

# **Altova GDPR Compliance Database**

## **User Guide**

# **Altova GDPR Compliance Database User Guide**

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Published: 2020

© 2020 Altova GmbH

---

# Table of Contents

<b>1</b>	<b>About Altova GDPR Compliance Database</b>	<b>5</b>
<b>2</b>	<b>User Management</b>	<b>7</b>
2.1	Define System Users and Settings.....	9
2.2	Send Access Information to System Users.....	12
<b>3</b>	<b>General Information about the Compliance Database</b>	<b>13</b>
3.1	Terminology.....	14
3.2	How the GDPR Compliance Database Works.....	17
3.3	Overview Page.....	20
3.4	Navigational Links.....	22
3.5	Metadata Relationships.....	23
3.6	Login and Logout.....	24
<b>4</b>	<b>GDPR Metadata</b>	<b>25</b>
4.1	Define the Company.....	26
4.2	Configure Company Information.....	27
4.2.1	Departments.....	28
4.2.2	Persons.....	31
4.3	Configure Data Information.....	35
4.3.1	Data Classifications.....	36
4.3.2	Data Usage Classifications.....	39
4.3.3	Data Processors.....	42
4.4	Define Data Properties and Relationships.....	44
4.4.1	Define Data Categories.....	45
4.4.2	Define Data Storage Entities.....	49
4.4.3	Define Processing Activities.....	52

---

<b>5</b>	<b>Approvals</b>	<b>56</b>
5.1	Approval Requests.....	57
5.2	Authorize an Approval.....	59
<b>6</b>	<b>Discussions</b>	<b>62</b>
6.1	Discussions about a Single Metadata Item.....	63
6.2	Discussions about All Items of a Metadata Type.....	65
6.3	Start a Discussion.....	67
6.4	Available Functionality.....	69
<b>7</b>	<b>Reports</b>	<b>71</b>
7.1	Processing Activities.....	72
7.2	Critical Processing Activities.....	73
7.3	Category Approvals.....	75
<b>8</b>	<b>Additional Features</b>	<b>77</b>
8.1	Changes.....	78
8.2	Search Filters on Pages.....	80
	<b>Index</b>	<b>81</b>

# 1 About Altova GDPR Compliance Database

The **General Data Protection Regulation (GDPR)** is a regulation in EU law that protects the data and privacy of persons living in the EU and European Economic Area (EEA). It became binding beginning 25 May 2018. Businesses that process personal data of people living in the EU and EEA must now ensure that this data is handled in line with the principles of the GDPR and that this data is protected. Data protection measures are required to be built into the design of business processes that collect personal data. If a data breach occurs and the breach compromises the privacy of a person, then the breach must be reported to the supervisory authority. (For more information about the GDPR, see [the EU web page on GDPR](#) and [Wikipedia](#)).

In order to make sure that all the personal data of EU/EEA residents held by your organization is in compliance with GDPR, you should build and continuously track all repositories of personal data that you maintain. The **Altova GDPR Compliance Database** enables you to quickly organize information about your repositories of personal data in a structured way.

The **Altova GDPR Compliance Database** enables you to do the following:

- Quickly configure departments and people in your organization that are involved in the collection and processing of personal data
- Quickly configure details of external entities that process personal data your organization collects
- Quickly create a list of all repositories in your organization where personal data is stored
- Set up criteria for classifying data (such as sensitivity, source, protection level), and assign a set of appropriate values for each classification. For example, a data classification might be named *Storage duration* and be defined to have one of the following values: 1 year, 2 years, 3 years, 5 years, 7 years
- Define data categories. In a given data category, the data classifications you have created are each assigned a value (from among their respective allowed values). For example, if you define a data category named *Billing Address*, then this category could have the following classification values: (i) *Type of data = personal data*; (ii) *Encryption = none*; (iii) *Storage duration = 7 years*
- List and define all the data-processing activities that are used by your organization, including applications used by external agents that are tasked with processing data for your organization (for example, an external organization that sends promotional emails to your customers)
- Automatically link information that is entered in one part of the compliance database so that this information is reused in related parts of the database; this provides efficiency and accuracy while entering information in the database, as well as a better overview of information
- Enable distributed use of a central system (the compliance database) by multiple users
- Enable users of the compliance database to independently modify the structure of the system, subject to an approval process that is built into the system
- Track changes to the structure and other aspects of the system
- Quickly generate different kinds of reports, which will be based on the information currently held in the compliance database
- Start discussions about different items of the compliance database, and invite specific users to join the discussion; discussion threads can be read directly in the system and in the context of the discussed item
- An internal correspondence system between users of the system, in which metadata items are directly linked to discussion threads about the respective item
- Discussion participants are notified by email about new messages in the discussion

## Demo video

To see a demo video that explains how the Altova GDPR Compliance Database works, go to [this URL](#) at the [Altova website](#).

## This documentation

This documentation is organized into the following sections:

- [User Management](#)<sup>7</sup> shows how to configure system users and system settings via the User Management app
- [General Information about the Compliance Database](#)<sup>13</sup> describes how to set up the compliance database, terms used in the compliance database, and how to navigate the compliance database
- [GDPR Metadata](#)<sup>25</sup> explains how to enter information about your data collection processes into the compliance database
- [Approvals](#)<sup>56</sup> explains the process of approving changes made to the metadata structure of the compliance database
- [Discussions](#)<sup>62</sup> describes a feature that enables questions and suggestions about individual metadata items to be discussed internally, within the compliance database system
- [Reports](#)<sup>71</sup> documents how to generate different types of reports from the information held in the compliance database
- [Additional Features](#)<sup>77</sup> describes features that provide additional functionality, such as search filters on pages, and context-sensitive listings of changes to metadata

## 2 User Management

The compliance database has been designed to be used in a distributed way across an organization. Multiple **GDPR compliance monitors**, who are based in different departments of an organization, individually maintain parts of the organization-wide system. Together, they contribute to a single unified system that provides an overview of the organization's use of personal data.

With this design goal in mind, the Altova GDPR Compliance Database is deployed to a server, from where it is accessed and updated by its distributed users. The setup is a simple procedure, and involves the following: (i) deploying the Compliance Database to a special server, Altova's MobileTogether Server; (ii) defining authorized users of the system and other system settings; (iii) sending users their credentials and access information.

This section describes the user-management setup procedure and is organized as follows:

- [Define System Users and Settings](#) <sup>9</sup>
- [Send Access Information to System Users](#) <sup>12</sup>

### Demo video

To see a demo video that explains how the Altova GDPR Compliance Database works, go to [this URL](#) at the [Altova website](#).



## 2.1 Define System Users and Settings

The User Management app of the Compliance Database enables you to do the following:

- Create users of the Compliance Database system and configure key user properties, such as password and email.
- Define the date format that will be used in the Compliance Database.
- Define system-wide email settings.

How to create and edit these definitions is described below.

### Open the User Management app

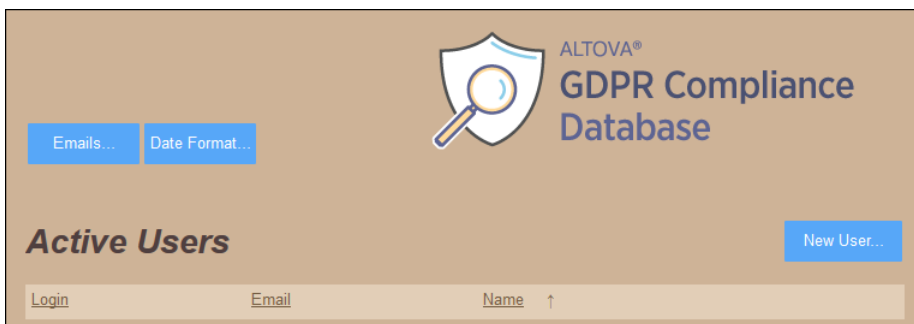
There are two ways to open the User Management App:

- Enter the URL of the app in a browser. The URL has this pattern: `http:<server-address>:8085/run?d=<path-to-compliance-database-container>`. Note that 8085 is the default port for administrator access to the server; if you have changed this default setting in the settings of MobileTogether Server, then enter the correct port. Here is an example URL: `http://127.0.0.1:8085/run?d=/public/GDPRUsers`. The URL of the app can be obtained from the *Workflows* tab (see next point).
- Access the Web UI of MobileTogether Server. (For information about how to do this, see [https://www.altova.com/manual/MobileTogether/mobiletogetherserveradvanced/mts\\_webui\\_workflows.htm](https://www.altova.com/manual/MobileTogether/mobiletogetherserveradvanced/mts_webui_workflows.htm).) Go to the *Workflows* tab and then to the container to which you deployed the `GDPRUsers.mtd` app. Locate the app in the list of deployed apps, and click the link in the app's *Run in Browser* column.

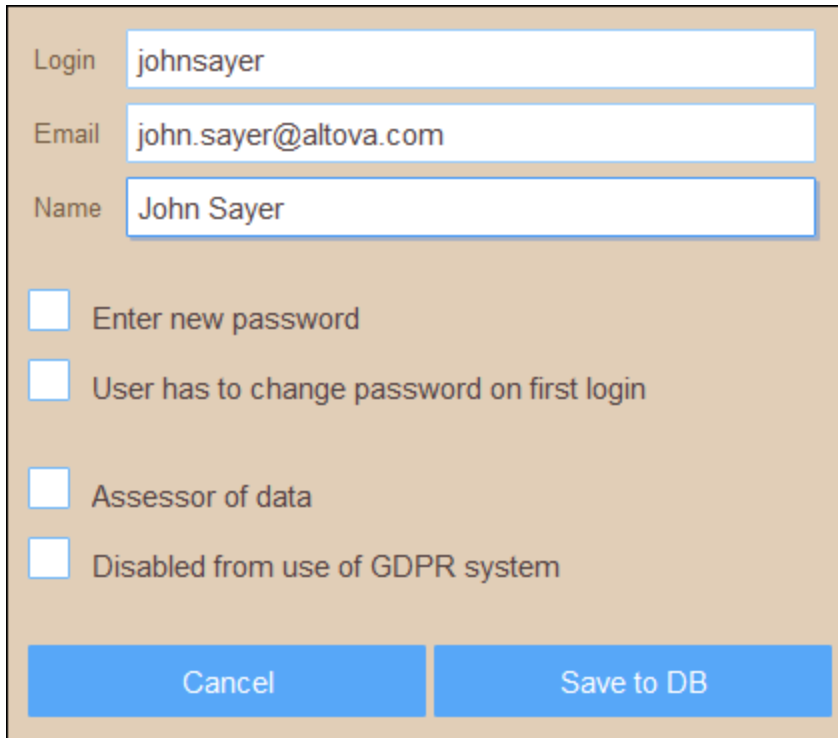
The User Management app will open in a browser.

### Adding new users and editing user properties

The interface of the User Management app will look something like the screenshot below.



To add a new user and edit the user's properties, click **New User** and, in the screen that appears (screenshot below), enter the new user's details.



The screenshot shows a user management form with the following fields and options:

- Login: johnsayer
- Email: john.sayer@altova.com
- Name: John Sayer
- Enter new password
- User has to change password on first login
- Assessor of data
- Disabled from use of GDPR system

At the bottom of the form are two buttons: "Cancel" and "Save to DB".

The following user properties can be set:

- *Login*: The login name, which can also be an email address (but see also [Email settings](#)<sup>11</sup> below)
- *Email*: An email address, in case the login is not an email address
- *Name*: The name of the user
- *Enter new password*: Check this option to enter an initial password for the user, and then enter the new password in the *Password* field that appears
- *User has to change password on first login*: Forces the user to select a password not known to the administrator
- *Assessor of data*: Specifies that the user can [authorize requests to modify the data classifications of data categories](#)<sup>56</sup>
- *Disabled from use of GDPR system*: Disables the user from using the system for as long as this setting is selected

When you are done, click **Save to DB** to finalize the addition of the user to the system.

After a user has been added, that user's properties can be modified. Clicking the **Edit** icon of that user in the opening interface window opens the user properties screen (*screenshot above*), where edits can be made and the changes saved to the Compliance Database.

### Date format and email settings

In the opening screen, there are buttons to open, respectively, a screen for date format settings and a screen for email settings.

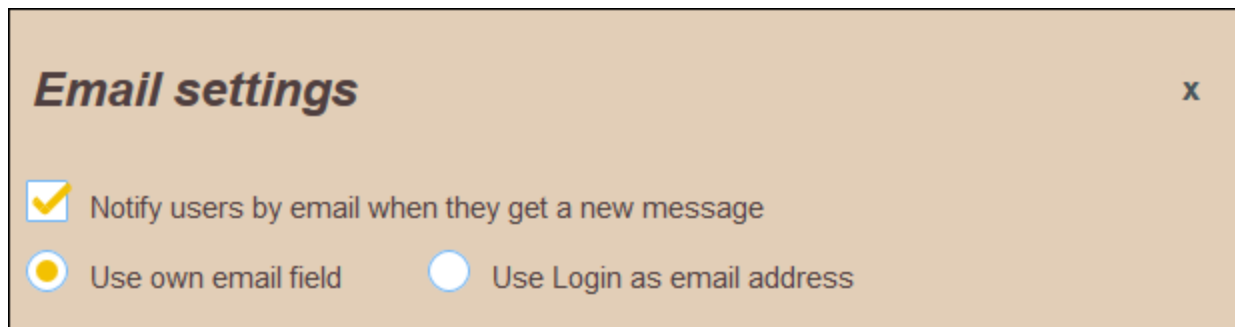
### Date format settings

The date format you specify here will be used to represent dates in the Compliance Database. First, select a date format from the available options. Next, specify the format of individual parts of the date. The first and second splitters refer to the separator between, respectively, the first and second date components, and the second and third date components. For each splitter, you can select one from a slash, period, comma, dash, or empty space, and you can optionally add extra space. Click **Save** to finalize the format.

### Email settings

The email settings screen (*screenshot below*) enables you to:

- Specify whether users are notified by email when [a new message is sent to them](#)<sup>62</sup> within the Compliance Database system.
- Set up email addresses from the *Email* property of user definitions (the default) or the *Login* property of user definitions. Note that this is a global property. As a result, email addresses for **all users** must be entered either as the value of the *Login* property or the *Email* property; they cannot be entered as the value of *Login* for some users and the value of *Email* for other users.

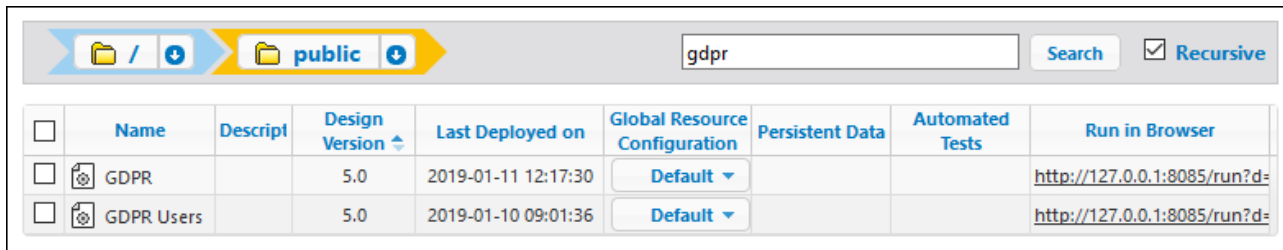


These settings can be changed at any time. Note that any change of these settings is applied as soon as you leave the screen; there is no need to explicitly save any change.

## 2.2 Send Access Information to System Users

After the Compliance Database has been deployed to the server and [configured](#)<sup>9</sup>, the URL of the Compliance Database on the server can be sent to users of the system, ideally as a link. When a user opens the resource that is stored at the URL location, the user login page of the Compliance Database is displayed, Users can now log in ([with login name and password](#)<sup>9</sup>), and use the system.

The URL of the deployed Compliance Database is displayed in the *Run in Browser* column of the Workflows tab (see *screenshot below*). This is the URL that accesses the Compliance Database, and opens the login page of the system.



<input type="checkbox"/>	Name	Descript	Design Version ↕	Last Deployed on	Global Resource Configuration	Persistent Data	Automated Tests	Run in Browser
<input type="checkbox"/>	GDPR		5.0	2019-01-11 12:17:30	Default ▾			<a href="http://127.0.0.1:8085/run?d=">http://127.0.0.1:8085/run?d=</a>
<input type="checkbox"/>	GDPR Users		5.0	2019-01-10 09:01:36	Default ▾			<a href="http://127.0.0.1:8085/run?d=">http://127.0.0.1:8085/run?d=</a>

After users in the organization have received (i) the URL of the Compliance Database and (ii) their respective access credentials, multiple users can independently access the system and update the compliance metadata.

For information about how the Compliance Database works and how to use it, see the following sections of this documentation.

### 3 General Information about the Compliance Database

This section provides an overview and outline of how the Altova GDPR Compliance Database works. It is organized into the following sections

- [Terminology](#)<sup>14</sup>: Lists key terms used in discussing GDPR, especially as these terms are used in the context of the Altova GDPR Compliance Database.
- [How the GDPR Compliance Database Works](#)<sup>17</sup>: Provides a broad outline of how the compliance database is to be used.
- [Overview Page](#)<sup>20</sup>: Explains how to navigate with reference to the Overview page, which is the central page from which all other pages may be reached.
- [Navigational Links](#)<sup>22</sup>: Provides a diagrammatic description of the navigational links between pages.
- [Metadata Relationships](#)<sup>22</sup>: Provides a diagrammatic description of the relationships between the metadata on different pages.
- [Login and Logout](#)<sup>24</sup>: How to log in and out of the compliance database

## 3.1 Terminology

The terminology used in the Altova GDPR Compliance Database is first explained in a descriptive text that shows the meaning of key terms in context. The key terms are shown in bold. These descriptive paragraphs are followed by a list of term definitions.

### Descriptive text containing explanation of key terms

**Personal data** (also called **data** for short) is collected by an organization or some such similar entity. Such an entity is known as a **data controller**—because it is solely responsible for controlling the data that it collects. A data controller is typically a commercial **company**. The collected data is stored physically in a **data storage entity** (such as a file or a database), and is used by the organization for specific purposes. For each of these purposes, the data is processed differently (usually via a computer application). Each processing method is known as a **processing activity**.

A data controller might sell or pass some of the data it collects to an external entity. The following scenarios are possible:

- If the data is sold to the external entity, then the external entity itself becomes a **data controller** of the data it bought and is responsible for the data it now has in its possession.
- If the external entity uses a processing activity to process the data for the data controller—that is, the processing activity is outsourced—then the external entity is known as a **data processor**. In this case, a contract between the two parties must specify how the data will be processed and the level of responsibility undertaken by the data processor. However, overall responsibility for the data in such cases lies with the data controller.
- If the external entity does not process the data, it is known as a **data receiver**. The data controller is responsible for data it passes to a data receiver.

In order to monitor the (personal) data that it collects, an organization might set up a GDPR system, such as the Altova GDPR Compliance Database, which uses *information about the personal data* that the organization collects, such as the type of personal data, the source of the personal data, etc. Such information about personal data is known as **GDPR metadata** (or **metadata** for short). Metadata includes: (i) information about the organizational structure of the data controller, (ii) information about the data that is collected, and (iii) information about the processing activities that process the personal data. The Altova GDPR Compliance Database provides a system for organizing and presenting GDPR metadata, thus enabling a data controller to have a continuous and thorough overview of the personal data that it has collected.

### General terms

#### Data and metadata

**Data** refers to the personal data collected by a data controller. **Metadata** refers to information about the personal data (such as the source of the personal data, departments of the organization that process personal data, etc).

#### Data controller

An entity (company, organization, person, etc) that collects or buys personal data for business, research, or other use. A data controller is responsible for protecting the data it has collected or bought, and it should maintain a system that provides an overview of all the data it has collected and stored.

### Data processor

An entity (company, organization, person, etc) that receives data from a data controller and processes it for the data controller. Typically, a data processor is a sub-contractor of a data controller, and receives data in order to provide some service to the data controller.

### Data receiver

An entity (company, organization, person, etc) that receives data from a data controller, but does not process it for the data controller.

### Data protection officer

A data protection officer is a data professional who is designated as the person responsible for ensuring that the GDPR is correctly applied and that personal data held by the organization is protected. Data protection officers are especially a requirement when the data processing involves regular monitoring of data, or large amounts of data, or sensitive data.

## Terms related to organizational structure

### Department

A department in an organization, which, in the GDPR context, processes personal data..

### Department role

Department roles are used to describe who has access to data of a specific data category. Assigning a department role rather than a specific person to a data category provides the system with a long-term resilience that is not affected by personnel changes. For example: an *Accounts department* might have the following roles: (i) *Accounting Manager*, (ii) *Accountant*, while an *IT department* might have these roles: (i) *IT Manager*, (ii) *Helpdesk Engineer*, (iii) *Security Engineer*, (iv) *Backup Engineer*. These department roles are then used to specify access to the data categories.

### Person

GDPR requires that a specific person be responsible for a specific processing activity. This relationship (between person and processing activity) is defined by associating the person with a department role. The department role is linked via a data category to the processing activity. So: *Person* --> *Department Role* --> *Data Category* --> *Processing Activity*.

## Terms related to data-processing activities

### Processing activity

An application or set of procedures that processes personal data for a specific purpose. For example, an application that sends promotional mailers to a company's newsletter recipients; it processes data of the newsletter recipients.

### Data storage entity

A physical storage system where personal data records are held. Typically, this would be a database or a file.

## Terms related to the description of personal data

### Data classification and values of a data classification

A data classification is defined by you. It is a criterion that describes some aspect of the collected data. Each data classification has its own set of allowed values. For example, one classification might indicate the relationship to the person who is the subject of the data, with possible values being *employee*, *customer*, *partner*, etc; another classification might be the type of consent obtained for collecting the subject's data, with possible values *explicit (with contract)*, *explicit (outside contract)*, *parental*, etc. Data classifications are defined for the entire system.

### Data category

You can define a data category at as broad or narrow a level as you like. For example, you can define one single customer-contact category to cover a customer's name, address, telephone number, and email address. Alternatively, this data can be described through four data categories (name, address, telephone, email), or six data categories (name, street, city, country, telephone, email). The definition of every data category consists of multiple data classifications, where each classification is given a value. The advantage of having fewer data categories is that the overall number of data classifications you will have to define will also be fewer. The disadvantage of having fewer categories is that the data might not be adequately described.

### Data usage classification and values of data usage classification

How a processing activity uses a data category is defined through **data usage classifications** (not the same as **data classifications**, which are described above). A single data category might be used by more than one processing activity, with each processing activity using the data category in a specific way. The procedure works as follows: (i) A number of data usage classifications are configured at system level, for each of which a set of allowed values are defined; (ii) When a data category is selected for a processing activity, the data category is defined by selecting one or more allowed values for each of the system's data usage classifications. For example, a data usage classification named *Data Transfer* might be configured to specify where the data of a data category will be processed: (i) within the organization's physical premises (a value of, say, *Internal processing*), or (ii) sent to an external processor (a value of, say, *External processing*). When the data category of a processing activity is defined, the appropriate value of the *Data Transfer* data usage classification is specified for this data category when it is used by that processing activity.

## Terms specific to Altova GDPR Compliance Database

### Approval request and authorization

If a data classification is added to a data category, or if an existing classification of a category is modified, then approval of the addition/modification can be requested by the person making the change. An authorized person can then approve the change. Since data categories are crucial for monitoring the data-protection requirements of the data held in the system, the approval process helps to centralize control and to keep track of changes to an important component of the system.



## 3.2 How the GDPR Compliance Database Works

The Altova GDPR Compliance Database's working mechanism can be thought of as being a user interface that provides functionality to deal with relevant aspects of the meta-information pertaining to the personal data that an organization collects. In the framework of the Compliance Database, this meta-information can be grouped into the following inter-related components:

- *Metadata*: This is information about personal data held by the organization, and it can be of two kinds. (A) Descriptive information about the data (for example: source of data, whether data is encrypted, etc.); (B) Information about how the data is related to physical aspects of the organization (for example: what is the storage medium of the data, who in the organization is responsible for the data, etc.). *Note that while data refers to the personal data collected by the organization, metadata refers to GDPR-related information that describes the personal data.*
- *Approvals*: An internal approvals system for changes made to key metadata. For example, if a user of the compliance database assesses that the encryption level of a data category needs to be changed, then that person can create an approval request directly in that data category. When a person authorized to make the change approves the request, the change is applied to the data category. Furthermore, these changes—in our example case, to the data category—are logged and can be read subsequently in the change log of that metadata item—in our example, the data category.
- *Reports*: Functionality to generate various types of reports about the metadata contained in the compliance database. For example, a report that lists the processing activities, or one that lists all the pending approval requests.
- *Administrative*: Functionality to conduct database-internal discussions of issues that may arise, and to track changes to metadata. For example, if a user has a question about the protection level of data in the *Billing Address* data category, then the user can initiate a discussion from within the *Billing Address* data category and invite selected users to participate in the discussion. The invited participants can be automatically notified by email. Discussions are grouped under their respective metadata items and can be viewed subsequently. Note also that a discussion about, say, a data category, will not only be listed under that data category; it will also be listed at higher levels: (i) under all data categories, and (ii) all metadata items of the compliance database.

The Altova GDPR Compliance Database implements these goals through a network of pages that serve as input and/or display mechanisms for metadata or for the other functionality listed above.

### Metadata input and display

A number of the compliance database's pages provide an interface for entering and displaying metadata. The metadata that is entered in these pages builds a network of relationships across pages, and this provides the metadata with an internally coherent structure. Consequently, a major part of the work related to the compliance database is to enter the relevant metadata; the internal linkages are built automatically.

The following metadata is used to build up the compliance database

- *Company Information*
  - Departments<sup>15</sup>: The departments in the company that process personal data. Within each department, roles are created. For example, within the Accounting department, two possible roles are *Salaries* and *Sales revenues*. A role can be associated with one or more persons. A role is also associated with one or more processing activities. A department role thus builds a relationship between a processing activity and a person. In order to specify that a certain person is involved in a certain processing activity, the person is assigned to the relevant department role. In this way, personnel changes are easily accommodated.

- [Persons](#)<sup>15</sup>: Contact data and description of company personnel who are involved in processing personal data. Each person is assigned to a department and to a role in that department.
- Data information
  - [Data Classifications](#)<sup>15</sup>: These are the criteria that you will define and that will be used across the system to describe data. For example: the encryption level of a piece of data can be a data classification. In a specific data category, the encryption data classification is given a specific value (for example: *No encryption required*).
  - [Data Usage Classifications](#)<sup>15</sup>: These are criteria that specify how a data category will be used by a processing activity. For example: a data usage classification might specify the location where a certain processing activity processes a certain data category (for example: in-house or externally). Multiple data usage classifications are defined at the system level. When defining how a processing activity processes a data category, each relevant data usage classification of the processing activity is given a value. These values describe aspects of how that processing activity processes a given data category.
  - [Data Controllers, Processors, Receivers](#)<sup>14</sup>: Contact information and description of external entities with which the company shares collected data in any way. If the external entity processes data for the company, it is linked to the company via the relevant processing activity.
- Data properties and relationships
  - [Data Categories](#)<sup>15</sup>: A data category defines the data that is collected. For example, you can define a data category that describes customer address data. The data category definition consists of the data classifications of the system, with each data classification being given a specific value. For example, the data category for customer addresses can be defined so that the data classification that describes the source of this address data is set to a value of something like *Online customer submission*.
  - [Data Storage Entities](#)<sup>15</sup>: This metadata is applied to a data category and defines the type and location of the physical data storage facility that is used to hold data that belongs to the specified data category. For example, a data category of customer address can specify that the data storage entity of this category's associated data is a file at a specific URL.
  - [Define Processing Activities](#)<sup>15</sup>: A processing activity typically processes multiple data categories. For each of these data categories, the values of the system's data usage classifications describe how this data category is processed. For example, consider that (i) there exists a processing activity named *Frequent Buyer*, which processes a data category named *Customer's Monthly Income*, and (ii) there exists a mandatory data usage classification in the system named *Purpose of processing*. This data usage classification, since it is mandatory, will appear in the definitions of all data categories that are assigned to any processing activity, and will need to be given a specific value in each data-category definition. For example, the *Purpose of processing* data usage classification of our example could be given a value of *EU law*. This indicates the purpose of processing of the *Customer's Monthly Income* data category, when this data category is processed by the *Frequent Buyer* processing activity.

For a description of how to enter metadata, see the section [GDPR Metadata](#)<sup>25</sup>.

## Approvals

The most important meta-information about a processing activity (that processes personal data) is the data category of the data that is processed. When a change is made to a data classification of a data category, the change can be submitted with an approval request. The approval request is logged within the compliance database, and can be approved by an authorized person.

The Approvals mechanism enables oversight, as well as keeps track of changes made to the structure of the metadata. See [Approvals](#)<sup>56</sup> for a description of the Approvals system.

## Reports

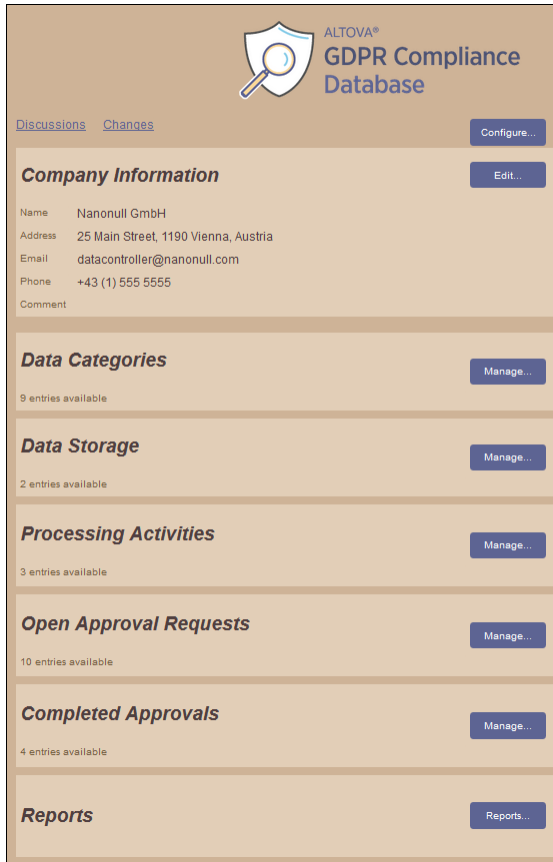
The compliance database enables the following reports to be generated: (i) about metadata, on the basis of [processing activities](#)<sup>14</sup>, and (ii) about approval status of a category's classifications. See the section [Reports](#)<sup>71</sup> for information.

## Administrative

The compliance database provides functionality to track changes to metadata and to search for text on compliance database pages. These are described in the section [Additional Features](#)<sup>77</sup>.

### 3.3 Overview Page

On successfully logging in, the compliance database's **Overview** page is displayed. This page provides links to all the other pages of the compliance database, and is therefore central to navigating the compliance database.



The Overview page provides links to the following pages:

- **Configuration page:** For defining (i) the organization's departments, (ii) the persons responsible for maintenance of data, (iii) data classifications that will be used to build data categories, (iv) data usage classifications, and (v) external entities that process data for the organization. Click **Configure** at top right to go to the Configuration page.
- **Data Categories page:** Lists the data categories that are used to specify properties of the data that processing activities process (processing activities are applications that process personal data). Via this page you can add, modify, and delete data categories. On the Overview page, click the items's **Manage** button (see screenshot above) to go to the Data Categories page.
- **Data Storage page:** Lists the organization's data repositories. Via this page you can add, modify, and delete data repositories. On the Overview page, click the items's **Manage** button (see screenshot above) to go to the Data Storage page.
- **Processing Activities page:** Lists processing activities (which are applications that process personal data). On this page you can add, modify, and delete processing activities. On the Overview page, click the items's **Manage** button (see screenshot above) to go to the Processing Activities page.

- *Open Approval Requests and Completed Approvals pages*: Lists, respectively, (i) approvals that have been requested but not authorized, and (ii) approvals that have been authorized. On the Overview page, click the respective item's **Manage** button (see screenshot above) to go to the respective page.
- *Reports page*: Provides links to configure and generate different types of reports.
- *Discussions page*: Shows all discussions carried out within the system. On the Overview page, click **Discussions** at top left (see screenshot above) to go to the Discussions page.
- *Changes page*: Shows all modifications to information held in the system. On the Overview page, click **Changes** at top left (see screenshot above) to go to the Changes page.

### Returning to the Overview page

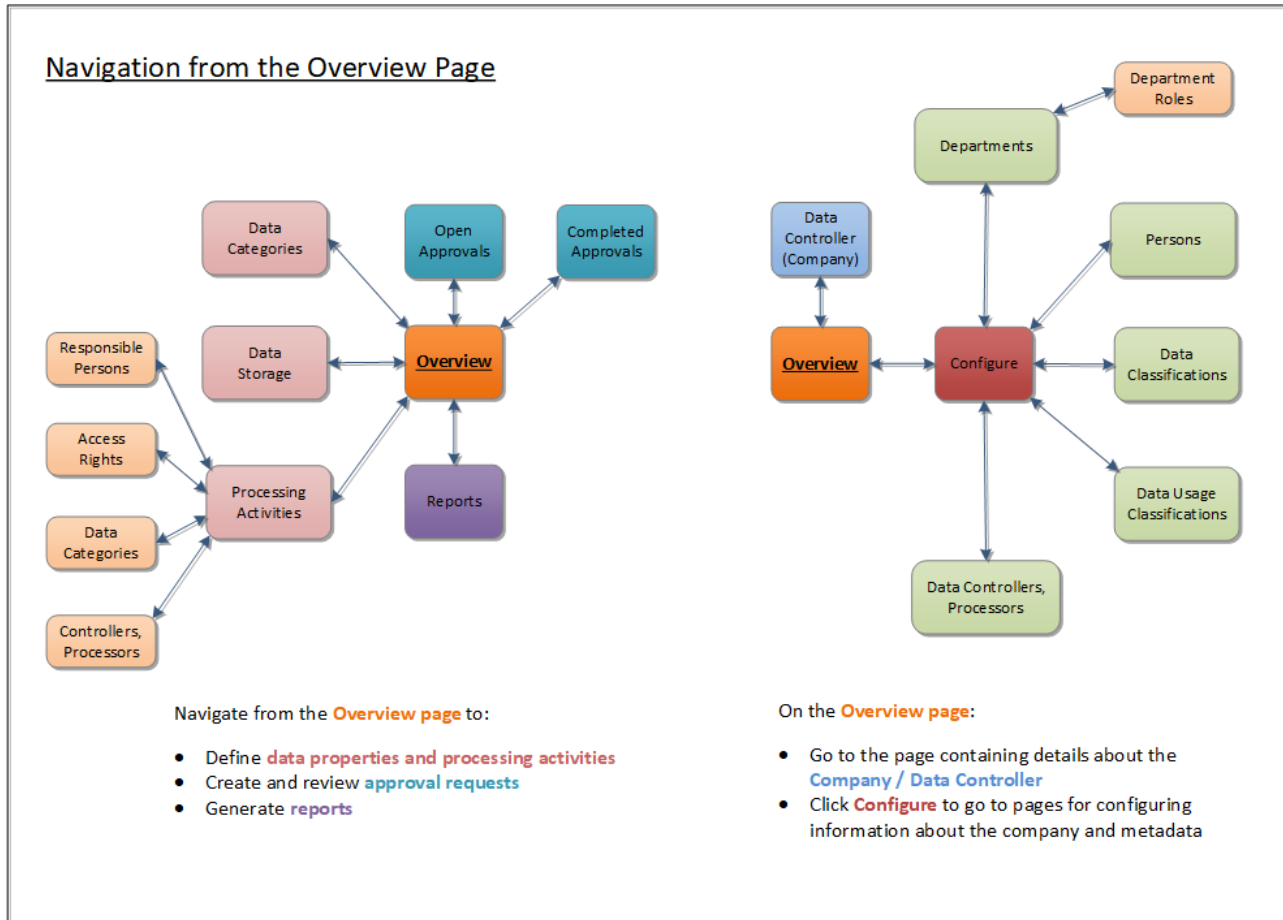
Since the Overview page is the access point for all pages, you must often return to the Overview page in order to navigate to another page of the compliance database. To return to the Overview page, click **Back** at the top right of the page that you are on. If the page you are on is twice removed from the Overview page, then click **Back** twice to return to the Overview page. For a diagram of links to navigate the pages of the compliance database, go to the section [Navigational Links](#)<sup>22</sup>.

### Logging out of the system

At the bottom of the Overview page will be a line: *You are logged in as <User Name>*. Click the user name and, then, **Yes** to log out.

## 3.4 Navigational Links

The diagram below shows how the pages of the compliance database are linked, starting from the Overview page.

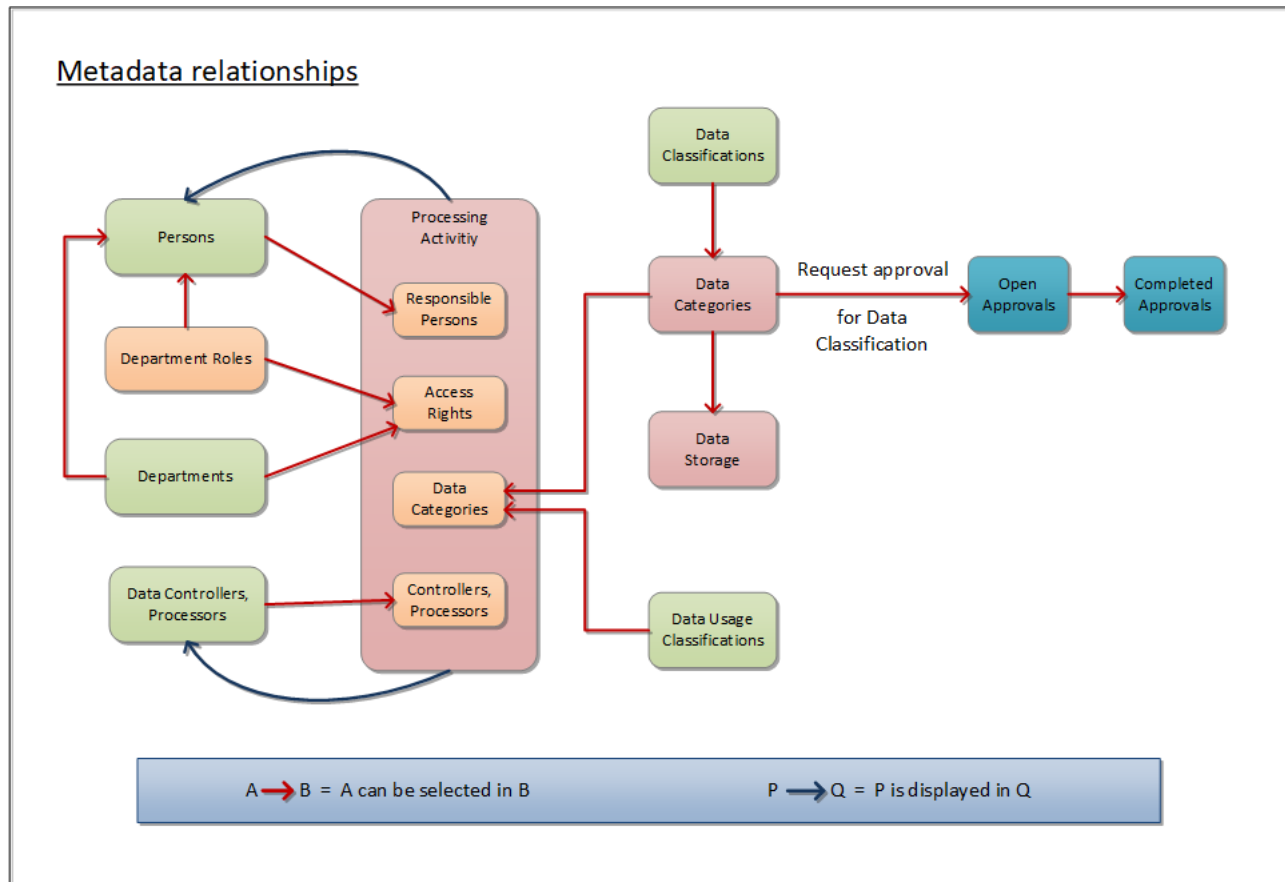


The Overview page is the central page for navigation:

- From the Overview page, you can go to a page to edit information about the data controller (your company).
- On the Overview page, you can click the **Configure** button to go the Configuration page, where you can configure information about the company (persons, departments, and department roles) and metadata (data classifications, data usage classifications, and data controller, processors and receivers).
- From the Overview page you can go to pages for defining data categories, data storage systems, and processing activities.
- The Overview page also provides access to pages where approvals can be viewed and displayed, and where reports can be configured.

### 3.5 Metadata Relationships

The relationships between metadata on different pages of the compliance database are shown in the diagram below.



These relationships are built up as follows:

- Metadata is entered in the respective pages. For example: the departments of a company, the roles of a department, and the persons of a company.
- When certain kinds of metadata are being defined, other metadata that is relevant for the definition and that has already been entered is available for selection in the definition's parameters. For example, when a person is being defined, the departments that have already been entered will be available for selection. The person is thus defined to belong to the selected department: a relationship is built automatically. This relationship, where one type of metadata is available for selection in another, is shown with red arrows in the diagram above.
- Once the network of relationships has been built, one type of metadata is displayed reflexively in other types of metadata. This type of relationship is shown with blue arrows in the diagram above. For example, once a person has been selected as the responsible person of a processing activity, then that processing activity is automatically displayed in the definition of that person.

## 3.6 Login and Logout

### Logging in

The Login screen is the first screen that is displayed when the GDPR Compliance Database is started. Enter your user name and password, and then click **Login**.

### Logging out

To log out of the system, do the following:

1. Go to the [Overview page](#)<sup>20</sup>.
2. At the bottom of the page will be a line: *You are logged in as <User Name>*. Click the user name and, then, **Yes** to log out.



## 4 GDPR Metadata


As described in the topic [How the Compliance Database Works](#)<sup>17</sup>, an important part of building up a GDPR compliance system with the Altova GDPR Compliance Database is to enter the relevant GDPR metadata. (Note that while data refers to the personal data collected by the organization, metadata refers to GDPR-related information that describes the personal data.) This metadata comprises not only information about the personal data that is being collected, but also information related to the structure of the organization collecting the personal data: the departments, persons, external entities, and storage locations involved with the processing of personal data held by the organization.

This metadata is entered via different pages of the compliance database, and the different pieces of information are built up by the compliance database into an internally held network of metadata relationships. This section describes how to enter these different items of related metadata. It is structured as follows:

- [Information about the company](#)<sup>26</sup> (the data controller)
- [Company information](#)<sup>27</sup>, which consists of [departments that process personal data](#)<sup>28</sup>, and [people in these departments](#)<sup>31</sup> who are responsible for the data and metadata
- [Information about the collected data](#)<sup>35</sup>: this information is structured by identifying and defining [data classifications](#)<sup>36</sup>, each of which is a criterion for describing personal data. Additionally, information about any [external data processor](#)<sup>42</sup> that uses the collected data in any way is also recorded
- Data categories are needed so that the data used by each [processing activity](#)<sup>14</sup> can be properly described. A [data category is defined](#)<sup>45</sup> by assigning specific values for the data classifications that comprise the category.
- [Data storage entities](#)<sup>49</sup> define the physical aspect of data storage, such as location and medium
- The [Processing Activities section](#)<sup>52</sup> describes how processing activities (applications that process personal data) are defined

## 4.1 Define the Company

The Company Information item contains information about the entity (company, organization, person, etc) that is collecting or processing the personal data that you want to place under GDPR compliance. Note that companies can be [data collectors](#)<sup>14</sup> in some processing activities and [data processors](#)<sup>14</sup> in others.



<b>Company Information</b>		Edit...
Name	Nanonull GmbH	
Address	25 Main Street, 1190 Vienna, Austria	
Email	datacontroller@nanonull.com	
Phone	+43 (1) 555 5555	
Comment		

To enter or edit information about your company, go to the Overview page, click the **Edit** button of the Company Information item (see *screenshot above*) and edit information in the screen that appears. Click **Save** when done.

## 4.2 Configure Company Information

This section describes how to configure company-related information that will be used in defining various aspects of the GDPR compliance system:

- On the [Departments](#) <sup>28</sup> page, you can configure the various departments that are involved in maintaining or processing personal data.
- On the [Persons](#) <sup>31</sup> page, you can configure the persons who are involved in maintaining or processing personal data. Each person is assigned to a department and a department role.









To access these two pages, do the following:

1. On the [Overview page](#) <sup>20</sup>, click **Configure**. The Configuration page appears.
2. In the Company Information section of the Configuration page (*screenshot below*), click the respective **Manage** button of the *Departments* or *Persons* item.



### Example

In this section, we will show how to configure information about the company's [departments](#) <sup>28</sup>, [department roles](#) <sup>28</sup>, and [persons](#) <sup>31</sup> that are involved with the personal data collected by the company. In our example company, named Nanonull GmbH, we first create four departments (*Accounting; Human Resources; IT; Sales & Marketing; see screenshot below*), each having one or two department roles (as shown in the screenshot below), making for a total of seven department roles.

Departments		X	New Department...
Department	Description		
	Comment		
Accounting	Management of company finances		
Roles in Accounting			
Salaries	Payroll management		
Sales Revenues	Accounting of sales revenues		
Human Resources	Responsible for employee affairs		
Roles in Human Resources			
Employee Data	Personal data of company employees		
IT	Maintainence of company network and IT resources		
Roles in IT			
Network and Technology	Manage computer and network resources		
Software	Manage internal software resources		
Sales & Marketing	Building and maintaining customer and partner relationships		
Roles in Sales & Marketing			
Customer DB	Maintenance of customer database		
Mailers	Sending promotional emails		

After that, we create entries for [persons](#)<sup>31</sup> who are involved with the personal data collected by the company. (This involvement could be in the form of data maintenance or processing of data.) Note that the entries for persons are at a company-wide level. Each person is then associated with (i) a department, and (ii) a department role. After the association between a person and a department role is made, the person will be listed in the respective department as being assigned to the selected department role. In our example, we create six persons and assign them to six different department roles (see the [Persons](#)<sup>31</sup> section).

### 4.2.1 Departments

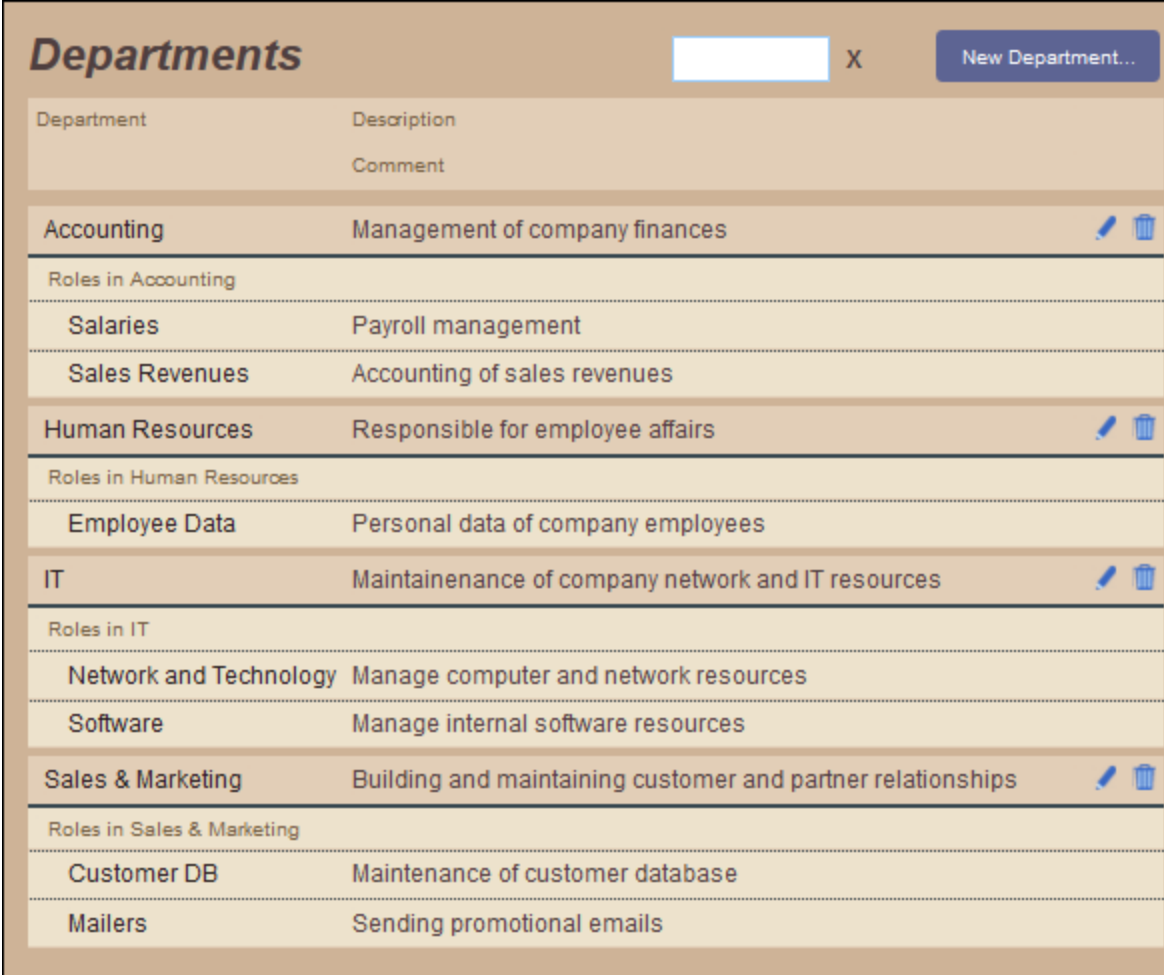
All departments that are involved with the processing of personal data should be added to the compliance database. Each department must have department roles, which are functions that are carried out in the department. The department roles that are of significance to the compliance database are those that involve the use of personal data. For example, in the Accounting department, one role that uses personal data would be that for processing salaries (personal data of employees); another might be that for maintaining the accounts of sales revenues (personal data of customers).









Note that access rights to the [data categories of a processing activity](#)<sup>52</sup> are specified by way of department roles. This is significant because persons are assigned to department roles. These associations build a relationship between persons and processing activities: *Person --> Department Role --> Data Category --> Processing Activity*. An important point to note is this: Since persons are not directly assigned access rights to data categories—but indirectly via department roles—personnel changes in the company will require only minimal updates of the compliance database (namely, in the definition of Persons only).

## Create/edit Department information

To create/edit Department information, do the following:

1. On the Overview page, click **Configure**.
2. On the Configuration page that appears, click the **Manage** button of the Departments item. The Departments page (*screenshot below*), which lists all the defined departments, is displayed.



Department	Description	
Accounting	Management of company finances	 
Roles in Accounting		
Salaries	Payroll management	
Sales Revenues	Accounting of sales revenues	
Human Resources	Responsible for employee affairs	 
Roles in Human Resources		
Employee Data	Personal data of company employees	
IT	Maintainance of company network and IT resources	 
Roles in IT		
Network and Technology	Manage computer and network resources	
Software	Manage internal software resources	
Sales & Marketing	Building and maintaining customer and partner relationships	 
Roles in Sales & Marketing		
Customer DB	Maintenance of customer database	
Mailers	Sending promotional emails	

3. To create a new department, click **New Department**. To edit a department's information or delete a department, click the department's **Edit** or **Delete** icon, respectively.

## Edit Department information

When you click **New Department** or the **Edit** icon of a department, the individual department's screen is displayed. Here you can edit information about the department (*see screenshot below*).

### Department Accounting

Save

#### Name & Description

Name

Description

Comment

#### Department Roles

New Role...

Name	Description	Comment
Salaries	Payroll management	✎ 🗑
Persons assigned to Salaries role		
Barbara Hofer		
Processing activities accessible by Salaries role		
Employee Salaries	Contracted to 123 Paychecks GmbH	
Sales Revenues	Accounting of sales revenues	✎ 🗑
Persons assigned to Sales Revenues role		
Annette Wenz		
Processing activities accessible by Sales Revenues role		
Invoices	Creates and sends invoices for custom	Invoices exported to accounting system

The department must have at least one *Role* property (since it is in at least one role that a department fulfills its function as a user of personal data). Add a new role by clicking **New Role** (*see screenshot above*). To edit or delete a role, click its **Edit** or **Delete** icon, respectively. Click **Save** when done. In the screenshot above, the Accounting department has two roles: *Salaries* and *Sales Revenues*.

**Note:** The department role/s to which a person is assigned is defined as a [property of the Person](#)<sup>31</sup>.

### Relationships with other metadata

A **department** has the following relationships with other metadata:

It can be selected for...	Which sets up...
<a href="#">Persons</a> <sup>31</sup>	The department to which a person belongs.
<a href="#">Processing activity &gt; Access rights</a> <sup>52</sup>	Which departments have access rights to the processing activity.

A **department role** has the following relationships with other metadata:

It can be selected for...	Which sets up...
<a href="#">Persons</a> <sup>31</sup>	The department role to which a person is assigned. The person is displayed reflexively in the department role (see <i>screenshot above</i> ).
<a href="#">Processing activity &gt; Access rights</a> <sup>52</sup>	Which department roles have access rights to the processing activity. The processing activity is displayed reflexively in the department role (see <i>screenshot above</i> ).

## 4.2.2 Persons

All persons that are involved with the use of personal data should be added to the compliance database. A person must be assigned to a department and a department role so that the compliance database's information can be properly structured. There are two types of person:

- *Responsible persons:* A responsible person is assigned to a processing activity and is responsible for: (i) how it works, (ii) determining who has access to relevant data, (iii) any other matters related to the processing activity. These are the persons who are relevant for GDPR conformance reports. They are assigned to department roles.
- *Users of personal data:* This information is not relevant for GDPR conformance reports but provides a convenient overview of the roles of persons in each department; it also indirectly indicates—via associated processing activities—to which data these persons have access. Just as for responsible persons, users are assigned to department roles.

If a department role is assigned to a processing activity, it means that the persons in this department role will have access to the data used by the processing activity. In the compliance database, the description of a department lists each department role together with the persons assigned to the respective department roles (see [Departments](#)<sup>28</sup>).

#### Example

If (i) a person in the Accounting department is assigned to that department's *Salaries* role, and (ii) the *Salaries* department role is assigned to the *Employee Salaries* processing activity, then that person has access to the

data used by the *Employee Salaries* processing activity. If, additionally, this person is defined as a *Responsible Person* of the *Employee Salaries* processing activity, then this person is accountable for the *Employee Salaries* processing activity and protection of the data used by *Employee Salaries*.

In our example, we create six persons and assign them to six different department roles (see screenshots below).

## Create/edit Person information

To create/edit Person information, do the following:

1. On the Overview page, click **Configure**.
2. On the Configuration page that appears, click the **Manage** button of the Persons item. The Persons page (screenshot below), which lists all the defined persons of the entire organization, is displayed.



Name	Role (Department)	E-mail	Phone
Annette Wenz	Sales Revenues (Accounting)	annette.wenz@nanonull.com	341
Barbara Hofer	Salaries (Accounting)	barbara.hofer@nanonull.com	345
Jason Brown	Network and Technology (IT)	jason.brown@nanonull.com	856
Jaya Okri	Employee Data (Human Resources)	jaya.okri@nanonull.com	712
Niki Devgood	Customer DB (Sales & Marketing)	niki.devgood@nanonull.com	423
Robert Arroz	Mailers (Sales & Marketing)	robert.arroz@nanonull.com	454

3. To create a new person, click **New Person**. To edit a person's information or delete a person, click the person's **Edit** or **Delete** icon, respectively.

## Edit Person information

When you click **New Person** or the **Edit** icon of a person, the individual person's screen is displayed, in which you can edit the person's information (see screenshot below).



## Person

Save

### Personal Data

Name

Department  <

Role  <

Comment

E-mail

Phone

Data Protection Officer

### Responsible for Processing Activities

Name	Description
	Comment
Invoices	Creates and sends invoices for customer orders <i>Invoices exported to accounting system</i>

A Person item has the following properties:

- *Department*: Select one from existing departments, or create and select a new department
- *Role*: Select one from existing roles of the selected department, or create a new role for the selected department and select it.
- *Email and phone*: These are optional.
- *Data Protection Officer*: A data protection officer is a designation that indicates persons who are responsible for designing and maintaining data protection processes for data.

Click **Save** when you finish. In the [department's description](#) <sup>28</sup>, this person is now shown as being assigned to that department role.

**Note:** If a person is responsible for a certain processing activity, then this is defined as a [property of the respective processing activity](#)<sup>52</sup>.

### Relationships with other metadata

A **person** has the following relationships with other metadata:

It selects...	Which sets up...
<a href="#">Departments</a> <sup>28</sup>	The department to which a person belongs.
<a href="#">Department roles</a> <sup>28</sup>	The department role to which a person is assigned. A person is then displayed reflexively in the respective <a href="#">department role</a> <sup>28</sup> .

It can be selected for...	Which sets up...
<a href="#">Processing activity &gt; Responsible person</a> <sup>52</sup>	Which persons have responsibility for the processing activity. Once a person is selected, the processing activity appears reflexively as part of the information about the person.

## 4.3 Configure Data Information

This section describes how to configure key data-related information that will be used for describing the data processing activities of the company (data controller):

- [Data Classifications](#)<sup>36</sup> are created to describe a specific property of the collected personal data. As such, a classification is a piece of metadata about the data. Each classification is defined with a set of allowed values. The classifications are used to compose [data categories](#)<sup>45</sup>, which in turn indicate the kind of data that a [processing activity](#)<sup>52</sup> uses.
- [Data Usage Classifications](#)<sup>39</sup> are created, each with its own set of allowed values, to describe [how a processing activity uses its data categories](#)<sup>52</sup>. For each data category, one set of data usage classifications defines how the relevant processing activity uses that data category.
- [Data Processors](#)<sup>42</sup> are external entities that provide data-processing services.

The three items of data information listed above are configured via their respective pages. To access these pages, do the following:

1. On the [Overview page](#)<sup>20</sup>, click **Configure**. The Configuration page appears.
2. In the Data Information section of the Configuration page (*screenshot below*), click the respective **Manage** button of the *Data Classifications*, *Data Usage Classifications*, or *Data Processors* item.



### Example

In this section, we will show to configure data information about our example company, Nanonull GmbH. We will configure the following:

- Eight [data classifications](#)<sup>36</sup> and the allowed values of each. We will define six of these classification to be mandatory in data categories and two to be able to have multiple values.
- Six [data usage classifications](#)<sup>39</sup> and the allowed values of each. All six classifications are mandatory (when defining the [usage of a data category by a processing activity](#)<sup>52</sup>) and three allow multiple entries.

- Two [data processors](#)<sup>42</sup> named 123 Paychecks and Acme Invoice Management, which, respectively, create employee paychecks and customer invoices and export these to the accounting system of Nanonull GmbH.

### 4.3.1 Data Classifications

A data classification is a criterion that describes some aspect of the collected personal data. As such, a classification is a piece of metadata about the data. Each classification is defined with a set of allowed values. For example, one data classification might be about the *subject* of the collected data (with possible values being: employee, customer, partner, etc); another classification might be the type of consent obtained for collecting the subject's data (where values could be: explicit, parental, etc). Each data classification has its own set of allowed values. You can create your own classifications, and for each classification you can create suitable values.

All the data classifications that are defined for the compliance database are used to build up individual **data categories**. If a data classification has been defined to be mandatory, then that data classification must be assigned a value when the classification is used in the definition of a data category. If a data classification has been defined as being not mandatory, then no value needs to be defined for it when the classification is used in the definition of a data category. So, say that eight data classifications have been defined, of which six are mandatory. In this case, for each data category in the compliance database, the eight data classifications will be displayed and available for use in the category's definition. The classification is used by specifying a value for it in the category's definition. You must define a value for the six mandatory classifications, and you may define values for the non-mandatory classifications. How to build a data category is described in the section [Define Data Categories](#)<sup>45</sup>.

#### Manage data classifications

The Data Classifications page (*screenshot below*) enables you to manage data classifications: that is, (i) to create a new data classification (by clicking **New Classification**), (ii) to edit a data classification (by clicking the **Edit** icon of a classification), and (iii) to delete a data classification (by clicking the **Delete** icon of a classification).

Name	Description	mandatory	multiple entries allowed		
Data Subjects	Which group of individuals is the focus of this data category	yes			
Encryption	With what encryption method is this data category stored		yes		
Protection Measures	Technical and/or organizational measures to protect this data category	yes	yes		
Risk	What is the risk in case a security breach occurs	yes			
Source of Data	What is the source of this data	yes			
Storage duration	How long should the data for this data category be stored	yes			
Type of Consent	Which kind of consent (if any) was obtained for this data category				
Type of Data	If this is personal data, what type of personal data	yes			

When you add a new classification or edit a classification, a page with the classification's definition is displayed (see below). On this page, you can edit the definition of the selected data classification.

### Edit a data classification

The definition of a data classification consists of two parts (see screenshot below): (i) fields that describe and comment on the classification, and (ii) a list of the values of the classification.

## Data Classification Save

### Classification Description

Name

Description

Comment

Mandatory value
  Multiple values allowed
  Obsolete

---

### Classification Values New Value

Value	Description	Obsolete	
<input style="width: 95%; border: 1px solid #ccc;" type="text" value="Data Subject"/>	<input style="width: 95%; border: 1px solid #ccc;" type="text" value="Data was provided by data subject."/>	<input type="checkbox"/>	+ -
<input style="width: 95%; border: 1px solid #ccc;" type="text" value="Public Source"/>	<input style="width: 95%; border: 1px solid #ccc;" type="text" value="Data was collected from public source."/>	<input type="checkbox"/>	+ -
<input style="width: 95%; border: 1px solid #ccc;" type="text" value="Purchased"/>	<input style="width: 95%; border: 1px solid #ccc;" type="text" value="Data was purchased from commercial source."/>	<input type="checkbox"/>	+ -
<input style="width: 95%; border: 1px solid #ccc;" type="text" value="Data Controller"/>	<input style="width: 95%; border: 1px solid #ccc;" type="text" value="In case or Data Processor date comes from other data controller."/>	<input type="checkbox"/>	+ -

Note the following:

- If you want a data classification to be mandatory in the definition of a data category, check the classification's *Mandatory value* check box. If a classification is mandatory, then a value must be selected for this data classification in every data category.
- If a data classification can take multiple values—for example, if multiple levels of data protection are available—then check the *Multiple values allowed* check box. This enables multiple values to be specified for this data classification when it is used in the definition of a data category.
- If a data classification is marked as *Obsolete* (in the *Classification Description* pane), then that classification is not available for selection in new data categories, that is, in data categories that are created new after the classification is marked as obsolete. Data categories that were created prior to the classification being marked as obsolete will continue to have the classification in its definition.
- To append a classification value, click **New value** (see *screenshot above*) and, in the new field that appears, enter the value and a description of it. Alternatively, to insert a value above an existing value, click the **Plus** icon of the existing value. You can enter as many classification values as you like. The values defined here are the allowed values. One value (or more, if multiple values are allowed; see *above*) can be selected when the data classification is used in the definition of a category.
- If a value is marked as *Obsolete*, then that value cannot be selected from this point onwards in both existing data categories and new data categories.
- After you finish editing a data classification, click **Save** to save the changes.

### Relationships with other metadata

A **data classification** has the following relationships with other metadata:

It can be selected for...	Which sets up...
<a href="#">Data categories</a> <sup>45</sup>	The availability of classifications in the definition of data categories. A classification can be mandatory and can have multiple values. Classification values are selected in the category definition.

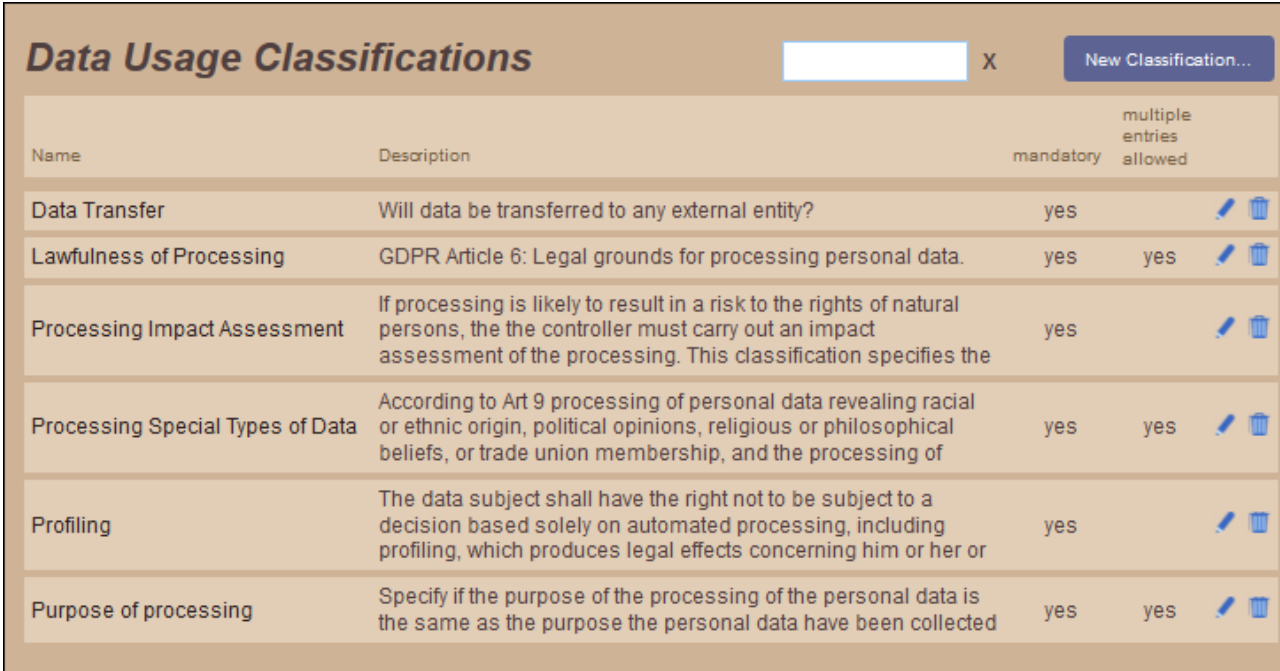
## 4.3.2 Data Usage Classifications













How a processing activity uses a data category is defined through **data usage classifications**. A single data category might be used by more than one processing activity, with each processing activity using the data category in a different way. The procedure works as follows: (i) A number of data usage classifications are configured at system level, for each of which a set of allowed values are defined; (ii) When a data category's usage by a processing activity is defined, one or more allowed values for each data usage classification are selected.

In this section, we describe how to configure the system-level data usage classifications. For a description of how to assign a value to a data usage classification when a data category's usage by a processing activity is defined (its usage definition), see the section [Define Processing Activities](#)<sup>52</sup>.

## Manage data usage classifications

The Data Usage Classifications page (*screenshot below*) enables you to manage data classifications: that is, (i) to create a new data classification (by clicking **New Classification**), (ii) to edit a data usage classification (by clicking the **Edit** icon of a classification), and (iii) to delete a data usage classification (by clicking the **Delete** icon of a classification).



Name	Description	mandatory	multiple entries allowed	
Data Transfer	Will data be transferred to any external entity?	yes		 
Lawfulness of Processing	GDPR Article 6: Legal grounds for processing personal data.	yes	yes	 
Processing Impact Assessment	If processing is likely to result in a risk to the rights of natural persons, the the controller must carry out an impact assessment of the processing. This classification specifies the	yes		 
Processing Special Types of Data	According to Art 9 processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of	yes	yes	 
Profiling	The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or	yes		 
Purpose of processing	Specify if the purpose of the processing of the personal data is the same as the purpose the personal data have been collected	yes	yes	 

When you add a new classification or edit a classification, a page with the classification's definition is displayed (*see below*). On this page, you can edit the definition of the selected data usage classification.

## Edit a data usage classification

The definition of a data usage classification consists of two parts (*see screenshot below*): (i) fields that describe and comment on the classification, and (ii) a list of the values of the classification.



### Data Usage Classification Save

---

#### Classification Description

Name

Description

Comment

Mandatory value
  Multiple values allowed
  Obsolete

---

#### Classification Values New Value

Value	Description	Obsolete	
<input style="width: 100%;" type="text" value="Not necessary"/>	<input style="width: 100%;" type="text" value="No high risk is associated with data processing"/>	<input type="checkbox"/>	+ -
<input style="width: 100%;" type="text" value="Possibly necessary"/>	<input style="width: 100%;" type="text" value="This data processing must be assessed in detail to decide if impact assessment is necessary (GDPR Art 35)"/>	<input type="checkbox"/>	+ -
<input style="width: 100%;" type="text" value="Required"/>	<input style="width: 100%;" type="text" value="Required due to supervising authority decision according to GDPR Art 35 (4)"/>	<input type="checkbox"/>	+ -
<input style="width: 100%;" type="text" value="Not Required"/>	<input style="width: 100%;" type="text" value="Not required due to supervising authority decision according to GDPR Art 35 (5)"/>	<input type="checkbox"/>	+ -

Note the following:

- If you want a data usage classification to be mandatory (in the definition of the usage of a data category by a processing activity), check the classification's *Mandatory value* check box. If a classification is mandatory, then a value must be selected for this data usage classification when defining the usage of every data category.
- If a data usage classification can take multiple values—for example, when describing on what grounds health-related or race-related data may be legally processed—then check the *Multiple values allowed* check box. This enables multiple values to be specified for this data usage classification when it is used in the definition of a data category's usage by a processing activity.

- If a data usage classification is marked as *Obsolete* (in the *Classification Description* pane), then that classification is not available for selection in new definitions of the usage of data categories in processing activities. Usage definitions that were created prior to the classification being marked as obsolete will continue to have the classification in its definition.
- To append a classification value, click **New value** (see *screenshot above*) and, in the new field that appears, enter the value and a description of it. Alternatively, to insert a value above an existing value, click the **Plus** icon of the existing value. You can enter as many classification values as you like. The values defined here are the allowed values. One value (or more, if multiple values are allowed; see *above*) can be selected when the classification is used in the definition of a category's usage by a processing activity.
- If a value is marked as *Obsolete*, then that value cannot be selected from this point onwards in both existing usage definitions and new usage definitions.
- After you finish editing a data usage classification, click **Save** to save the changes.

### Relationships with other metadata

A **Data usage classification** has the following relationships with other metadata:

It can be selected for...	Which sets up...
<a href="#">Processing activity &gt; Data categories</a> <sup>52</sup>	The definition of the data category's usage by the processing activity.

## 4.3.3 Data Processors

A data processor is an agent that processes personal data for the data controller, typically to provide a service. Data processors are listed and managed on the Data Processors page (*screenshot below*). Here, new data processors can be added (click **New Data Processor**), and information about existing data processors can be edited (click the **Edit** icon of a data processor). Both actions open the definition page of the relevant data processor (respectively, a new data processor or an existing one); see *below*. To delete a data processor, click its **Delete** icon.

Name	Description	Domain
123 Paychecks GmbH	Processes Nanonull employee salaries	EU
Acme Invoice Management	Processes invoices of Nanonull GmbH	EU

**Note:** If a data processor buys the data it processes, or in some other way becomes responsible for it, then it is a data controller and is responsible for the protection of that data. This role (data controller or data processor) is selected for a data processor when the data processor is selected in the [definition of a processing activity](#) <sup>52</sup>.

### Edit data processor

The definition page of a data processor (*screenshot below*) consists of two panes: (i) a pane in which you enter and edit information about the data processor; (ii) a pane that lists the processing activities the data processor uses (this association is created in the [definition of the respective processing activities](#)<sup>52</sup>).

## Data Controller, Processor or Receiver

Save

---

Name

Street

ZIP/City

Country  Domain

E-mail

Phone

Description

Comment

---

### Used by Processing Activities

Name	Description
Invoices	Creates and sends invoices for customer orders <i>Invoices exported to accounting system</i>

After you finish editing information about a data processor, click **Save** to save the changes.

### Relationships with other metadata

A **data processor** has the following relationships with other metadata:

It can be selected for...	Which sets up...
<a href="#">Processing activity &gt;Data processors</a> <sup>52</sup>	Which data processors use the processing activity, and the role (controller or processor) in which a data processor acts. Once a data processor is selected for a processing activity, the processing activity appears reflexively as part of the information about the data processor ( <i>see lower pane in screenshot above</i> ).

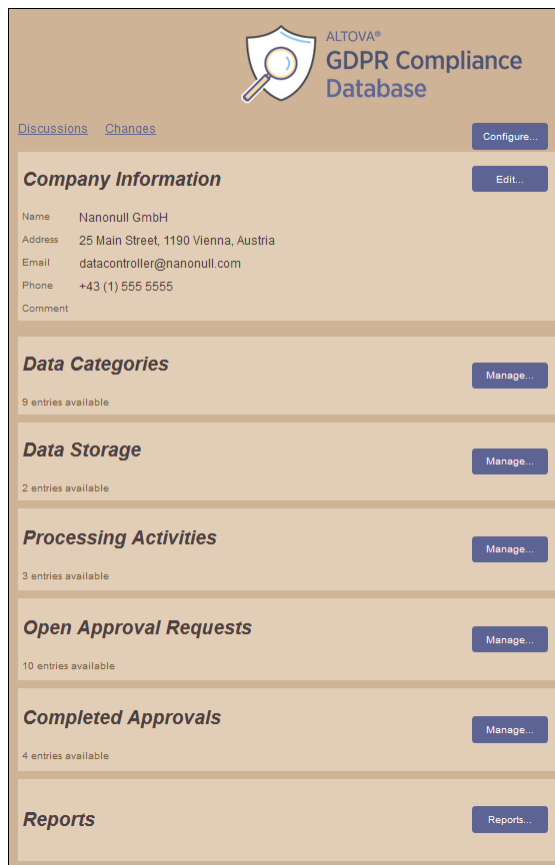
## 4.4 Define Data Properties and Relationships

This section describes how to define and manage the following:

- [Data Categories](#)<sup>45</sup>, which are created to describe a type of data, with each data category being composed by assigning values to [data classifications](#)<sup>36</sup>.
- [Data Storage Entities](#)<sup>49</sup>, which are created to relate data categories to physical storage entities.
- [Processing Activities](#)<sup>52</sup>, which define various aspects of a processing activity: (i) the responsible persons, (ii) department roles that have access rights to the processing activity, (iii) data categories that are processed and in what way they are respectively used, (iv) external processors, if any, that use the processing activity.

### Accessing the management pages

To access the management page of Data Categories, Data Storage Entities or Processing Activities, go to the [Overview page](#)<sup>20</sup> and click the respective **Manage** button (see screenshot below).



### Example

In this section, we will show to define data categories, data storage entities, and processing activities about our example company, Nanonull GmbH. In our example, we have defined the following:

- Nine [data categories](#)<sup>36</sup> that describe data categories related to customer orders and employee salaries.
- Two [data storage entities](#)<sup>39</sup> that hold the data that is used to process customer orders and employee salaries, respectively.
- Three [processing activities](#)<sup>42</sup>, which process, respectively, customer orders, employee salaries, and mailers to customers.

### 4.4.1 Define Data Categories

The Data Categories page (*screenshot below*) is accessed from the [Overview page](#)<sup>20</sup>. It lists the data categories that have been defined and enables you to manage data categories. Here, new data categories can be added (click **New Data Category**), existing data categories can be edited (click the **Edit** icon of a data category), and existing data categories can be deleted (click the **Delete** icon of a data category).

Data Categories			X	New Data Category...
Name	Description			
	Comment			
Customer Address *	Customer's mailing address for invoices <i>For most orders, the billing and mailing address are the same</i>			
Customer Credit Card Data	Credit card number, expiration date, cardholder name <i>CVC is not stored</i>			
Customer ID	Customer's name and internal ID			
Customer IP address	IP address of customer placing order <i>Used to check if entered country and country IP match for tax calculation purposes.</i>			
Employee Address	Employee address, email, and telephone number			
Employee Bank Details	Employee bank account number			
Employee ID	Employee name and internal office IDs			
Order Details	Order number, customer ID, order items, item codes, prices and quantities, bill amount			
Salaries *	Information for payment of employee salaries			

When you add a new data category or edit a data category, a page with the data category's details is displayed (*see below*). On this page, you can edit the definition of the selected data category.

#### Example

In our example (*see screenshot above*), we have created data categories to describe basic personal data of customers and employees.

#### Points to note

Note the following points about data categories:

- You are free to define data categories as you like and according to what is suitable for your purposes.
- Each data category is composed of the [data classifications of the system](#)<sup>36</sup>, for each of which one (or more) of that classification's allowed values is assigned. (Values do not need to be assigned for non-mandatory classifications.)
- A data category can cover as broad or narrow a field of data as is suitable. For example, you might create individual data categories for first name, last name, street, building number, city, postal code, country, and so on. Alternatively, you might create a single data category to contain the customer's name, address, telephone number, email address, and credit card details. The disadvantage of the first (narrow) categorization is that for each data category, values must be assigned to all the mandatory classifications, as well as maintained over time—which could prove very time-consuming, difficult, and tedious, besides being unnecessary. The disadvantage of the second (broad) approach is that multiple data items of quite different types and security significance will be clubbed together—for example, address and financial information—and could prevent a sensible breakdown of data into categories needing different levels of protection. You should create data categories that are appropriate. In our example, for instance (see *screenshot above*), we have created separate data categories, respectively, for the customer's (i) name and ID, (ii) mailing address, (iii) IP address, and (iv) credit card details.
- The key GDPR rule to hold to is that all the data you collect must be covered by the data categories you define.

### Create or edit a data category

The definition of a data category (see *screenshot below*) consists of: (i) a name and description, and (ii) the system's data classifications, each with one or more allowed values selected for it. For example, the screenshot below shows the data category named Customer Credit Card Data (refer also to the *screenshot above*). The top pane contains the category's name and description. The bottom pane contains the system's data classifications, for each of which you can select one or more of the allowed values from the respective combo boxes. For example, the first data classification in the screenshot below is *Data Subjects*, and the value selected in its combo box is *Customers*. Additional information about the selection has been added in the *Description* field. The second data classification is *Encryption*. The third data classification is *Protection Measure*, which can take multiple values

## Data Category Customer Credit Card Data

Save

---

**Name & Description**

Category Name

Description

Comment

---

**Classifications**

**Data Subjects**

Customers of the Company (Controller)

Description

Comment

Request approval

---

**Encryption**

Advanced Data Encryption Standard

Description

Comment

Request approval

Last approved on Feb 01, 2019 17:45 by Niki Devqood

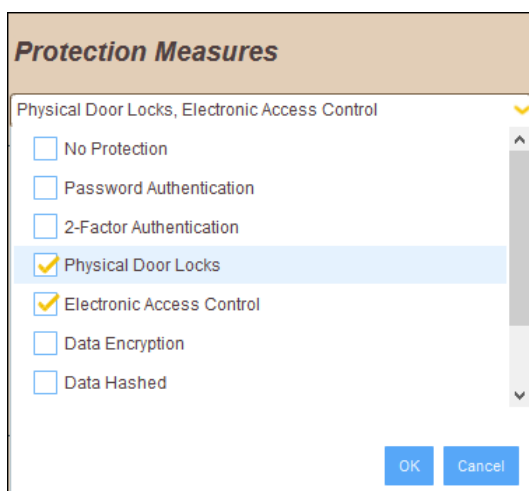
---

**Protection Measures**

Physical Door Locks *Access to data requires a physical key to unlock door.*

Note the following points about how the data classifications of a data category are specified:

- All the data classifications that have been configured for the compliance database are displayed.
- For each classification, select from among its allowed values. Alternatively, you can add a new value to the classification directly from the value field's combo box; to do this click the *+New Value* item. If you enter a new value via the combo box, the value will automatically be added to the global definition of that classification.
- A mandatory classification (defined via the classification's *Mandatory value*<sup>36</sup> property) is displayed in red if no value is selected for it.
- If a data classification has been defined to allow multiple values (via its *Multiple values allowed*<sup>36</sup> property), then (in the definition of the data category) the value field's combo box (of that data classification) will drop down a list of check boxes—which allows you to select multiple values (see *screenshot below*).



- The **Save** button of the Data Categories page becomes enabled after (i) the data category has been given a name, and (ii) a value has been selected for every mandatory *data classifications*<sup>36</sup>.
- When modifying the definition of a data classification, it might be desirable for modifications to be approved by a person with oversight of the system. If approval is required, then the *Request Approval* check box should be checked. In such an event, the request will appear in the *Approval Requests*<sup>56</sup> list.

After modifying the definition of a data category, click **Save** to save the changes.



### Relationships with other metadata

A **data category** has the following relationships with other metadata:

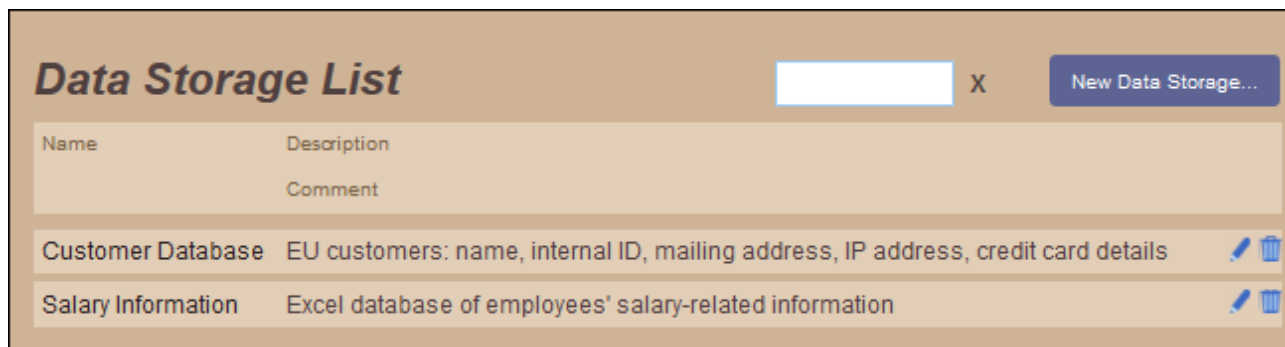
It selects...	Which sets up...
<a href="#">Data classifications</a> <sup>36</sup>	The value/s of classifications in the definition of the category.
<a href="#">Data classification &gt; Approval request</a> <sup>57</sup>	An approval request for a change to a data classification.

It can be selected for...	Which sets up...
<a href="#">Processing activity &gt; Data categories</a> <sup>52</sup>	To which data categories data that is used by the processing activity belongs.
<a href="#">Data storage entities</a> <sup>49</sup>	The data category of each data tier of the storage entity.

## 4.4.2 Define Data Storage Entities

The Data Storage List page (*screenshot below*) is accessed from the [Overview page](#) <sup>20</sup>. It lists the data storage entities that have been defined in the compliance database. Each data storage entity refers to a physical storage location where data belonging to one or more data categories is stored. The definition of the data storage entity expresses the relationship between the physical storage location and data categories. For example, if customer addresses are stored in a database, then the data storage location can be linked to the data category for customer addresses. This enables the physical locations of different data categories to be quickly looked up.

On the Data Storage List page you can add a new data storage entity (click **New Data Storage**; see *screenshot below*), edit details of existing data storage entities (click the **Edit** icon of a data storage entity), and delete existing data storage entities (click the **Delete** icon of a data storage entity).



## Add a new data storage entity

When you add a new data storage entity (by clicking **New Data Storage**), a window appears asking you to specify the type of data storage that you want to define (*screenshot below*).

**Data Storage Type**

Please select the type of the new data storage and its tiers. Once selected it cannot be changed anymore for this storage.

Database

File in the local filesystem

File on a web site

Own data definition

**Predefined Data Tiers**

Database

Table

Field

Cancel OK

Select the type of the data storage entity. The data tiers for each data storage type are predefined.

- **Database:** The data tiers of a *Database* type are: Database, Table, and Field. For each *Database* storage type, you can enter multiple Database tiers. For each Database tier, you can enter multiple Table tiers. And for each Table tier, you can enter multiple Field tiers. Each tier can be associated with a data category, which indicates what kind of data is stored in that tier. See *the screenshot below for an example of how database tiers are used*.
- **File in the local filesystem:** The data tier is the file path of the data storage entity. Multiple file paths can be assigned, with each file path being associated with a data category, indicating what kind of data is stored at that file path location. Enter the file path in the *Name* field of the tier.
- **File on a website:** The data tier is the URL of the data storage entity. Multiple URLs can be assigned, with each URL being associated with a data category, indicating what kind of data is stored at that URL location.
- **Own data definition:** The number and type of data tier can be freely specified. Click **New Tier** to specify a new tier and add a descriptive phrase as the name of the tier.

After the data storage type is selected, click **OK**. The data storage entity is created (*see screenshot below*).

## Data Storage

Save

### Storage Description

Name

Description

Comment

### Data Tiers

New Database...

Name	Description	Categories
		Comment
Database <span style="float: right; background-color: #4a7ebb; color: white; padding: 2px 10px; border-radius: 3px;">New Table...</span>		
▼ Customers EU	EU customers, organized into sales regions	Customer Address, Customer Credit Card Data, <span style="font-size: 0.8em;">✎ + -</span>
Table <span style="float: right; background-color: #4a7ebb; color: white; padding: 2px 10px; border-radius: 3px;">New Field...</span>		
▼ Customers Region-01	Region-01: UK, Ireland	Customer Address, Customer Credit Card Data, <span style="font-size: 0.8em;">✎ + -</span>
Field		
Customer ID	ID and name	Customer ID <span style="font-size: 0.8em;">✎ + -</span>
Customer IP address	IP address	Customer IP address <span style="font-size: 0.8em;">✎ + -</span>
Customer Mailing Address	Mailing address	Customer Address <span style="font-size: 0.8em;">✎ + -</span>
Customer Credit Card	Credit card data	Customer Credit Card Data <span style="font-size: 0.8em;">✎ + -</span>
Table <span style="float: right; background-color: #4a7ebb; color: white; padding: 2px 10px; border-radius: 3px;">New Field...</span>		
▼ Customers Region-02	Region-02: Germany, Austria, Switzerland	Customer Address, Customer Credit Card Data, <span style="font-size: 0.8em;">✎ + -</span>
Field		
Customer ID	ID and name	Customer ID <span style="font-size: 0.8em;">✎ + -</span>
Customer IP Address	IP address	Customer IP address <span style="font-size: 0.8em;">✎ + -</span>
Customer Mailing Address	Mailing address	Customer Address <span style="font-size: 0.8em;">✎ + -</span>
Customer Credit Card	Credit card data	Customer Credit Card Data <span style="font-size: 0.8em;">✎ + -</span>

Add a name for the data storage entity, and optionally a description and comment. In the Data Tiers section, specify the data tiers. This could be a file path, or a URL, database, table or field. For each data tier you can associate a data category, which indicates for what data category that data tier is being used.

After you finish entering the details of the data storage entity, click **Save** to save the data storage entity to the compliance database.

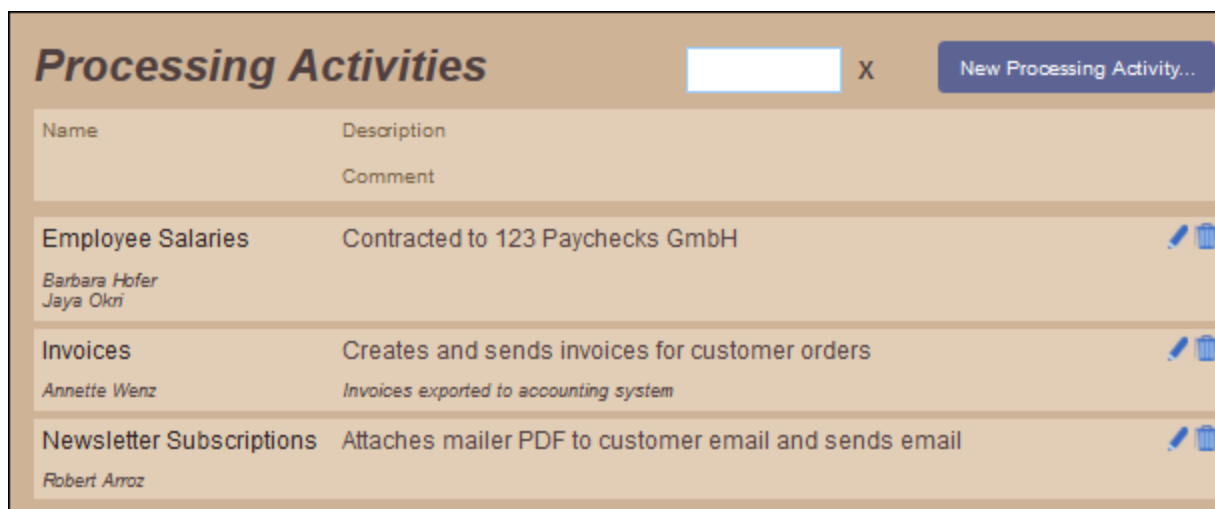
## Relationships with other metadata

A **data storage entity** has the following relationships with other metadata:

It selects...	Which sets up...
<a href="#">Data categories</a> <sup>45</sup>	The data category of each data tier of a storage entity.

### 4.4.3 Define Processing Activities

The Processing Activities page (*screenshot below*) is accessed from the [Overview page](#) <sup>20</sup>. The page lists all the data processing activities across the data controller's organization, and enables you to manage the list of processing activities. Here, new processing activities can be added (click **New Processing Activity**), existing processing activities can be edited (click the **Edit** icon of a processing activity), and existing processing activities can be deleted (click the **Delete** icon of a processing activity).



When you add a new processing activity or edit a processing activity, a page containing the processing activity's details is displayed (*see below*). On the Processing Activity page (*see below*), you can edit the definition of the processing activity.

#### Create/edit a processing activity

The definition of a processing activity is shown in the screenshot below.

## Processing Activity

Save

### Description of Processing Activity

Name

Description

Comment

### Responsible Persons

[Add Person...](#)

Name	Description	
	Comment	
Barbara Hofer		<a href="#">✎</a> <a href="#">🗑</a>
Jaya Okri		<a href="#">✎</a> <a href="#">🗑</a>

### Access Rights

[Add Access Right...](#)

Role (Department)	Description	
	Comment	
Employee Data (Human Resources)		<a href="#">✎</a> <a href="#">🗑</a>
Salaries (Accounting)		<a href="#">✎</a> <a href="#">🗑</a>

### Data Categories

[Add Category...](#)

Data Category	Description	
	Comment	
Salaries	Calculates deductions from gross salary to give net monthly	<a href="#">✎</a> <a href="#">🗑</a>

### Controllers and Processors

[Add Processor...](#)

Name	Description	Role	
	Comment		
123 Paychecks GmbH	Processes Nanonull employee salaries and exports to Nanonull Accounting system	Processor	<a href="#">✎</a> <a href="#">🗑</a>

It consists of the following:

- The name and a description of the processing activity
- A list of persons responsible for deciding features and users of the processing activity; click **Add Person** and select a person.
- A list of roles (within departments) that have access rights to the processing activity; click **Add Access Rights** and select a department and department role.
- A list of all the data categories used by the processing activity; click **Add Category** and select a data category. For each data category, you must select a value for each mandatory [data usage classification](#) <sup>39</sup> so as to describe how the processing activity processes that particular data category. If a data usage classification has been [configured to accept multiple values](#) <sup>39</sup>, you can select more than one value for that classification. The screenshot below shows how a data category is defined within a processing activity; the list of usage classifications start with the *Data Transfer* usage classification; values are selected in the respective combo box.

**Data Category**

Data Category: Salaries

Describe how the data category is being used by the processing activity: Calculates deductions from gross salary to give net monthly

Comment:

Data Transfer: External Processing

Lawfulness of Processing: Employment and Social Security - Article 6 2(b)

Processing Impact Assessment: Not necessary

Processing Special Types of Data: Employment and Social Security - Article 9 2(b)

Profiling: No Profiling

Purpose of processing: Same purpose as when data collected

Buttons: Cancel, OK

- A list of external data processors that are involved with this processing activity. Click **Add Processor**, then select an existing data processor and assign it a role (as data controller or data processor). Alternatively, you can define a new data processor that will be added to the list of existing data processors.

## Relationships with other metadata

A **processing activity** has the following relationships with other metadata:

It selects...	Which sets up...
<a href="#">Persons</a> <sup>31</sup>	Persons who are responsible for a processing activity. The processing activity appears reflexively as part of the information about the person.
<a href="#">Departments</a> <sup>28</sup>	Departments that have access rights to a processing activity.
<a href="#">Department roles</a> <sup>28</sup>	Department roles that have access rights to a processing activity.
<a href="#">Data categories</a> <sup>45</sup>	Data categories of the data that is processed by the activity.
<a href="#">Data processors</a> <sup>42</sup>	Data controllers or processors that use the processing activity. The processing activity appears as part of the information about the data processor.

## 5 Approvals

The Approvals process enables users of the compliance database to modify a data category and to then submit the modification/s for approval by an authorized person. The process consists of three steps:

1. A user [modifies a data category](#)<sup>45</sup> by changing the value/s of a data classification of the category, or adding a comment to the data classification.
2. The change to the data classification is [submitted for approval](#)<sup>57</sup>.
3. The submitted approval is listed on the [Open Approval Requests page](#)<sup>20</sup>, where it can be authorized at any time by an authorized person. (*For information, see [Authorize an Approval](#)<sup>59</sup>.*) The authorized approval request is moved automatically to the [Completed Approvals page](#)<sup>20</sup>.

These steps are described in the subsections of this section.

Note also that a discussion about an approval request can be initiated directly from the page of that approval request, with discussion participants being selected from among users of the compliance database. See the topic [Discussions](#)<sup>62</sup> for details.



## 5.1 Approval Requests

A data category can be modified by (i) changing the value/s of one of its data classifications, or (ii) adding a comment (for example, querying the accuracy of a classification's selected value). After modifying a data category in one of these ways, modification can be submitted for approval. This is done as follows:

1. Navigate to the definition of the [data category](#)<sup>45</sup> that you want to modify.
2. In the definition, locate the data classification that you want to modify and make the modification. For example, in the screenshot below, in the *Salaries* data category, the *Risk* data classification has been modified to a value of *High* and a comment has been added.

**Risk**

High Breach would impose a high risk for the data subject rights and freedom.

Description

Comment  
This is a significant risk and should be given a value of "High"

Approval requested on Feb 01, 2019 17:44

3. To request approval of the change, check the *Request approval* check box.
4. Click **Save**. The text near the check box changes to state (i) that the approval has been requested, and (ii) the date and time of the approval request.

If you now navigate to the Open Approval Requests page (from the [Overview page](#)<sup>20</sup>), you will see that the approval request for this modification has been added to the list of open requests (see *screenshot below*).

Approval Requests		<input type="text"/> X
Category	Classification	
Description, Comment, Date		
Salaries	Risk: High	
<i>Approval requested on Feb 01, 2019 17:44</i>		
Salaries	Storage duration: 7 years after contract	
<i>Approval requested on Feb 01, 2019 17:44</i>		
Salaries *	Protection Measures: Physical Door Locks	
<i>Approval requested on Feb 04, 2019 15:52</i>		
Customer Address	Protection Measures: Password Authentication	
Can only be accessed when the user is logged in with a password		
<i>Approval requested on Feb 01, 2019 17:44</i>		
Customer Address *	Storage duration: infinite	
<i>Is this accurate, or is it only stored for years?</i>		
<i>Approval requested on Feb 01, 2019 17:06</i>		

An [approval request in this list can now be authorized](#)<sup>59</sup> by a person who is authorized to do so.

### Canceling an approval request

To cancel an approval request, go to the definition of the relevant data category and data classification. Then uncheck the *Approval* check box, and click **Save**.

### Relationships with other metadata

An **approval request** has the following relationships with other metadata:

It is created for...	Which sets up...
<a href="#">A modification of a data category</a> <sup>45</sup>	The listing of the modification under <a href="#">Open Approval Requests</a> <sup>59</sup> .

It provides...	Which sets up...
The possibility of starting a <a href="#">discussion</a> <sup>62</sup>	A discussion thread about the approval request.

## 5.2 Authorize an Approval

A person who is authorized to approve a data-category modification can do this as follows:

1. Navigate to the Open Approval Requests page via the [Overview page](#)<sup>20</sup> (screenshot below).



Category	Classification	Description, Comment, Date
Salaries	Risk: High	Approval requested on Feb 01, 2019 17:44
Salaries	Storage duration: 7 years after contract	Approval requested on Feb 01, 2019 17:44
Salaries *	Protection Measures: Physical Door Locks	Approval requested on Feb 04, 2019 15:52
Customer Address	Protection Measures: Password Authentication	Can only be accessed when the user is logged in with a password Approval requested on Feb 01, 2019 17:44
Customer Address *	Storage duration: infinite	Is this accurate, or is it only stored for years? Approval requested on Feb 01, 2019 17:06

2. Click the **Edit** icon of an approval request. The approval request will be displayed (screenshot below).

[Discussions](#) [Changes](#) Back

## Approval Request

Approve

### Category and Classification

Name Salaries / Data Subjects: Employees  
 Description  
 Comment

### Approval Notes

Was modified from "Past and Present Employees"

Approval requested on 2018-12-17 16:47

- The *Name* line contains the following information: <Name of Data Category> / <Data Classification>: <Classification Value>. Make notes related to the approval in the *Approval Notes* section. If you wish to start a discussion thread about this approval request, click *Discussions*. See the topic [Discussions](#)<sup>62</sup> for more information.
- Click **Approve** to authorize the approval. The approval request will be moved from the Open Approval Requests page to the Completed Approvals page (see screenshot below). (The Completed Approvals page is accessed from the [Overview page](#)<sup>20</sup>.)

Approved Assessments		<input type="text"/>	X
Category	Classification	Description, Approval Notes, Date	
Salaries	Data Subjects: Employees	Was modified from "Past and Present Employees"	
		Approval requested on 2018-12-17 16:47	
		Approved on 2018-12-20 17:39 by [redacted]	
Salaries	Data Protection Impact Assessment: Not necessary	Approved	
		Approval requested on 2018-12-10 17:52	
		Approved on 2018-12-11 13:00 by [redacted]	

Clicking the **Edit** button of a completed approval (*see screenshot above*), opens a page displaying details of that approval request.

## 6 Discussions

A discussion can be started about an individual metadata item, for example, about a specific data category or a specific processing activity. When starting a discussion, the initiator of the discussion can select discussion members from among the compliance database users. These users will be notified about the creation of the discussion thread and about any modifications to the thread.

A discussion is accessed via the *Discussions* link located at the top left of the page; (note that the link is not available on all pages). Clicking the *Discussions* link results in one of two displays, depending on the type of page:

- If the page displays the **definition of a single metadata item**, then all discussion threads related to that metadata item (for example, a specific processing activity) are displayed. For example: On the page that defines a specific processing activity, clicking the *Discussions* link opens a frame that displays discussions related to that processing activity. See [Discussions about a Single Metadata Item](#)<sup>63</sup> for additional information.
- If the page displays a **group of metadata items** (for example, the [Processing Activities](#)<sup>72</sup> page, which lists all processing activities), then clicking the *Discussions* link displays discussion threads related to **all** processing activities.

**Note:** New discussions can be started only from the definition pages of single metadata items. For example: from a page that defines a specific processing activity. See the section [Start a Discussion](#)<sup>67</sup> for more information.

**Note:** A discussion will be displayed to a user only if that user is a participant (initiator or member) in that discussion.

## 6.1 Discussions about a Single Metadata Item

Discussions about a single metadata item are available for the following metadata items. The table lists the respective pages from which the discussions about that metadata item can be accessed.

Metadata item	Accessed from page defining that specific...
Company (Data controller)	<a href="#">Company information</a> <sup>26</sup>
Individual department	<a href="#">Department's information</a> <sup>28</sup>
Individual person	<a href="#">Person's information</a> <sup>31</sup>
Individual data classification	<a href="#">Data classification's information</a> <sup>36</sup>
Individual data usage classification	<a href="#">Data usage classification's information</a> <sup>39</sup>
Individual data processor	<a href="#">Data processor's information</a> <sup>42</sup>
Individual data category	<a href="#">Data category definition</a> <sup>45</sup>
Individual data storage entity	<a href="#">Data storage entity definition</a> <sup>49</sup>
Individual processing activity	<a href="#">Processing activity definition</a> <sup>52</sup>
Individual approval request	<a href="#">Approval request definition</a> <sup>57</sup>

On clicking the *Discussions* link on the definition page of a metadata item, the discussion threads are displayed in a frame that looks something like this:

**Discussions related to Customer Address**

Classification: Encryption

Thread: Encryption level of Customer Addresss should be Medium

By: Mark Parsons

Members: Jason Brown, Niki Devgood

Mark Parsons Feb 20, 2019 16:00

Encryption level of all address types should be High since it includes email and telephone info. Would you agree?

---

Thread: Billing address or Delivery address

By: Mark Parsons

Members: Jason Brown, Niki Devgood

Mark Parsons Feb 20, 2019 15:40

Shoud we not split this category into two in case data protection requirements for the two address types are different in the future.

[New Discussion](#)

The screenshot above shows two **discussion threads** of the data category *Customer Address*. Note that this is one specific data category. Both threads have been initiated by Mark Parsons; *see screenshot*. In both cases, the discussion participants (in addition to the initiator) are Jason Brown and Niki Devgood. Each thread currently has a single **message** (in both cases sent by Mark Parsons).

To close a frame, click the frame's **Close** button (located at top right; see screenshot above).

For information about what a discussion participant can do, see the section [Available Functionality](#)<sup>69</sup>.



## 6.2 Discussions about All Items of a Metadata Type

Discussions in the compliance database can also be viewed as a group of threads, with the grouping being according to metadata type; an example of a metadata type is a processing activity. This is useful if you wish to have an overview of discussions about all threads of all items of a metadata type. For example, you can view a list of all threads relating to all departments or all processing activities (which are examples of metadata types). The table below lists the available groups and the respective pages from which each group of discussions is accessed.

Discussions about...	Accessed from page...
All discussions	<a href="#">Overview page</a> <sup>20</sup>
All departments	<a href="#">Departments page</a> <sup>28</sup>
All persons	<a href="#">Persons page</a> <sup>31</sup>
All data classifications	<a href="#">Data Classifications page</a> <sup>36</sup>
All data usage classifications	<a href="#">Data Usage Classifications page</a> <sup>39</sup>
All data processor	<a href="#">Data Processors page</a> <sup>42</sup>
All data categories	<a href="#">Data Categories page</a> <sup>45</sup>
All data storage entities	<a href="#">Data Storage entities</a> <sup>49</sup>
All processing activities	<a href="#">Processing activities</a> <sup>52</sup>
All approval requests	<a href="#">Approval Requests</a> <sup>57</sup>

On clicking the *Discussions* link on any of the pages listed above, the discussions are displayed in a frame that looks something like this:

**Discussions related to Data Categories**

This view shows discussions based on criteria below in a flat list. To see all record related discussions in conversation view go to the corresponding record.

Unread    Max  10     30     50

Search       

Thread     Message

---

Thread    **Consent is now explicit.**

Related to    [Customer Credit Card Data / Type of Consent](#)

From    **Mark Parsons**    Feb 21, 2019 16:12

Message    **We have added a form in which customers must agree the purchase contract before c...**

---

Thread    **Billing address or Delivery address**

Related to    [Customer Address](#)

From    **Jason Brown**    Feb 21, 2019 12:47

Message    **It would depend on whether we are ever going to ship physical disks. Decision need...**

The screenshot above shows discussions related to all data categories. In it, there are two **discussion threads**, for two different data categories: (i) Customer Credit Card Data, and (ii) Customer Address. For each thread, the latest message is displayed. Unread messages are displayed in bold.

The frame has the following filters:

- *Unread*: Check this option to filter threads, all messages of which have been read. Only threads with at least one unread message will be displayed.
- *Max*: Select the maximum number of discussions to display, starting with the newest.
- *Search*: Enter the text string to search for, either in the text of thread headers or in the text of messages. Searches are case-insensitive.

A discussion participant can do the following:

- Click the data category (in the *Related to* field) to go to the definition page of that data category.
- Click a thread's latest message to go to the thread. Inside the thread, you can do the following:
  - Click a message to read the full message.
  - If a message has been sent by another participant, click the message to reply to it. You can also mark the message as unread.
  - If a message has been sent by you, click it to add another message. If there has been no reply to the message, you can edit the message or delete it.

To close a frame, click the frame's **Close** button (located at top right).

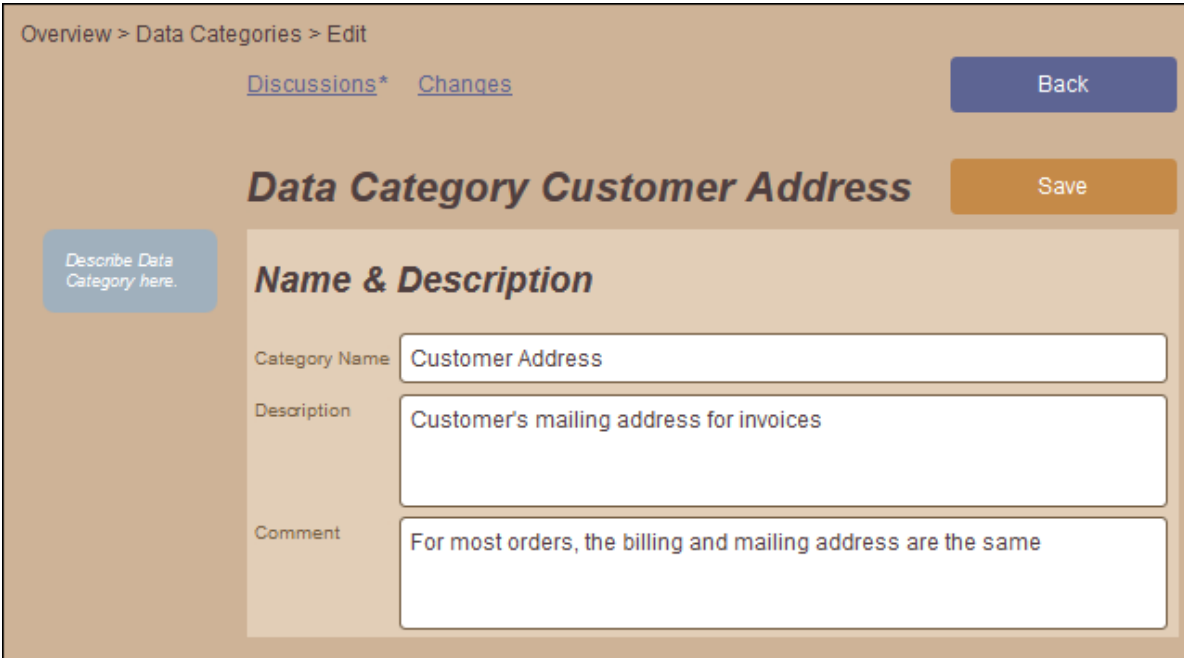
For more information about what a discussion participant can do, see the section [Available Functionality](#) <sup>69</sup>.

## 6.3 Start a Discussion

Every discussion is about a specific metadata item, for example about a specific data category or a specific processing activity. Any user of the compliance database can start a discussion. On doing so, this user is known as the discussion initiator. The discussion initiator can add and remove discussion members. The discussion initiator and discussion members together comprise a group known as the discussion participants.

To start a new discussion, do the following:

1. Go to the configuration/definition page of that specific metadata item. For example, if you want to start a discussion about the data category *Customer Address*, then go to the definition page of the *Customer Address* data category (see screenshot below).



Overview > Data Categories > Edit

[Discussions\\*](#) [Changes](#) [Back](#)

### Data Category Customer Address [Save](#)

[Describe Data Category here.](#)

#### Name & Description

Category Name

Description

Comment

2. Click **Discussions** (see screenshot above) and then **New Discussion**.
3. In the frame that appears (screenshot below), select a specific data classification if the discussion is about one classification only. Otherwise (if the discussion is about the entire data category), do not check the option for a specific classification. Note that this example is for a discussion about the *Storage Duration* data classification of the *Customer Address* data category.

**Start new discussion related to Customer Address**

Classification

This discussion is about specific classification

Discussion participants

Discussion Subject/Thread

First Message

4. Select the discussion members from among current users.
5. Enter a title for the discussion.
6. Enter the first message of the discussion thread.
7. Click **Send**. The message will be added to the discussion thread, and all persons listed as members, as well as the discussion initiator, will be able to access the thread.

## 6.4 Available Functionality

A discussion thread can be read and participated in only by discussion participants (who are: the discussion initiator plus the discussion members); the discussion initiator can do a few more things than what discussion members can do. The functionality available to discussion participants is explained below.

### Functionality available to discussion members

All discussion participants (initiator and members) are able to do the following:

- Read the thread. To do this you must open the thread. Do this by clicking a message of that thread in any listing that contains the thread (whether for a [single metadata item](#)<sup>63</sup> or a [group of all items of a metadata type](#)<sup>65</sup>). You can access listings via the [Discussions](#)<sup>62</sup> link.
- Reply to a message on the thread. To do this, open the discussion thread, click the message you wish to respond to, click **Reply**, enter your response, and click **Send**.
- Edit or delete an own message as long as there has been no reply to that message. To do this, open the discussion thread, click the message, and then click **Edit** or **Delete**, respectively. If there has already been a reply to your message, these two buttons will be disabled.

### Functionality available to discussion initiators

Discussion initiators can do a few more things than what discussion members can do (*see previous section*). This additional functionality is available via links in the discussion thread in the list of [threads for a single metadata item](#)<sup>63</sup> (*see screenshot below*).

The screenshot shows a window titled "Discussions related to Customer Address" with a close button (X) in the top right corner. It displays two discussion threads. Each thread includes a classification, thread title, author, members, and a message snippet.

Classification	Thread	By	Members	Message Snippet
Storage duration	Extension of storage duation	Mark Parsons	Annette Wenz, Niki Devgood	It woud help Marketing to keep data for seven years instead of five. Would this be ok legally and tec...
Encryption	Encryption level of Customer Addresss should be Medium	Mark Parsons	Jason Brown, Niki Devgood	Encryption level of all address types should be High since it includes email and telephone info. Wo...
		Jason Brown		Yes. One point: If there is a possibility that at some future time we ship software on disk, should we...

Discussion initiators can carry out the following additional actions:

- Add a discussion member at any time. To do this, click the link in the *Members* field. In the frame that appears (*screenshot below*), add the new member/s, and click **Change**. The new participants will have access to the entire thread.
- Remove a member if that member has not yet taken part in the discussion. To do this, click the link in the *Members* field. In the frame that appears (*screenshot below*), deselect the member/s you want to remove, and click **Change**.
- Change the name of the discussion thread if no member has posted a message to the thread. If the name may be changed, the link in the *Thread* field is enabled (see the *Extension of storage duration* thread in the screenshot above); otherwise the link is disabled (see the *Encryption level of Customer Address should be Medium* thread in the screenshot above). Click **Change** after editing the name (see *screenshot below*).

**Discussion related to Customer Address**

You may add discussion participants any time. You may remove them only as long as they didn't reply to this discussion.

Annette Wenz

You may edit discussion subject as long as there were no replies.

Extension of storage duration

Cancel Change

To close this frame (screenshot above) without making a change, click **Cancel**.

## 7 Reports

The following types of reports, in PDF and MS Word formats, can be generated from the metadata information held in the compliance database:

- [Processing Activities](#) <sup>72</sup>
- [Critical Processing Activities](#) <sup>73</sup>
- [Category Approvals](#) <sup>75</sup>

All reports are generated from the Reports page (*screenshot below*), which is accessed from the [Overview page](#) <sup>20</sup> (by clicking the **Reports** button).



Click the appropriate **Configure** button to go to the page for the respective report type and start the steps to generate the report.

### System requirements for report generation

In order for PDF reports to be generated, the system administrator must ensure that the following applications/components have been installed on the server machine:

- Altova StyleVision Server
- Java Runtime Environment 1.6 or later

**Note:** The server machine is the machine on which Altova MobileTogether Server has been installed. The Compliance Database is deployed to MobileTogether Server.

**Note:** For details, see the section Software Requirements of the Standard Installation Guide.

## 7.1 Processing Activities

The **Processing Activities report** contains information about processing activities described in the system. The report can be filtered according to the following criteria:

- Descriptions of data classifications (defined in the data categories of the processing activities) can be shown or not.
- The report will cover the processing activities of all companies stored in the compliance database. To restrict the report to a selected set of companies, select the Restrict report check box and then select the companies you want to include in the report. Select a company role (data controller or data processor) to further filter the contents of the report. The option to select companies becomes available only when the *Restrict* option's check box is selected (see screenshot below).

The screenshot shows a web interface for generating a report. At the top, it says "Records of Processing Activities" with a "Create..." button. Below this is a section titled "Output Format & Details" with two radio buttons: "PDF" (selected) and "Word". There is a checked checkbox for "Show classification descriptions". The next section is "Companies involved in activities" with a checked checkbox for "Restrict report to activities which use companies selected below in a specified role". Below this are two dropdown menus: "Companies" with "123 Paychecks GmbH" selected and "Role" with "Data Processor" selected.

To generate the report, select the report format (PDF or Word; see screenshot above), and click **Create**. Downloading the report opens the PDF in a browser, or the Word file (.docx format) in an application of your choice.



## 7.2 Critical Processing Activities

The **Critical Processing Activities report** enables you to specify certain classification values as critical, and to then generate a report for only those processing activities that fulfill the criteria that have been configured as critical. So, for example, if a *Data Encryption* classification with a value of *DES* or *RSA* (see *screenshot*) is considered critical, then processing activities which have a data category with this critical classification will be included in the report. If multiple critical classifications are defined, then a processing activity that has any one of the critical classifications will be included in the report.

To set up a classification as a critical classification, do the following:

1. On the page for the Critical Processing Activities report (see *screenshot below*), click **Add Classification**.

Classification	Values
Encryption	DES 3DES
Risk	High Medium

2. In the dialog that appears, select (i) a [data classification](#)<sup>36</sup>, and (ii) values defined for that classification, and then click **OK**. The classification (with the selected values) will be added as a critical classification criterion.
3. You can add as many critical classifications as you like.
4. After specifying the critical classifications that you want, select *List only critical processing activities* to generate a report containing information about only the processing activities that fulfill the criteria specified in the critical classifications. If this option is not selected, all processing activities are reported, with the critical processing activities being marked in bold.
5. You can also choose whether descriptions of data classifications (defined in the data categories of the processing activities) should be shown or not.
6. Select the report format (PDF or Word), and click **Create**.

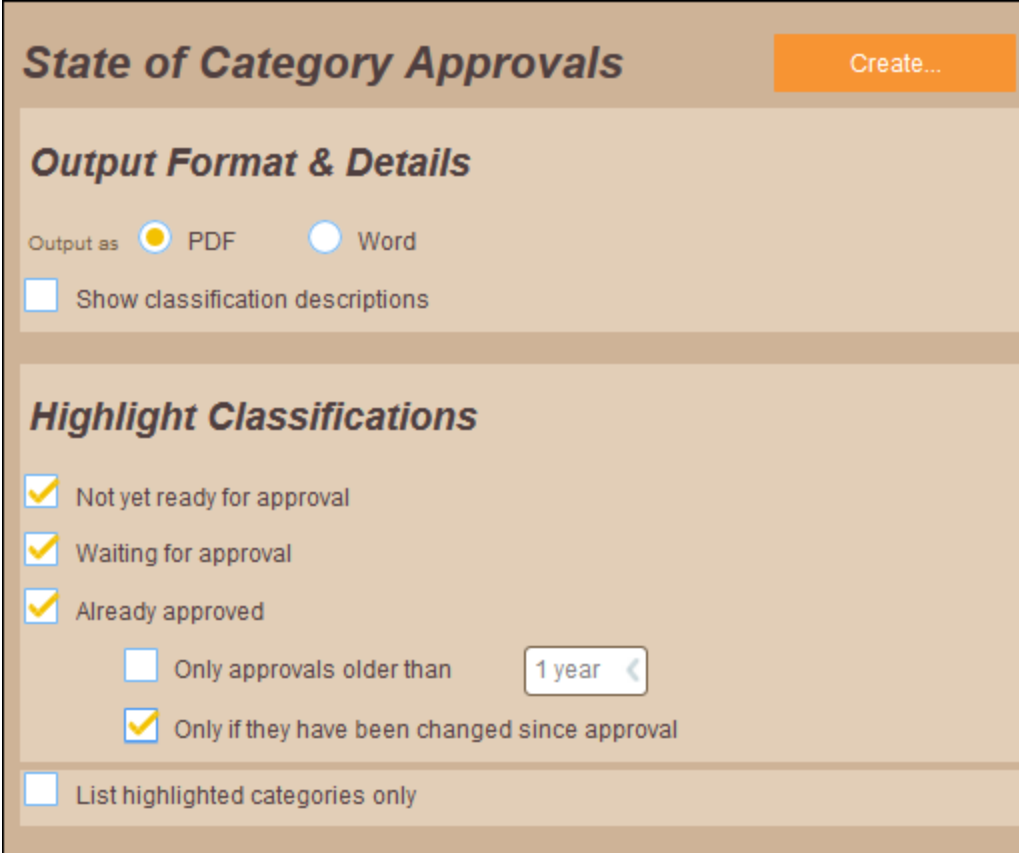
Downloading the report opens the PDF in a browser, or the Word file (.docx format) in an application of your choice. Critical processing activities are displayed in the report in a bold font.

## 7.3 Category Approvals

The **Category Approvals report** enables you to generate reports on the basis of the [approval status of a category's classifications](#)<sup>45</sup>.

To set up a category approvals report, do the following:

1. On the page for this report (see *screenshot below*), check the options that you wish to include (see *list below screenshot*).



**State of Category Approvals** Create...

**Output Format & Details**

Output as  PDF  Word

Show classification descriptions

**Highlight Classifications**

Not yet ready for approval

Waiting for approval

Already approved

Only approvals older than

Only if they have been changed since approval

List highlighted categories only

- *Show classification descriptions*: Whether the descriptions of classifications will be shown or not.
  - *Not yet ready for approval*: Classifications for which no approval request has been submitted.
  - *Waiting for approval*: Classifications for which an approval request has been submitted, but which approval has not yet been authorized.
  - *Already approved*: Classifications for which an approval request has been authorized.
  - *Only approvals older than*: Selects approved classifications based on when the approvals were made.
  - *Only if they have been changed since approval*: Selects approved classifications that have been changed since approval was granted.
  - *List highlighted categories only*: Only [data categories](#)<sup>45</sup> containing any of the above classifications are listed. Otherwise all categories are listed
2. Select the report format (PDF or Word), and click **Create**.

Downloading the report opens the PDF in a browser, or the Word file (.docx format) in an application of your choice. Classifications that were selected for highlighting are displayed in a bold font.

## 8 Additional Features

This section explains features of the Altova GDPR Compliance Database that are additional to those described in preceding sections. The following features are described:

- [Changes](#)<sup>78</sup>
- [Search Filters on Pages](#)<sup>80</sup>

## 8.1 Changes

The Changes page lists changes that were made to the metadata held in the system (see screenshot below). It is accessed by clicking the *Changes* link at the top left of any page of the compliance database. The type of the changed metadata item that is listed depends on the page on which the *Changes* link is clicked. For example: if the *Changes* link is clicked on the [Overview page](#)<sup>20</sup>, then changes to all types of metadata item are shown (as in the screenshot below); but if the *Changes* link is clicked on the [Data Categories page](#)<sup>45</sup>, then only changes to data category items are listed.



The screenshot above shows the following:

- Changes made to all types of metadata item. (Access was via the [Overview page](#)<sup>20</sup>.)
- Changes made on 25.02.2019. The date can be:
  - navigated by using the navigation arrows (double arrowheads navigate through days on which changes exist, single arrowheads navigate through each day even if no change exists on that day);
  - selected via the icon in the central date field;
  - made the current date by clicking the icon at extreme left.
- Descriptions of changed metadata items, listed down to the fourth level of detail. The current level of detail is shown at the top right of the page. Click the arrowheads at top right to change the level of detail (Level 1 through Level 4). Descriptions at Level 4 show the status of approval requests. The screenshot below shows the same page at the first level of detail. The level of detail is useful for switching between an overview of changes and a detailed view of changes.

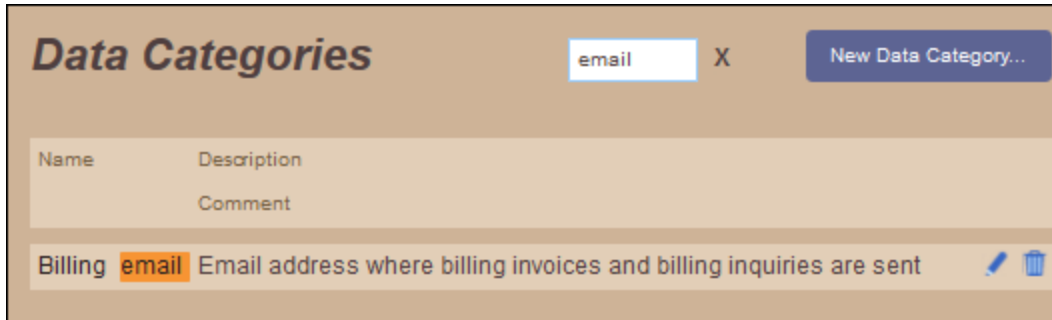


- The two screenshots above show that changes have been made to the data category *Customer Address* and to the processing activity *Employee Salaries*.
- The listing of each metadata item is a link that takes you directly to the definition of that item. For example, clicking on the *Category Customer Address* link in the screenshot above takes you to the definition of the *Customer Address* data category.
- If a discussion thread is available for a particular metadata item, then a *Discussions* link to the discussion threads of that item is displayed at the top right of the item's entry (see screenshots above).

To exit the Changes page you are on, click **Back**.

## 8.2 Search Filters on Pages

At the top of several pages, a field for entering search terms enables you to filter the items displayed on that page (see screenshot below).



Note the following points:

- The filter is applied as you type.
- Matches are case insensitive.
- To delete a search term, click the **Delete** icon located to the right of the search field.



# Index

## A

**Access information, 12**

**Altova GDPR Compliance Database,**

features, 5

**Approval request,**

definition of, 14

**Approval requests,**

authorizing, 59

creating, 57

discussions of, 59

relationships with other metadata, 57

## C

**Changes listing, 78**

**Changes to metadata,**

and discussions, 78

at different levels of detail, 78

filtered by date, 78

for different types of metadata item, 78

**Compliance database,**

user access, 12

**Compliance database's working mechanism, 17**

## D

**Data and metadata,**

definition of, 14

**Data categories,**

and obsolete classifications, 36

defining data usage classifications of, 52

managing and editing, 45

relationships with other metadata, 45

removing classifications for new categories, 36

**Data category,**

definition of, 14

**Data classification,**

definition of, 14

**Data classifications,**

managing and editing, 36

marking as obsolete, 36

relationships with other metadata, 36

**Data controller,**

definition of, 14

**Data controller metadata, 26**

**Data processor,**

definition of, 14

**Data processors,**

managing and editing metadata of, 42

relationships with other metadata, 42

**Data protection officer,**

definition of, 14

**Data receiver,**

definition of, 14

**Data storage entities,**

managing and editing information about, 49

relationships with other metadata, 49

**Data storage entity,**

definition of, 14

**Data usage classifications,**

managing and editing, 39

marking as obsolete, 39

of data categories in processing activities, 52

relationships with other metadata, 39

**Date format of system, 9**

**Department,**

definition of, 14

**Department role,**

definition of term, 14

**Department roles, 27**

creating, 28

relationships with other metadata, 28

**Departments, 27**

managing and editing metadata of, 28

relationships with other metadata, 28

**Discussion header,**

modifying, 69

**Discussion members,**

adding and removing, 69

**Discussions, 62**

available functionality, 69

initiator, member, participants, 67

listings of threads, 62

participating in, 69

starting, 67

threads of a single metadata item, 63

**Discussions, 62**

threads of all items of a metadata type, 65

**Discussions about approval requests, 59****E****Email of system users, 9****F****Features of the GDPR Compliance Database, 5****G****GDPR Compliance Database features, 5****L****Link of compliance database, 12****Logging out from the system, 24****Login of system users, 9****M****Metadata,**

definition of, 14

**Metadata relationships,**

description and diagram, 23

**N****Navigating the compliance database, 20****Navigation of compliance database,**

description and diagram, 22

**O****Overview page, 20****P****Password of system users, 9****Person,**

definition of, 14

**Persons, 27**

managing and editing metadata of, 31

relationships with other metadata, 31

**Processing activities,**

managing and editing information about, 52

relationships with other metadata, 52

**Processing activity,**

definition of, 14

**R****Reports, 71**

of categories based on approval status, 75

of critical processing activities, 73

of processing activities, 72

system requirements for, 71

**S****Search filters on pages, 80****T****Terminology, 14****U****URL of compliance database, 12**

**User management, 7**

**User management app,**

how to access and use, 9

**Users of compliance database,**

creating new, 9

editing properties of, 9