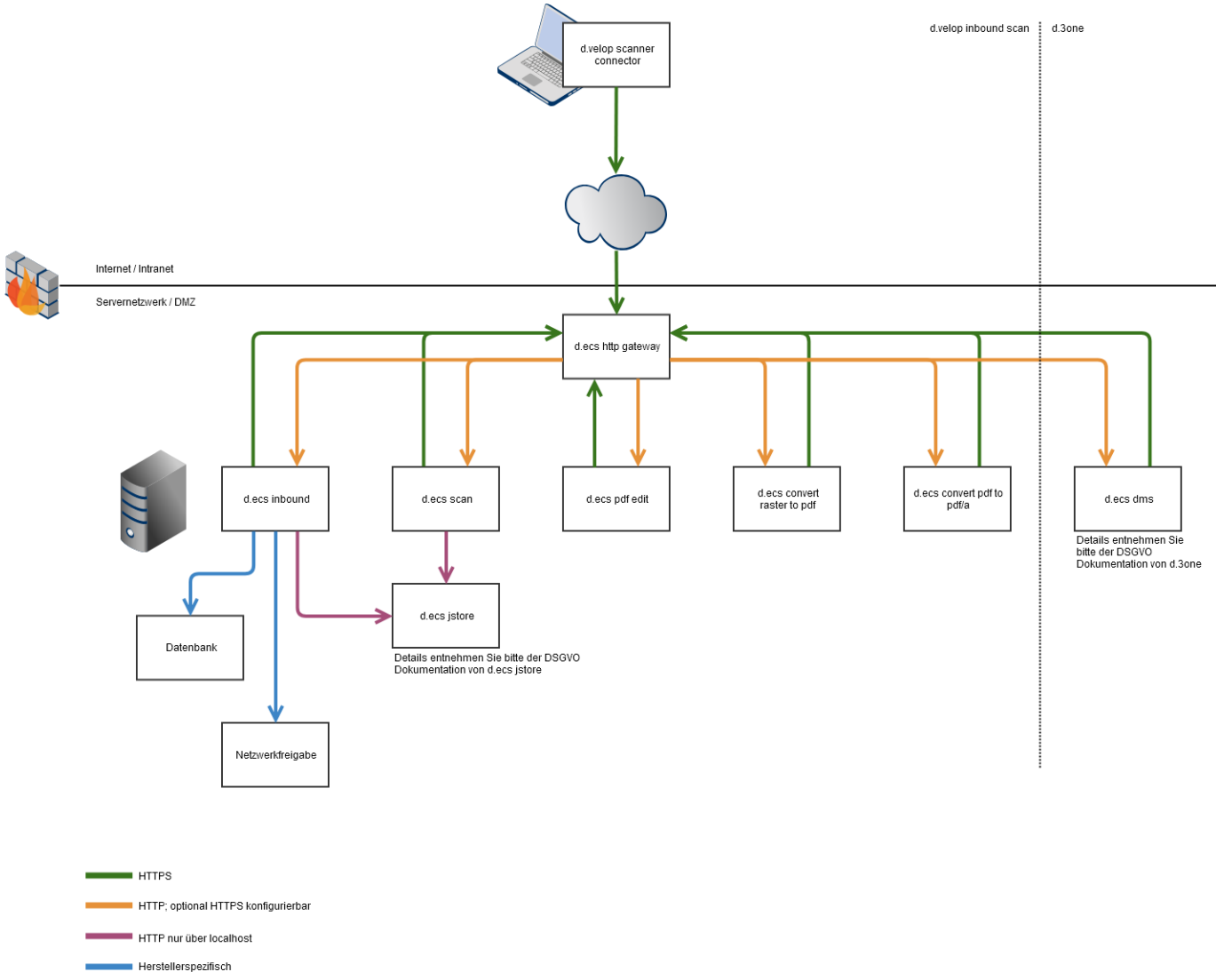
The leading SAP systems and the interface d.velop ilm archiving for SAP Solutions (WebDAV Server) communicate via the WebDAV protocol (RFC4918), which has been supplemented with ILM-specific functions. Communication is via the HTTP/HTTPS protocol, which is configurable in the SAP RFC destinations (transaction SM59). SAP Information Lifecycle Management (ILM) is the managing system and it administers and controls the data transferred to the ILM storage.

1.2.30. Data communication d.velop inbound scan

The individual components of the d.velop inbound suite exclusively communicate among each other via the encrypted HTTPS protocol via the d.ecs http gateway. The d.ecs http gateway forwards requests to the individual backend components in the server network using the unencrypted HTTP protocol. This communication can optionally be encrypted.

The communication with d.ecs jstore is unencrypted via the HTTP protocol. However, the communication takes places exclusively via the local network device and cannot be intercepted over the network.

The communication with infrastructure components is partially only possible in unencrypted form or an encryption is optionally possible, depending on the vendor.



1.2.31. Data communication d.velop personnel file for SAP ERP

In d.velop personnel file for SAP ERP, the documents are stored and read via the SAP standard interface Archivelink.

d.velop personnel file for SAP ERP has an interface for communication with the personnel file Fiori add-on. The information required for the Fiori display is provided via the interface. Additional authorizations are required to use the interface.

You can find more information in the product documentation.

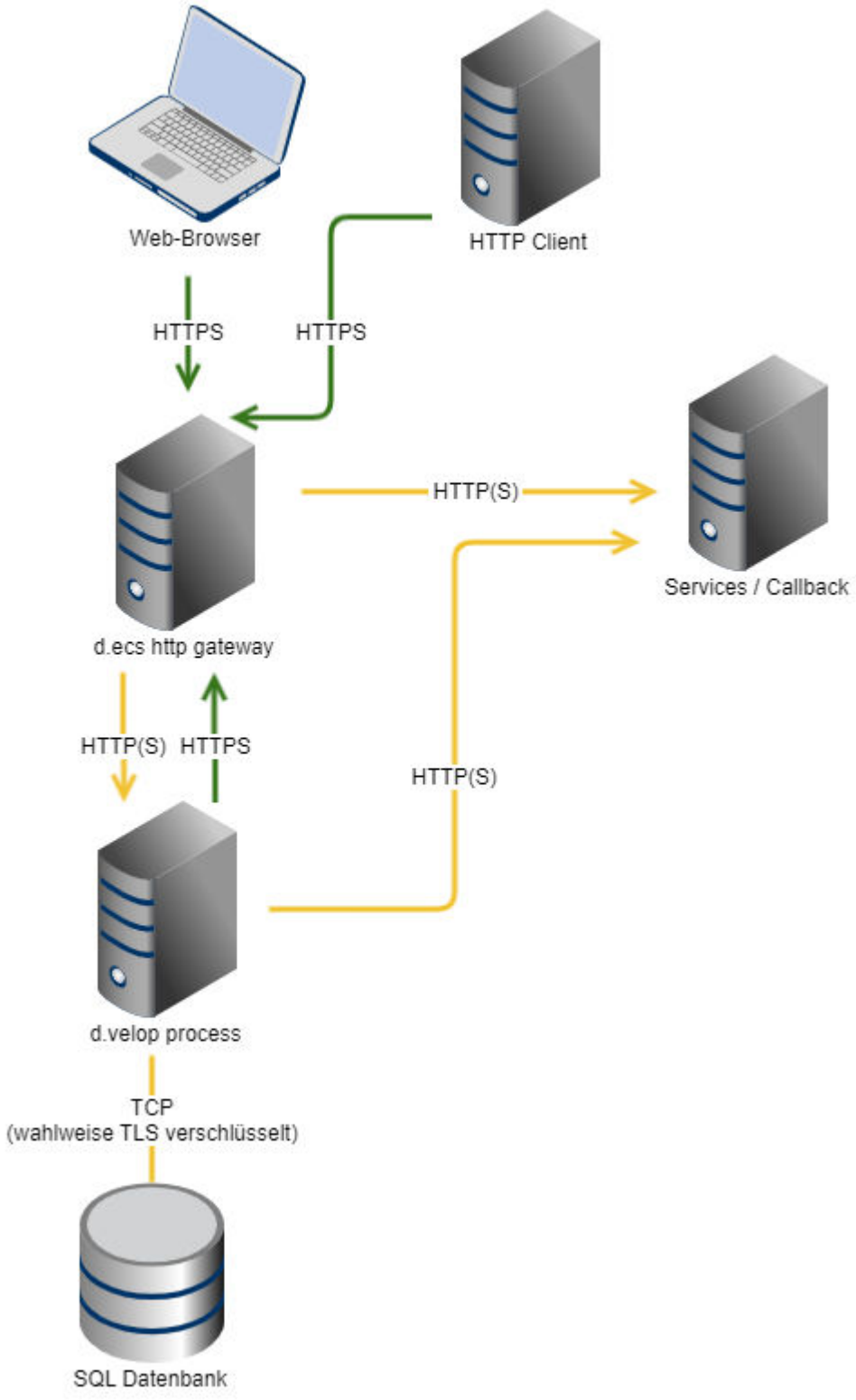
1.2.32. Data communication d.velop process

Representation of the dataflow in d.velop process

d.velop process can be used in a web browser as well as via HTTP-API. Communication always takes place via HTTPS via d.ecs http gateway. d.ecs http gateway serves as a proxy that forwards the requests to d.velop process via HTTP(S). d.velop process stores runtime data and history data in an SQL database. This database is addressed by TCP.

Depending on the use case, d.velop process can call callback and service interfaces of external apps during a process execution. d.velop process also communicates with the external apps via HTTP(S).

Communication with services also takes place via d.ecs http gateway. Callbacks can also be called directly. When called directly, runtime data of the specific process instance is transferred to the external app.



1.2.33. Data communication d.velop task processor

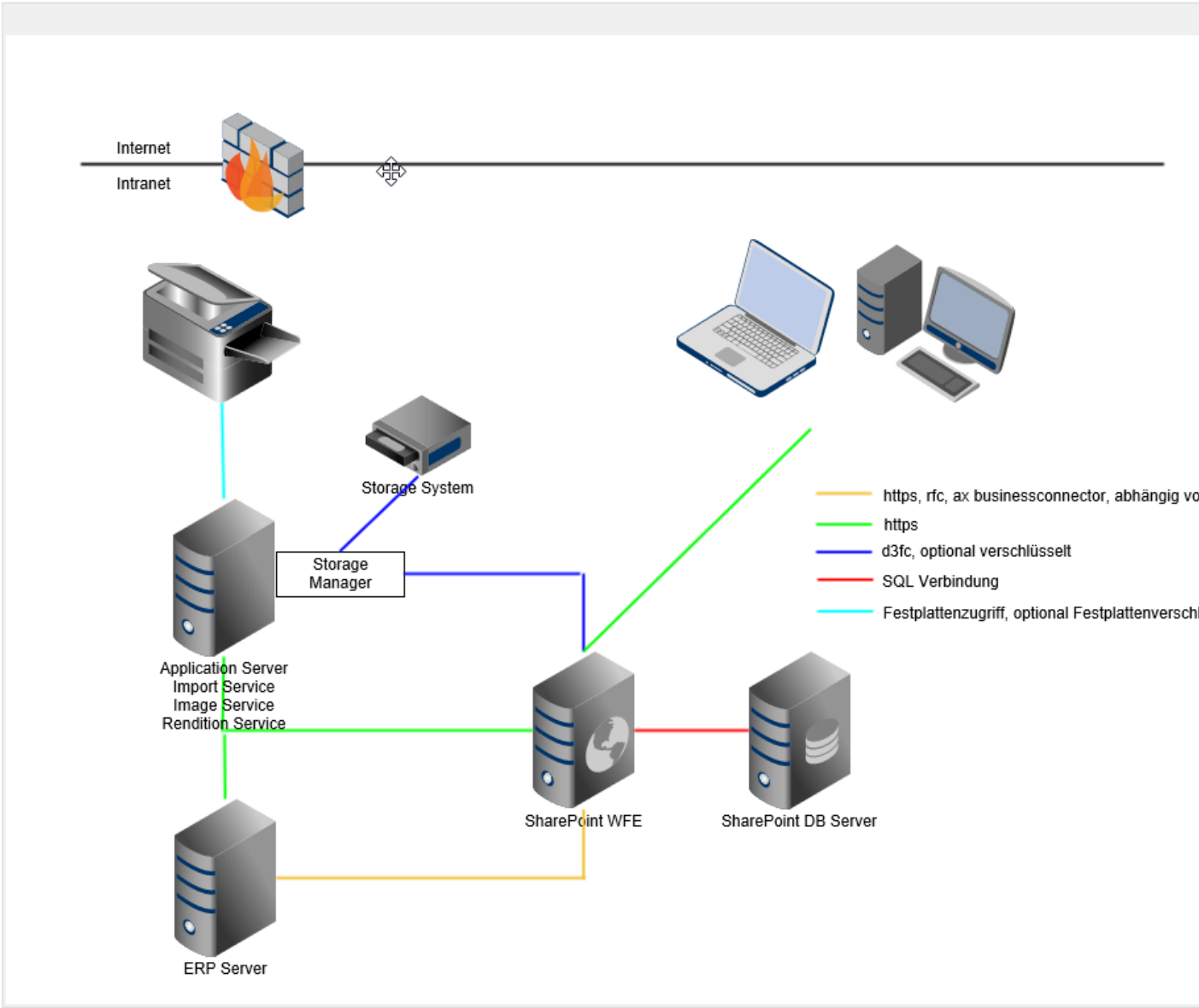
Typical topology

If we consider a typical topology when using ecspand, we usually find the d.velop task processor on the application server.

The d.velop task processor has a generic character. Its concrete form is determined by its configuration. With PowerShell or even your own assemblies you set up concretely how the d.velop task processor works.

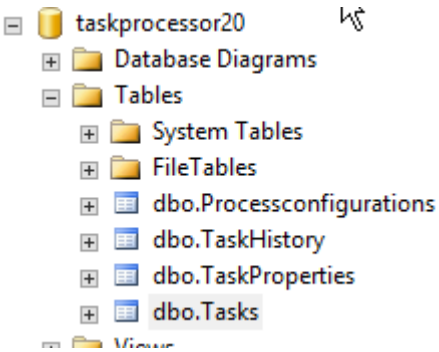
You can find an example of a usage in ecspand invoice processing.

d.velop task processor works as a Windows service, has its own data storage in a Microsoft SQL database, as well as a configuration interface.



Data storage

The d.velop task processor has its own data storage in a Microsoft SQL database. It is structured as follows:



The database has purely technical character and exclusively ensures the functionality of the d.velop task processor.

Depending on your specific project-specific implementation, it is theoretically possible for personal data to be submitted and processed as TaskProperty. Then please make sure that these data are protected and that they are cleared again.

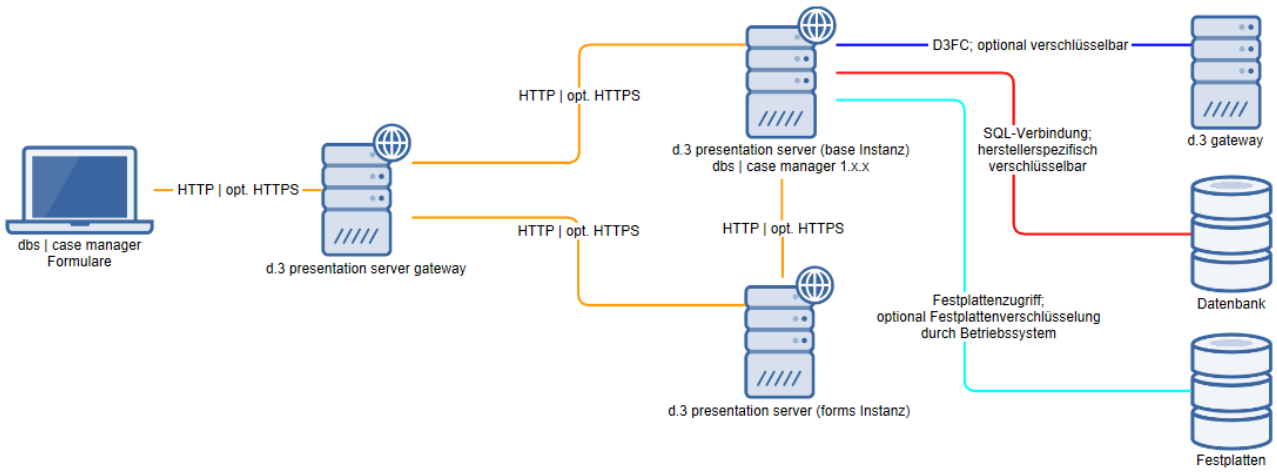
The d.velop task processor has mechanisms at its own disposal which remove the data after its processing and work according to the principle of data minimization.

Data communication

The actual communication with other systems depends on your specific project-specific implementation. In the case of ecspand invoice processing, PowerShell scripts communicate with your Microsoft SharePoint via the client side Object Model. If your Microsoft SharePoint has been set up with SSL, communication with the system also takes place with SSL, i.e. secured. The scripts are executed in the context of the service Account, with which the Windows service of the d.velop task processor was installed.

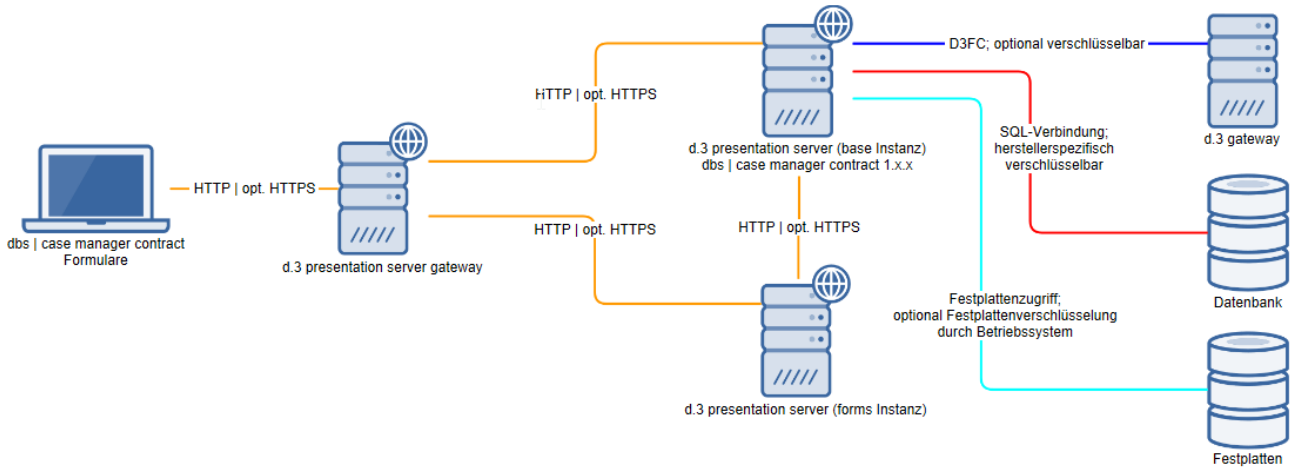
1.2.34. Data communication dbs | case manager

dbs | case manager is being operated within d.3 presentation server. This results in the following supplementary presentation of the data flow:



1.2.35. Data communication dbs | case manager contract

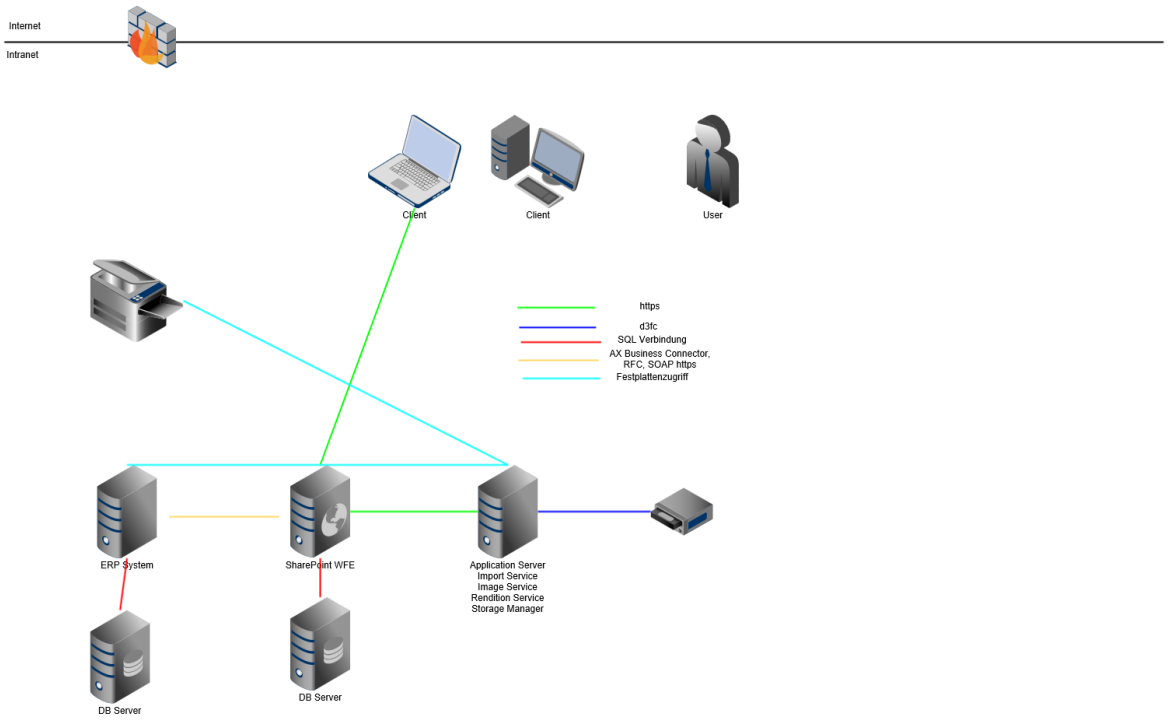
dbs | case manager contract is being operated within d.3 presentation server. This results in the following supplementary presentation of the data flow:



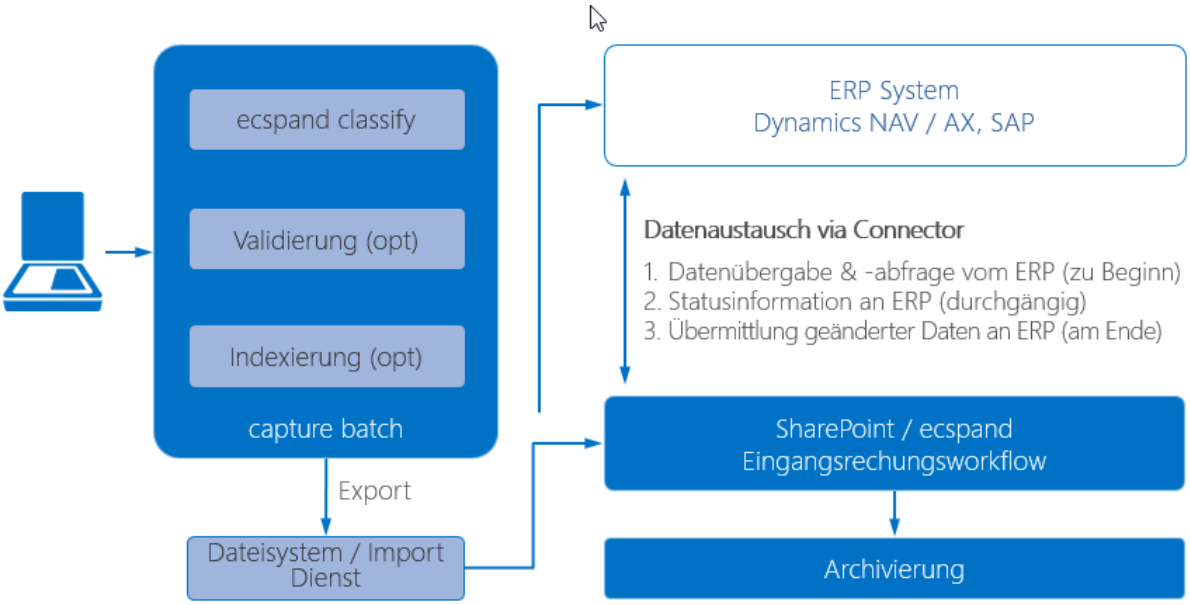
1.2.36. Data communication ecspand invoice processing

To get a general understanding of how to approach the DSGVO with regards to ecspand invoice processing, it is necessary to explain which data and services actually exist and how they store this information and how they communicate with each other. Since ecspand invoice processing is typically a process with a large number of operated components, we exclusively focus on the data storage of the product ecspand invoice processing.

Representation of the data stream in a typical ecspand invoice processing installation



.



In a typical structure of a process chain for invoice processing, the following components are involved.

- a scanning line for the digitization of invoices
- an ImportService for the transmission of data to SharePoint
- an ArchiveConnect module for an import into the ERP system (SAP, Dynamics NAV, Dynamics AX)
- ecspand invoice processing in Microsoft SharePoint
- a d.ecs storage manager with a connection to an archive
- the d.velop task processor

As mentioned above, we only look at the data storage and data communication flows of the ecspand invoice processing in Microsoft SharePoint and additionally look at direct transmission paths.

General

Depending on your country's principles, incoming invoices are documents which are often subject to superordinate legislation in addition to the EU-GDPR.

The obligation for the retention of documents is regarded as higher than the consideration of a request for erasure by a natural person. The objects come from suppliers or creditors and are located there.

Handover from the scanning line to the ecspand Import Service

Depending on your actual installation of the ecspand Import Service, you will probably have one or more folders where the scanned invoices are stored for the import in Microsoft SharePoint.

If the Import Service is enabled and the documents stored there have no errors, they are processed asynchronously after a short while.

However, this means that invoices may remain in these folders if they are faulty and cannot be processed, or if the Import Service is not active at all to process these invoices.

If you have identified that the scanned invoices are eligible for special protection, make sure that the folder is not accessible by everyone although it is typically not located on publicly accessible servers.

Configure a permission on the folder for example for the service account of the Import Service. Thus, the invoices are not directly accessible. Optionally configure a monitoring with the d.ecs which actively notifies you if the folder contains objects remaining longer than desired.

Also take into account, if you may have to consider the paper-based invoices in this scenario and you handle the physical objects in this process.

After the import into Microsoft SharePoint, a so-called receipt file is provided for the import of the ERP system which is stored by the ERP system and generates respective objects. The considerations above also apply to this folder.

Moreover, please consult the documentation on the scanning products used, on the general procedure on the physical handling and protection of the operated disks.

Data storage in the ERP system

Consider the data storage in the ERP system separately with reference to the EU GDPR and use the information provided by the vendor. The communication with the ERP system depends on the system:

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

Data storage in Microsoft SharePoint

Havin transmitted the invoice and imported it into Microsoft SharePoint, you are operating within the Microsoft SharePoint standard with regards to security. Check the security policies in the product documentation or your actual implementation.

You will find a personal reference in SharePoint at least whenever a UserField is used. In the context of the invoice processing and depending on your installation, you will typically find a personal reference at the following positions.

- In the list of persons in charge for cost centers and the delegates.
- In der the list of distribution groups as a member of a group.
- In the list of workflow as a recipient.
- In the actual invoice in the library “Invoices” as the accounting clerk, factual verifier, additional verifier, approver, in the internal notes, in the history, or in the default fields **Creator**, **Edited by** and **Checked out by**.
- In the protocol of the workflow history as a participant in the workflow in the library **Workflow reports**.

Should you find out that a right of an affected person applies in this information, please search in the lists and libraries mentioned above. Please also consider these subjects in your erasure concept.

An example: If a member of staff who took part in this process is leaving your company:

- Remove the member of staff from all groups in the list of persons in charge.
- Remove the member of staff as a recipient from the list of workflow types.
- Remove the member of from the groups Accounting, Verifiers or the distribution lists.

According to the German “Principles of proper accounting and electronic storage” (GoBD), a logged participation in a release process or the invoice itself must not be prematurely deleted. Thus, you must apply exceptional deletion procedures in all invoices and workflow protocols.

Please consider the terms of the GoBD and apply regular deletion cycles on expiry of the respective retention times. Please define the deletion cycles in your individual deletion concept.

Structure and handling of individual tables in the context of invoice processing

When installing the invoice processing, an individual database is generated providing the following data.

- IPConfiguration to store the configuration. The storing person is maintained.
  - The login name is stored here but the record is merely technical.
- IPGOBD to maintain the communication with the ERP system.
  - This information is required for the auditing based on the German principles of proper accounting and electronic storage (GODB) and is thus regarded as superior than the EU GDPR.
- ObjectLocks to prevent a parallel processing of one invoice by two competing users
  - This technically maintains, if a an invoice is currently being processed by another person. This also stores the user name. This table is of mere technical nature and does not contain any personal data. This table is automatically cleared on a regular basis
- TaskGridSettings to store the views in the task webpart of the user
  - Apart from a technical login name, this table only contains technical data to store a personalized view of a task webpart.
- TaskGridLastSelectedSettings to store the last use of a view in the task webpart containing the login name to identify the personal view.
- WorkflowTaskHistory to store all user decisions and comments.

1.2.37. Data communication ecspand HR management

General

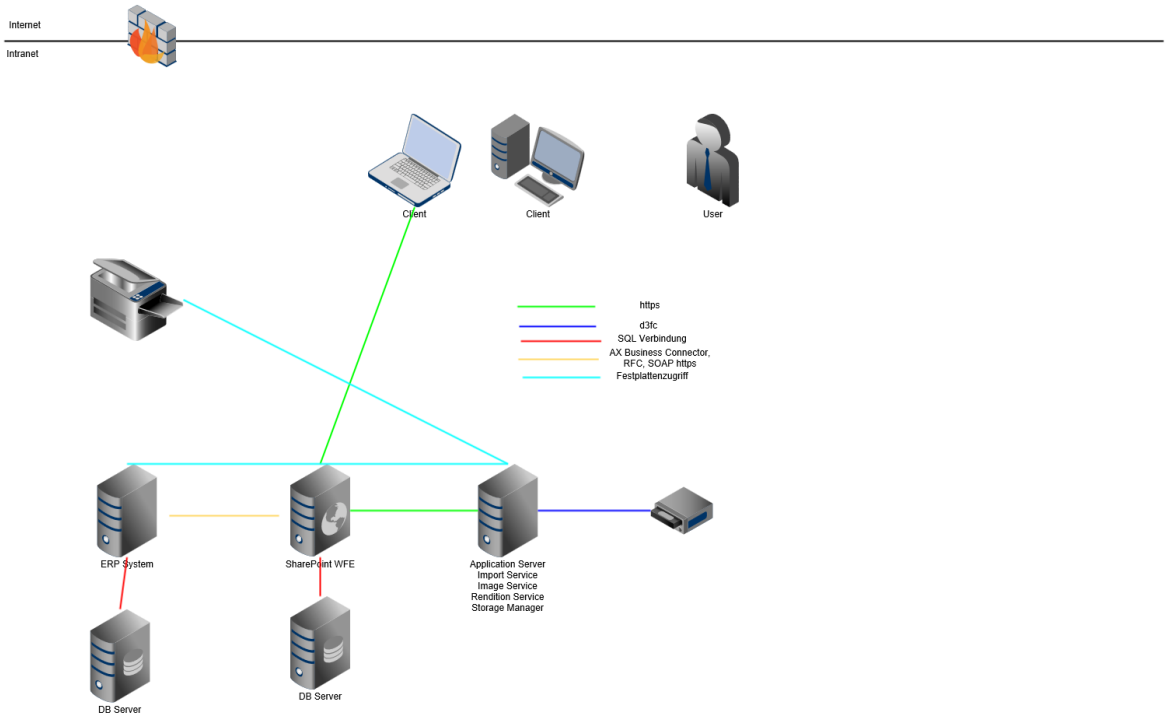
In general, all data, whether entered by the user or data and documents generated via automated mechanisms, are always stored directly in the SharePoint, or more precisely in the content database of the SharePoint site collection.

Information and documents can enter the ecspand HR management through the following channels:

- Manually via drag & drop by a user from the desktop or another folder in the Windows file system.
- Manually with the ecspand sidebar, also via drag & drop by a user from the desktop, another folder in the Windows file system or from a program of the Microsoft Office Suite (Outlook, Word, Excel, PowerPoint).
- Manually based on a template within a personnel file.
- Manually based on a workflow that automatically generates a document.

A wide range of information on a person can be entered for all documents. In general, only information that is document related is stored. These document properties do not contain any personal data in the standard system. However, especially in a personnel department there is a lot of data that is stored about a person. These are basically maintained in the personnel file itself, but can also be stored in documents. An example would be the use of expiry dates on documents (certificates, training confirmations) or court-related documents.

The following graphic shows a classical data communication in the ecspand environment:



(Ident with ecspand invoice processing)

After creating a personnel file, you move from a security perspective in Microsoft SharePoint Standard.

Creation and transfer of personnel data

Via standard interfaces, which are provided by d.velop, personnel files can be transferred automatically from a leading system. Exemplary:

- ecspand Import Service
  - Using control files, files and documents can be automatically transferred from a leading system. The control files are shared via a Windows share folder. By default, only service accounts that run as Windows services and monitor them have access to this directory.
  - By using a monitoring software it can be ensured that the Windows service runs smoothly and the documents do not remain on the Windows share.
- d.velop FlowHeater
  - If data is available in a database, the data can be synchronized directly into the SharePoint without a Windows share folder. This service also runs under a service account.
- Scan line
  - Documents that are to be transferred to the personnel file via a scanning process are supported here by automatic processes. These Windows services also run under a service account and ensure a smooth and secure transfer of documents to the personal files. As with the other products, this data transmission is already in use several times and can be monitored via monitoring software.

Own work tables

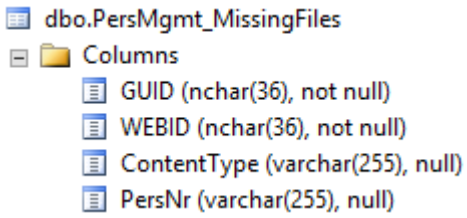
To be able to map more complex work processes in ecspand HR management there are 2 modules which also use their own work tables:

- Missing Files
- Expiration Files

Missing Files

With this module you can search for missing documents. For example, it is possible to determine in which personnel the driving licence has not yet been filed.

In this table, which is located in the ecspand content database, the following properties are stored for documents:



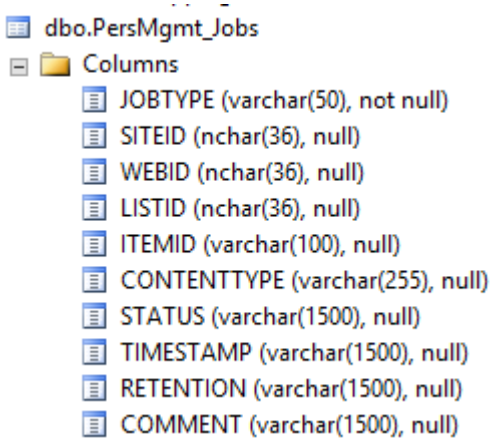
- GUID
  - Technical SharePoint identification of a document (cryptic letters and number combination)
- WEBID
  - Technical identification of the document group (cryptic letters and number combination)
- ContentType
  - Technical identification of the document type (cryptic letters and number combination)
- PersNr
  - The personnel number for the document

No further personal data is stored. With the help of this data such a search query can be created.

Expiration Files

With this module expiring documents are marked, which are legally obliged to be deleted.

In this table, which is located in the ecspand content database, the following properties are stored for documents:



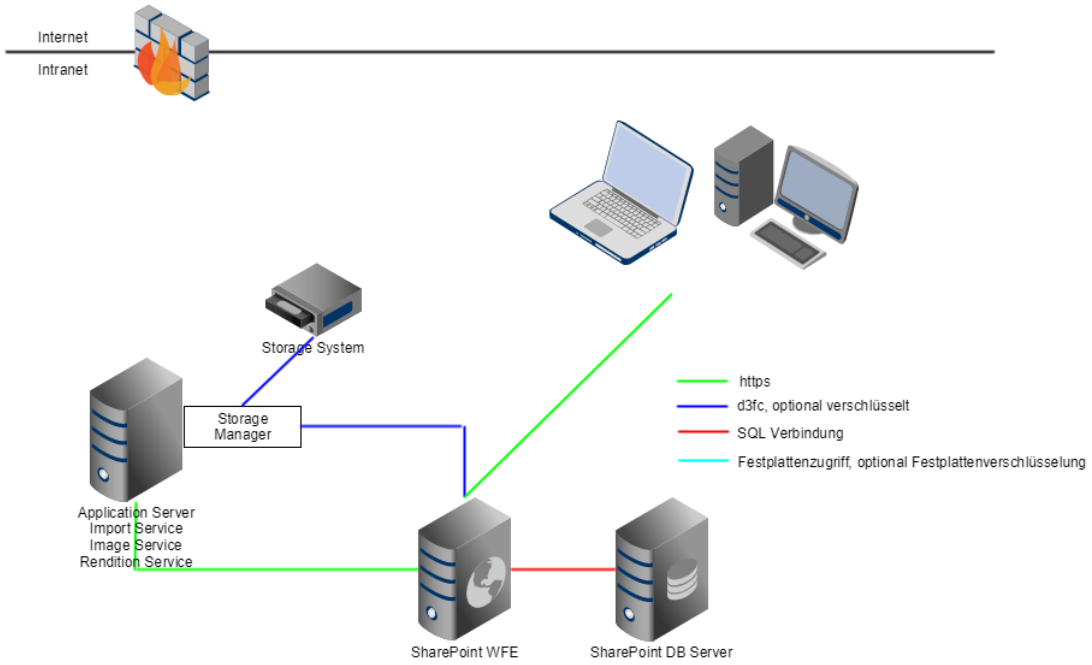
- JOBTYPE
  - Currently only expiring documents are stored. In later versions this can be extended and further job types can be added.
- SITEID
  - Technical identification of the site collection (cryptic letters and number combination)
- WEBID
  - Technical identification of the document group (cryptic letters and number combination)
- LISTID
  - Technical identification of the storage location in SharePoint (cryptic letters and number combination)

- ITEMID
  - Technical identification of a document to the document type (not unique) (cryptic letters and number combination)
- CONTENTTYPE
  - Technical identification of the document type (cryptic letters and number combination)
- STATUS
  - Number or description of the status of the document
- TIMESTAMP
  - Date and time for the job
- RETENTION
  - Number of months when the document expires
- COMMENT
  - If the document is extended (because a court case is actively underway), the comment includes the person who extended the document and when this was done.

1.2.38. Data communication ecspand quality management

To get a general understanding of how to approach the DSGVO with regards to ecspand quality management, it is necessary to explain which data and services actually exist and how they store this information and how they communicate with each other. Since ecspand quality management is typically a process with a large number of operated components, we exclusively focus on the data storage of the product ecspand quality management.

Representation of the data stream in a typical ecspand quality management installation



Data storage in SharePoint

After creating a document via ecspand quality management, you proceed from a security perspective in Microsoft SharePoint Standard. Check the security policies in the product documentation or your actual implementation.

You will find a personal reference in SharePoint at least whenever a user field is used. In the context of the quality management and depending on your installation, you will typically find a personal reference at the following positions.

- In the authorization rules
- In a document in the library in the workspace and portal as Edited by, Deactivated by, Approved by, Authorized by, Verified by, Allocated to, Created by, Modified by, Checked out by and in the workflow comment
- In the task list as “Allocated to”.

Should you find out that a right of an affected person applies in this information, please search in the lists and libraries mentioned above. Please also consider these subjects in your erasure concept.

> **Note**
> If a member of staff who took part in this process is leaving your company:
>
> - Remove the member of staff from all groups in the quality management.
> - Remove the member of from the authorization rules.

1.2.39. Data communication ecspand services

In order to basically understand where in the context of the GDPR an installation of ecspand services can be approached, it is necessary to briefly explain which data and services exist in principle and how these data are stored or communicate with each other. Since ecspand services is a wide range of generically usable components, this is an example of an usage.

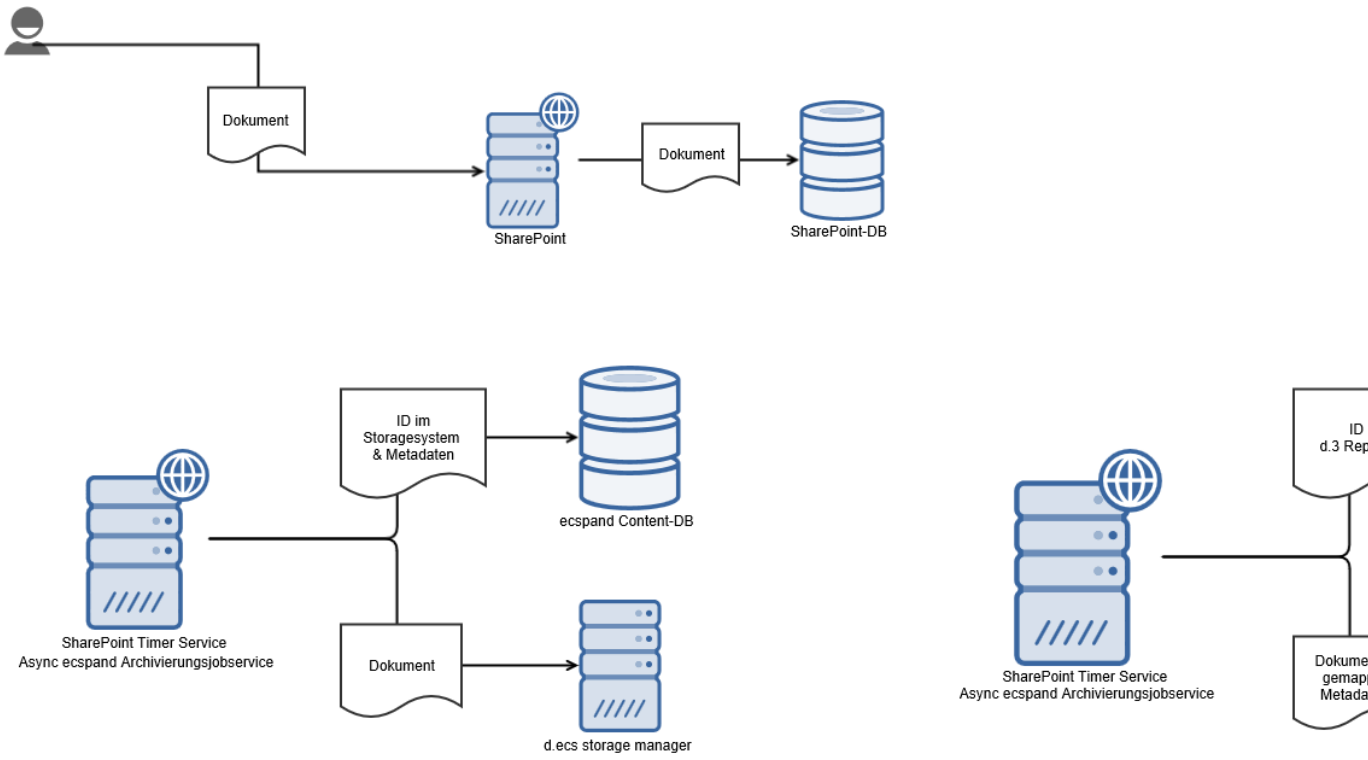
You must transfer this information to your specific specification.

Typical topology

In a typical topology in the ecspand environment, we usually find a configuration with the following components.

- An ERP-system is integrated into the environment and processes.
- Documents are scanned. An import service is used.
- Documents are rendered, i.e. converted to PDF. A rendition service is used.
- Documents are archived. A storage manager is used.

The following illustration shows the technical components to be considered:



This is an example only and your actual configuration may deviate from this topology. The only intention is to illustrate which databases and systems are usually used.

Please refer to your customer-specific installation documentation to find out which specific services are used by your company.

ecspand services - own management data

ecspand has its own databases for managing configurations and tasks (archiving, rendition, etc.)

The structure of the databases, as well as the authorization technical equipment are described in the documentation of ecspand services.

The tables are now explained in detail:

Tables for the Compliance area:

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

With one exception, these tables do not contain any personal data and are not affected by the GDPR. They have a technical character.

However, the table **ComplianceListItemsMetaData** is structured in such a way that metadata of archived objects is stored in the respective version of your customization.

This table will therefore contain metadata information for all objects that are to be archived, provided that you have specified in the archiving rule that this should also be done.

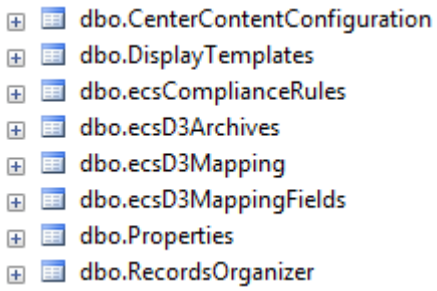
The regular and also the privileged deletion is considered and explained separately in the documentation of ecspand services.

When you open the version page of the corresponding object in SharePoint, the information from this table is displayed.

The tables **ecspandJobs**, as well as **LinkItems** are purely technical and are not affected by the GDPR.

In the table **LinkMappings** you can find information about which LinkItem (links) should be displayed for which person. Only the login name is included. Apart from this user information, this table does not contain any other information about the person. If the links are deleted from the center user interface, they are also removed from the database table.

Configuration in the settings file:



In den Tables **CenterContentConfiguration** and **DisplayTemplates** configurations of the ecspand center are persisted. The person who stores this configuration is recorded, or the account is logged as the Windows logon name with which the change was made.

The table **ecsComplianceRules** is not affected by the GDPR. It does not contain any personal data.

The table **ecsD3Archives** records d.3 instances with corresponding service accounts (user, password). The password is stored with double encryption. The table is of a technical nature and does not contain any further information about the service account.

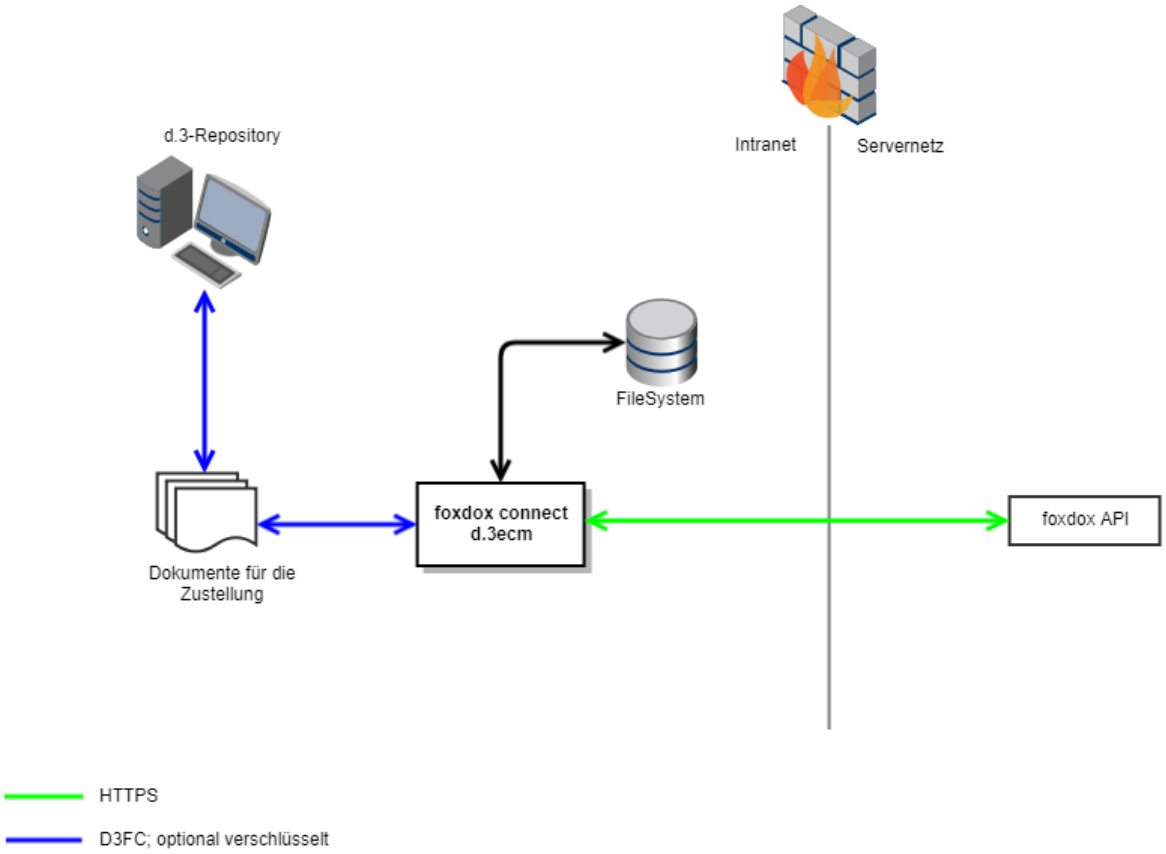
The tables **ecsD3Mapping**, **ecsD3MappingFields**, **Properties** and **RecordsOrganizer** do not contain any personal data and are therefore not relevant for the GDPR.

1.2.40. Data communication foxdox connect d.3ecm

Display of the data flow of foxdox connect d.3ecm

foxdox connect d.3ecm is a software component that is responsible for exchanging documents between a d.3 installed at the customer and foxdox. This is software installed on the customer's system. Documents from a d.3 repository can be delivered to a foxdox user and documents from a foxdox user can be archived in d.3. A document is always delivered in the context of a provider service.

Communication with the foxdox API takes place via an encrypted connection.



Delivery of documents for delivery

The administrator selects documents from the d.3 repository that he wants to send to the foxdox user. foxdox connect d.3ecm retrieves the selected documents from the d.3 repository, creates a.fdx file and compresses them in a password-protected container. AES-256 is used as encryption for the container. The randomly generated password is encrypted RSA-2048 and sent to the foxdox API together with the container via https. For further information, please refer to the documentation of the delivery process.

Receipt of documents

In foxdox, the foxdox user selects a document to send to the foxdox provider. foxdox connect d.3ecm asks the foxdox API in a configured interval whether there are new documents to receive. If this is the case, these documents are downloaded and stored in the local file system. Afterwards, foxdox connect d.3ecm uploads the documents to the d.3 repository and deletes the documents from the local file system.

1.2.41. Data communication foxdox link

Delivery of documents for delivery

The provider creates a .fdx file in the outbox folder in which the delivery folder, recipient and documents to be sent are defined. The files to be sent are stored next to it. The directory monitoring tells the program that documents have been stored there for sending. The folder content is compressed by an asynchronous process and combined in a password-secured container. AES-256 is used as encryption for the container. The randomly generated password is encrypted RSA-2048 and sent to the foxdox API together with the container via https.

Receipt of documents

An asynchronous process queries at a configured interval via the API whether new documents are available for the provider. If this is the case, these documents are downloaded and stored in the local file system.

Manage initial accounts

The provider can create initial accounts for multiple users. These are already linked to the provider's service. A PSUID is used to assign users and recipients of documents.

Manage direct keys

The provider can create socalled direct keys. These can be used by foxdox users to connect to a specific service of the provider. A PSUID is used to assign users and recipients of documents.

Configure provider

No personal data is processed here.

Configure services

No personal data is processed here.

Configure user

These are the users who have access to foxdox.link. No personal data is processed here.

Manage master data

The master data for data entry can be set here. No personal data is processed here.

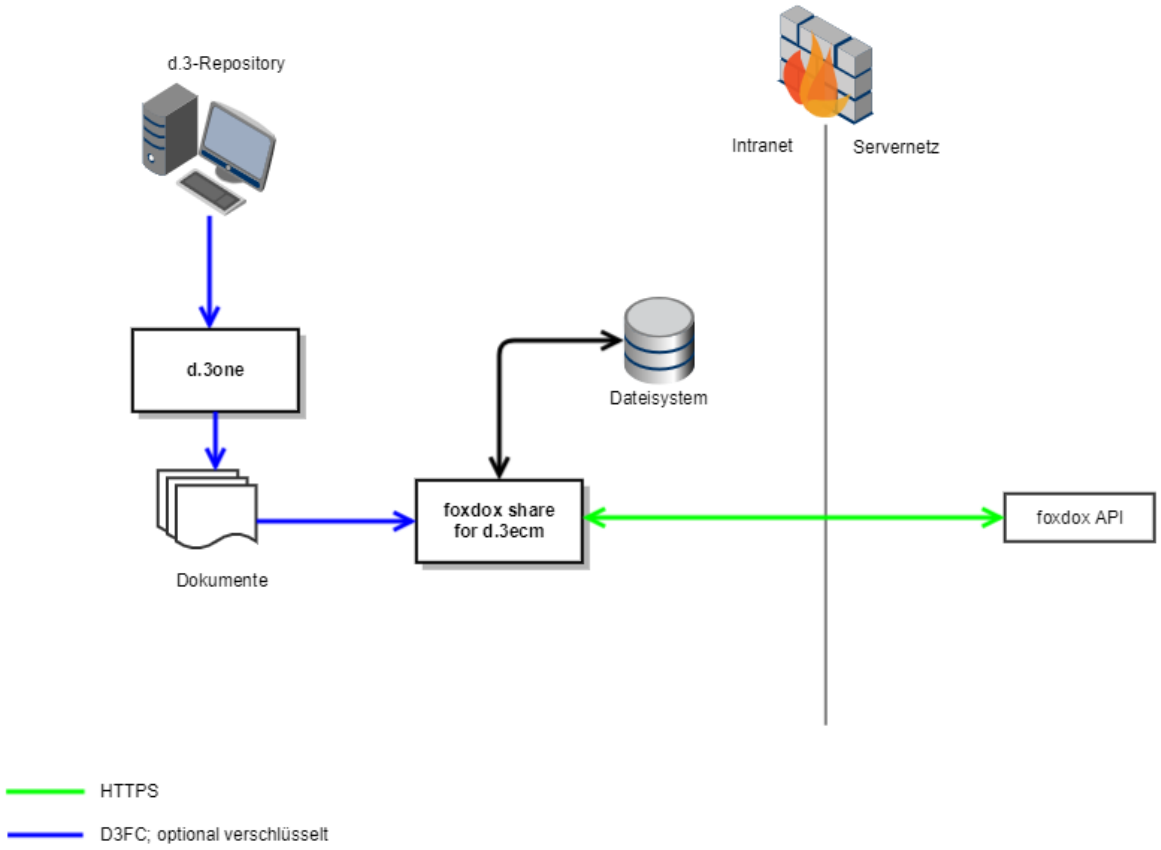
1.2.42. Data communication foxdox share for d.3ecm

Representation of the data flow of foxdox share for d.3ecm

foxdox share for d.3ecm is a software component that can be used to send documents to foxdox from a d.3one installed at the customer. This is software installed on the customer's system.

The component is integrated into d.3one for this purpose.

Communication with the foxdox API takes place via an encrypted connection.

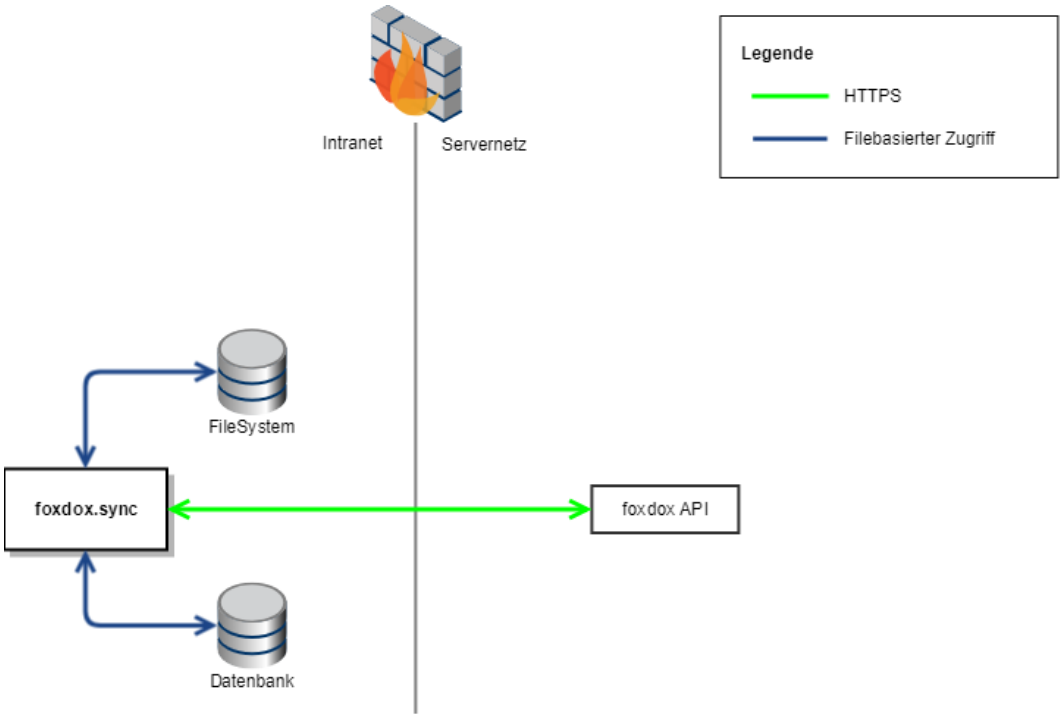


Delivery of documents for delivery

The d.3one user selects documents in d.3one which he or her wants to send to a foxdox user. The documents are temporarily written to the local file system and then uploaded via the foxdox API.

1.2.43. Data communication foxdox sync

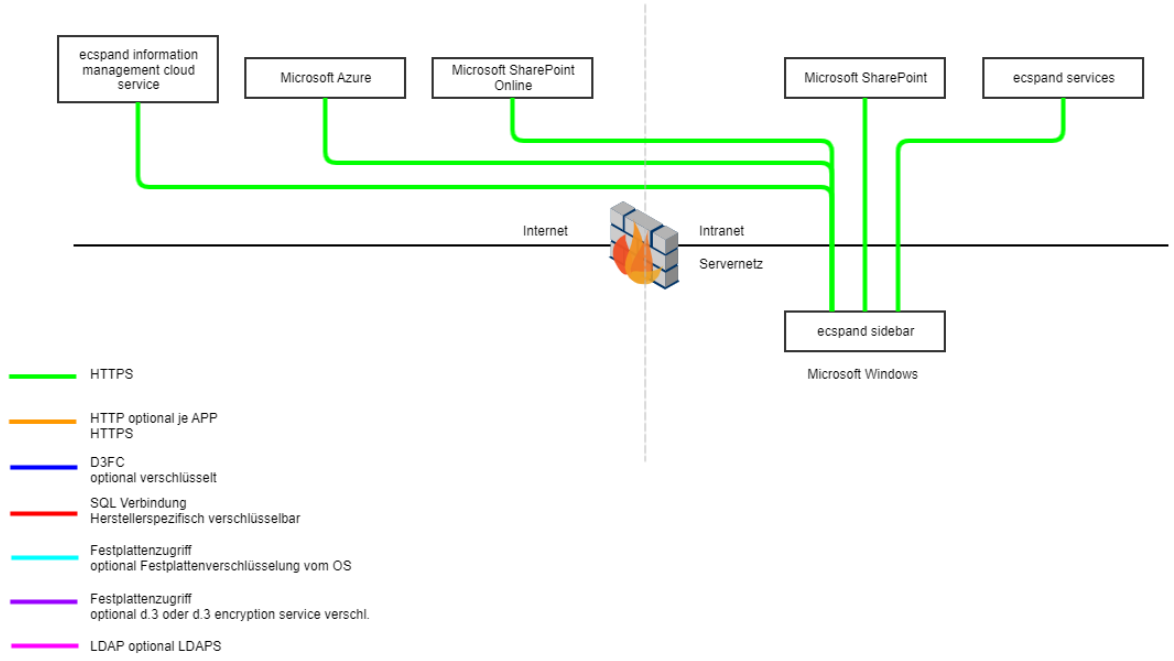
Representation of the data flow of foxdox sync with the foxdox backend



Synchronization of the local data with the foxdox services

foxdox sync synchronizes local data with the foxdox services. For this purpose, foxdox sync accesses local data via file-based access and stores document and folder details for synchronization in a local database. Changes to documents or folders are synchronized via the foxdox API. Communication takes place via https.

1.2.44. Data communication ecspand sidebar



ecspand sidebar accesses Microsoft SharePoint, Microsoft Azure, ecspand services and d.velop composer (formaly: ecspand information management cloud service) via the Client Side Object Model, REST services and SOAP services. This depends on your connection configuration.

If you have identified for yourself that the communication should be encrypted, an https connection with SSL can be set up in the connection configuration.

1.2.45. Data processing for integrations of d.velop documents

In this article, you will find important information about data processing for integrations of d.velop documents for Microsoft 365 so that you can understand the technical and legal aspects. The following questions are answered:

- **Technical requirements**: What are the technical requirements for using the integrations?
- **Data transmission**: How is the data technically transmitted to Microsoft?
- **Contractual basis**: What is the contractual basis?
- **Data centers**: In which data centers are Microsoft Office documents processed?

Technical requirements

To use the integrations, you need d.velop documents (cloud or hybrid) and a valid Microsoft 365 subscription.

Data transmission

- d.velop documents provides a Web Application Open Platform Interface Protocol (WOPI) API that is addressed Microsoft. You can find additional information on the topic at: Web Application Open Platform Interface Protocol (WOPI)
- Communication between d.velop documents and Office for the web is encrypted (transport encryption) in combination with individually provided access tokens for each document.

Contractual basis

- d.velop has joined the Office Cloud Storage Partner Program. As such, the following Microsoft guidelines apply: Microsoft Cloud Storage Partner Program Integration Terms
- When the Microsoft 365 subscription is concluded, the customer is responsible for concluding the respective data processing agreements with Microsoft.

Data centers

- According to Microsoft, they attempt to process documents that are edited with Office for the web in the nearest data center. However, Microsoft cannot guarantee that processing will occur in the nearest data center.
- You can find more information about processing on the Microsoft website at: FAQ - How does Office for the web determine the datacenter to route a given user to?

1.3. Rights of the data subjects

The new data protection law restructures the rights of data subjects. This chapter tells you how the revision of the rights of the data subjects affects your d.velop product.

1.3.1. Information

Information d.3 search

Data to be disclosed can be retrieved via the leading d.3 application and can be displayed there in the context of all other stored information.

Information d.classify

The **Anonymization wizard ()** allows you to search for documents of the affected person in the documents specified in d.classify.

Information d.ecs forms

You can use the instance search in d.ecs forms to determine form instances containing a specified keyword. These instance can be exported technically.

Information d.velop GDPR compliance center

Personal data within d.velop GDPR compliance center are only stored in two contexts:

- For each data protection object, a person responsible and an approver can be specified in the form of a user name or user ID.
- In the configuration of the directory of processing activities it is possible to store contact persons with surname, first name, position, department and telephone number.

Information on the deposit of a person as the person responsible or approver of a data protection object can simply be provided via the overview of data protection objects and sorting by person responsible and approver.

Information about the deposit of a person as contact person can take place after calling up the configuration of the directory of processing activities.

Information d.velop process

An automated search for runtime data and history data is currently not possible.

Please note that GDPR relevant user data should not be saved in the runtime data or in the history data of processes but only in referenced thrid-party systems.

Information dbs | case manager

Below you will find a list of the personal data stored in the standard within dbs | case manager contract. If, as the person responsible, you have to comply with the right to information of a person concerned, you can research the corresponding data via the corresponding interfaces. In addition, depending on the properties and configuration, the full-text search, the operation overview incl. facetting as well as the standard search within the d.3ecm system can also be used for the search.

The product dbs | case manager serves to summarize all essential information in the enterprise such as documents, information, tasks and conversations process-oriented and to make them available digitally. Using case types, status models, extended master data and task templates, it is possible to flexibly model the company's individual business processes. dbs | case manager therefore represents a generic product that can be used for any processes and thus also within any processing activities in the sense of the DSGVO. The following explanations can therefore only refer to the product as such and its standard scope of delivery. An analysis and evaluation of the data protection relevant aspects of processing activities realized on the basis of dbs | case manager therefore requires a concrete consideration of the customer-specific processes realized.

Within dbs | case manager different personal data can be stored. The following list only refers to personal data that can be stored based on the product standard:

- Surname, first name:
  Name and first name in the form of user-defined text entries are only entered in the standard system to store the person contact of a business partner.
  You do this in partner management or in the case form by entering an external contact person or when the business partner enters a notice.
- User/d.3 user:
  User IDs or d.3 users are always used if the user is relevant with regard to process control or logging.

User IDs are therefore used primarily for assigning responsibilities for cases, periods, tasks, and as recipients of mailbox entries and messages, as well as for logging activities within case management. In the same way, a user can be stored as the deputy of another user within the scope of these responsibilities.
In addition, user IDs are used to give them corresponding rights to functions in case management.

- E-mail addresses:
  E-mail addresses are used to send external conversations. Thus, an e-mail address can be used as the recipient of an individual conversation or can be stored in the partner administration for the contact person in order to simply select the e-mail address in the external conversations.
- Telephone number and address data:
  Telephone number and address data can optionally be stored for the business partner's personal contact.

Information dbs | case manager contract

Below you will find a list of the personal data stored in the standard within dbs | case manager contract. If, as the person responsible, you have to comply with the right to information of a person concerned, you can research the corresponding data via the corresponding interfaces. In addition, depending on the properties and configuration, the full-text search, the operation overview incl. facetting as well as the standard search within the d.3ecm system can also be used for the search.

The product dbs | case manager contract is designed as an integrated contract management system. The digital contract process includes all essential information such as documents, master data, tasks and conversations. The integrated case management allows individual modeling of the business process contract management based on contract types, status models, advanced master data and task templates. In this respect, the following core explanations refer to the standard product and the standard processes delivered with it. Essential aspects relevant to a list of processing activities, such as the purpose or groups affected, depend, however, on the types of contracts for which dbs | case manager contract is used or in which processing activities this product is used.

Within dbs | case manager contract different personal data can be stored. The following list only refers to personal data that can be stored based on the product standard:

- Surname, first name:
  Name and first name in the form of user-defined text entries are only entered in the standard system to store the person contact of a business partner.
  You do this in partner management or in the contract form by entering an external contact person or when the business partner enters a notice.
- User/d.3 user:
  User IDs or d.3 users are always used if the user is relevant with regard to process control or logging. User IDs are therefore used primarily for assigning responsibilities for contracts, periods, tasks, and as recipients of mailbox entries and messages, as well as for logging activities within contract management. In the same way, a user can be stored as the deputy of another user within the scope of these responsibilities.
  In addition, user IDs are used to give them corresponding rights to functions in contract management.
- E-mail addresses:
  E-mail addresses are used to send external conversations. Thus, an e-mail address can be used as the recipient of an individual conversation or can be stored in the partner administration for the contact person in order to simply select the e-mail address in the external conversations.
- Telephone number and address data:
  Telephone number and address data can optionally be stored for the business partner's personal contact.

Information ecspand

From a formal point of view, Art.12 Para. 5 GDPR specifies that the information must always be provided free of charge.

To do this, the person responsible must respond without undue delay, but within one month at the latest.

If the request for information has been received in electronic form, the reply should also be in electronic form.

If you have identified that you must fulfil this right, please identify the places where personal data exist in your processing directory. Use the ecspand search, if necessary also in several queries, in order to list all identified objects in a respective search result.

From there you are able to export the result itself, not the objects themselves, electronically as a .csv file.

If you have identified objects that must be handed over, you may work with your own ContentTypes or fields that mark this handover obligation. However, since the product has a high generic character and we do not know exactly what you are implementing with the product, you can easily implement this simplification in the Microsoft SharePoint standard.

Information ecspand invoice processing

From a formal point of view, Art.12 Para. 5 GDPR specifies that the information must always be provided free of charge.

To do this, the person responsible must respond without undue delay, but within one month at the latest.

If the request for information has been received in electronic form, the reply should also be in electronic form.

If you have found out that you must comply with this right, identify the locations of the existing personal data based on your actual implementation of ecspand invoice processing and with reference to the chapter Data storage and data communication flows.

Are you processing invoices by natural persons or only by legal persons?

Use the structured ecspand search, with several queries if necessary, to list all identified objects in one respective search result.

From there you are able to export the result itself, not the objects themselves, electronically as a .csv file.

Please consult the documentation of the ecspand services for additional information on this subject.

As a rule, invoices should not be subject to surrender as they are subject to further rights. In the incoming invoice processing, your are the invoice recipient. A potential applicant should therefore be in control of the document.

With a request for disclosure by a member of staff or process participant, follow the procedure described above. Invoices do not have to be disclosed as these documents are subject to additional rights.

Information ecspand HR management

From a formal point of view, Art.12 Para. 5 GDPR specifies that the information must always be provided free of charge.

To do this, the person responsible must respond without undue delay, but within one month at the latest.

If the request for information has been received in electronic form, the reply should also be in electronic form.

If you have identified for yourself that you have to comply with this right, all data concerning a person are stored in his or her personal file.

Please refer to the documentation of the ecspand HR management.

If you need to download the complete file, the following two modules can be helpful:

- ecspand document cart (only on-premise) d.velop AG
  - Documents can be selected here and transferred to the document cart. This document cart can then be downloaded as a ZIP package.
- ecspand Offline Synchronization (currently only On-Premise) d.velop GmbH Vienna
  - Files can be downloaded in one.

Information ecspand quality management

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data.

Based on the chapter **Data communication** it can be identified where personal data exist.

The structured ecspand search can be used, with several queries if necessary, to list all identified objects in one respective search result.

Using it, the result but not the objects can be exported as a `csv` file. The documentation of the ecspand services provides additional information on this subject.

Information foxdox connect d.3ecm

No personal data is stored within foxdox connect d.3ecm.

There may be personal details in the log files. Therefore, we recommend that you delete the log files after 30 days at the latest.

Whether personal details are included in the log files depends on the use of the product. For example, certain sensitive personal details may be contained in document names.

Information foxdox share for d.3ecm

No personal data is stored within foxdox share for d.3ecm.

There may be personal details in the log files. Therefore, we recommend that you delete the log files after 30 days at the latest.

Whether personal details are included in the log files depends on the use of the product. For example, certain sensitive personal details may be contained in document names.

Information foxdox sync

Information about personal data of others

If you have stored personal data of others in documents in your DMS, you are obliged under Art. 12 para. 5 GDPR to provide information about the stored data free of charge. To do this, the person responsible must respond without undue delay, but within one month at the latest. If the request for information has been received in electronic form, the reply should also be in electronic form. If you have identified that you must fulfil this right, please identify the places where personal data exist in your processing directory. Use the foxdox search, if necessary also in several queries, in order to list all identified objects in a respective search result. From there, you can open the document directly or open the folder where the document is stored.

If you have identified objects requiring publication for yourself, you may work with your own document types that mark these objects requiring publication. However, since the product has a high generic character and we do not know exactly what you are doing with the product, you can easily implement this relief in foxdox. In order to define your own document types, you need a foxdox account with costs.

Information about your personal data

If you would like to receive information about your personal data, you can do this directly in your account settings.

If you would also like to know what other personal data is stored, please send an e-mail to datenschutz@foxdox.de. You will receive information from us within one month.

1.3.2. Right to erasure

Erasure d.3 search

The deletion takes place via the leading system d.3. Data that is deleted there will also be removed in d.3 search. In this process, the words used are not immediately deleted from the index but all references to the respective documents are removed. When reindexing the index is cleaned up accordingly so that the words no longer used are also removed from the index.

Data in temporary directories are removed daily.

Erasure d.classify

The **Anonymization wizard** in d.classify Admin allows you to search for documents of the affected person in the specified references.

The identified documents can be viewed and anonymized or deleted, if necessary.

Erasure d.ecs forms

You can use the instance search to determine form instances containing data on a specified search term. These can then be deleted from the instance database using the identifiers.

Erasure d.ecs storage manager

d.ecs storage manager passes the deletion request from the calling application (e.g. d.3 or ecspand) to the storage systems, if possible. It must be ensured here that these systems also support the privileged deletion to be able to remove data from the storage prior to the end of the retention time.

Erasure d.velop GDPR compliance center

The deletion of the user name or user ID stored as the person responsible or approver of a data protection object is done by calling up the data protection object and changing the respective person responsible or approver.

The deletion of personal data relating to a contact person deposited for the list of processing activities shall take place within the configuration of the list of processing activities.

Erasure d.velop process

An automated search for runtime data and history data is currently not possible.

Please note that GDPR relevant user data should not be saved in the runtime data or in the history data of processes but only in referenced thrid-party systems.

Erasure dbs | case manager + contract

An erasure of the personal data takes place via the respective interfaces.

Erasure ecspand

Article 17 para. 1 GDPR does not initially represent any significant changes with regard to the right to delete personal data compared to the corresponding § 35 para. 2 Federal Data Protection Act (BDSG). The most important case groups in which the deletion of data can be requested remain the same. According to Art. 17 para. 3b GDPR, deletion is still ruled out if there are legal retention periods (see § 35 para. 3 no. 1 Federal Data Protection Act (BDSG)).

In a deletion concept, define which objects actually need to be deleted when you request deletion. Check the rights of third parties and retention rights of the objects and whether these may actually be deleted.

Check whether any objects to be deleted are archived. If this is the case, please check whether your archive system supports privileged deletion or whether you need to perform further configurative and commercial measures there, e.g. the acquisition of an extended license.

The deletion of documents with expired retention period and the privileged deletion of documents in ecspand services is described in the chapter **GDPR**.

Erasure ecspand invoice processing

With the right for erasure of personal data, article 17 section 1 of the EU-GDPR DSGVO does not bring about relevant changes compared to the respective § 35 section 2 of the German “Federal data protection law” (BDSG). The most important case groups in which the deletion of data can be requested remain the same. According to Art. 17 para. 3b GDPR, deletion is still ruled out if there are legal retention periods (see § 35 para. 3 no. 1 Federal Data Protection Act (BDSG)).

This also applies to incoming invoices.

In case of a request for erasure by a (former) member of staff, you operate within the SharePoint standard. In this case, you do not have to delete any documents but the membership in process groups must be adjusted. You can find additional information on this in the chapter data storage and data communication flows.

In a deletion concept, define which objects actually need to be deleted when you request deletion. Check the rights of third parties and retention rights of the objects and whether these may actually be deleted.

Check whether any objects to be deleted are archived. If this is the case, please check whether your archive system supports privileged deletion or whether you need to perform further configurative and commercial measures there, e.g. the acquisition of an extended license. Optionally check the document in the d.velop service portal mentioned in the introduction which provides you with additional information on this subject.

What do I have to do to be able to delete data to be erased and how do I actually delete them?

Define the objects to be actually deleted in you deletion concept.

Supplement the general case with your actual implementation of the invoice processing. Consider the following documents:

- the incoming invoice
- uploaded dependent documents
- uploaded dependent accounting documents
- the workflow report
- GoBD (German “principles of proper accounting and electronic storage”) data accessible in the section of the invoice processing configuration page
- Workflow history information accessible in the section of the invoice processing configuration page
- additional documents used in your process

Erasure ecspand quality management

Expiring documents

Some types of documents are obliged by law to be deleted after a regulated number of months. The person stored for this purpose receives a notification and must manually delete the documents marked for deletion on a separate page.

This feature can also be used for those not legally required to delete. All document types and information types are stored in the configuration.

EUROPEAN GDPR

In order to guarantee the new EU data protection basic regulation (2016/679) - which comes into force on 25 May 2018 (transition period has been running since 2016) - various measures are necessary. This includes the compilation of a list of procedures (Art. 30) on the basis of the data analysed (Art. 9):

- Definition of processes based on data relating to persons (printed and digital)
- What categorization does this data have
- What is the purpose of storing this data
- Where are these data stored, processed and collected

The categorisation of data according to Art. 9 can be divided into the following levels:

- High / very high (confidential)
  - Racial and ethnic origin, political opinion, trade union membership, criminal data, data subject to professional secrecy, health data, behaviour control, bank or credit card data, biometric data (e.g. photo)
- Medium
  - Contract data, order data, credit check, personnel planning, private contact data of employees, data on employment relationship
- Low
  - Data from publicly accessible sources, address data from the telephone directory, data which do not require a legitimate interest of the data subject

Erasure ecspand quality management

What do you have to do to be able to delete data to be erased or how do you actually delete them?

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay, if the conditions stipulated under article 17 of the EU-GDPR apply,

In case of a request for erasure by a (former) member of staff, you operate within the SharePoint standard. In this case, you do not have to delete any documents but the membership in process groups must be adjusted. You can find additional information on this in the chapter data storage and data communication flows.

In a deletion concept, define which objects actually need to be deleted when you request deletion. Check the rights of third parties and retention rights of the objects and whether these may actually be deleted.

Check whether any objects to be deleted are archived. If this is the case, please check whether your archive system supports privileged deletion or whether you need to perform further configurative and commercial measures there, e.g. the acquisition of an extended license.

What do I have to do to be able to delete data to be erased and how do I actually delete them?

Define the objects to be actually deleted in you deletion concept.

Supplement the general case with your actual implementation of the ecspand quality management. Consider the following documents:

- the document
- uploaded dependent documents
- the workflow report
- additional documents used in your process

Right to erasure foxdox connect d.3ecm

Since no personal data is recorded, erasure is not planned.

There may be personal details in the log files. Therefore, we recommend that you delete the log files after 30 days at the latest.

Right to erasure foxdox share for d.3ecm

Since no personal data is recorded, erasure is not planned.

There may be personal details in the log files. Therefore, we recommend that you delete the log files after 30 days at the latest.

Right to erasure foxdox sync

You have the right to request that we delete any personal information about you immediately if any of the following scenarios apply:

- The personal data is no longer necessary for the purposes for which it was collected or otherwise processed.
- You withdraw your consent on which the processing was based pursuant to Article 6 Para. 1 Letter a) or Article 9 Para. 2 Letter a) of the GDPR and there is no other legal basis for the processing.
- You object to the processing under Article 21 Para. 1 of the GDPR and there are no overriding legitimate reasons for the processing, or you object to the processing under Article 21 Para. 2.
- The personal data was processed unlawfully.
- Deletion of the personal data is necessary to fulfil a legal obligation under European Union law or the law of the Member States to which the data controller is subject.
- The personal data was collected in relation to information society services pursuant to Article 8 Para. 1 of the GDPR.

If we have ever made your personal data public and are obliged to delete it in accordance with the above points, we will take appropriate measures, including technical measures, and taking into account the available technology and the costs of implementation, to inform the third parties responsible for processing the personal data that you have requested us to delete all links to this personal data or copies or replications of this personal data.

We are not obliged to delete the data or inform third parties of your request for deletion if further processing of your personal data is necessary for the following purposes:

- To exercise the right to freedom of expression and information
- To fulfil a legal obligation required by the law of the European Union or of the Member States to which we are subject, or to perform a task carried out in the public interest or in the exercise of official authority vested in us
- For reasons of public interest in the field of public health pursuant to Article 9 Para. 2 Letter h) and i) and Article 9 Para. 3 of the GDPR
- For archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes pursuant to Article 89 Para. 1 of the GDPR, insofar as the regulation referred to in Para. 1 presumably makes impossible or seriously impairs the attainment of the objectives of such processing
- To assert, exercise or defend against legal claims

You can delete the data contained in your foxdox account at any time by accessing your foxdox account.

You have the following options for deleting your data:

- Delete your entire foxdox account
- Find specific documents in your account and then delete them.

In formal terms, Art. 12 Para. 5 of the GDPR stipulates that, in principle, this portability must be offered free of charge. We must also examine your request without undue delay, but within one month at the latest, and comply with it under the aforementioned conditions.

1.3.3. Rights of the data subjects ecspand sidebar

The rights of data subjects cannot be applied to the data of ecspand sidebar, as these are exclusively of a technical nature, e.g. in the configuration or in temporary files. All temporary files are deleted when the program is started.

Configurations are user-specific, but also only suitable in the context of the user and limited to the specific end user by mechanisms of the operating system. This applies to both access (login) and storage (protected local user directory) of this data.