

## Auflösung der Mitgliedschaften

Wird eine Gruppe ausgewählt, so befindet sich unterhalb eine Liste aller Mitglieder der Gruppe. Wird ein Benutzer ausgewählt, so befindet sich unterhalb eine Liste aller Gruppen des Benutzers. Die Anzeige der Mitglieder der Gruppe beziehungsweise der Mitgliedschaften des Benutzers umfasst nur die direkt zugeordneten Benutzer / Gruppen. Es erfolgt in dieser Ansicht keine automatische Auflösung dieser Objekte.

## Neue Berechtigung setzen

Um eine neue Berechtigung für einen Benutzer oder eine Gruppe zu setzen, geben Sie zuerst einen Suchbegriff in der linken Seite der Maske in das Suchfeld ein.

### **Suchbegriff**

Sie müssen mindestens 4 Zeichen eingeben, damit die Suche aktiviert wird.

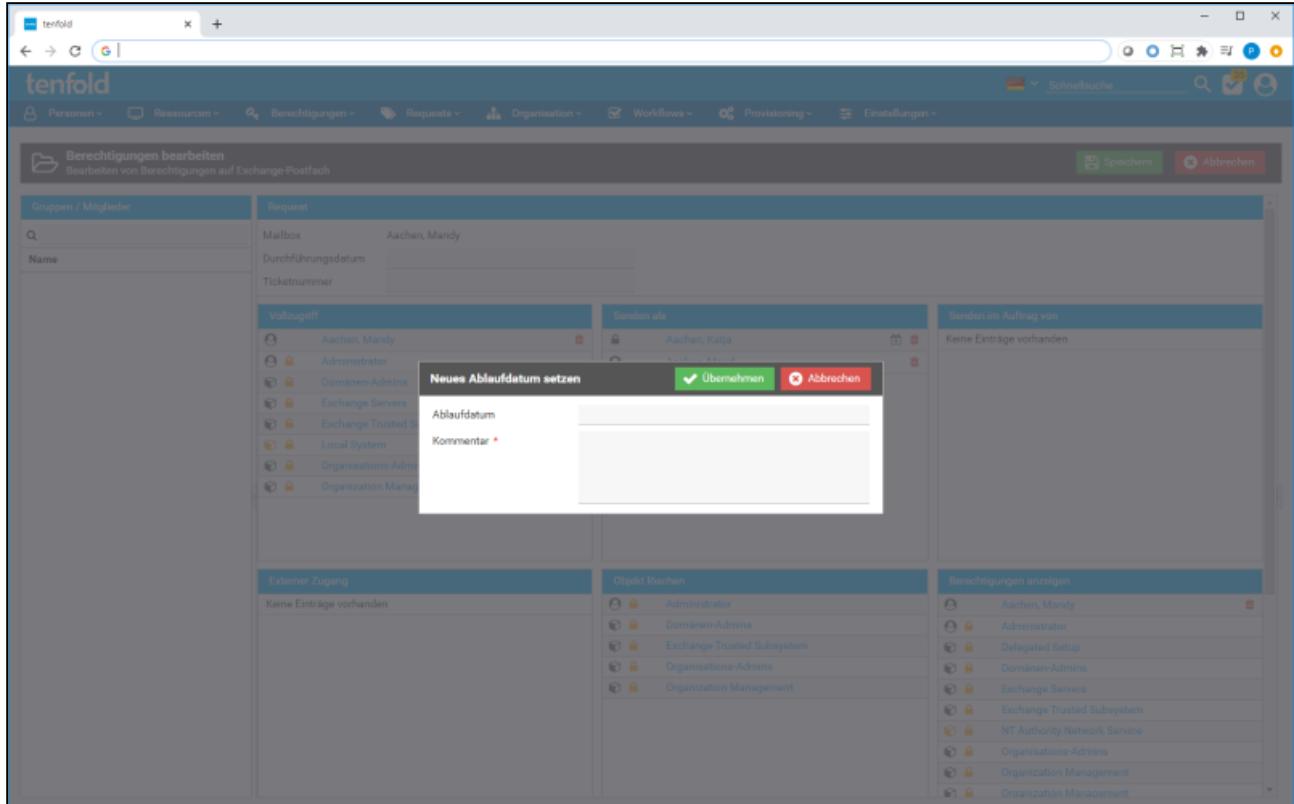
Dieser Begriff kann sein:

- Anzeigename einer Gruppe
- Benutzername eines Benutzers
- Anzeigename eines Benutzers

Wenn Sie den genauen Benutzer- oder Gruppennamen nicht kennen, geben Sie einfach den Teil ein, der Ihnen bekannt ist. Sie müssen hierbei keine Wildcards (Platzhalter) wie "\*" oder "%" nutzen.

Die Suche listet alle passenden Benutzer und Gruppen (erkennbar an den üblichen Symbolen) auf. Sie können diese nun per Drag & Drop in eines der Berechtigungsfelder ziehen. Der Eintrag erscheint daraufhin im gewählten Berechtigungsfeld mit einem Plussymbol. Dies kennzeichnet, dass die Berechtigung nun zur Zuordnung vorgesehen ist. Es bedeutet nicht, dass die Berechtigung schon zugeordnet ist. Der Request für die Änderung der Berechtigungen wird erst im System gespeichert, wenn sie den Speichern-Button in der Toolbar anwählen.

## Berechtigungen befristen



Sie haben sowohl für bestehende, als auch für gerade neu zuzuordnende Berechtigungen die Möglichkeit, diese zu befristen. Um eine Befristung einzustellen (oder eine bestehende Befristung zu ändern), klicken Sie auf das Kalendersymbol innerhalb der gewünschten Zeile im Berechtigungsfeld.

Im Dialog, der sich durch Klick auf das Kalendersymbol öffnet können Sie das gewünschte Enddatum sowie eine Begründung für die Befristung hinterlegen. Abhängig von den Systemeinstellungen

"Postfachberechtigungen bearbeiten - Kommentar anzeigen" und "Postfachberechtigungen bearbeiten - Kommentar verpflichtend" (siehe [Systemparameter\(see page 484\)](#)) ist die Eingabe eines Kommentars verpflichtend oder optional.

## Berechtigung löschen

Bestehende Berechtigungen können gelöscht werden, indem Sie in der gewünschten Zeile im jeweiligen Berechtigungsfeld auf das Papierkorbsymbol klicken. Neben dem Eintrag erscheint nun ein rotes Kreuzsymbol, womit vermerkt ist, dass die Berechtigung zur Löschung vorgesehen ist. Es bedeutet allerdings *nicht*, dass die Berechtigung schon gelöscht wurde! Der Request für die Änderung der Berechtigungen wird erst im System gespeichert, wenn sie den Speichern-Button in der Toolbar anwählen.

## Änderungen speichern

Um die Änderungen als Request zu speichern, klicken Sie abschließend auf den Speichern-Button in der Toolbar. Sie können, abhängig von der Konfiguration, zusätzlich folgende Informationen festlegen:

- Durchführungsdatum: Legt fest, dass die Durchführung frühestens zum angegebenen Datum gestartet werden soll. Sollte der Request zu diesem Zeitpunkt noch nicht genehmigt sein, verzögert dies die Durchführung zusätzlich.
- Ticketnummer: Ticketnummer, die im Request abgelegt werden soll. Hier kann beispielsweise eine Referenz zu einem Helpdesk-Ticket hinterlegt werden, welches die Änderung veranlasst hat.
- Kommentar: Es kann hier ein erklärender Kommentar hinterlegt werden, zum Beispiel eine Begründung für die Änderung, die zur Genehmigung durch den Dateneigentümer erforderlich ist.

Durch das Speichern werden die gewünschten Änderungen als Request in der Datenbank abgelegt. Die tatsächliche Durchführung der Änderung hängt vom hinterlegten Genehmigungsworkflow sowie anderen Einstellungen ab.

### 7.4.4 Weitere Aktionen

Die nachfolgenden Aktionen können über das Menü "Aktion" durchgeführt werden.

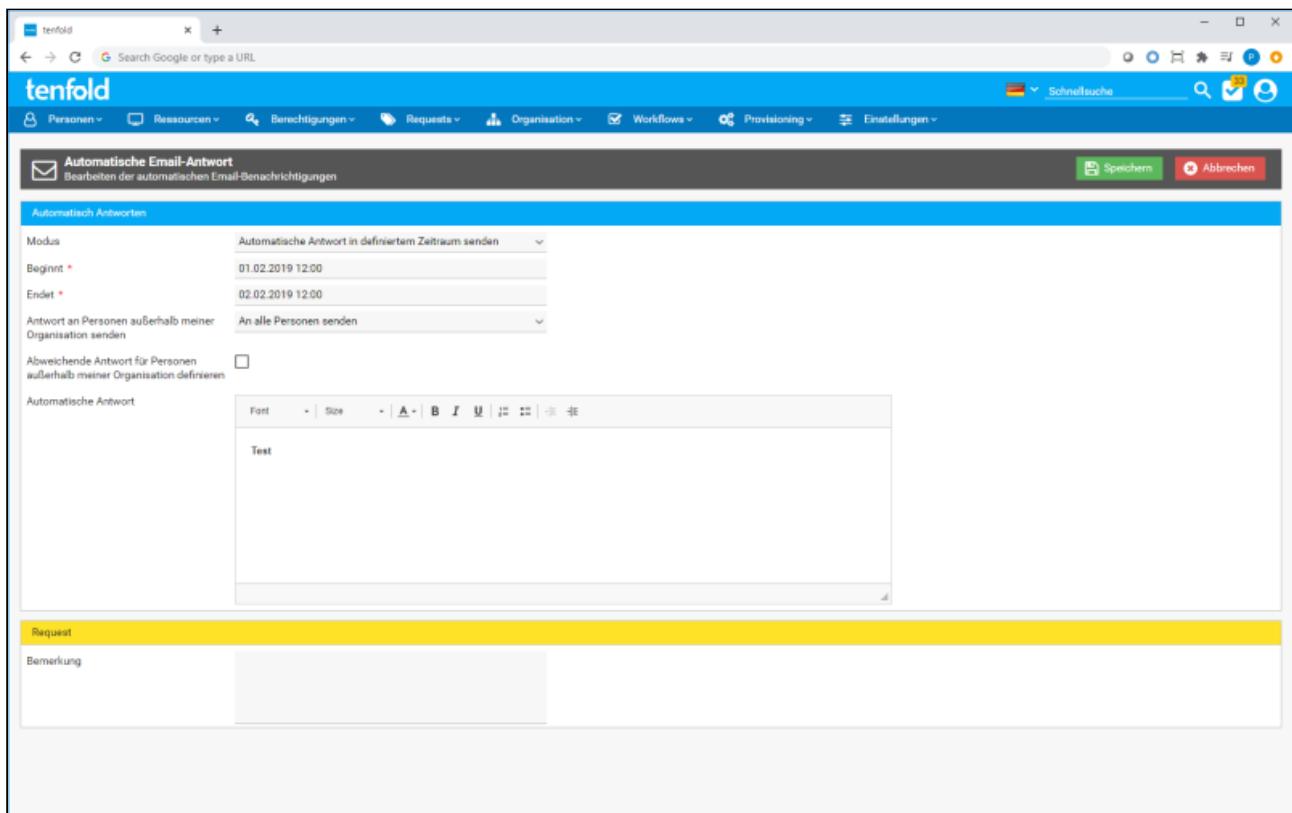
#### Verfügbarkeit

Die Verfügbarkeit der nachfolgend beschriebenen Aktionen hängt von den Berechtigungen des angemeldeten Benutzers sowie davon ob das ausgewählte Objekt ein Verzeichnis oder ein Postfach ist.

#### Automatisch Antworten

#### Postfachfunktion

Diese Funktion steht nur für Postfächer zur Verfügung und kann für Verzeichnisse nicht ausgewählt werden.



Mit dieser Maske lässt sich für beliebige Postfächer die Funktion "Automatisch Antworten" aktivieren, deaktivieren bzw. die jeweiligen Einstellungen anpassen und auslesen. Dies kann zum Beispiel dann von Nutzen sein, wenn Mitarbeiter vergessen haben, vor einer längeren Abwesenheit (Urlaub, Elternzeit) ihre Abwesenheitsnachrichten zu setzen.

Die Einstellungen entsprechen hier den jeweiligen Einstellungsmöglichkeiten in Exchange.

Einstellung	Beschreibung
Modus	Mit dieser Einstellung kann konfiguriert werden, ob und wann automatische Antworten für dieses Postfach gesendet werden sollen. Die möglichen Einstellungen sind: "Keine automatischen Antworten senden", welche diese Funktion deaktiviert, "Automatische Antwort senden", welche automatische Antworten für einen unbestimmten Zeitraum aktiviert, und "Automatische Antwort in definiertem Zeitraum senden", womit sich diese Funktion ab und bis zu einem definierten Zeitraum aktivieren lässt.
Beginnt	Definiert das Datum, ab dem die automatischen Antworten gesendet werden. Diese Einstellung ist nur verfügbar, wenn der Modus "Automatische Antwort in definierten Zeitraum senden" ausgewählt wurde.
Endet	Definiert das Datum, bis wann automatische Antworten gesendet werden. Diese Einstellung ist nur verfügbar, wenn der Modus "Automatische Antwort in definierten Zeitraum senden" ausgewählt wurde.

Einstellung	Beschreibung
Antwort an Personen außerhalb meiner Organisation senden	Mit dieser Option lässt sich einstellen, an welche Personen, außerhalb der Organisation des Postfachs, Antworten gesendet werden. Mit der Auswahl "Nicht senden" werden automatische Antworten nur an Personen innerhalb der eigenen Organisation gesendet.
Abweichende Antwort für Personen außerhalb meiner Organisation definieren	Diese Option steht nur zur Verfügung, wenn automatische Antworten gesendet werden und ausgewählt wurde, dass Personen außerhalb der eigenen Organisation Antworten erhalten sollen. Bei Auswahl dieser Option können zwei verschiedene Antworten definiert werden.
Automatische Antwort	Legt den Text fest, welcher an Personen innerhalb und außerhalb der eigenen Organisation gesendet werden soll. Dieses Feld steht nur zur Verfügung, wenn die Option "Abweichende Antwort für Personen außerhalb meiner Organisation definieren" nicht ausgewählt wurde.
Automatische Antwort innerhalb meiner Organisation	Legt den Text fest, welcher an Personen innerhalb der Organisation des Postfachs gesendet werden. Diese Einstellung steht nur zur Verfügung, wenn die Option "Abweichende Antwort für Personen außerhalb meiner Organisation definieren" ausgewählt wurde.
Automatische Antwort außerhalb meiner Organisation	Legt den Text fest, welcher an Personen außerhalb der Organisation des Postfachs gesendet werden. Diese Einstellung steht nur zur Verfügung, wenn die Option "Abweichende Antwort für Personen außerhalb meiner Organisation definieren" ausgewählt wurde.

Zusätzlich zu den Einstellungen für die automatischen Antworten kann auch noch ein Kommentar eingegeben werden, welcher bei dem Request hinterlegt wird, der entsteht, wenn Sie "Speichern" betätigen.

## Stellvertreter

### Postfachfunktion (Exchange 2013+)

Diese Funktion steht nur für Postfächer zur Verfügung. Außerdem wird diese Funktion von Exchange Servern vor der Version 2013 nicht unterstützt.

Mit dieser Aktion lassen sich Mailbox-Stellvertreter definieren, welche diverse Zugriffsberechtigungen auf das gewählte Postfach haben.

## Details

-  Ackermann, Gabriele
-  tenfold\gackermana
-  S-1-5-21-566901642-699043585-1907573982-1111
-  CN=Gabriele\, Ackermann,OU=Zürich,OU=tenfold,DC=tenfold,DC=local
-  tenfold

## Mitglied von

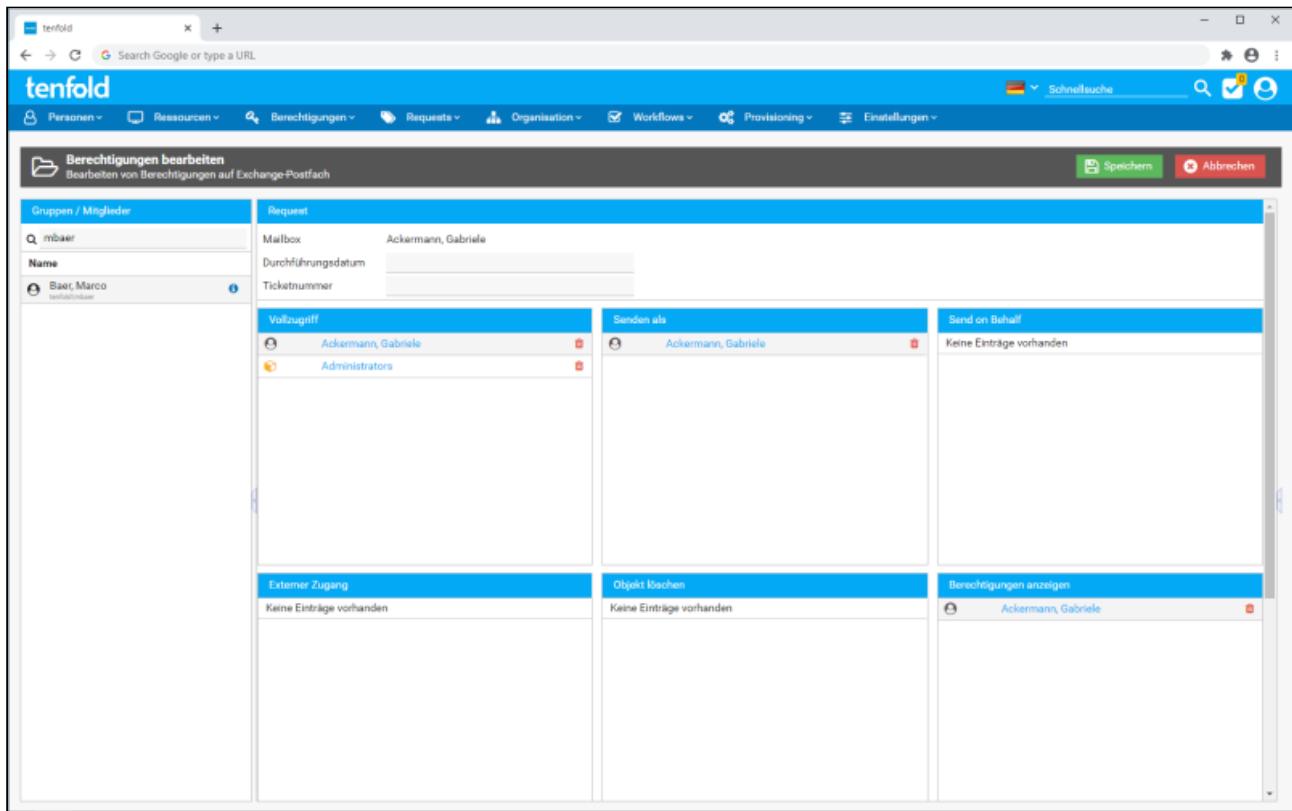
### Name

-  Domain Users
-  Org.IT
-  org\_toronto
-  Users

### Stellvertreter in tenfold und Exchange

Bitte beachten Sie, dass es sich bei den Postfach-Stellvertretern um eine Berechtigungseinstellung von Exchange handelt und nicht mit der Stellvertreterfunktion von tenfold verwechselt werden darf (siehe [Stellvertretungen\(see page 372\)](#)).

Um einen neuen Stellvertreter für das Postfach festzulegen, geben Sie einen Suchbegriff im linken Bereich ein und ziehen Sie dann mittels Drag & Drop ein gefundenes Objekt in den Zentralen Bereich des Schirms. Es öffnet sich ein Dialog, in dem Sie die Berechtigungen für die einzelnen Bereiche festlegen können.



Wählen Sie hier die gewünschten Berechtigungen, welche Sie dem Postfachstellvertreter erteilen möchten und klicken Sie anschließend auf die Schaltfläche "Speichern".

Sie können auch bestehende Stellvertretungen bearbeiten indem Sie die Schaltfläche "Bearbeiten" des jeweiligen Eintrages betätigen oder durch einen Klick auf "Löschen" die Stellvertretung entfernen.

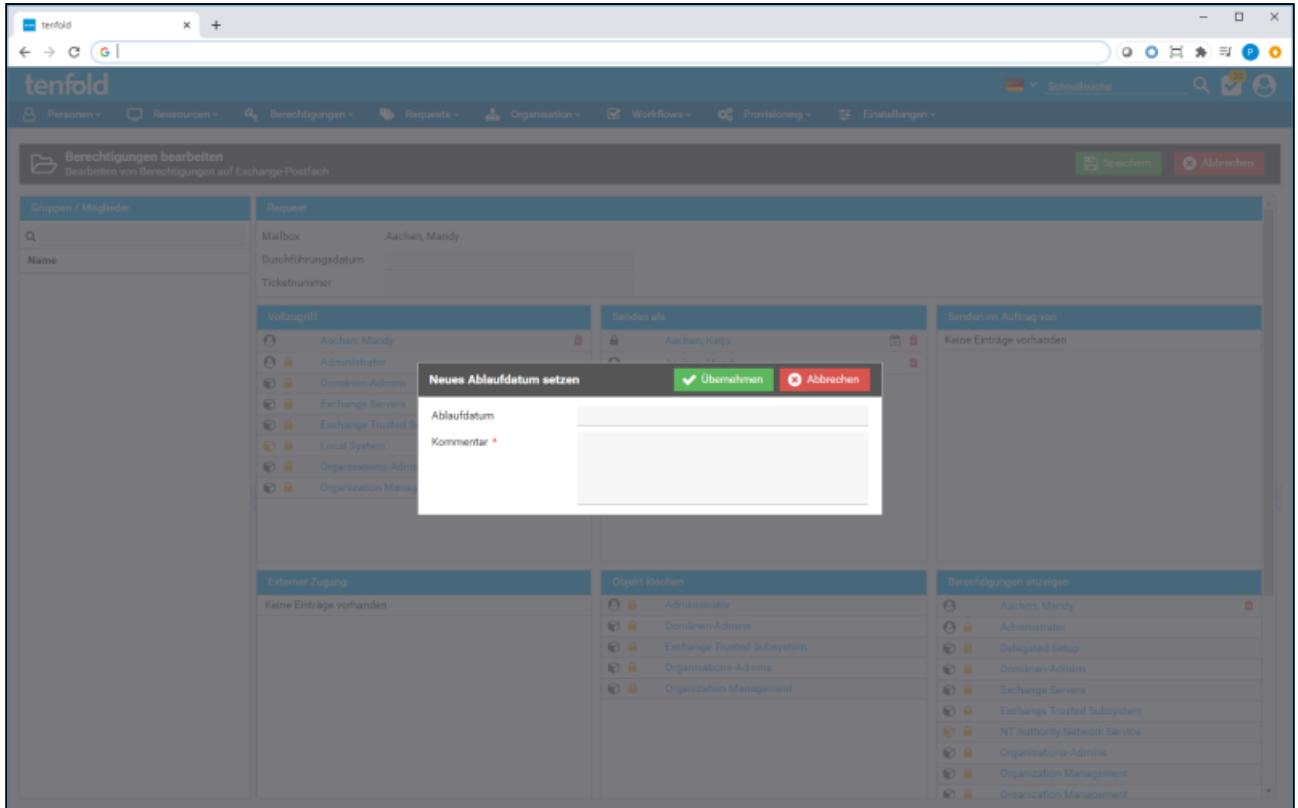
#### **Speichern nicht vergessen**

Die gewählten Einstellungen werden erst übernommen, wenn Sie auf der Maske die Schaltfläche "Speichern" betätigten.

## Aktualisieren

Die Darstellung der Exchange-Berechtigungen und Einstellungen basiert auf dem aktuellen Datenstand der tenfold Datenbank. Diese wird in regelmäßigen Abständen von einem Job aus Exchange ausgelesen und in die tenfold Datenbank übertragen. Sollte es notwendig sein, kann mit der Aktion "Aktualisieren" tenfold dazu veranlasst werden ein einzelnes Objekt und alle darunterliegenden Elemente neu einzuscanen um den aktuellen Stand in der Datenbank zu erhalten.

## Dateneigentümer



Mit dieser Funktion können Sie Dateneigentümer für Verzeichnisse und Postfächer definieren, welche in die Genehmigungsworflows zu Exchange Requests eingebunden werden können. Über die Schaltfläche "Hinzufügen" können Sie einen neuen Eintrag in die Liste hinzufügen. Im darauf folgenden Dialog wählen Sie einfach eine Person aus und haken an ob der neue Dateneigentümer E-Mail Benachrichtigungen über anstehende Genehmigungen erhalten soll oder nicht.

Über das Aktionsmenü des jeweiligen Eintrages können Sie bestehende Dateneigentümer löschen oder die Einträge bearbeiten.

Die getroffenen Änderungen werden mit einem Klick auf die Schaltfläche "Speichern" übernommen.

## Einstellungen

Mit der Aktion "Einstellungen" erscheint ein Dialog in welchem Sie die Einstellung des ausgewählten Genehmigungsworflow für ein einzelnes Postfach oder Verzeichnis überschreiben können.

Genehmigungsworflows lassen sich für den gesamten Exchange Server einstellen (siehe [Einrichtung der Exchange Server](#)(see page 233)) bzw. existiert ein vordefinierter Genehmigungsworflow "Ex request approval" (siehe [Genehmigungsworflows](#)(see page 380)) welcher als Fallback fungieren kann, sollte am jeweiligen Objekt oder Exchange Server kein anderer Workflow hinterlegt sein.

## 7.5 Verwaltung der SharePoint-Berechtigungen

### 7.5.1 Allgemeines

The screenshot shows the tenfold SharePoint Server management interface. On the left, a tree view lists SharePoint sites under a user named Charlie. One site, 'Projekte - Moonshot (P111)', is selected and highlighted in yellow. The right side displays detailed information for this selected item, including its URL (<http://dv-srv-sharepoi/websites/P111>), type (Webseite), and details for all permissions (2). It also shows the Site Administrators and the specific user Bachmeier, Alexander.

#### Benötigte Berechtigung

Um die Maske zur Verwaltung der SharePoint-Berechtigungen nutzen zu können ist eine administrative Berechtigung auf zumindest einem SharePoint-Server erforderlich (siehe [Berechtigungen\(see page 457\)](#)).

Auf der Maske "SharePointServer" (erreichbar im Menü unter *Berechtigungen > SharePoint Server*) können Sie die Berechtigungen Ihrer SharePoint-Server verwalten. Ähnlich wie die Maske zur Verwaltung der Fileserver-Berechtigungen (siehe [Verwaltung der Fileserver-Berechtigungen\(see page 269\)](#)) finden Sie hier Ihre eingelesenen SharePoint-Server in einer Baumstruktur vor, in welcher Sie die Berechtigungen zu jedem Item einsehen bzw. verändern können.

#### Objektverwaltung

Im Gegensatz zur Maske für Fileserver-Berechtigungen können die Items hier nicht verwaltet werden. Das bedeutet, dass Sie keine Items anlegen, löschen, umbenennen, etc. können. Es werden lediglich die Berechtigungen verwaltet.

## 7.5.2 Berechtigungen anzeigen

Die Anzeige der Berechtigungen ist Analog zur Maske der Fileserver-Berechtigungen aufgebaut (siehe [Verwaltung der Fileserver-Berechtigungen\(see page 269\)](#)). Im linken Bereich der Maske finden Sie den Bereich "SharePoint", welcher eine Baumansicht aller eingescannten SharePoint Server enthält.

### Zugriff auf SharePoint

Diese Maske greift nicht direkt auf Ihren SharePoint zu, sondern liest die Daten aus der tenfold-Datenbank, welche in konfigurierten Intervallen mit Ihren SharePoints synchronisiert wird (siehe [Jobs\(see page 443\)](#)).

Folgende Informationen zu den Items finden Sie in der Ansicht:

Spalte	Beschreibung
(Item)	In der linksten Spalte (ohne Titel) finden Sie den Namen des Items sowie ein Icon, welches auf den Typ des Items hinweist. <b>Hinweis:</b> Im Tooltip des Icons finden Sie die Bezeichnung der Item-Art.
Eigenschaften	In dieser Spalte finden Sie verschiedene Informationen zu dem Item, in Bezug auf dessen Berechtigungen oder tenfold-Einstellungen. Diese werden in Form von Icons dargestellt. Im Tooltip des jeweiligen Icons erfahren Sie nähere Informationen. Folgende Eigenschaften werden angezeigt: <ul style="list-style-type: none"> <li>• Ob die Vererbung der Berechtigungen auf diesem Item unterbrochen wurde.</li> <li>• Ob ein individueller Genehmigungsworkflow (siehe <a href="#">Genehmigungsworkflows(see page 380)</a>) für dieses Item in tenfold eingestellt wurde.</li> <li>• Wieviele Berechtigungen auf diesem Item gesetzt wurden (muss über "Eigenschaften" aktiviert werden)</li> <li>• Wieviele Berechtigungen auf Unter-Items direkt gesetzt wurden (muss über "Eigenschaften" aktiviert werden)</li> <li>• Auf wievielen Unter-Items die Vererbung aufgebrochen wurde (muss über "Eigenschaften" aktiviert werden)</li> </ul>
URL	Der URL der Website, unter welchem das Item in Ihrem SharePoint abrufbar ist.

Im Kopfbereich der Maske finden Sie die Schaltfläche "Eigenschaften". Durch einen Klick auf die Schaltfläche erhalten Sie ein Dropdown, in welchem Sie erweiterte Eigenschaften einblenden können oder wieder ausblenden, wenn diese gerade angezeigt werden. Folgende Auswahlmöglichkeiten stehen zur Verfügung:

Option	Beschreibung
Anzahl expliziter Berechtigungen	Mit dieser Option wird die Anzahl der direkt gesetzten Berechtigungen auf einem Unterobjekt angezeigt. Außerdem wird auch die Anzahl der direkt gesetzten Berechtigungen auf den Unter-Items eines jeden Items angezeigt.

Option	Beschreibung
Anzahl unterbrochener Vererbungen	Zeigt an, bei wievielen Unter-Items des Items die Vererbung aufgebrochen wurde. <b>Hinweis:</b> Unabhängig von dieser Einstellung wird immer angezeigt, ob die Vererbung auf dem Item selbst aufgebrochen wurde.

#### Anzahl nicht sichtbar

Unter Umständen ist die Anzahl der gesetzten Berechtigungen erst nach dem zweiten Scan Ihres SharePoints verfügbar. Sollte Ihnen die Anzahl der Berechtigungen nicht angezeigt werden, führen Sie erneut einen Scan durch (siehe [Jobs\(see page 443\)](#)).

Im rechten Teil der Maske sind mehrere Bereiche vorhanden, welche Ihnen Details zum aktuell ausgewählten Item in der Baumansicht anzeigen. Im Bereich "Details" finden Sie allgemeine Informationen zum ausgewählten Item:

- Name des Items
- Status der Berechtigungsvererbung
- Typ des Items
- Link zur Seite des Items in SharePoint

Sollte die Vererbung der Berechtigungen aktiv sein, erhalten Sie an dieser Stelle einen Hinweis, dass auf diesem Item keine Berechtigungen gesetzt werden können.

#### Berechtigungen und Vererbung

SharePoint erlaubt das Setzen von Berechtigungen nur auf Items mit deaktivierter Vererbung. Dies ist **keine** Einschränkung seitens tenfold. Wenn Sie Berechtigungen vergeben möchten, müssen Sie zuerst an dieser Stelle die Vererbung aufbrechen.

Im Bereich "Berechtigungen" finden Sie eine Baumansicht aller vergebenen Berechtigungen auf diesem Item. Der oberste Knoten der Ansicht ist "Alle Berechtigungen", unter welchem sich Knoten mit allen auf diesem Item vergebenen Berechtigungen befinden. Unterhalb der Berechtigungsknotens finden Sie die Gruppen und Konten, welche die jeweilige Berechtigung erhalten haben. Im Falle von Gruppen können Sie diese weiter aufklappen, um die Mitglieder der Gruppen anzuzeigen.

Unterhalb finden Sie den Bereich "Details für ...". In diesem Bereich finden Sie eine Auflistung sämtlicher Konten, welche auf dem Item berechtigt sind. In dieser Ansicht sind bereits sämtliche Gruppen aufgebrochen, so dass Sie hier ausschließlich Konten vorfinden. Sie können die jeweiligen Konten aufklappen, um anzusehen, durch welche Gruppen (oder direkten Berechtigungen) die Berechtigung erhalten wurde.

Normalerweise werden hier alle Konten angezeigt, egal welche Berechtigung sie auf diesem Item besitzen. Durch einen Klick auf einen der Berechtigungsknoten im Bereich "Berechtigungen" können Sie die Ansicht "Details für..." auf die jeweilige Berechtigung filtern. Es werden daraufhin nur noch Konten angezeigt, welche die ausgewählte Berechtigung besitzen.

#### Filter aufheben

Durch einen Klick auf den Knoten "Alle Berechtigungen" im Bereich "Berechtigungen" werden wieder alle Konten angezeigt.

Die ausgewählte Berechtigung spiegelt sich im Titel des Bereichs wieder. (Beispiel: "Details für Alle Berechtigungen", "Details für Vollzugriff", etc.).

### 7.5.3 Berechtigungen bearbeiten

Um die Berechtigungen auf einem Item zu bearbeiten, wählen Sie ein Item mit aufgebrochener Vererbung im Item-Baum aus und betätigen anschließend im Bereich "Details" die Schaltfläche "Berechtigungen".

Im Bereich "Gruppen / Mitglieder" befindet sich ein Suchfeld, mit welchem Sie nach Gruppen und Konten suchen können. Geben Sie einen Text ein und es wird Ihnen eine Liste aller Gruppen/Konten dargestellt, welche den eingegebenen Text enthalten.

#### Mindestanzahl an Zeichen

Die Suche startet erst, wenn Sie mindestens drei Zeichen eingegeben haben. Sollten Sie mit weniger Zeichen eine Suche starten wollen, können Sie auch die "Enter"-Taste betätigen.

Diese Suche kann Ihnen SharePoint-, Active Directory-, sowie Microsoft 365-Objekte liefern. Welche Objekte gefunden werden, hängt von der Art Ihres SharePoints ab:

- **On Premises:** Es werden Active-Directory sowie SharePoint-Objekte gefunden
- **Microsoft 365:** Es werden Microsoft-365 sowie SharePoint-Objekte gefunden

Sie erhalten nur jene SharePoint-Objekte, die auf dem jeweiligen SharePoint vorhanden sind.

Im Bereich "Request" können Sie Einstellungen vornehmen, welche die Erstellung der Requests (siehe [Requests\(see page 352\)](#)), die durch die Berechtigungsvergabe entstehen, beeinflusst. Folgende Einstellungen stehen zur Verfügung:

Einstellung	Beschreibung
Durchführungsdatum	Geben Sie hier ein Datum ein, dann werden die Berechtigungen erst an diesem Datum vergeben. Wenn Sie das Datum leer lassen, werden die Requests sofort erstellt.
Ticketnummer	Sie können hier eine Ticketnummer eingeben, die allen erzeugten Requests beigelegt wird.

Unterhalb dieses Bereiches finden Sie Bereiche für alle zur Verfügung stehenden Berechtigungen dieses Items. Innerhalb dieser werden Ihnen die aktuell berechtigten Konten/Gruppen angezeigt.

Wenn Sie auf einen der Einträge in einem dieser Bereich klicken, wird Ihnen ein weiterer Bereich auf der rechten Seite der Maske eingeblendet, welcher Ihnen Details zum ausgewählten Berechtigungsinhaber anzeigt.

### Vergabe neuer Berechtigungen

Um eine neue Berechtigung zu vergeben, suchen Sie in der Suchleiste nach dem gewünschten Objekt und ziehen es dann mit der Maus in den Bereich der gewünschten Berechtigung. Daraufhin erscheint in diesem Bereich ein neuer Eintrag mit dem gesuchten Objekt. Rechts neben dem Icon, welches den Typ des berechtigten Objektes angibt, wird Ihnen ein Plus-Icon angezeigt, welches verdeutlicht, dass es sich um eine Berechtigung handelt, die noch nicht gespeichert wurde. Durch einen Klick auf das Mülleimer-Icon am rechten Ende der jeweiligen Zeile können Sie die gerade hinzugefügte Berechtigung wieder entfernen. Sie können beliebig viele neue Berechtigungen zu dem Item hinzufügen. Wenn Sie fertig sind, betätigen Sie die Schaltfläche "Speichern". Es werden daraufhin Requests für alle neuen Berechtigungen erstellt. Sobald die Requests genehmigt wurden oder wenn keine Genehmigung eingerichtet wurde (siehe [Genehmigungsworkflows\(see page 380\)](#)), werden die Berechtigungen zum jeweiligen Durchführungsdatum (oder sofort) angepasst.

### Entfernen vorhandener Berechtigungen

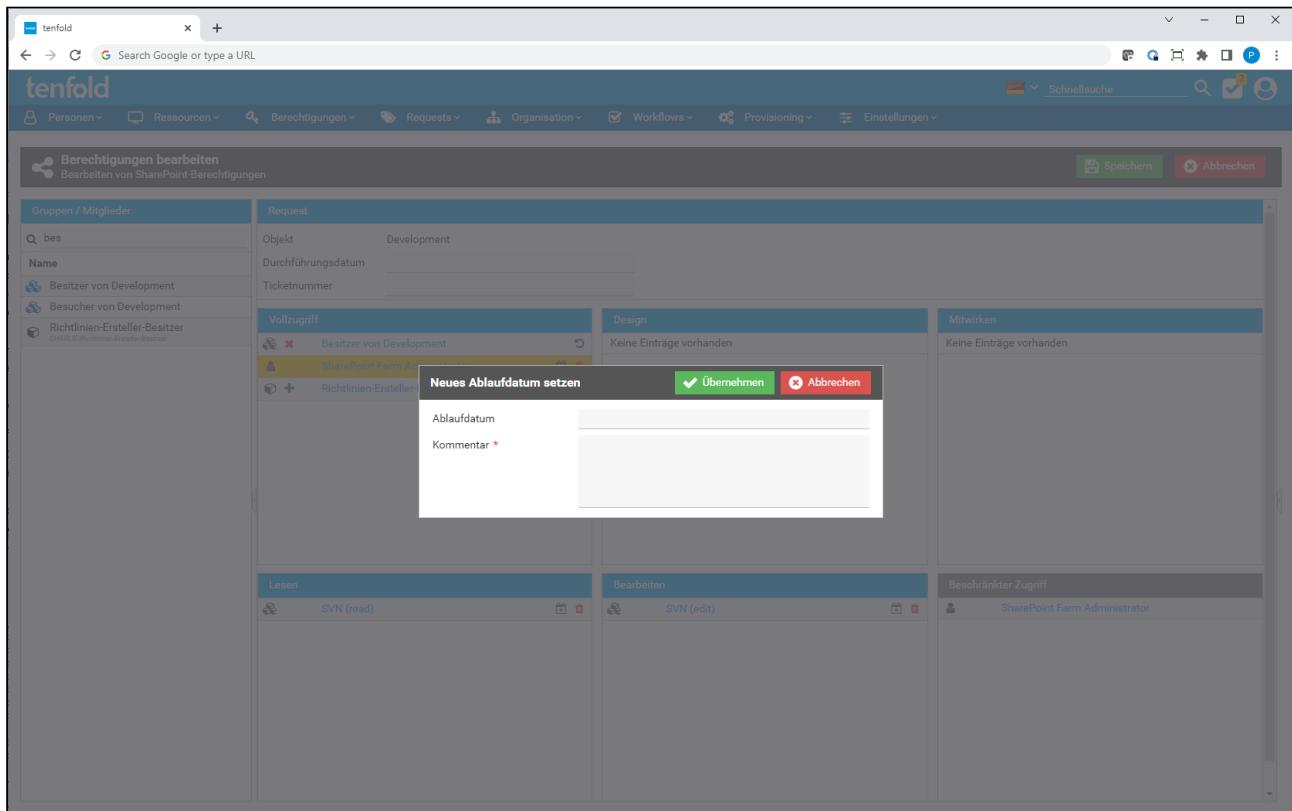
Zum Entfernen vorhandener Berechtigungen, klicken Sie auf das Mülleimer-Icon am rechten Rand des jeweiligen Eintrags. Daraufhin wird dieser zu einem Rückgängig-Icon, welches Sie betätigen können, falls Sie es sich anders überlegt haben. Sie können beliebig viele Löschen durchführen. Sollten Sie mit Ihren Einstellungen zufrieden sein, betätigen Sie die Schaltfläche "Speichern", um für alle entfernten Berechtigungen Requests anzulegen. Sobald die Requests genehmigt wurden oder wenn keine Genehmigung eingerichtet wurde (siehe [Genehmigungsworkflows\(see page 380\)](#)), werden die Berechtigungen zum jeweiligen Durchführungsdatum (oder sofort) angepasst.

#### Hinzufügen & Löschen

Sie können in einem Durchgang sowohl Berechtigungen hinzufügen als auch entfernen.

### Ablaufdatum von Berechtigungen ändern

Durch einen Klick auf das Kalender-Icon neben einem Eintrag öffnet sich ein Dialog, in welchem Sie ein Ablaufdatum für eine Berechtigung eingeben können.



Im Feld "Ablaufdatum" kann ein Datum hinterlegt werden, zu welchem die ausgewählte Berechtigung entfernt werden soll. Sollte bereits ein Ablaufdatum eingetragen sein, so kann dieses durch leeren des Eingabefeldes auch wieder entfernt werden. Weiters muss ein Kommentar hinterlegt werden, welcher angibt, warum das Datum geändert werden soll.

Durch einen Klick auf die Schaltfläche "Übernehmen" werden die vorgenommen Änderungen in die Maske übernommen.

Sobald Sie die Schaltfläche "Speichern" betätigen werden Requests zur Änderung aller Ablaufdaten angelegt. Sobald diese genehmigt wurden oder falls keine Genehmigung eingerichtet wurde, werden die Änderungen der Ablaufdaten aktiv.

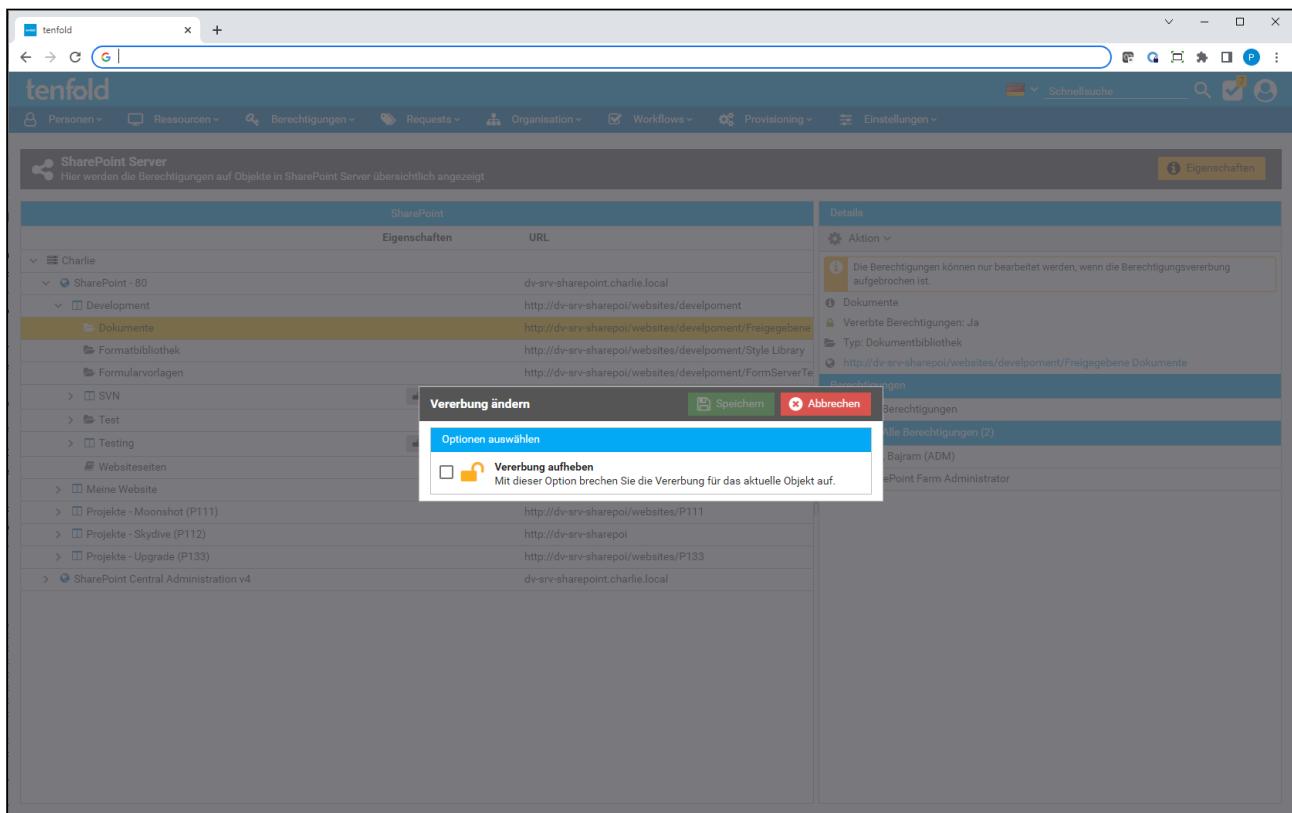
#### **tenfold-Funktion**

Die Funktion für Ablaufdaten von Berechtigungen wird rein durch tenfold umgesetzt. SharePoint bietet hierfür keine Funktion an. Die eingestellten Ablaufdaten sind daher in SharePoint nicht ersichtlich.

#### **Vererbung ändern**

Um die Vererbung von Berechtigungen zu ändern, wählen Sie in der Übersichtsmaske ein Item aus und wählen im Bereich "Details" im Aktionsmenü die Aktion "Vererbung ändern".

Sollte die Vererbung aktiviert sein öffnet sich ein Dialog, in welchem Sie die Vererbung aufheben können.

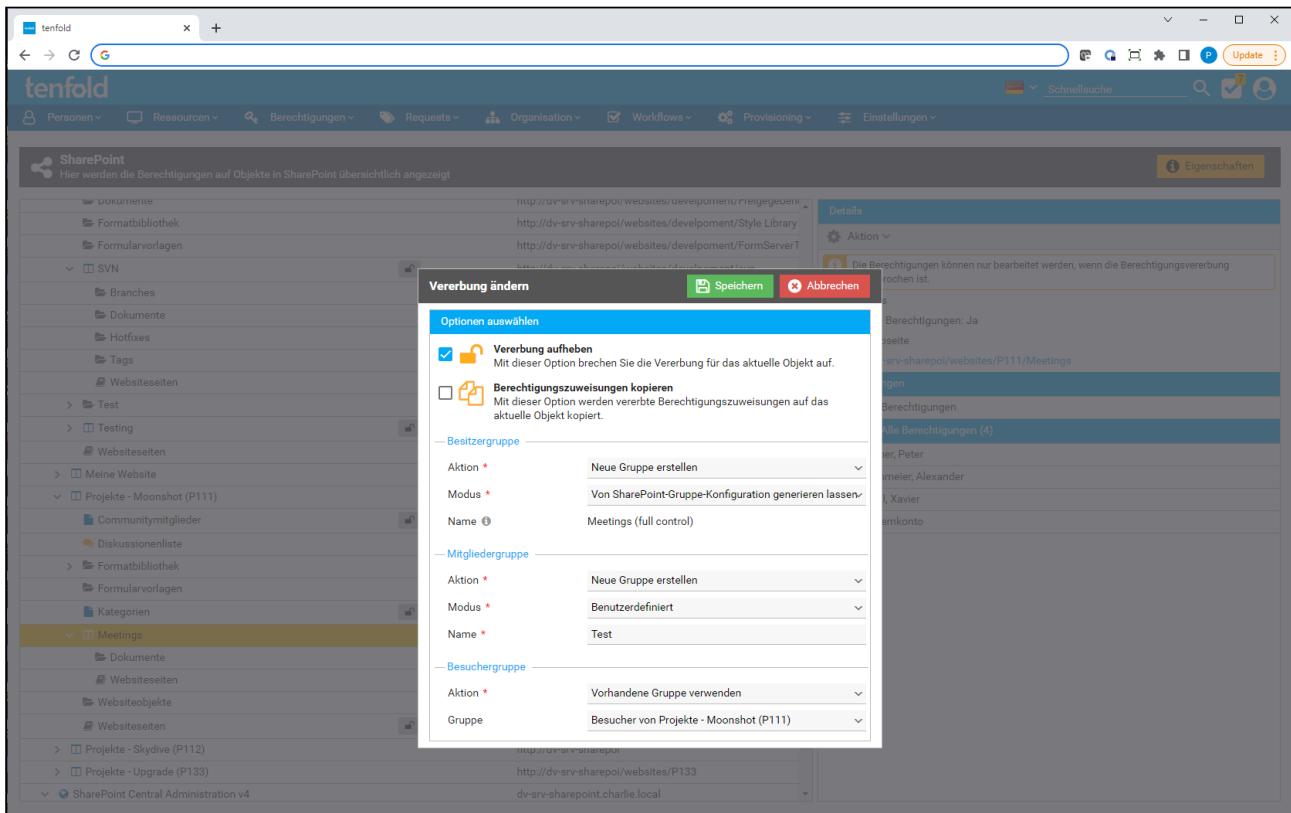


Haken Sie "Vererbung aufheben" an und es erscheint eine weitere Option, mit welcher Sie entscheiden können, ob die Berechtigungen, die aktuell geerbt werden, auf dieses Item kopiert werden sollen oder nicht. Wenn Sie diese Option nicht anwählen, gibt es zunächst keinen Zugriff auf das Item, bis Berechtigungen gesetzt werden.

Sollte es sich bei dem Item um eine "Website" handeln, dann erhalten Sie außerdem noch weitere Optionen zur Anlage der Standardberechtigungsgruppen von SharePoint.

### Top-Level Websites

Auf den Websites auf der obersten Ebene lässt sich die Vererbung nicht verändern. Daher sind diese Einstellungen für diese Websites auch nicht verfügbar.



Hierbei handelt es sich um die Gruppen für:

- Besitzer (Vollzugriff)
- Mitglieder (Bearbeiten)
- Besucher (Lesen)

Für jede dieser Gruppen können Sie folgende Einstellungen treffen:

Einstellung	Beschreibung
Aktion	Legt fest, ob eine neue Gruppe für diese Website angelegt werden soll oder ob eine vorhandene Gruppe verwendet werden soll.
<b>Aktion "Neue Gruppe erstellen"</b>	
Modus	Mit dieser Einstellung wird festgelegt, wie der Name der Gruppe erzeugt werden soll. Es stehen folgende Optionen zur Auswahl: <ul style="list-style-type: none"> <li>• <b>Von SharePoint-Gruppe-Konfiguration generieren lassen:</b> Der Gruppenname wird anhand der eingestellten Namensrichtlinie automatisch generiert.</li> <li>• <b>Benutzerdefiniert:</b> Der Name der Gruppe muss händisch eingegeben werden.</li> </ul>

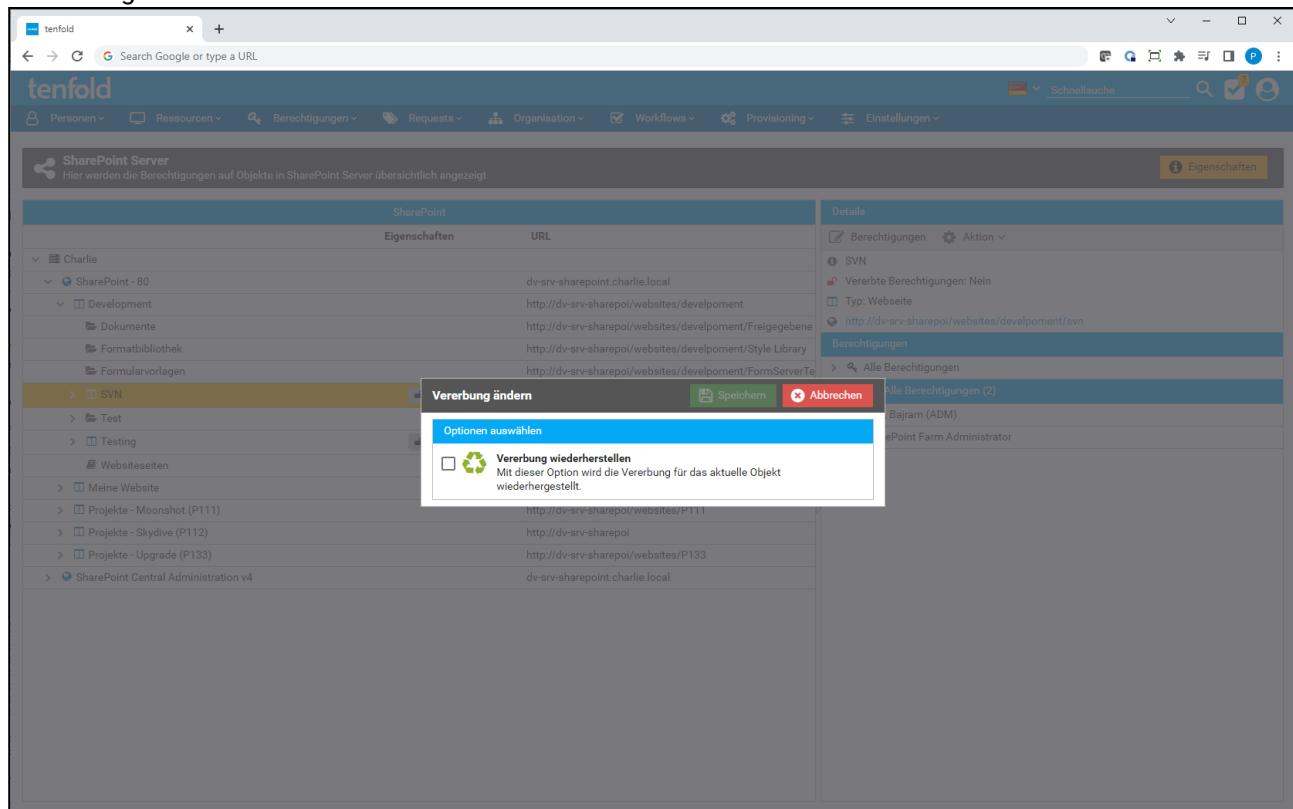
Name	An dieser Stelle kann entweder der Name der zu erzeugenden Gruppe eingegeben werden, wenn in der Einstellung "Modus" die Option "Von SharePoint-Gruppe-Konfiguration generieren lassen" gewählt wurde oder es wird eine Vorschau des generierten Namens angezeigt, sollte die Option "Benutzerdefiniert" gewählt worden sein.
<b>Aktion "Vorhandene Gruppe verwenden"</b>	
Gruppe	Mit dieser Einstellung muss eine bestehende Gruppe gewählt werden, welche als Berechtigungsgruppe für diese Website verwendet wird.

### Berechtigungsgruppen

Die Gruppen, welche an dieser Stelle erzeugt oder übernommen werden, werden von tenfold auch gleichzeitig als Berechtigungsgruppen für diese Website registriert und für die zukünftigen Vergaben von Berechtigungen herangezogen.

Sobald alle Einstellungen getroffen sind können Sie diese durch einen Klick auf die Schaltfläche "Speichern" übernehmen. Es wird daraufhin ein Request zur Änderung der Vererbung erzeugt. Durchgeführt werden diese Einstellungen dann mit der Durchführung des Requests.

Sollte die Vererbung bereits deaktiviert sein, erscheint stattdessen ein Dialog, mit welchem die Vererbung wiederhergestellt werden kann.



Haken Sie hier "Vererbung wiederherstellen" an und betätigen Sie die Schaltfläche "Speichern". Es wird daraufhin ein Request zur Wiederherstellung der Vererbung auf diesem Item angelegt.

### Durchführungsdatum

Die Vererbung wird aufgebrochen/wiederhergestellt, sobald die Requests genehmigt wurden. Die Eingabe eines Durchführungsdatums ist nicht möglich.

## 7.5.4 Einstellungen bearbeiten

Neben den Einstellungen zur Berechtigung existieren noch eine Reihe von Einstellungen, welche nur die Verarbeitung in tenfold betreffen. Diese Einstellungen sind nicht in SharePoint ersichtlich. Außerdem erzeugt eine Änderung dieser Einstellungen **keine** Requests.

### Allgemeine Einstellungen

Wählen Sie in der Übersichtsmaske ein SharePoint Item aus und betätigen im Aktionsmenü des Bereichs "Details" die Aktion "Einstellungen". Daraufhin erscheint ein Dialog, in welchem Sie die allgemeinen Einstellungen des jeweiligen Items ändern können.

The screenshot shows the tenfold SharePoint interface. On the left, there's a navigation tree under 'SharePoint Server'. In the center, a specific item is selected. A modal dialog titled 'Einstellungen bearbeiten' is open over the main content area. This dialog contains several sections: 'Scan-Einstellungen' (with dropdowns for 'Items mit aufgebrochener Vererbung immer scannen' and 'Scan-Tiefe'), 'Genehmigungsworkflow' (with a dropdown for 'Genehmigungsworkflow'), and a large list of URLs for various SharePoint sites. At the bottom right of the dialog are 'Speichern' and 'Abbrechen' buttons. The background shows the SharePoint navigation bar and some other items in the list.

Sie finden hier folgende Einstellungen:

Einstellung	Beschreibung
<b>Bereich "Scan-Einstellungen"</b>	

Items mit aufgebrochener Vererbung immer scannen	<p>Legt fest, ob Items mit aufgebrochener Vererbung unterhalb dieses Items immer gescannt werden sollen, unabhängig von den Einstellungen der Scan-Tiefe. Sie haben folgende Auswahlmöglichkeiten:</p> <ul style="list-style-type: none"> <li>• <b>SharePointserver-Einstellung übernehmen:</b> Übernimmt die Einstellung, welche beim jeweiligen SharePoint-Server hinterlegt wurde.</li> <li>• <b>Ja:</b> Scannt Items mit aufgebrochener Vererbung unterhalb dieses Items immer, unabhängig von der Einstellung, welche beim SharePoint-Server hinterlegt wurde.</li> <li>• <b>Nein:</b> Beachtet immer nur die Einstellung zur Scan-Tiefe, unabhängig davon, ob die Einstellung "Items mit aufgebrochener Vererbung immer scannen" beim SharePoint-Server aktiviert wurde oder nicht.</li> </ul> <p>Diese Einstellung ist nur auf Items vom Typ "Dokumentbibliothek" verfügbar.</p>
Scan-Tiefe	<p>Mit dieser Einstellung kann festgelegt werden, wieviele Ebenen unterhalb dieses Items gescannt werden. Die Anzahl der Ebenen geht hierbei immer vom aktuell ausgewählten Item und nicht von der obersten Ebene aus. Folgende Einstellungen stehen zur Verfügung:</p> <ul style="list-style-type: none"> <li>• <b>SharePointserver-Eisntellung übernehmen:</b> Übernimmt die Einstellungen, welche beim SharePoint-Server hinterlegt wurden.</li> <li>• <b>Keine Einschränkung:</b> Es werden alle Ebenen unterhalb dieses Items gescannt, unabhängig von Einschränkungen, welche auf dem SharePoint-Server oder darüberliegenden Items getroffen wurde.</li> <li>• <b>Anzahl an Ebenen:</b> Es wird bis zu einer Anzahl an Ebenen unterhalb des Items gescannt, welches hier ausgewählt wurde. Dies überschreibt die Einstellungen, die am SharePoint-Server oder auf darüberliegenden Items getroffen wurden. Sie können 0-10 Ebenen auswählen. Wählen Sie 0 Ebenen, werden keine Kinder des Items gescannt.</li> </ul> <p>Diese Einstellung ist nur auf Items vom Typ "Dokumentbibliothek" verfügbar.</p>
<b>Bereich "Genehmigungsworkflow"</b>	

## Genehmigungsworkflow

Mit dieser Einstellung kann überschrieben werden, welcher Genehmigungsworkflow für Requests dieses Items verwendet werden soll. Sie können hier entweder "SharePoint-Server Einstellung übernehmen" wählen, womit der Workflow verwendet wird, welcher beim SharePoint-Server hinterlegt wurde oder einen spezifischen Workflow, welcher verwendet werden soll.

### 7.5.5 Dateneigentümer

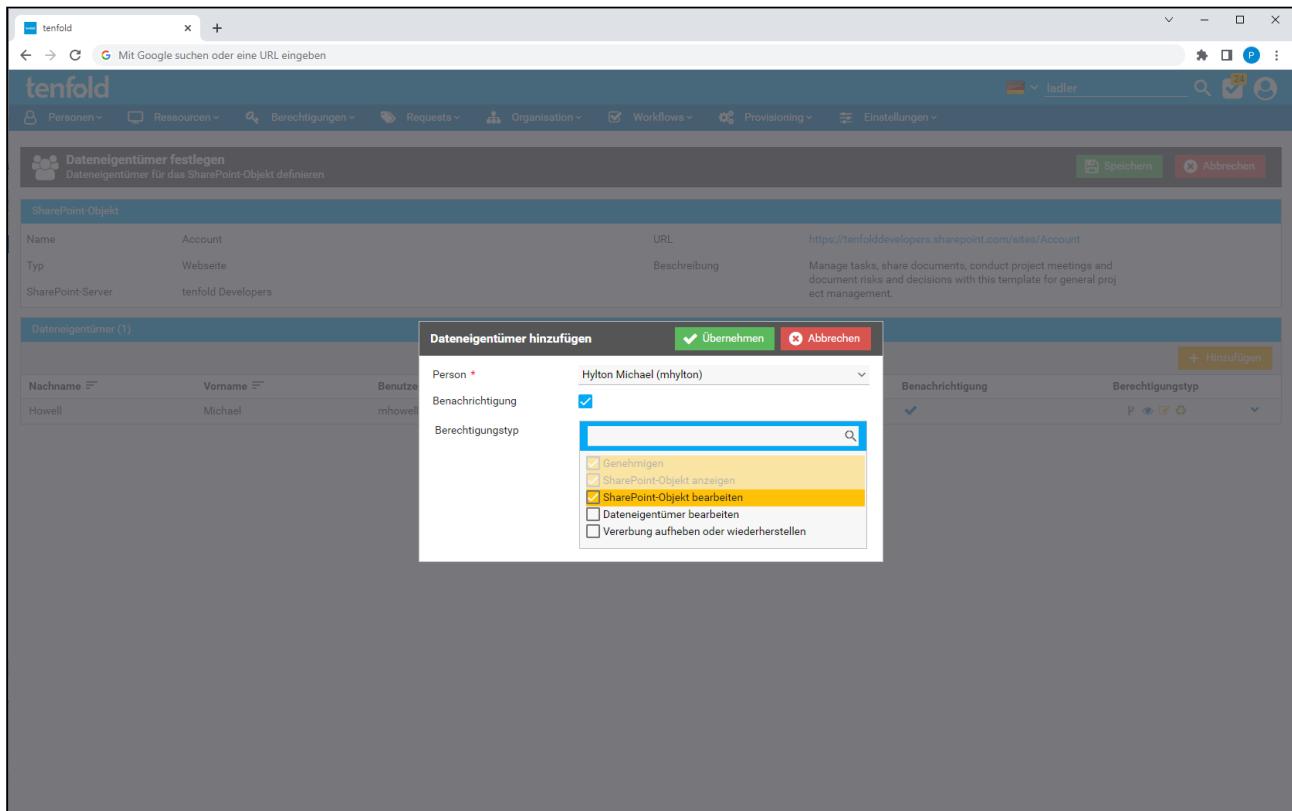
Genau wie für Fileserver können Sie auch für SharePoint-Objekte Dateneigentümer festlegen.

Dateneigentümer können Requests für einen Teilbaum der SharePoint-Struktur genehmigen und, je nach Dateneigentümerberechtigungen, diesen Teilbaum einsehen oder auch verwalten.

Um einen Dateneigentümer festzulegen, wählen Sie ein Objekt in der Baumstruktur aus und klicken im Menü "Aktion" auf die Aktion "Dateneigentümer".

Nachname	Vorname	Benutzername	Personalnummer	Abteilung	Benachrichtigung	Berechtigungstyp
Howell	Michael	mhowell	10607	Logistics	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

Sie gelangen daraufhin zur Maske zur Bearbeitung der Dateneigentümer, wo Sie zunächst eine Übersicht über alle bestehenden Dateneigentümer und deren Berechtigungen erhalten. Mit der Schaltfläche "Hinzufügen" können Sie einen neuen Dateneigentümer hinzufügen. Es öffnet sich daraufhin ein Dialog für die Eingabe der Einstellungen.



Einstellung	Beschreibung
Person	Die Person, welche die Dateneigentümerberechtigungen erhalten soll
Benachrichtigung	Hier können Sie festlegen, ob der Dateneigentümer bei offenen Genehmigungen benachrichtigt werden soll.

Einstellung	Beschreibung
Berechtigungstyp	<p>Wählen Sie hier aus welche Dateneigentümerberechtigungen der Dateneigentümer erhalten soll. Folgende stehen zur Auswahl:</p> <ul style="list-style-type: none"> <li>• <b>Genehmigen:</b> Der Dateneigentümer darf Requests zu seinen Objekten Genehmigen. (Diese Berechtigung ist immer ausgewählt und kann nicht entzogen werden).</li> <li>• <b>SharePoint-Objekt anzeigen:</b> Erlaubt es dem Dateneigentümer, seine Objekte in der Dateneigentümeransicht einzusehen.</li> <li>• <b>SharePoint-Objekt bearbeiten:</b> Erlaubt es dem Dateneigentümer, seine Objekte in der Dateneigentümeransicht zu bearbeiten (z.B. Berechtigungen ändern).</li> <li>• <b>Dateneigentümer bearbeiten:</b> Erlaubt es dem Dateneigentümer, weitere Dateneigentümer zu setzen oder zu entfernen. <b>Hinweis:</b> Dateneigentümer können keine anderen Dateneigentümer mit dieser Berechtigung entfernen. Diese können nur von Benutzern mit Verwaltungsberechtigungen auf der SharePoint-Farm wieder entfernt werden.</li> <li>• <b>Vererbung aufheben oder wiederherstellen:</b> Erlaubt es dem Dateneigentümer, die Vererbungseinstellungen auf seinen Objekten zu ändern.</li> </ul>

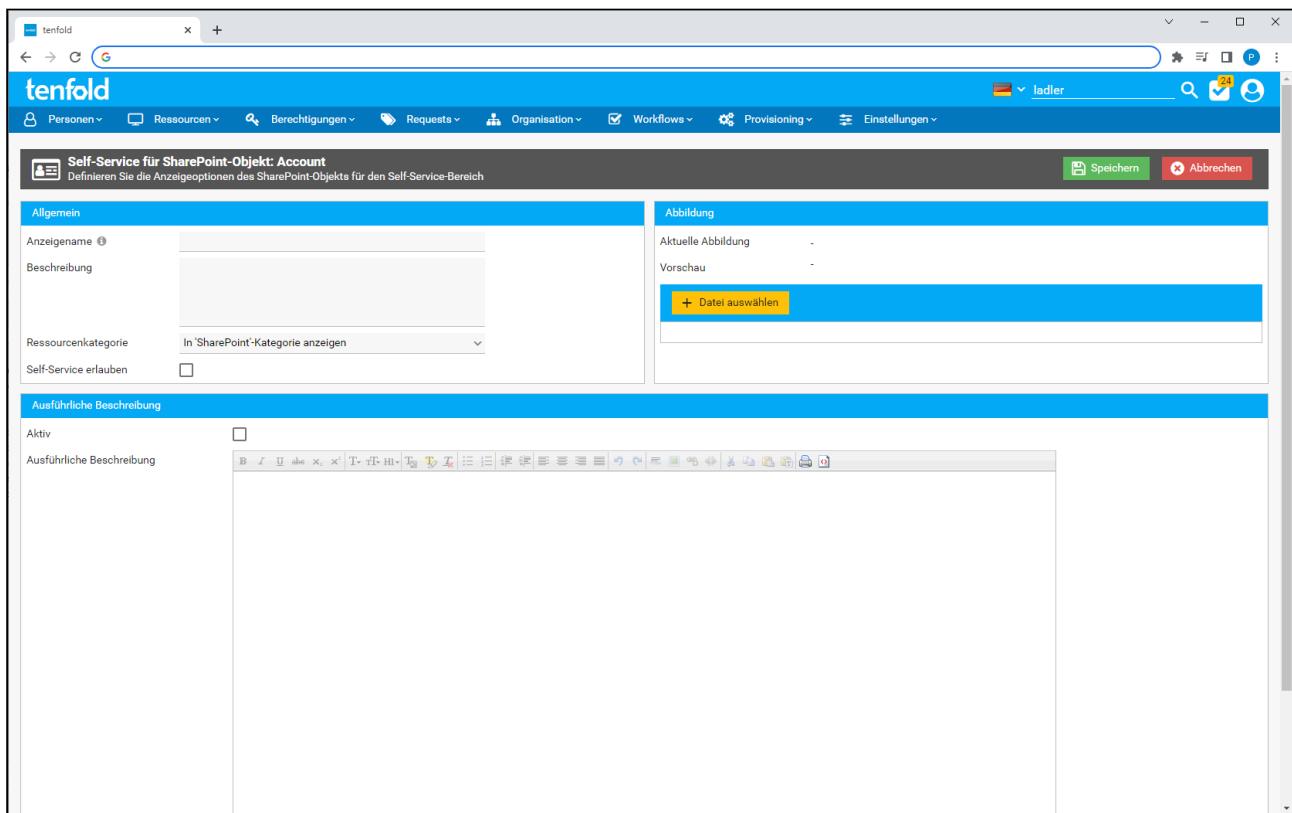
Klicken Sie auf "Übernehmen", um die Bearbeitung des Dateneigentümers abzuschließen.

Sie können die Einstellungen von bestehenden Dateneigentümern mit der Aktion "Bearbeiten" im Aktionsmenü des jeweiligen Dateneigentümers im Nachhinein ändern oder einen Dateneigentümer mit der Aktion "Löschen" entfernen.

Alle Änderungen in dieser Maske werden mit der Schaltfläche "Speichern" im Kopfbereich der Maske festgeschrieben. Mit der Schaltfläche "Abbrechen" verwerfen Sie alle Änderungen, die Sie seit betreten der Maske getätigt haben. In beiden Fällen gelangen Sie zurück zur Übersichtsmaske der SharePoint-Farben.

## 7.5.6 Self-Service

Sie können einzelne Objekte im Self-Service freigeben, damit Benutzer ohne Zugriff auf die SharePoint-Maske Berechtigungen bestellen können. Wählen Sie hierfür das gewünschte Objekt in der Baumstruktur aus und wählen dann die Aktion "Self-Service". Sie gelangen daraufhin zur Maske für die Self-Service Einstellungen.

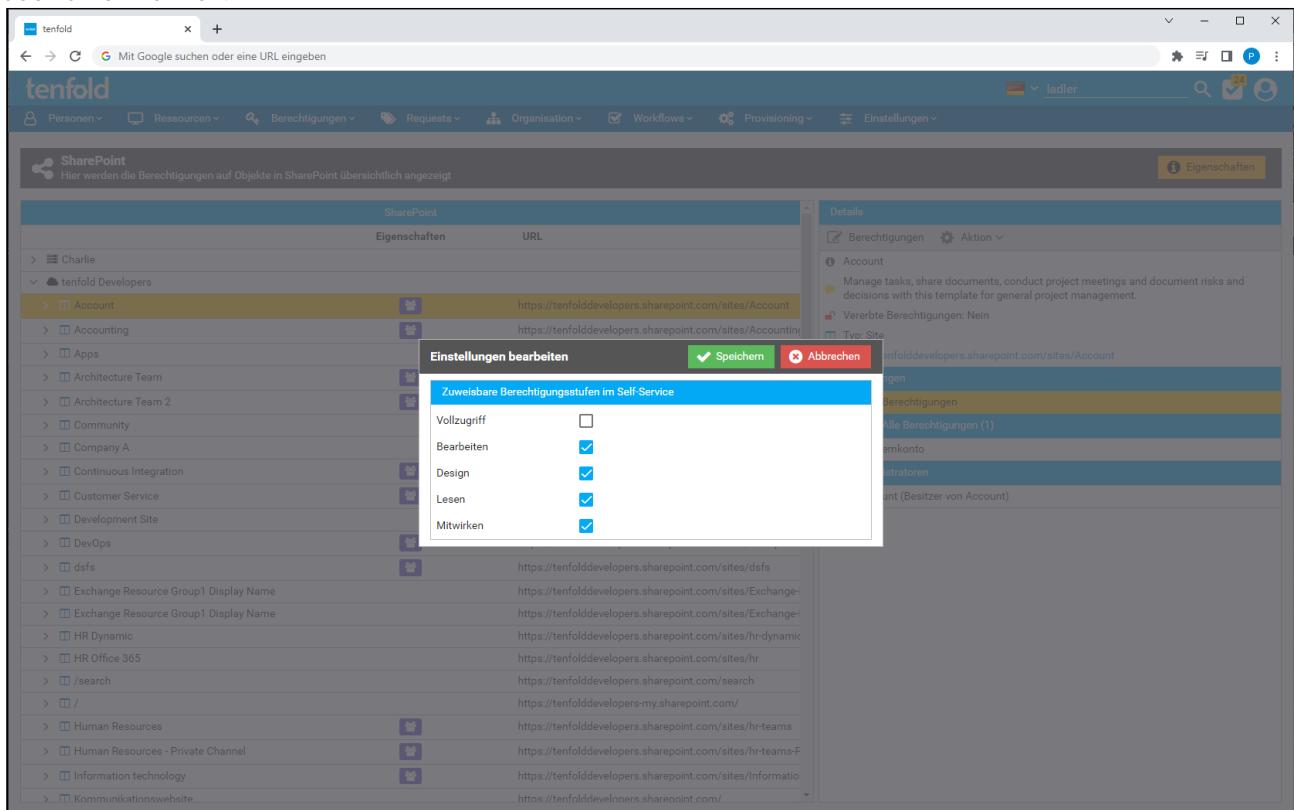


Einstellung	Beschreibung
<b>Bereich "Allgemein"</b>	
Anzeigename	Geben Sie hier einen Namen ein, unter welchem das Objekt im Self-Service-Bereich geführt wird. Wird der Anzeigename leer gelassen, wird stattdessen der Name des Objektes verwendet.
Beschreibung	Hier können Sie eine Beschreibung für das Objekt eintragen, um Benutzern des Self-Service besser zu verdeutlichen, worum es sich bei dem Objekt handelt.
Ressourcenkategorie	Wählen Sie hier eine Ressourcenkategorie aus, unter welcher das Objekt im Self-Service bestellbar ist. Standardmäßig wird es in der speziellen Kategorie "SharePoint" geführt.
Self-Service erlauben	Mit dieser Einstellung geben Sie das Objekt im Self-Service frei.
<b>Bereich "Abbildung"</b>	
Aktuelle Abbildung	Zeigt die aktuelle Abbildung des Objektes im Self-Service an. Ist keine Abbildung vorhanden, so wird ein generisches Icon des Objekttyps im Self-Service angezeigt.
Vorschau	Zeigt eine Vorschau der gerade hochgeladenen Abbildung an.

Datei auswählen	Öffnet einen Dialog, über den eine beliebige Bilddatei hochgeladen werden kann, welche im Self-Service anstatt des Standardicons angezeigt wird.
<b>Bereich "Ausführliche Beschreibung"</b>	
Aktiv	Legt fest, ob die ausführliche Beschreibung im Self-Service angezeigt werden soll.
Ausführliche Beschreibung	Wie das Feld "Beschreibung" im Bereich "Allgemein", erlaubt zusätzlich jedoch eine Formatierung des Textes. Ist sowohl eine normale als auch eine ausführliche Beschreibung angegeben, so wird die ausführliche Beschreibung unterhalb der Beschreibung dargestellt.

Betätigen Sie die Schaltfläche "Speichern", um die Einstellungen für den Self-Service zu speichern. Mit der Schaltfläche "Abbrechen" verwerfen Sie sämtliche Änderungen, welche Sie seit betreten der Maske getätigter haben. In beiden Fällen gelangen Sie zurück zur Übersichtsmaske der SharePoint-Farmen.

Wenn Sie auf der SharePoint-Maske ein Objekt auswählen und die Aktion "Berechtigungsstufen" betätigten, öffnet sich ein Dialog, in welchem Sie die im Self-Service bestellbaren Berechtigungsstufen für dieses Objekt auswählen können.



Klicken Sie auf die Schaltfläche "Speichern", um die Änderungen abzuschließen.

## 7.6 Verwaltung der Microsoft 365 Lizenzen

Nachdem ein Microsoft 365-Mandant eingerichtet und ausgelesen wurde (siehe [Einrichtung von Microsoft 365 Mandanten](#)(see page 243)), können, analog zu Active Directory Gruppen, Lizenzen mittels tenfold verwaltet werden.

The screenshot shows the tenfold web interface with the URL 'tenfold' in the address bar. The top navigation bar includes links for Personen, Ressourcen, Berechtigungen, Requests, Organisation, Workflows, Provisioning, and Einstellungen. The current page is 'Microsoft 365-Lizenzen'. The main content area has a title 'Microsoft 365-Objekte' and a search field. Below it, a table lists 'Zuordnungen' (Assignments) with columns for Name, E-Mail, and Eigenschaften (Properties). A yellow box highlights the 'Gruppen' (Groups) node in the tree view. On the right, there's a separate panel titled 'Zuordnungen' with a 'Löschen' (Delete) button and a list of items with checkboxes.

Für die Verwaltung der Microsoft 365-Lizenzen, navigieren Sie über das Menü zu *Berechtigungen > Microsoft 365-Lizenzen*.

#### Benötigte Berechtigung

Für den Zugriff auf diese Maske benötigen Sie eine der Berechtigungen "Lizenzen anzeigen", "Lizenzen bearbeiten" oder "Lizenzen-Dateneigentümer bearbeiten" für zumindest einen eingerichteten Microsoft 365-Mandanten.

### 7.6.1 Vergabe von Lizenzen

Um eine Lizenz an einen Benutzer, Gastbenutzer oder eine Gruppe zu vergeben, öffnen Sie im Baum im mittleren Bereich zunächst die gewünschte Lizenz auf dem gewünschten Mandanten. Wählen Sie daraufhin einen der Unterknoten "Benutzer", "Gastbenutzer" oder "Gruppen". Es öffnet sich daraufhin auf der rechten Seite der Maske ein Bereich "Zuordnungen" und der linke Bereich "Microsoft 365-Objekte" wird für eine Suche freigeschalten. Benutzen Sie nun die Suche auf der linken Seite um das Objekt zu suchen, welchem die Lizenz zugeordnet werden soll.

#### Gefundene Objekte

In der Suche werden all jene Objekte aufgelistet, welche den Suchbegriff enthalten. **Achtung: Es werden nur Objekte des ausgewählten Knotens gefunden.** Wenn Sie zum Beispiel den Knoten "Gruppen" ausgewählt haben, erscheinen in der Suche nur Gruppen-Objekte. Achten Sie daher darauf im Vorfeld, den richtigen Knoten auszuwählen.

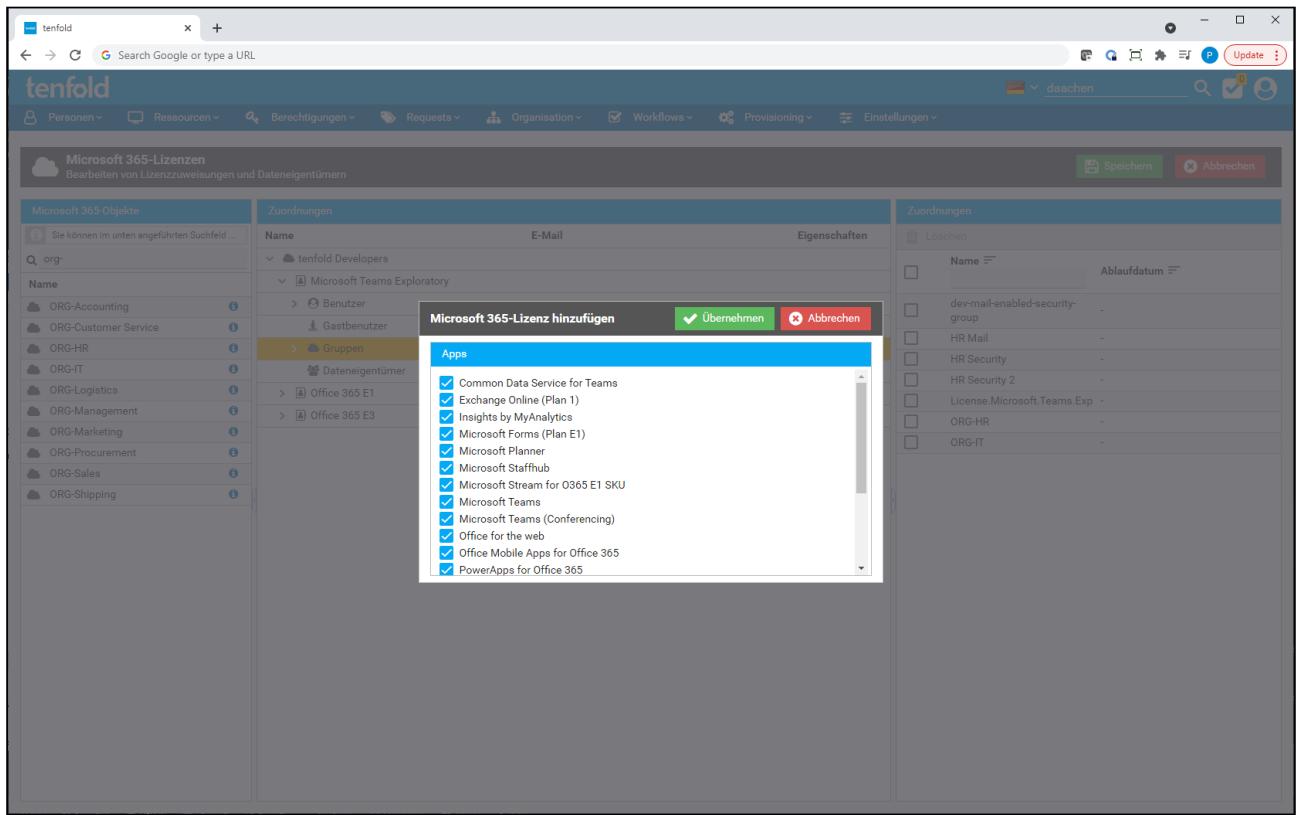
Ziehen Sie nun mittels Drag & Drop das gewünschte Objekt in den Bereich "Zuordnungen" auf der rechten Seite der Maske.

The screenshot shows the tenfold Microsoft 365 Licenses interface. On the left, there's a sidebar with a search bar and a list of organizational objects like ORG-Accounting, ORG-Customer Service, etc. The main area has two columns: 'Zuordnungen' (Assignments) and 'Zuordnungen' (Assignments). The first column lists items with checkboxes for selection. The second column is a 'DROP ZONE' where selected items can be moved. A yellow bar highlights the 'Gruppen' (Groups) item in the first column, and a green bar highlights the 'ORG-Customer Service' item in the second column.

### Farbliche Hervorhebung

Solange Sie das gewünschte Objekt per Drag & Drop ziehen, wird der rechte Bereich gelb eingefärbt. Sobald Sie das Objekt über den rechten Bereich gezogen haben, wird der Bereich grün eingefärbt. Erst wenn der Bereich grün aufscheint, wird das Objekt durch loslassen der Maustaste hinzugefügt.

Es erscheint daraufhin ein Dialog, in welchem Sie anpassen können, welche der in der Lizenz enthaltenen Apps dem Objekt hinzugefügt werden sollen.



Zu Beginn sind alle in der Lizenz enthaltenen Apps angehakt. Bei Bedarf, wählen Sie alle Apps aus, welche das Objekt nicht erhalten soll. Bestätigen Sie daraufhin Ihre Auswahl durch einen Klick auf die Schaltfläche "Übernehmen". Das Objekt erscheint daraufhin im rechten Bereich "Zuordnungen" und ist mit einem "Plus"-Symbol markiert um zu verdeutlichen, dass dieses eben hinzugefügt wurde.

Wenn Sie Ihre Entscheidung rückgängig machen wollen, können Sie auf das "Rückgängig"-Symbol in der rechten Spalte klicken. Das Objekt wird daraufhin wieder aus dem Bereich entfernt.

Im mittleren Bereich über "Zuordnungen" erhalten Sie eine aufklappbare Liste aller Requests, welche tenfold nach den aktuellen Zuordnungen anlegen würde.

Wiederholen Sie dies, bis sie alle gewünschten Objekte den entsprechenden Lizenzen zugeordnet haben und klicken Sie auf die Schaltfläche "Speichern", um die Operationen durchzuführen. Bevor Sie die Schaltfläche nicht betätigten haben, werden keine Operationen auf den jeweiligen Microsoft 365-Mandanten vorgenommen.

## 7.6.2 Entzug von Lizenzen

Sie können Lizenzen ebenso auch wieder über die Maske *Berechtigungen > Microsoft 365-Mandanten* entfernen.

Öffnen Sie dafür, wie im vorhergehenden Abschnitt beschrieben, die entsprechende Lizenz auf einem Ihrer Mandanten und wählen dort einen der Knoten "Benutzer", "Gastbenutzer" oder "Gruppen". Es erscheint der Bereich "Zuordnungen" auf der rechten Seite der Maske. Haken Sie dort alle zu entfernden Objekte an und betätigen die Schaltfläche "Löschen".

The screenshot shows the tenfold Microsoft 365 Licenses interface. On the left, there's a sidebar with 'Microsoft 365-Objekte' and a search bar. The main area has three tabs: 'Zuordnungen' (Assignments), 'E-Mail' (Email), and 'Eigenschaften' (Properties). In the 'Zuordnungen' tab, a list of objects is shown, including 'tenfold Developers', 'Microsoft Teams Exploratory', 'Benutzer', 'Gästbenutzer', 'Gruppen' (with items like 'dev-mail-enabled-security-group' and 'HR Mail'), 'HR Security', 'HR Security 2', 'License.Microsoft.Teams.Exploratory', 'ORG-HR', 'ORG-IT', and 'Dateneigentümer'. To the right, a modal window titled 'Löschen' (Delete) lists objects with checkboxes: 'dev-mail-enabled-security-group', 'HR Mail', 'HR Security', 'HR Security 2', 'License.Microsoft.Teams.Exploratory', 'ORG-HR' (which is checked), and 'ORG-IT' (which is also checked).

Nachdem Sie die Schaltfläche "Löschen" betätigt haben werden die gewählten Objekte durch ein "Entfernen"-Symbol markiert. Im mittleren Bereich, über "Zuordnungen", erscheint eine Liste der Requests, welche erzeugt werden.

The screenshot shows the tenfold Microsoft 365 Licenses interface. On the left, there's a sidebar with 'Microsoft 365-Objekte' and a search bar. The main area has a header 'Neue Requests (2)'. It lists two requests: 'Lizenz Microsoft Teams Exploratory entziehen von ORG-HR' and 'Lizenz Microsoft Teams Exploratory entziehen von ORG-IT', both marked as 'UNGEHEIMIGT'. Below this is a 'Zuordnungen' section showing a tree view of users, groups, and accounts under 'tenfold Developers'. To the right is a 'Zuordnungen' table with columns 'Name', 'E-Mail', and 'Eigenschaften'. The table includes rows for 'ORG-HR', 'ORG-IT', 'dev-mail-enabled-security-group', 'HR Mail', 'HR Security', 'HR Security 2', and 'License.Microsoft.Teams.Exploratory'. At the bottom right are 'Speichern' and 'Abbrechen' buttons.

Sobald Sie alle gewünschten Änderungen eingetragen haben, betätigen Sie die Schaltfläche "Speichern", um die Requests zu erzeugen und die Änderungen damit, nach möglicher Genehmigung, durchzuführen. Bis dahin werden noch keine Operationen auf den betroffenen Microsoft 365-Mandanten durchgeführt.

### 7.6.3 Dateneigentümer bearbeiten

Analog zu Active Directory oder Microsoft 365-Gruppen können auch für Microsoft 365-Lizenzen Dateneigentümer bestimmt werden. Diese können dann mittels Genehmigungsworkflows dafür verantwortlich gemacht werden, Requests zu ihren Lizenzen zu genehmigen. Darüber hinaus kann Ihnen auch die Möglichkeit gegeben werden, in ihrem Dateneigentümerbereich Lizenzen anzuzeigen oder auch zu bearbeiten.

Zum Hinzufügen eines neuen Dateneigentümers, verfahren Sie wie vorher im Abschnitt "Vergabe von Lizenzen" beschrieben, wählen jedoch den Knoten "Dateneigentümer" aus.

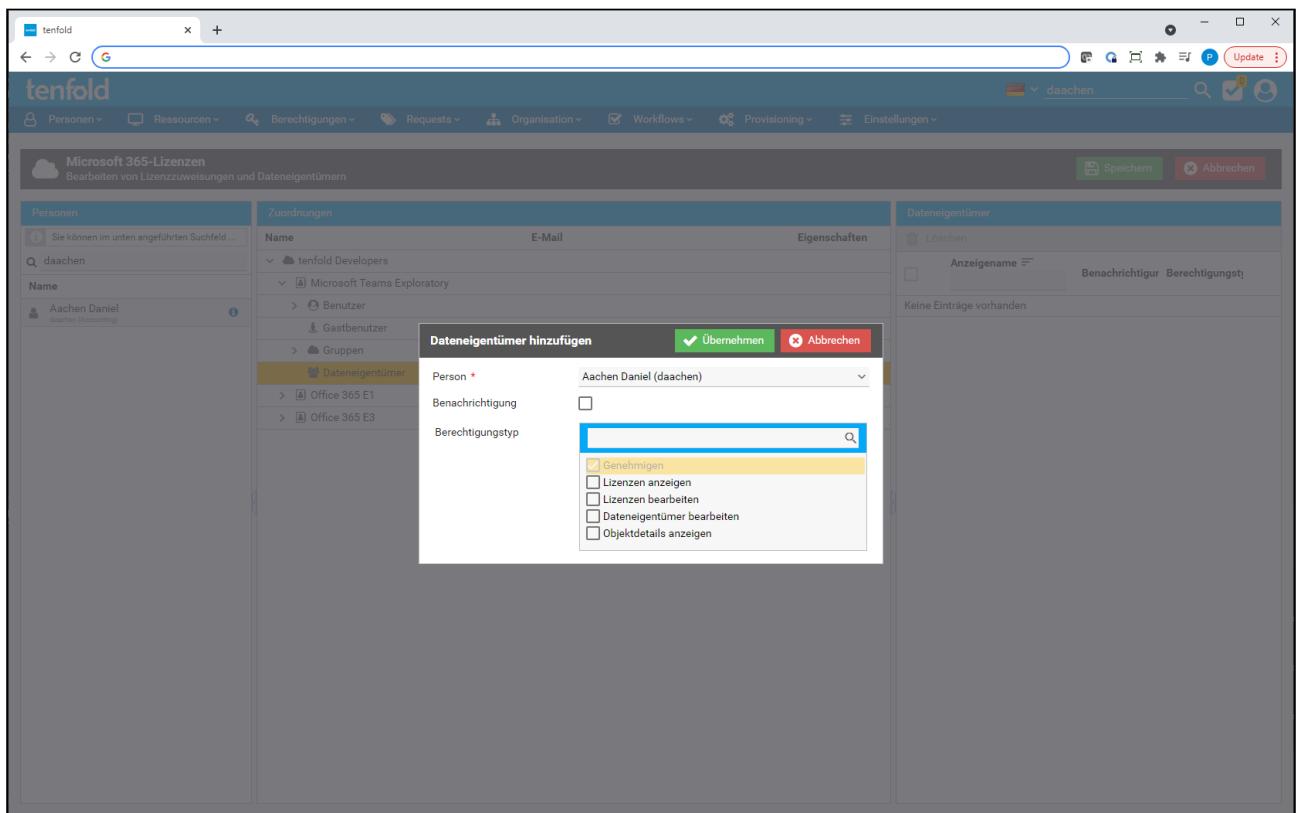
Sie können daraufhin in der Suche auf der linken Seite tenfold-Personen suchen und mittels Drag & Drop hinzufügen.

#### tenfold-Personen

Beachten Sie, dass nur tenfold-Personen zu Dateneigentümern gemacht werden können.

Dateneigentümerberechtigungen können nicht an Gruppen oder Accounts vergeben werden, welche nicht als Personen in tenfold existieren.

Nachdem Sie einen Dateneigentümer hinzugefügt haben, erscheint ein Dialog, in welchem Sie die gewünschten Berechtigungen vergeben können und festlegen können, ob der Dateneigentümer über ausstehende Genehmigungen benachrichtigt werden soll.



Alle Dateneigentümer dürfen immer Requests zu ihren Lizzenzen genehmigen. Diese Berechtigung kann einem Dateneigentümer nicht entzogen werden.

### Genehmigungsworkflows

Es kann vorkommen, dass Dateneigentümer im verwendeten Genehmigungsworkflow nicht vorkommen. In diesem Fall wird keiner der Dateneigentümer zur Genehmigung herangezogen. Sollten Dateneigentümer im Genehmigungsworkflow herangezogen werden, so kann jeder der Dateneigentümer genehmigen.

Darüber hinaus lassen sich noch folgende weitere Berechtigungen vergeben:

Berechtigung	Beschreibung
Lizenzen anzeigen	Fügt die Lizenz zum Dateneigentümerbereich der gewählten Person hinzu, so dass dieser sich anzeigen lassen kann, welche Gruppen oder Accounts über diese Lizenz verfügen.
Lizenzen bearbeiten	Fügt die Lizenz zum Dateneigentümerbereich der gewählten Person hinzu, so dass dieser die Inhaber der Lizenz bearbeiten kann.
Dateneigentümer bearbeiten	Erlaubt es dem Dateneigentümer, im Dateneigentümerbereich weitere Dateneigentümer hinzuzufügen.
Objektdetails anzeigen	Erlaubt es dem Dateneigentümer, im Dateneigentümerbereich Details zu den gewählten Objekten (Accounts, Gruppen) anzuzeigen.

Klicken Sie auf die Schaltfläche "Übernehmen", um die gewünschten Einstellungen zu übernehmen. Sobald Sie alle Dateneigentümer hinzugefügt haben, betätigen Sie die Schaltfläche "Speichern", um die vorgenommen Änderungen festzuschreiben. Für eine Änderung der Dateneigentümer werden keine Requests ausgelöst.

Um Dateneigentümer zu löschen, verfahren Sie analog zum Prozess wie unter "Lizenzen entziehen" beschrieben.

## 7.7 Verwaltung der Microsoft 365 Gruppen

Name	E-Mail	Eigenschaften
tenfold Developers		
Microsoft 365 (5)		
All Company	AllCompany.7020298241.dphntv@tenfold-developer.com	
Mitglieder (1)		
Bezieher (1)		
Dateneigentümer (1)		
Company A	company-a@tenfold-developers.com	
Exchange Resource Group1 Display Name Exchange-Resource-Group1@tenfold-developers.com		
HR Microsoft 365	hr-microsoft365@tenfold-developers.com	
HR Office 365	hr@tenfold-developers.com	
Sicherheit (22)		
E-Mail-aktivierte Sicherheit (12)		
Verteilerlisten (2)		
Teamsgruppen (1)		

Löschen	Anzeigename	Mitglied bis
<input type="checkbox"/>	Gustl, Xavier	-

Auf dieser Maske können die Mitglieder von Microsoft 365 Gruppen verwaltet werden.

### Personen bearbeiten

Die Zuordnung von Microsoft 365 Gruppen kann für einzelne Personen ebenso auf der Maske zur Bearbeitung von Personen verwaltet werden (siehe [Personenverwaltung](#)(see page 63)).

### 7.7.1 Bereich Zuordnungen (Zentraler Bereich)

Im Hauptbereich der Seite werden die Gruppenmitgliedschaften in Form eines Baumes dargestellt. Die oberste Ebene des Baumes bilden die Microsoft 365 Mandanten. Darunter befindet sich die Gruppen, kategorisiert nach Gruppenarten. Bei diesen handelt es sich um:

- Office 365
- Sicherheit
- E-Mail-aktivierte Sicherheit
- Verteilerliste
- Teams-Gruppen

Unterhalb dieser Knoten befinden sich die eigentlichen Gruppen. Darunter können sich je nach Art der Gruppe folgende Knoten befinden:

Knoten	Beschreibung
Mitglieder	Enthält alle Mitglieder der Gruppe. Alle Gruppen besitzen diesen Knoten. Hierbei kann es sich um Benutzerkonten handeln. Bei manchen Gruppenarten können auch andere Gruppen Mitglieder sein.
Mitglied von	Enthält alle Gruppen, denen diese Gruppe zugeordnet ist. Nicht alle Gruppenarten können Mitglieder von anderen Gruppen sein.
Besitzer	Hierbei handelt es sich um die Besitzer der Gruppe im Azure Active Directory (AAD). Dies entspricht dem "Managed By"-Attribut in Ihrer lokalen Domäne. Nur Benutzerkonten können Besitzer von Gruppen sein.
Dateneigentümer	Unterhalb dieses Knotens befinden sich die tenfold-Dateneigentümer dieser Gruppe. Diese Eigenschaft wird nur in tenfold gespeichert und findet sich nicht in den Attributen der Gruppe wieder. Nur Personen in tenfold können Dateneigentümer sein, sie müssen kein Benutzerkonto im AAD besitzen.
Office 365-Lizenzen	Kinder dieses Elementes stellen die Lizenzen/Apps dar, welche dieser Gruppe zugeordnet sind.

Zu jedem Objekt werden folgende Informationen in Spalten innerhalb des Baumes angezeigt:

Spalte	Beschreibung
Name	Der Anzeigename des Objektes. Diese Spalte existiert für alle Objekte des Baumes.
E-Mail	Die E-Mail Adresse der Gruppe oder des Mitgliedes, falls vorhanden.
Eigenschaften	In dieser Spalte werden Icons dargestellt, um folgende Umstände für Gruppen anzuzeigen: <ul style="list-style-type: none"> <li>Die Gruppe hat einen Dateneigentümer</li> <li>Die Gruppe hat einen vom Standard abweichenden Genehmigungsworkflow</li> </ul>

## 7.7.2 Bereich Office 365-Objekte (Linker Bereich)

<b>Name</b>	Keine Einträge vorhanden
-------------	--------------------------

Im linken Bereich der Seite findet sich das Suchfeld wieder, mit welchem Sie nach Objekten suchen können, um diese als Mitglieder oder Dateneigentümer von Gruppen hinzuzufügen. Damit das Suchfeld angezeigt wird, muss zuerst im Baum im zentralen Bereich eines der folgenden Kindelemente einer Gruppe ausgewählt werden:

- Mitglieder
- Mitglied von
- Besitzer
- Dateneigentümer

Nachdem Sie einen Suchbegriff mit mindestens 3 Zeichen eingegeben haben (oder die Enter-Taste betätigt haben), werden Ihnen alle möglichen Objekte angezeigt, welche zum Suchkriterium passen und zur ausgewählten Gruppe als Mitglied/Mitglied von hinzugefügt werden können. Der Suchfilter verhält sich hierbei wie bei der Schnellsuche (siehe [Schnellsuche\(see page 350\)](#)).

## Hinzufügen von Mitgliedern und Besitzern

The screenshot shows the tenfold Microsoft 365 Groups interface. On the left, there's a sidebar with a search bar and navigation links like Personen, Ressourcen, Berechtigungen, Requests, Organisation, Workflows, Provisioning, and Einstellungen. The main area has tabs for Microsoft 365-Gruppen and Bearbeiten von Gruppen, Mitgliedschaften und Dateneigentümern. The central part is divided into two sections: 'Zuordnungen' (Assignments) and 'Mitglieder' (Members). In the 'Zuordnungen' section, there's a tree view of groups and their members. One item under 'Mitglieder' is highlighted with a yellow background. In the 'Mitglieder' section, there's a table with columns for 'Anzeigename' (Display name), 'Mitglied bis' (Member until), and a 'DROP ZONE' header. A user's cursor is shown dragging an item from the assignments list into this drop zone. Buttons for Löschen (Delete), Speichern (Save), and Abbrechen (Cancel) are at the top right.

Sie können neue Mitglieder und Besitzer zu Gruppen hinzufügen, indem Sie ein durch die Suche gefundenes Objekt mittels Drag & Drop in den Detailbereich im rechten Teil der Seite ziehen. Daraufhin wird Ihnen das neue Mitglied bzw. der neue Besitzer mit einem Plus-Symbol in der Tabelle angezeigt, um zu signalisieren, dass dieser gerade hinzugefügt wurde. Durch Betätigen der Schaltfläche "Rückgängig machen" können Sie diese Operation umkehren.

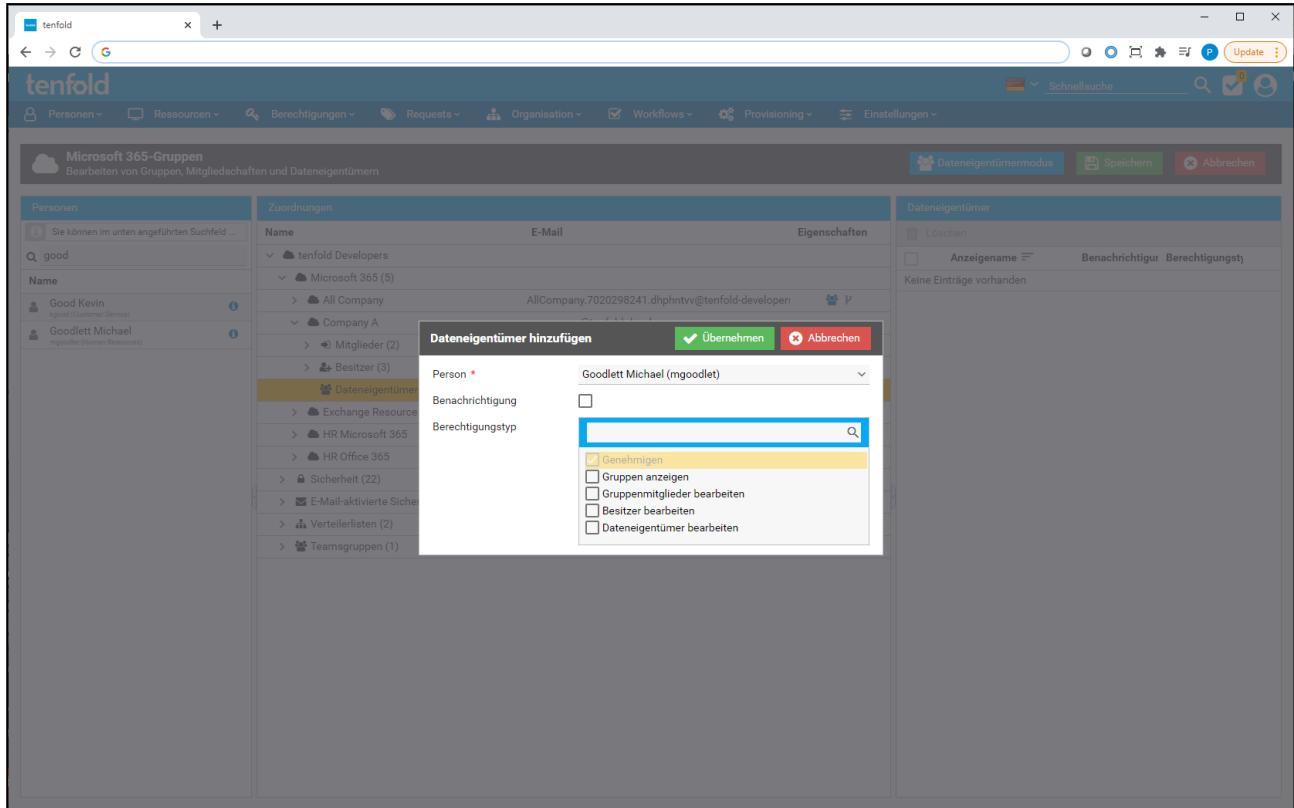
Über dem Bereich "Zuordnungen" im zentralen Bereich werden Ihnen daraufhin sämtliche Requests im Panel "Neue Requests" angezeigt, welche durch die getroffenen Operationen erzeugt werden.

Durch einen Klick auf die Schaltfläche "Speichern" lassen sich alle neuen Requests speichern. Der weitere Verlauf ist abhängig von den Berechtigungen des angemeldeten Benutzers und ausgewählten Genehmigungsworkflows.

### Mitglied/Mitglied von

Wenn Sie eine Gruppe A als *Mitglied* einer Gruppe B hinzufügen, so ist das Ergebnis identisch, wenn Sie Gruppe B in den Bereich *Mitglied von* von Gruppe A hinzufügen.

## Hinzufügen von Dateneigentümern



Um einen neuen Dateneigentümer zur Gruppe hinzuzufügen, wählen sie eine Person, welche durch die Suche gefunden wurde und ziehen Sie mittels Drag & Drop in den Detailbereich auf der rechten Seite.

Es erscheint daraufhin ein Dialog zur Auswahl der Berechtigungen, die der neue Dateneigentümer haben soll. Folgende Berechtigungen stehen zur Auswahl:

Berechtigung	Beschreibung
Genehmigen	Erlaubt es dem Dateneigentümer, Requests zu dieser Gruppe zu genehmigen, wenn der Dateneigentümer im Genehmigungsworkflow herangezogen wird. Diese Berechtigung erhält jeder Dateneigentümer und kann sie nicht abgewählt werden.
Gruppen anzeigen	Erlaubt es dem Dateneigentümer diese Maske zu öffnen, um sich die Informationen zu seinen Gruppen anzeigen zu lassen. Diese Berechtigung wird automatisch angehakt und kann nicht mehr entfernt werden, wenn zumindest eine der unten angeführten Berechtigungen ausgewählt wurde.
Gruppenmitglieder bearbeiten	Erlaubt es dem Dateneigentümer, die Mitglieder der Gruppen zu bearbeiten.
Besitzer bearbeiten	Erlaubt es dem Dateneigentümer, die Besitzer der Gruppe zu bearbeiten.
Dateneigentümer bearbeiten	Erlaubt es dem Dateneigentümer, neue Dateneigentümer zur Gruppe hinzuzufügen oder bestehende zu entfernen.

Daraufhin erscheint ein neuer Eintrag in der Tabelle, welcher mit einem Plus-Symbol markiert ist, um anzuseigen, dass dieser Dateneigentümer gerade hinzugefügt wurde. Im Aktionsmenü lassen sich die ausgewählten Berechtigungen noch einmal bearbeiten oder das Hinzufügen rückgängig machen. Durch einen Klick auf *Speichern* werden die neuen Dateneigentümer gespeichert. Es werden hierfür keine Requests erzeugt.

### 7.7.3 Bereich Details (Rechter Bereich)

Der Detailbereich im rechten Teil der Seite umfasst mehrere verschiedene Modi. Welcher Modus dargestellt wird hängt davon ab, welche Art von Objekt im Zuordnungsbereich ausgewählt wurde.

#### Mandant/Gruppentyp

Zeigt den Namen des Mandanten/Gruppentyps an. Dies kann von Nutzen sein, wenn der Name zu lang ist, um im Baum angezeigt zu werden.

#### Gruppe

Zeigt folgende Daten zur Gruppe an:

Eigenschaft	Beschreibung
Anzeigename	Anzeigename der Gruppe
Typ	Der Gruppentyp
Quelle	Gibt an, ob es sich um eine reine Microsoft 365-Gruppe handelt (Cloud) oder eine aus der lokalen Domäne synchronisierte Gruppe (On-Premise)
Beschreibung	Die Beschreibung der Gruppe, die im (A)AD eingegeben wurde.
Mandant	Der Name des Mandanten, zu welchem die Gruppe gehört.

Zusätzlich zu diesen Eigenschaften wird für Gruppen mit der Quelle *Cloud* ein Aktionsmenü angezeigt, welches weitere Einstellungsmöglichkeiten bietet. In den Einstellungen kann ein Genehmigungsworkflow für die ausgewählte Gruppe individuell festgelegt werden.

Für Gruppen des Typs "Sicherheit", also Gruppen, welche mit On-Premises Active Directory-Gruppen verknüpft sind, können Sie sich über das Menü *Informationen > Gruppendetails* im Bereich *Microsoft 365-Gruppe* die Details zur verknüpften Active Directory-Gruppe anzeigen lassen.

#### Berechtigung

Die Informationen zur Active Directory-Gruppe können Sie sich nur einblenden lassen, wenn Sie die entsprechenden Berechtigungen besitzen, um die Gruppe auch über die Maske *Berechtigungen > Active Directory-Gruppen* anzeigen zu können. Siehe [Verwaltung der Active Directory Gruppen\(see page 265\)](#).

#### Mandantenworkflow

Ist kein Genehmigungsworkflow ausgewählt, wird der Genehmigungsworkflow angewendet, der beim Mandanten hinterlegt ist (siehe [Einrichtung von Microsoft 365 Mandanten\(see page 243\)](#)).

## On-Premise Gruppen

Zur Bearbeitung der Einstellungen von On-Premises gruppen, verwenden Sie bitte die Seite zur Verwaltung von Active Directory Gruppen (siehe [Verwaltung der Active Directory Gruppen\(see page 265\)](#)). Das Bearbeiten synchronisierter Gruppen wird von AAD nicht unterstützt.

## Mitglieder/Mitglied von/Besitzer

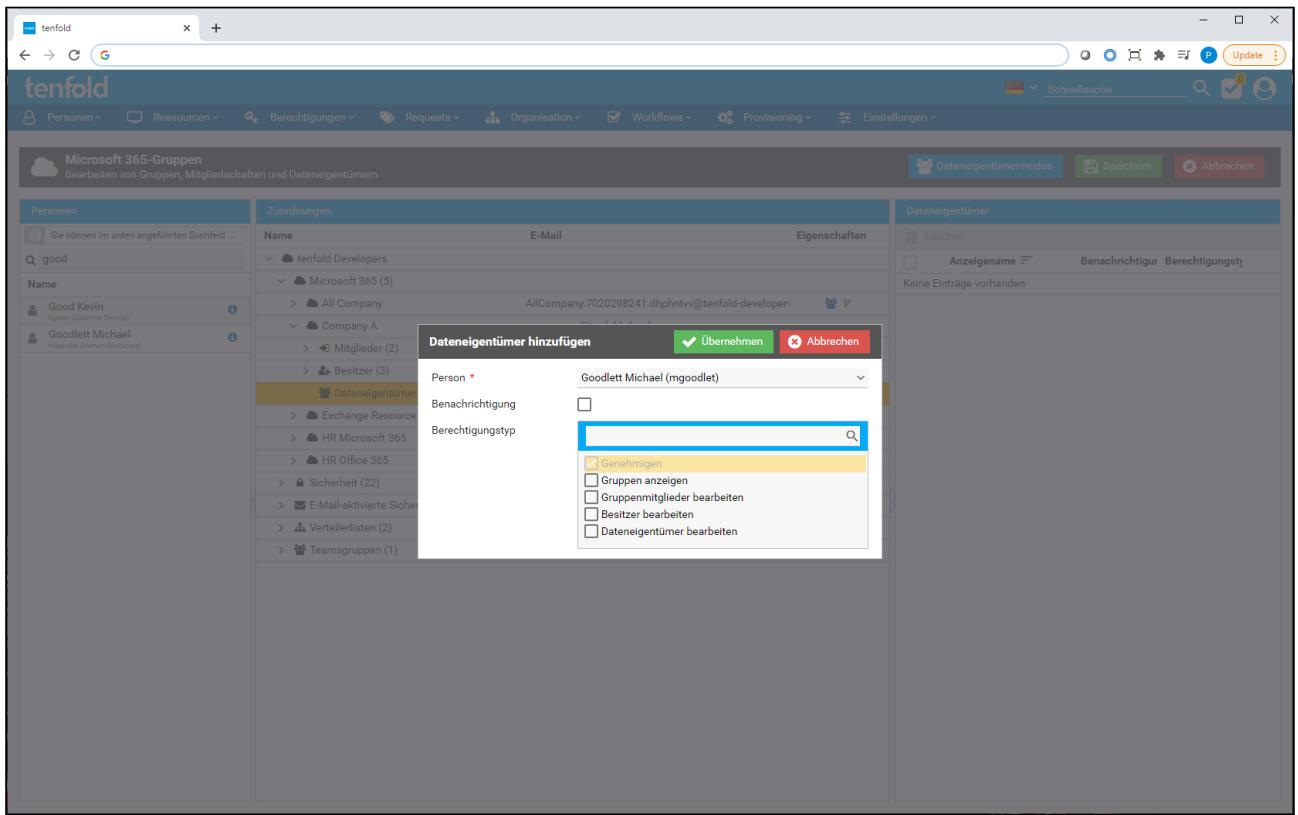
Name	E-Mail	Eigenschaften
tenfold Developers		
Microsoft 365 (5)		
All Company	AllCompany.7020298241.dhphttv@tenfold-developer...	
Mitglieder (1)		
Besitzer (1)		
Dateneigentümer (1)		
Company A	company-a@tenfold-developers.com	
Exchange Resource Group1 Display Name Exchange-Resource-Group1@tenfold-developers.com		
HR Microsoft 365	hr-microsoft365@tenfold-developers.com	
HR Office 365	hr@tenfold-developers.com	
Sicherheit (22)		
E-Mail-aktivierte Sicherheit (12)		
Verteilerlisten (2)		
Teamsgruppen (1)		

Anzeigename	Mitglied bis
Gustl, Xavier	xgustl@tenfold-developers.onmicrosoft.com
Goodlett, Michael	mgoodlett@tenfold-developers.onmicrosoft.com

Zeigt Anzeigenamen, E-Mail Adresse, sowie das Ablaufdatum der Mitgliedschaft an. Zusätzlich dazu können einzelne Mitglieder markiert werden und mit einem Klick auf die Schaltfläche *Löschen* gelöscht werden.

## Dateneigentümer



In einer Tabelle werden folgende Daten zu den einzelnen Dateneigentümern angezeigt:

Spalte	Beschreibung
Anzeigename	Zeigt, zusätzlich zum Anzeigenamen, Benutzername sowie die Abteilung der Person an.
Benachrichtigung	Der Haken zeigt an, dass der Dateneigentümer, im Falle von zu genehmigenden Requests, benachrichtigt wird.
Berechtigungstyp	Zeigt mittels Icons an, welche Dateneigentümer-Berechtigungen die Person besitzt.

Zusätzlich dazu können ein oder mehrere Dateneigentümer mit der Checkbox in der ersten Spalte markiert und anschließend mit der Schaltfläche *Löschen* zur Löschung markiert werden. Durch einen Klick auf die Schaltfläche *Speichern* werden diese Dateneigentümer daraufhin entfernt.

Mit der Aktion *Bearbeiten* im Aktionsmenü lassen sich die Dateneigentümerberechtigungen bearbeiten.

#### Lizenz/App

Im Falle der Auswahl einer Lizenz oder einer App wird hier der Name der Lizenz sowie das Ablaufdatum der Zuordnung angezeigt. Wenn eine Lizenz ausgewählt wurde, werden auch die dazugehörigen ausgewählten Apps angezeigt.

## 7.8 Microsoft Teams

Microsoft Teams ist eine Plattform, die Chat, Besprechungen, Notizen und Anhänge kombiniert. Die Microsoft Teams-Integration von tenfold ermöglicht es Ihnen, einen Überblick über die Berechtigungen, die in Ihren Teams vergeben wurde, zu behalten.

## SharePoint

Im Hintergrund verwendet Microsoft Teams SharePoint zur Datenhaltung. Daher ist es notwendig, Ihre SharePoint Online-Instanz in tenfold einzubinden, um alle Features der Teams-Integration nutzen zu können.

Wie Sie Ihre Teams-Umgebung in tenfold einrichten, erfahren Sie unter [Einrichtung von Microsoft 365 Mandanten](#)(see page 243).

### 7.8.1 Übersicht

#### Benötigte Berechtigung

Für die Anzeige wird die Berechtigung "Teams anzeigen" auf zumindest einem Microsoft 365-Mandaten (siehe [Berechtigungen](#)(see page 457)) oder die Dateneigentümerschaft für zumindest ein Team benötigt (siehe [Dateneigentümer](#)(see page 341)).

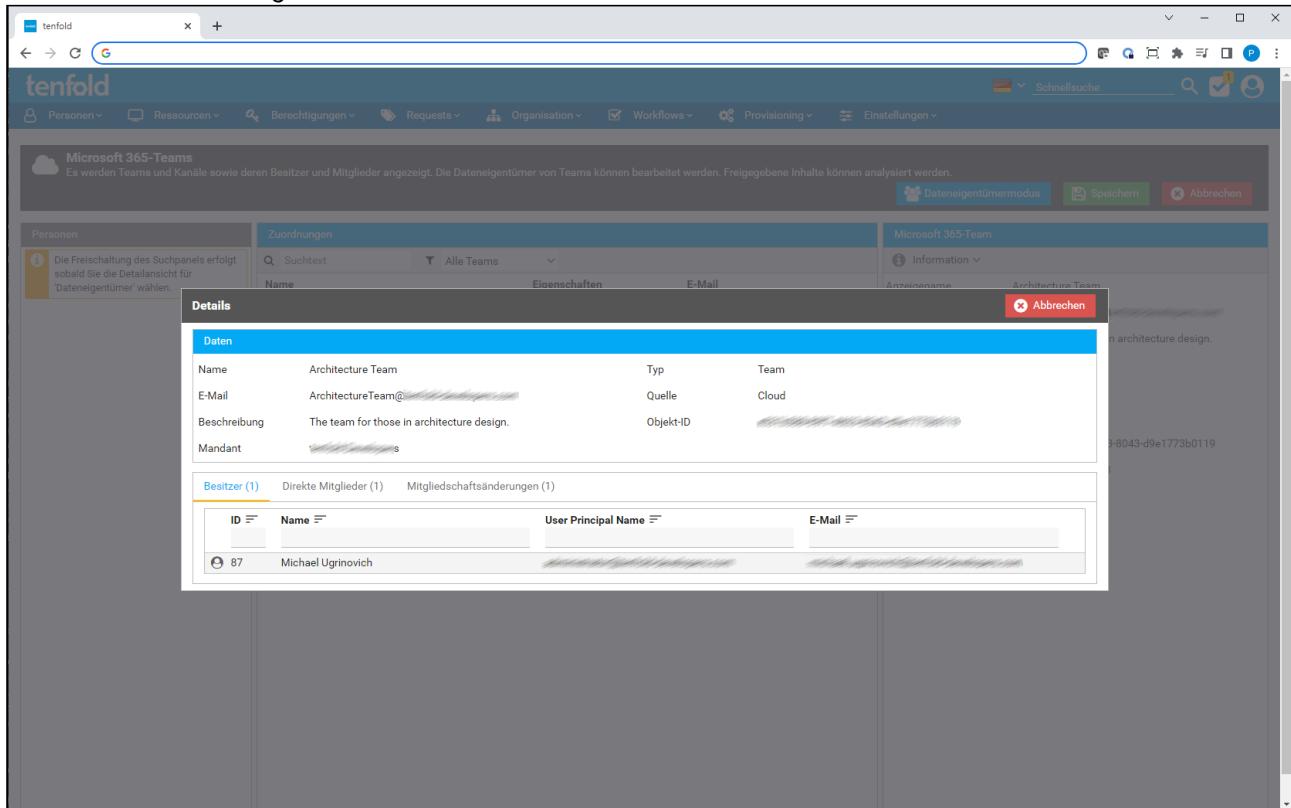
Im Hintergrund werden Ihre Teams als Webseiten in SharePoint Online verwaltet. Es ist daher prinzipiell möglich, sämtliche Informationen zu Ihren Teams-Berechtigungen auch über die SharePoint Maske von tenfold (siehe [Verwaltung der SharePoint-Berechtigungen](#)(see page 309)) zu erhalten. tenfold bietet Ihnen jedoch auch eine Maske, welche speziell darauf ausgelegt ist, Ihnen die Informationen Ihrer Teams zu liefern.

Navigieren Sie hierfür im Menü auf die Maske **Berechtigungen > Microsoft 365-Teams**. Sie erhalten daraufhin einen Überblick über sämtliche Teams aller Mandanten, auf denen Sie die tenfold-Berechtigung für Teams haben (Administratormodus) oder für sämtliche Teams, in welchen Sie als Dateneigentümer hinterlegt wurden (Dateneigentümermodus). Sollten Sie sowohl administrative Berechtigungen haben als auch

Dateneigentümer sein, so wird Ihnen auf der Maske zuerst der Administratormodus dargestellt. In diesem Fall können Sie mit der Schaltfläche "Dateneigentümermodus", welche sich in der Kopfzeile der Maske befindet, in den Dateneigentümermodus wechseln. Von dort kommen Sie dann über die Schaltfläche "Administratormodus" wieder zurück in den Administratormodus der Maske.

Sollten Sie nur über administrative Berechtigungen oder Dateneigentümerberechtigungen verfügen, wird die Maske automatisch im jeweiligen Modus dargestellt. Ein Wechsel ist dann nicht mehr möglich.

Im Bereich "Zuordnungen" der Maske erhalten Sie eine Baumansicht mit den Daten Ihrer Teams. Auf oberster Ebene der Ansicht befinden sich Ihre Microsoft 365-Mandanten. In der Ebene direkt darunter befinden sich Ihre Teams. Wenn Sie auf ein Team klicken wird Ihnen rechts ein Bereich, "Microsoft 365-Team", mit den Detailinformationen zu diesem Team eingeblendet. Im Menü "Informationen" können Sie mit der Aktion "Gruppendetails anzeigen" einen Dialog öffnen, der Ihnen Details zur SharePoint-Gruppe anzeigt, welche hinter diesem Team liegt.



In der Spalte "Eigenschaften" werden Ihnen Icons angezeigt, die Sie über gewisse Beschaffenheiten des Teams informieren.

Eigenschaft	Beschreibung
Dateneigentümer vorhanden	Wird Ihnen dieses Icon angezeigt, so bedeutet dies, dass auf diesem Team tenfold-Dateneigentümer hinterlegt wurden. Wurden keine Dateneigentümer hinterlegt, wird dieses Icon nicht angezeigt.
Privates Team	Wenn dieses Icon angezeigt wird, ist das Team privat. Für öffentliche Teams wird kein spezielles Icon angezeigt.

Eigenschaft	Beschreibung
Unterobjekte mit aufgebrochener Vererbung	Dieses Icon bedeutet, dass sich in diesem Team Inhalte befinden, für welche explizit Berechtigungen vergeben wurden. Dies geschieht häufig durch das Teilen von Inhalten. Sollte Ihnen dieses Icon angezeigt werden, können Sie im Knoten "Inhalte mit expliziten Berechtigungen", welcher sich unterhalb des Team-Knotens befindet, Details zu den Berechtigungen einholen.

Unterhalb eines Teams befindet sich der Knoten "Kanäle", unter dem Ihnen die angelegten Kanäle des Teams angezeigt werden. Sie können auf einen Kanalknoten klicken, um zusätzliche Detailinformationen zu diesem Kanal einzublenden. Darüber hinaus befinden sich hier die Knoten "Besitzer", "Mitglieder" und "Dateneigentümer". Die Knoten "Besitzer" und "Mitglieder" beinhalten jeweils eine Auflistung aller in SharePoint definierten Mitglieder und Besitzer des Teams. Hierbei handelt es sich um SharePoint-Objekte, die entweder Gruppen oder Benutzer sein können. Durch einen Klick auf das jeweilige Objekt können Sie Detailinformationen zu diesem Objekt einblenden. Unterhalb des Knotens "Dateneigentümer" finden Sie die in tenfold definierten Dateneigentümer für dieses Team (siehe [Dateneigentümer \(see page 341\)](#)). Bei den Dateneigentümern handelt es sich um tenfold-Personen.

#### **Dateneigentümer in Sharepoint/Teams**

Dateneigentümer sind nur in tenfold vorhanden und in SharePoint und Teams selbst nicht ersichtlich.

Darüber hinaus gibt es noch den Knoten "Inhalte mit expliziten Berechtigungen". Unterhalb dieses Knotens finden Sie eine Webseiten/Verzeichnis-Struktur mit sämtlichen Inhalten Ihres Teams, für welche explizit Berechtigungen vergeben wurden.

#### **SharePoint-Berechtigungen**

Da Microsoft Teams auf Microsoft SharePoint aufbaut bedeutet dies, dass das Vergaben von individuellen Berechtigungen auf einen Inhalt immer auch ein Aufheben der Berechtigungsvererbung bewirkt. Dies inkludiert auch geteilte Inhalte, da das Teilen eines Inhaltes immer die Vergabe von expliziten Berechtigungen bedeutet.

Mithilfe dieses Knotens erhalten Sie sehr schnell einen Überblick über die individuellen Berechtigungen der Inhalte Ihres Teams. Da durch das Teilen von Inhalten immer Vererbungen aufgebrochen und individuelle Berechtigungen vergeben werden, kann es sehr schnell unklar werden, welche Benutzer Berechtigungen auf die einzelnen Inhalte haben.

#### **Eigenschaft "Unterobjekte mit aufgebrochener Vererbung"**

Für Teams, bei welchen die Eigenschaft "Unterobjekte mit aufgebrochener Vererbung" nicht angezeigt wird, wird dieser Knoten niemals Elemente enthalten. Sie müssen daher nicht alle Teams aufklappen, um zu prüfen, in welchem Team Inhalte freigegeben wurden.

In der Spalte "Eigenschaften" können Ihnen folgende Icons zur Übersicht angezeigt werden:

Eigenschaft	Beschreibung
<b>Eigenschaften für Vererbung</b>	

Vererbung aufgebrochen	Diese Eigenschaft weist Sie daraufhin, dass auf diesem Objekt die Vererbung aufgebrochen wurde, um explizit Berechtigungen zu vergeben. Wird dieses Icon angezeigt bedeutet das, dass sich unterhalb dieses Inhaltes keine weiteren Inhalte mit aufgebrochener Vererbung mehr befinden.
Vererbung aufgebrochen, Unterobjekte mit aufgebrochener Vererbung	Dieses Icon zeigt Ihnen an, dass sowohl die Vererbung auf diesem Inhalt aufgebrochen wurde als auch, dass sich weitere Inhalte unterhalb befinden, bei welchen die Vererbung ebenfalls aufgebrochen wurde.
Vererbung aktiv, Unterobjekte mit aufgebrochener Vererbung	Wird Ihnen dieses Icon angezeigt, bedeutet dies, dass sich unterhalb dieses Inhaltes Inhalte mit expliziten Berechtigungen verborgen, auf diesem Inhalt selbst jedoch die Vererbung der Berechtigungen aktiv ist.
<b>Eigenschaften für externe Berechtigungen</b>	
Berechtigungen außerhalb des Teams/Kanals auf Unterobjekte	Dieses Icon spiegelt wider, dass Inhalte unterhalb dieses Knotens mit externen Konten geteilt wurden. Auf diesem Objekt selbst ist dies jedoch nicht der Fall.
Berechtigungen außerhalb des Teams/Kanals	Mit diesem Icon wird Ihnen dargestellt, dass dieser Inhalt mit Konten außerhalb des Teams geteilt wurde. Unterhalb dieses Inhaltes befinden sich keine weiteren extern geteilten Inhalte.
Berechtigungen außerhalb des Teams/Kanals (auch Unterobjekte)	Wenn Ihnen dieses Icon angezeigt wird bedeutet dies, dass sowohl dieser Inhalt mit externen Konten geteilt wurde als auch Inhalte, welche sich unterhalb des Inhaltes befinden.

## 7.8.2 Dateneigentümer

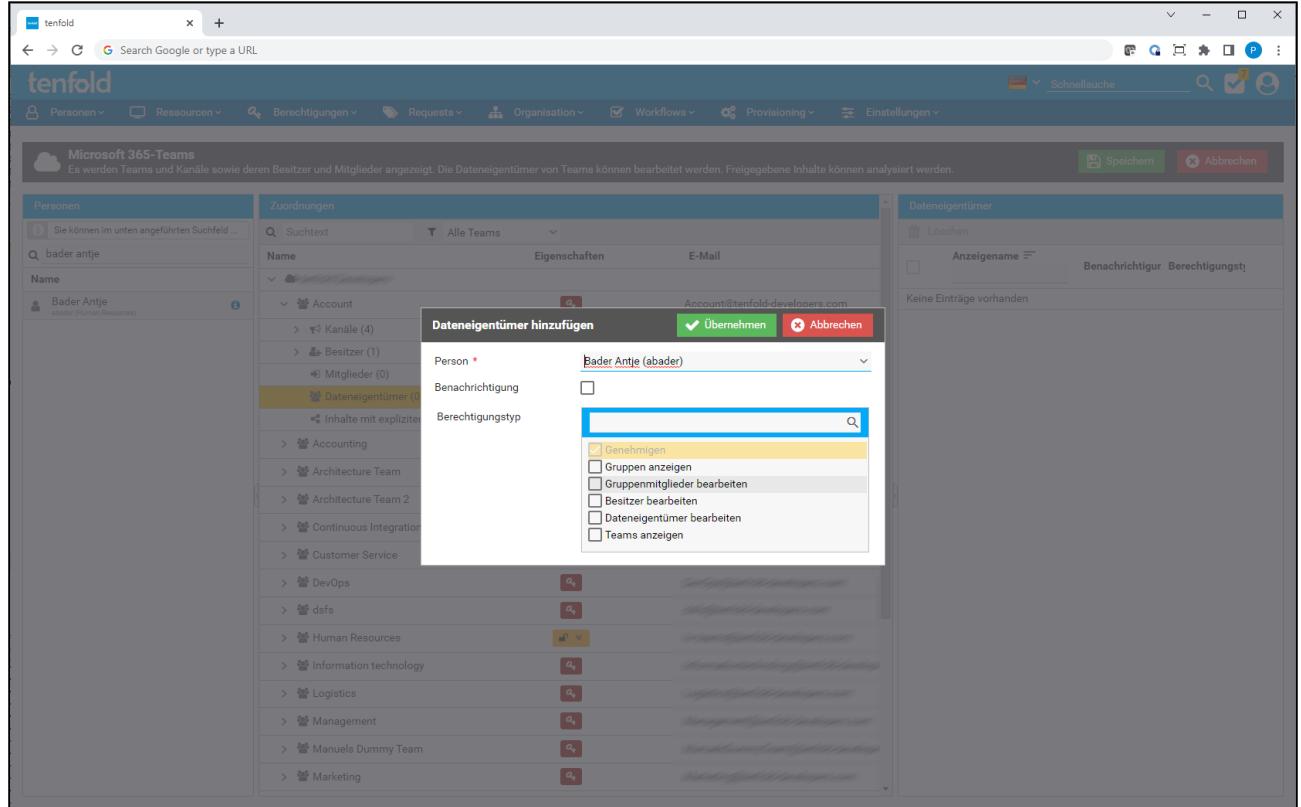
Um einzelnen Personen die Möglichkeit zu geben, Informationen bestimmter Teams in tenfold einzusehen, können diese zu Dateneigentümern von Teams gemacht werden.

### tenfold-Berechtigungen

Dateneigentümer können die Daten Ihrer Teams einsehen, ohne dass hierfür weitere Berechtigungen notwendig sind.

Um einen neuen Dateneigentümer hinzuzufügen, wählen Sie den Knoten "Dateneigentümer" des jeweiligen Teams aus. Daraufhin wird Ihnen das Suchfeld im Bereich "Personen" auf der linken Seite der Maske freigeschalten. Suchen Sie dort nach der gewünschten Person und ziehen diese dann per Drag & Drop in den Bereich "Dateneigentümer" auf der rechten Seite der Maske. Nachdem Sie die Person in den Bereich gezogen haben wird Ihnen ein Dialog angezeigt, in welchem die Dateneigentümerberechtigungen ausgewählt werden

können.



Für den Dateneigentümer können folgende Einstellungen getroffen werden:

Einstellung	Beschreibung
Person	Mit dieser Einstellung wird festgelegt, welche Person zum Dateneigentümer ernannt werden soll. Diese Einstellung ist vorbelegt mit der Person, welche Sie in den Bereich "Dateneigentümer" gezogen haben, um den Dateneigentümer anzulegen. Die Person kann hier noch einmal nachträglich geändert werden.
Benachrichtigung	Legt fest, ob die Person bei offenen Genehmigungen zu diesem Team benachrichtigt wird.
Berechtigungstyp	Hier können Sie festlegen, welche Berechtigungen die Person als Dateneigentümer bekommt. Details zu den Berechtigungen werden im Nachgang angeführt.

Die Berechtigungen aus der Einstellung "Berechtigungstyp" haben hierbei folgende Auswirkungen:

Berechtigung	Beschreibung
Genehmigen	Diese Berechtigung erlaubt es dem Dateneigentümer, Requests zu diesem Team zu genehmigen. Diese Berechtigung ist immer ausgewählt und kann nicht abgewählt werden. <b>Achtung:</b> Sollte in dem Genehmigungsworkflow, der für dieses Team angewendet wird, der Dateneigentümer nicht vorkommen, so hat diese Einstellung keine Auswirkung.

Berechtigung	Beschreibung
Gruppen anzeigen	Erlaubt es dem Dateneigentümer, die Gruppeninformationen auf der Maske "Office 365-Gruppen" (Berechtigungen > Office 365 Gruppen) anzuzeigen.
Gruppenmitglieder bearbeiten	Diese Berechtigung gestattet es dem Dateneigentümer, die Mitglieder des Teams zu bearbeiten. Diese Berechtigung schließt immer die Berechtigung "Gruppen anzeigen" mit ein.
Besitzer bearbeiten	Mit dieser Berechtigung kann der Dateneigentümer die Besitzer des Teams bearbeiten. Diese Berechtigung schließt immer die Berechtigung "Gruppen anzeigen" mit ein.
Dateneigentümer bearbeiten	Mit dieser Berechtigung kann der Dateneigentümer die Dateneigentümer dieses Teams selbst bearbeiten.
Teams anzeigen	Diese Berechtigung erlaubt es dem Dateneigentümer, die Maske "Microsoft 365-Teams" (Berechtigungen > Microsoft 365 Teams) zu benutzen.

Klicken Sie auf "Übernehmen" im Dialog und anschließend auf "Speichern" im Kopfbereich der Maske, um den neuen Dateneigentümer zu speichern.

### Teams und Microsoft 365-Gruppen

Im Hintergrund werden die Teams von Microsoft 365-Mandanten als Gruppen verwaltet. Die Mitglieder und Besitzer der Gruppe werden daher über die Maske *Microsoft 365-Gruppen* bearbeitet. Sollte der Dateneigentümer die Berechtigungen "Gruppen anzeigen", "Gruppenmitglieder bearbeiten" oder "Besitzer bearbeiten" erhalten haben, so bekommt er damit auch gleich Zugriff auf diese Maske. Eine Bearbeitung der Mitglieder und Besitzer direkt auf der Maske "Microsoft 365-Teams" ist nicht möglich. (Siehe [Verwaltung der Microsoft 365 Gruppen](#)(see page 331))

Um einen bestehenden Dateneigentümer zu bearbeiten, klicken Sie auf den Knoten "Dateneigentümer" des jeweiligen Teams und benutzen Sie die Aktion "Bearbeiten" im Aktionsmenü des jeweiligen Dateneigentümers im Bereich "Dateneigentümer" auf der rechten Seite der Maske. Sie erhalten daraufhin denselben Dialog wie zur Anlage neuer Dateneigentümer und können dort sämtliche Einstellungen, mit Ausnahme der Person, wieder ändern. Wenn Sie die Person selbst ändern möchten, löschen Sie den Dateneigentümer zunächst und fügen dann einen neuen Dateneigentümer hinzu. Geänderte Dateneigentümer werde Ihnen in der Liste durch ein entsprechendes Icon markiert.

Sobald Sie alle gewünschten Änderungen getroffen haben, speichern Sie die Einstellung durch Betätigen der Schaltfläche "Speichern" in der Kopfzeile der Maske.

Um einen Dateneigentümer zu löschen, wählen Sie entweder seinen Knoten in der Baumstruktur an und betätigen dann die Schaltfläche "Löschen" im Bereich "Dateneigentümer" auf der rechten Seite der Maske oder wählen den Knoten "Dateneigentümer" und wählen dann die Aktion "Löschen" im Aktionsmenü des jeweiligen Dateneigentümers im selben Bereich. Entfernte Dateneigentümer werden Ihnen mit einem entsprechenden Icon markiert. Abgeschlossen wird das Löschen durch Betätigung der Schaltfläche "Speichern" im Kopfbereich der Maske.

## 7.8.3 Microsoft 365 Teams-Vorlagen

### Benötigte Berechtigung

Für die Verwaltung ist die Systemberechtigung "Manage Microsoft 365 Team Templates" (9130) erforderlich.

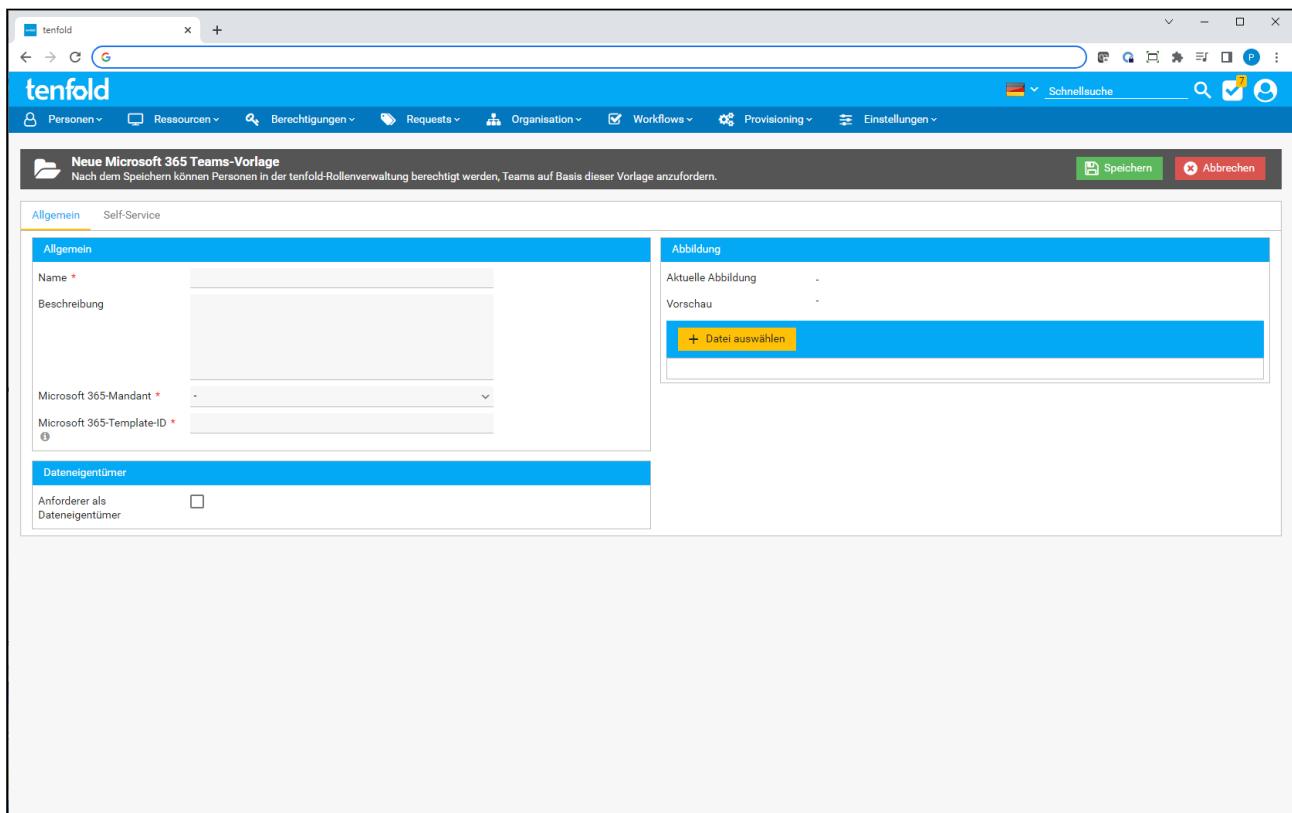
Microsoft 365 Teams erlaubt es Ihnen, Vorlagen zu erstellen, anhand derer neue Teams angelegt werden können. In diesen Vorlagen können Kanäle und Apps vordefiniert werden, die einem Team, welches mittels der Vorlage angelegt wurde, automatisch hinzugefügt werden. Diese Vorlagen lassen sich in tenfold integrieren, damit tenfold-Benutzer neue Teams anhand von Vorlagen bestellen können.

### Teams-Vorlagen

Damit eine Vorlage in tenfold integriert werden kann, muss diese zuerst in Teams, über das Admin-Portal (<https://aka.ms/admincenter>) in Ihrem Microsoft 365 Mandanten, angelegt werden. In tenfold selbst können die Vorlagen nicht angelegt werden.

Name	Self-Service	Kategorie
Consulting Team	✓	-
HR Team	✓	Projects
IT Team	-	-

Navigieren Sie im Menü über *Ressourcen > Microsoft 365 Teams-Vorlagen* auf die Maske zur Wartung der Teams-Vorlagen. Sie erhalten dort eine Übersicht über sämtliche bereits in tenfold registrierten Vorlagen. Um eine neue Vorlage anzulegen, betätigen Sie die Schaltfläche "Neu" im Kopfbereich der Maske. Bestehende Vorlagen bearbeiten Sie mittels der Aktion "Bearbeiten" im Aktionsmenü der jeweiligen Vorlage. Sie gelangen daraufhin auf die Maske zur Anlage/Bearbeitung von Teams-Vorlagen.



Im Karteireiter "Allgemein" legen Sie die notwendigen Einstellungen für die Integration in tenfold fest:

Einstellung	Beschreibung
<b>Bereich "Allgemein"</b>	
Name	Der Name der Vorlage. Dieser Name wird zur Anzeige in tenfold verwendet. <b>Hinweis:</b> Der Name muss nicht mit dem Namen Ihrer Vorlage in Microsoft 365 Teams übereinstimmen.
Beschreibung	Eine Beschreibung für die Vorlage. Verwenden Sie dieses Feld, um darauf hinzuweisen, wofür die Vorlage gedacht ist. <b>Hinweis:</b> Diese Beschreibung wird im Self-Service bei der Bestellung eines Teams angezeigt. Fügen Sie hier deshalb keine Anmerkungen ein, welche ausschließlich für Administratoren gedacht sind.
Microsoft 365-Mandant	Wählen Sie hier den Microsoft 365-Mandanten aus, auf welchem die Vorlage eingerichtet wurde.
Microsoft 365-Template-ID	Tragen Sie hier die ID der Vorlage aus Microsoft 365 ein. Sie finden die ID in Ihrem Admin Center ( <a href="https://aka.ms/admincenter">https://aka.ms/admincenter</a> ) <sup>7</sup> im Teams-Bereich.
<b>Bereich "Dateneigentümer"</b>	

<sup>7</sup> <https://aka.ms/admin-center>)

Anforderer als Dateneigentümer	Wird diese Einstellung ausgewählt, werden die Personen, die ein Team oder Teams mittels einer Vorlage anfordern, automatisch als Dateneigentümer gesetzt, sobald der Request zur Anlage durchgeführt wurde.
Berechtigungen	Legen Sie hier fest, welche Dateneigentümerberechtigungen (siehe <a href="#">Dateneigentümer(see page 341)</a> ) dem Anforderer zugeteilt werden. Diese Einstellung ist nur verfügbar, wenn zuvor "Anforderer als Dateneigentümer" ausgewählt wurde.
<b>Bereich "Abbildung"</b>	
Aktuelle Abbildung	Zeigt die Aktuell ausgewählte Abbildung an.
Vorschau	Zeigt eine Vorschau der hochgeladenen Abbildung an.
Datei auswählen	Diese Schaltfläche erlaubt es Ihnen, eine Bilddatei hochzuladen, welche im Self-Service angezeigt wird, um Ihre Vorlage zu repräsentieren.

Es können noch weitere Einstellungen im Karteireiter "Self-Service" getroffen werden, welche speziell für die Bestellung mittels der Vorlagen im Self-Service-Bereich relevant sind.

Einstellung	Beschreibung
Self-Service aktiv	Legt fest, ob mittels dieser Vorlage Teams im Self-Service bestellt werden können.
Kommentar erforderlich	Mit dieser Einstellung wird festgelegt, ob Anforderer einen Kommentar für die Bestellung hinterlegen müssen.
Ressourcenkategorie	Hier legen Sie fest, in welcher Kategorie im Self-Service die Vorlage angezeigt wird. Lassen Sie diese Einstellung leer, wird die Vorlage in einem speziellen Bereich "Microsoft 365-Teams" angezeigt.
Ausführliche Beschreibung verfügbar	Haken Sie dieses Feld an und geben einen Text ein, um eine ausführlichere Beschreibung im Self-Service anzuzeigen. In diesem Feld können Sie nicht nur Text eingeben, sondern diesen auch formatieren. <b>Hinweis:</b> Auch, wenn Sie diese Einstellung benutzen, wird das Feld "Beschreibung" aus dem Karteireiter "Allgemein" bei der Bestellung angezeigt.

Sind Sie mit den Einstellungen zufrieden, speichern Sie diese durch Betätigen der Schaltfläche "Speichern" im Kopfbereich der Maske.

### Änderungen von Vorlagen

Eine Änderung der Einstellungen wirkt sich nur auf neu angeforderte Teams aus. Auf bestehende Teams, welche mittels der Vorlage angefordert wurden, haben Änderungen keine Auswirkungen.

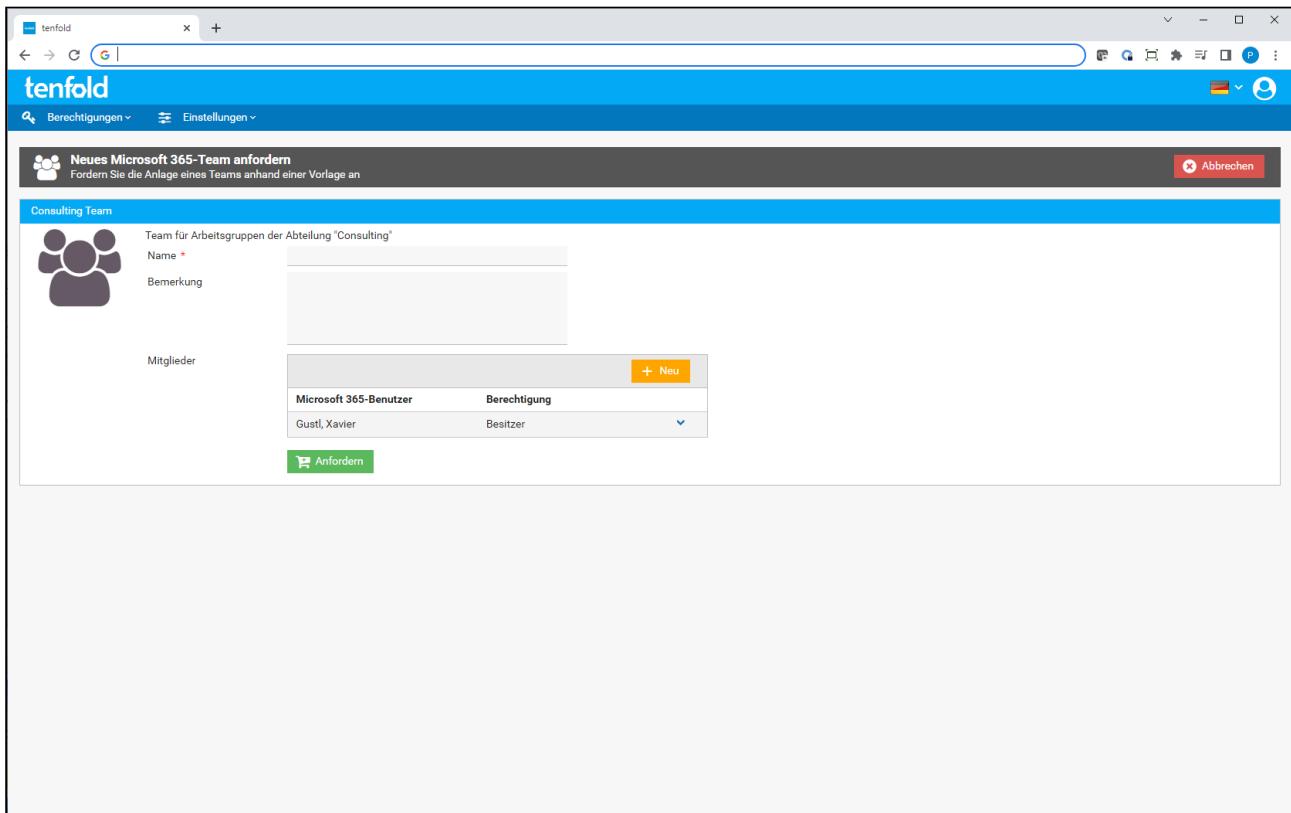
## Teams mittels Vorlage anfordern

### Benötigte Berechtigung

Zum Anfordern wird die Berechtigung "Request" auf zumindest eine Teams-Vorlage benötigt. Siehe [Berechtigungen\(see page 457\)](#).

Um ein Team mit den eingerichteten Vorlagen anzufordern, verfahren Sie wie üblich, um für sich selbst oder andere Personen Ressourcen anzufordern (siehe [Self-Service-Oberfläche\(see page 51\)](#)). Sie finden die Teams-Vorlagen entweder in der speziellen Ressourcenkategorie "Microsoft 365-Teams" oder in der Ressourcenkategorie, welche bei der Vorlage hinterlegt wurde.

Sobald Sie auf die Kachel einer Teams-Vorlage geklickt haben, gelangen Sie auf die Maske zur Bestellung des Teams. Sie können hier einen Namen für das Team und eine Bemerkung für den Request angeben, sowie weitere Besitzer/Mitglieder des Teams. Die Person, für welche das Team bestellt wird, wird automatisch als Besitzer des Teams hinterlegt. Betätigen Sie die Schaltfläche "Anfordern", um das Team in Ihre Anforderungsliste aufzunehmen. Die Anfrage für die Erstellung des Teams wird dann mit den restlichen Anforderungen angelegt, sobald Sie Ihre Anforderungen speichern.



### Besitzer entfernen

Die Person, für welche die Anfrage erstellt wird, wird automatisch als Besitzer unter "Mitglieder" eingetragen. Dieser Eintrag kann jedoch entfernt werden. Sie können dies benutzen, um die Anfrage unter Ihrem Namen zu starten, obwohl das Team für andere Benutzer gedacht ist.

### Besitzer ist nicht Dateneigentümer

Sollte die Einstellung "Anforderer als Dateneigentümer" bei der Teams-Vorlage aktiviert werden, so wird der Anforderer auch dann als Dateneigentümer hinterlegt, wenn er aus der Liste der Mitglieder entfernt wird. Andere als Besitzer hinterlegte Mitglieder werden nicht als Dateneigentümer eingetragen.

## 8 Funktionen für Suche und Reporting

### 8.1 Active Directory Pathfinder

Der Active Directory Pathfinder dient der Visualisierung von Active Directory-Strukturen. Er zeigt Mitgliedschaften grafisch an und ermöglicht so ein besseres und schnelleres Verständnis des Active Directory-Aufbaus.

Der Pathfinder kann aus unterschiedlichen Punkten in tenfold gestartet werden:

- Aus dem Kontextmenü der Schnellsuche im Tab "AD-Objekte"
- Aus der Verwaltung der Active Directory Gruppen

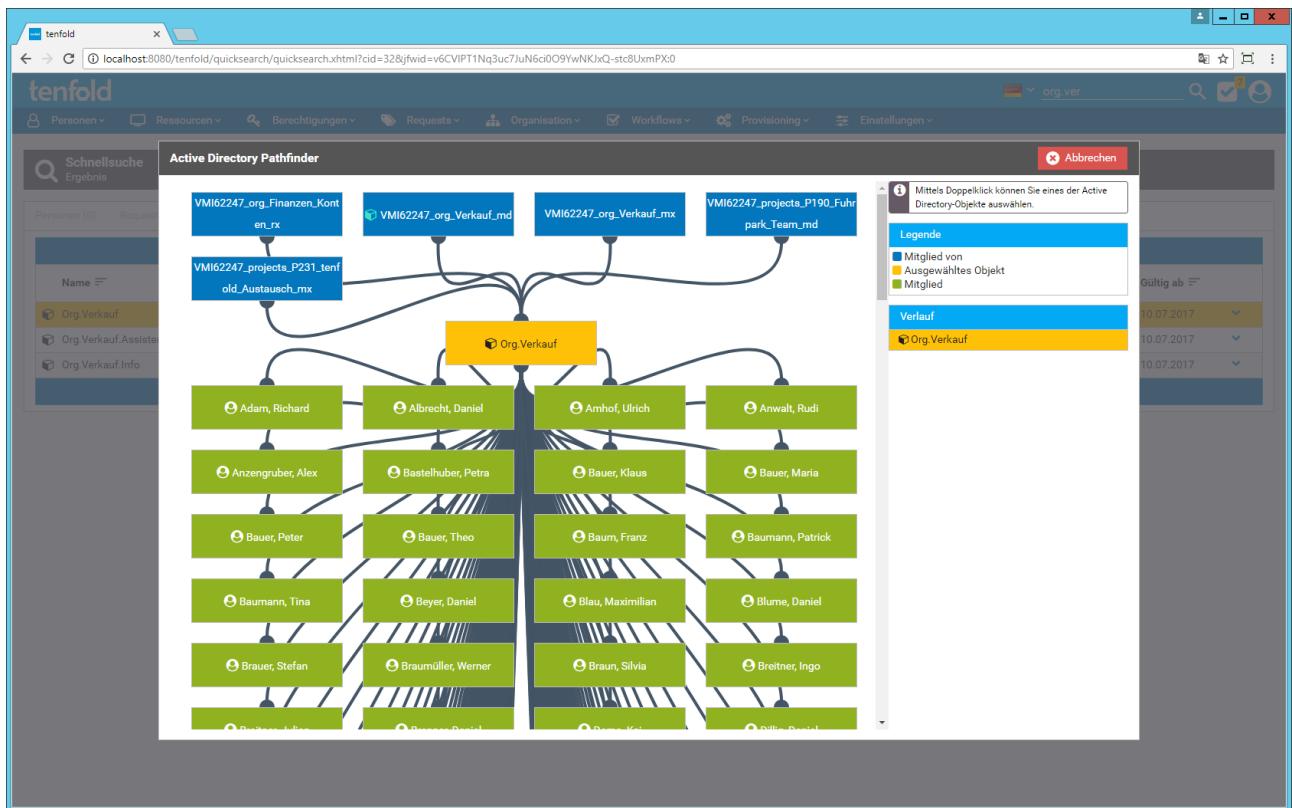
The screenshot shows a web-based application interface for 'tenfold'. At the top, there's a navigation bar with links like 'Personen', 'Ressourcen', 'Berechtigungen', 'Requests', 'Organisation', 'Workflows', 'Provisioning', and 'Einstellungen'. A search bar at the top right contains the text 'org.ver'. Below the navigation, a header bar says 'Schnellsuche' and 'Ergebnis'. Underneath, a sub-header shows 'AD-Objekte (3)'. The main content area displays a table with three rows of data:

Name	Anzeigename	Domäne	Besitzer	Person	Ablaufdatum	Gültig ab
Org.Verkauf	Org.Verkauf	TENFOLD				10.07.2017
Org.Verkauf.Assistenz	Org.Verkauf.Assistenz	TENFOLD				
Org.Verkauf.Info	Org.Verkauf.Info	TENFOLD				

On the right side of the table, there's a context menu with options: 'Anzeigen', 'Bearbeiten', 'Pathfinder', and 'Export'. Below the table, there's another set of navigation buttons labeled '(1 of 1)'.

Es werden im Pathfinder drei Typen - auch farblich - unterschieden:

- Gelb: Das ausgewählte Objekt
- Grün: Mitglieder des ausgewählten Objekts
- Blau: Gruppen, in denen das ausgewählte Objekt Mitglied ist



Sie können ein anderes Objekt in das Zentrum bewegen, indem Sie auf eines der blauen oder grünen Objekte doppelklicken. Auf der rechten Seite der Maske befindet sich eine Liste aller bereits betrachteten Objekte (Verlauf). Durch Klick auf ein Objekt wird dieses erneut ins Zentrum bewegt.

## 8.2 Schnellsuche

### 8.2.1 Sucheinstellungen

Die Schnellsuche stellt die zentrale Funktion da, um Objekte in tenfold schnell ausfindig machen zu können. Sie befindet sich in der Menüleiste ganz rechts neben der Symbolleiste und dem Einkaufswagen-Symbol.

Wenn Sie mit dem Cursor im Suchfeld stehen, so öffnet sich automatisch der Einstellungsbereich für die Schnellsuche. Hier kann ausgewählt werden, welche Objekttypen in der Suche miteingeschlossen werden sollen. Um die Performance der Suche zu erhöhen, selektieren Sie nur die Objekttypen, nach denen Sie tatsächlich suchen wollen. Unter dem jeweiligen Objekttyp befindet sich eine kurze Beschreibung.

### 8.2.2 Suche ausführen

Um die Suche auszuführen, geben Sie den gewünschten Suchbegriff ein und drücken Sie "Enter" oder klicken Sie den Button "Suche" an. Als Suchbegriff kann der gesamte Name des gesuchten Objekts, als auch ein Teil davon eingegeben werden. Um beispielweise nach Personen zu suchen, sind folgende Optionen möglich:

- Vorname (oder ein Teil davon)
- Nachname (oder ein Teil davon)
- Benutzername (oder ein Teil davon)

Das Suchergebnis erfasst dann alle Objekte der ausgewählten Typen, welche zum Suchbegriff passen.

### Beispiel

Wird beispielsweise mit dem Teil eines Benutzernamens gesucht, welcher auf drei Benutzer zutrifft, findet tenfold die zutreffenden drei Personen, die zutreffenden drei Active Directory Konten und alle Requests zu den betreffenden drei Personen (sofern die jeweiligen Objekttypen selektiert wurden).

## 8.2.3 Suchergebnis

Nachdem die Suche durchgeführt wurde, erscheint die Maske "Suchresultat". Die zutreffenden Objekte werden je nach Objekttyp in unterschiedlichen Karteireitern angezeigt. Jeder Karteireiter enthält eine Tabelle mit den gefundenen Objekten, welche die wichtigsten Daten zum jeweiligen Objekt in Spalten enthält.

### Anzeige

Neben dem Objekttyp wird die Anzahl der gefundenen Objekte dieses Typs angezeigt. Wurden keine Objekte gefunden (oder wurde der Objekttyp nicht in den Einstellungen ausgewählt), so ist der betreffende Karteireiter ausgegraut und wird mit Anzahl "0" angeführt.

## 8.2.4 Weitere Aktionen

Abhängig vom Objekttyp und den zur Verfügung stehenden Berechtigungen können für die einzelnen zutreffenden Objekte in der Spalte Aktion (ganz rechts) die passenden Aktionen gestartet werden. Folgende Aktionen stehen zur Verfügung:

Objekttyp	Aktion	Beschreibung
Personen	Anzeigen	Wechselt zur Anzeige der Person (read-only)
	Bearbeiten	Wechselt zur Bearbeitung der Person (es können Änderungen gemacht werden)
	Löschen	Löscht die Person. Vorab ist eine Bestätigung erforderlich.
	Sperren	Sperrt die Person. Vorab ist eine Bestätigung erforderlich.
	Passwort zurücksetzen	Startet den Vorgang des Zurücksetzens des Passworts der Person. Der weitere Verlauf hängt stark von der jeweiligen Konfiguration des Systems ab.
	Profile	Wechselt zu den Detailinformationen für die Profile der Person. Hier können unter anderem bestehende Profilzuordnungen angezeigt und bearbeitet werden.
	Bericht	Ermöglicht es den Benutzerbericht zu starten. Die weiteren Schritte hängen von der Systemkonfiguration und der verfügbaren Systeme ab.
Abteilungen	Abteilung anzeigen	Zeigt die Daten zur betreffenden Abteilung an.

Objekttyp	Aktion	Beschreibung
	Kostenumlage anzeigen	Zeigt die Informationen zum Finanzmanagement der Abteilung an. Die Verfügbarkeit dieser Funktion ist konfigurationsabhängig.
Niederlassungen	(keine Aktionen verfügbar)	-
Organisationseinheiten	Anzeigen	Zeigt die Daten zur betreffenden Organisationseinheit an.
Requests	Request anzeigen	Zeigt die Detailinformationen zum betreffenden Request an.
	Person anzeigen	Wechselt zur Anzeige der Person, für welche der Request erstellt wurde (read-only)
Kostenstellen	(keine Aktionen verfügbar)	-
Active Directory	Anzeigen	Wechselt zur Anzeige des jeweiligen Active Directory Objekts (dies kann ein Benutzer oder eine Gruppe sein).
	Bericht	Ermöglicht es den Benutzerbericht zu starten. Die weiteren Schritte hängen von der Systemkonfiguration und der verfügbaren Systeme ab.
Verzeichnisse	Berechtigungen	Wechselt direkt zur Bearbeitung der Berechtigungen des betreffenden Verzeichnisses.

## 8.3 Requests

### 8.3.1 Definition

Ein Request in tenfold entspricht einem Antrag, eine bestimmte Änderung durchzuführen. Diese Änderungen können unterschiedlicher Natur sein. Folgende Situationen sind grundsätzlich möglich:

Objekt / Modus	Aktion / Typ	Beschreibung
Personendaten	Anlegen	Eine neue Person wird angelegt
	Bearbeiten	Die Stammdaten einer bestehenden Person werden geändert
	Löschen	Eine bestehende Person wird gelöscht
	Sperren	Eine bestehende, nicht gesperrte Person wird gesperrt
	Entsperren	Eine bestehende, gesperrte Person wird entsperrt
Active Directory	Anlegen	Eine neue Active Directory Gruppe wird erzeugt

<b>Objekt / Modus</b>	<b>Aktion / Typ</b>	<b>Beschreibung</b>
	Löschen	Eine bestehende Active Directory Gruppe wird gelöscht
	Ändern	Die Eigenschaften der Gruppe (z.B. Name) werden geändert
	Mitglieder ändern	Es werden neue Mitglieder aufgenommen und/oder bestehende Mitglieder entfernt
Ressource	Zuordnen	Eine Ressource wird einer Person zugeordnet
	Löschen	Eine Ressource wird einer Person entzogen
	Bearbeiten	Eine bestehende Ressourcenzuordnung wird bearbeitet (z.B. Ändern von Optionen)
Applikationsberechtigung	Zuordnen	Eine Applikationsberechtigung wird einer Person zugeordnet
	Löschen	Eine Applikationsberechtigung wird einer Person entzogen
Fileserver	Anlegen	Ein Verzeichnis auf einem Fileserver wird angelegt
	Löschen	Ein bestehendes Verzeichnis auf einem Fileserver wird gelöscht
	Umbenennen	Ein Verzeichnis erhält einen neuen Namen
	Vererbung ändern	Die Vererbung auf einem Verzeichnis wird aufgehoben oder wiederhergestellt
	Berechtigungen	Es werden Berechtigungen auf dem Verzeichnis gesetzt oder gelöscht
Lifecycle	Neu	Es wird eine neue Phase im Lifecycle einer Person angelegt
	Löschen	Es wird eine Phase aus dem Lifecycle einer Person gelöscht
	Aktivieren	Eine vorhandene Phase im Lifecycle einer Person wird aktiviert
Datenkorrektur	Änderung	Eine Datenkorrektur im Fremdsystem wurde durchgeführt
Microsoft 365-Gruppe	Ändern	Neue Gruppenmitglieder werden hinzugefügt, bestehende Mitglieder werden entfernt oder Manager werden hinzugefügt/entfernt.
Microsoft 365-Lizenz	Ändern	Einem Objekt wird eine Lizenz hinzugefügt oder entzogen.

## 8.3.2 Liste der Requests

### Allgemeines

The screenshot shows the tenfold Requests list interface. At the top, there is a filter section with dropdowns for Abteilung (Privilegierte Abteilungen), Request-Typ (Alle), Request-Status (Alle), and Request-Modus (Alle). Below the filter are buttons for 'Aktualisieren' (Update) and 'Excel Export'. The main area displays a table with 181 rows, each representing a request. The columns include Objekt, Angefordert für, Angefordert am, Ticket, Zuletzt genehmigt von, Request-Quelle, Request-Typ, and Request-Status. Most requests are marked as 'FERTIG' (Completed). A message at the bottom left indicates that more items are available if the table reaches its end.

Objekt	Angefordert für	Angefordert am	Ticket	Zuletzt genehmigt von	Request-Quelle	Request-Typ	Request-Status
VPN-Zugang	Faber Franz	25.10.2017 15:26:04		Semmelmayer Helmut (systemfold)	tenfold	✗ Löschen	FERTIG
SugarCRM - Vertriebsanwendung	Faber Franz	25.10.2017 15:26:04		Semmelmayer Helmut (systemfold)	tenfold	✗ Löschen	FERTIG
SAP - ERP (Produktion)	Faber Franz	25.10.2017 15:26:04			tenfold	✗ Löschen	FERTIG
PMX Projektmanagement	Faber Franz	25.10.2017 15:26:04		Semmelmayer Helmut (systemfold)	tenfold	✗ Löschen	FERTIG
Desktop PC	Faber Franz	25.10.2017 15:26:04		Semmelmayer Helmut (systemfold)	tenfold	✗ Löschen	FERTIG
Person masterdata change	Faber Franz	25.10.2017 15:26:02	JIRA-124	Semmelmayer Helmut (systemfold)	tenfold	✗ Löschen	FERTIG
Team	Faber Franz	25.10.2017 15:18:16		Semmelmayer Helmut (systemfold)	tenfold	✍ Änderung	FERTIG
Austausch	4 Gruppen(n)	25.10.2017 15:14:31		Semmelmayer Helmut (systemfold)	tenfold	✍ Änderung	FERTIG
Org.Einkauf	Faber Franz	25.10.2017 15:03:20	JIRA-123	Semmelmayer Helmut (systemfold)	tenfold	✍ Änderung	FERTIG
SAP - ERP (Produktion)	Faber Franz	25.10.2017 15:03:20	JIRA-123		tenfold	✍ Änderung	FERTIG
Org.Finanzen	Faber Franz	25.10.2017 14:54:22		Semmelmayer Helmut (systemfold)	tenfold	✍ Änderung	FERTIG
SAP - ERP (Produktion)	Faber Franz	25.10.2017 14:54:22			tenfold	✍ Änderung	FERTIG
Org.Verkauf	Faber Franz	25.10.2017 14:54:09		Semmelmayer Helmut (systemfold)	tenfold	✍ Änderung	FERTIG
PMX Projektmanagement	Faber Franz	25.10.2017 14:54:09		Semmelmayer Helmut (systemfold)	tenfold	✍ Änderung	FERTIG

Die Liste der Requests gibt eine Übersicht über alle Requests, die bestimmten Kriterien entsprechen. Diese Kriterien können über entsprechende Filter eingestellt werden.

Um zur Liste der Requests zu gelangen, wählen Sie im Menü einen der folgenden Punkte:

- Requests > Offene Requests
- Requests > Fehlgeschlagene Requests
- Requests > Alle Requests

#### Menüpunkte

Die unterschiedlichen Menüpunkte führen grundsätzlich alle zur gleichen Maske ("Requests") und stellen dort den Filter "Request-Status" entsprechend vorab ein.

### Filter

Über den oberen Bereich der Maske (Abschnitt "Filter") kann die Liste der Requests eingeschränkt werden. Es stehen hierbei folgende Filtermöglichkeiten zur Verfügung:

Filter	Beschreibung
Abteilung	Nur Requests, die Personen betreffen, welche der gewählten Abteilung zugeordnet sind.

Filter	Beschreibung
Request-Typ	Nur Requests, die dem gewählten Typ entsprechen. Diese Angabe ist insbesondere in Kombination mit dem Filter "Request-Mode" sinnvoll. Siehe dazu die Tabelle oberhalb.
Request-Status	Nur Requests, die sich im gewählten Status befinden.
Request-Modus	Nur Requests, die dem gewählten Modus entsprechen. Diese Angabe ist insbesondere in Kombination mit dem Filter "Request-Typ" sinnvoll. Siehe dazu die Tabelle oberhalb.
Request-ID	Nur der Request mit exakt der eingegebenen ID wird angezeigt. <b>Achtung:</b> Wird eine ID angegeben, haben andere Filterkriterien keine Wirkung.
Von / Bis	Nur Requests, die im gewählten Zeitraum liegen.
Request-Quelle	Nur Requests, die aus der gewählten Quelle angesteuert wurden. Im Standardfall ist nur die Request-Quelle "tenfold" relevant. Eine andere Request-Quelle liegt bei Änderungen vor, die von Vorsystemen (z.B. einem HR-System) getriggert wurden.
Objekt	Nur Requests, deren Objekte (z.B. Verzeichnis auf dem Fileserver, AD-Gruppe, Microsoft 365 Lizenz) den eingegebenen Text im Namen enthalten, werden angezeigt.
Angefordert für	Nur Requests, welche für Personen angefordert wurden, die im Vor-, Nach- oder Benutzernamen den eingegebenen Text enthalten, werden angezeigt.

## Ergebnis

Das Ergebnis wird geladen und in einer Tabelle angezeigt, sobald alle Filter eingestellt wurden und Sie die Schaltfläche "Aktualisieren" betätigt haben. Folgende Spalte sind in der Tabelle enthalten:

Spalte	Beschreibung
Objekt	Bezeichnet den Namen des Objekts, das vom Request betroffen ist. Dies kann eine Ressource, eine Person, eine Active Directory Gruppe oder auch ein Verzeichnis sein. Je nach Objekt, können Sie auf den Namen klicken, um einen Dialog mit näheren Informationen zu dem Objekt anzeigen zu lassen.
Angefordert für	Gibt an, für welchen Benutzer der Request erstellt wurde. Im Fall der Änderung von Mitgliedschaften von Active Directory Gruppen oder von Verzeichnisberechtigungen können mehrere Benutzer und/oder Gruppen betroffen sein, in welchem Fall hier eine Zusammenfassung angezeigt wird. (z.B. "3 Benutzer und 2 Gruppen")
Angefordert am	Gibt an, wann der Request erstellt wurde
Ticketnummer	Gibt die Ticketnummer aus einem Service-Desk-System an, falls eine entsprechende Integration vorhanden ist, oder für den Request manuell eine Ticketnummer hinterlegt wurde.

Spalte	Beschreibung
Zuletzt genehmigt von	Entspricht dem letzten Genehmiger aus dem Workflow.
Request-Quelle	Gibt an, von welcher Quelle der Request angesteuert wurde. Im Standardverhalten ist lediglich die Request-Quelle "tenfold" relevant.
Request-Typ	Gibt den Request-Typ an (für Details siehe die Tabelle oben)
Request-Status	Gibt den Request-Status an (für Details siehe die Tabelle oben)

### 8.3.3 Requests anzeigen

The screenshot shows the tenfold software interface with the following details:

- Timeline:**
  - 25.10.2017 15:18:16: Semmelmayer Helmut Request erstellt
  - 15:18:17: Semmelmayer Helmut Dateneigentümer Genehmigungsschritt genehmigt
  - 15:18:21: Automatisch geschlossen Request geschlossen
- Request:**

Angefordert für	Faber Franz	Ticketnummer	-
Request-Typ	Änderung	Bemerkung	-
Request-Status	FERTIG		
- Verzeichnisdaten:**

Name	Team
Übergeordnetes Verzeichnis	\VMI62247\projects\P233_Zug
Fileserver	\VMI62247\projects
- Berechtigungsänderungen:**

Berechtigungsstufe	Objekt	Bemerkung
+ Ändern Plus	Faber, Franz	fafafa

Requests können über die Maske "Requests anzeigen" mit allen Detailinformationen angezeigt werden. Diese Maske kann, unter anderem, auf der Request-Liste über das Aktionsmenü (Punkt "Request anzeigen") aufgerufen werden.

#### Gültigkeit

Es gibt in tenfold zahlreiche Einsprungspunkte, die auf die Maske "Request anzeigen" verzweigen. Die Informationen in diesem Abschnitt sind für alle Einsprungspunkte identisch.

Die Maske besteht aus den folgenden Karteireitern (diese werden konfigurations- und berechtigungsabhängig angezeigt):

Karteireiter	Anzeige	Beschreibung
Allgemeines	Fix	Zeigt alle Kopfinformationen zum Request an.
EXEC-Verlauf	Fix	Es handelt sich hierbei um interne Informationen, welche lediglich für den Systemadministrator relevant sind
Ereignisse	Optional	Die internen Abläufe sowie die externen Kommunikationsbausteine (EXECs) von tenfold können für jeden ausgeführten Request Protokollinformationen niederschreiben. Diese Informationen werden auf diesem Tab angezeigt

## Karteireiter Allgemeines

Der wichtigste Karteireiter ist der Reiter mit der Bezeichnung "Allgemeines". Der Aufbau der Anzeige ist wie folgt:

- Die Timeline auf der linken Seite zeigt alle wichtigen Ereignisse zum Request an: Erstellung, Genehmigungen/Ablehnungen, Fehler, Abschluss.
- Für jeden Eintrag wird die Datums- und Uhrzeitangabe, der auslösende Benutzer und - sofern vorhanden - der eingegebene Kommentar angezeigt.
- Ist der Request im Status "Geplant", wird angezeigt, zu welcher Zeit der Request durchgeführt werden kann.

### Durchführungsdatum ändern

Sollte sich der Request im Status "Geplant" befinden und Sie die Berechtigung "Change Scheduled Request Execution Time" (9230) haben, wird Ihnen unterhalb der Statusanzeige, "Geplant", ein Link, "Durchführungszeitpunkt ändern", angezeigt. Mit diesem Link können Sie einen Dialog öffnen, in welchem Sie den Durchführungszeitpunkt ändern können.

Im Bereich "Request" sind folgende Informationen ersichtlich:

- Angefordert für: Gibt an, wer der Empfänger der angefragten Ressource ist
- Request-Typ: Gibt den Typ des Requests an (siehe oben)
- Request-Status: Zeigt den Status des Requests (siehe oben)
- Ticketnummer: Zeigt die hinterlegte Ticketnummer des Requests an
- Bemerkung: Zeigt die hinterlegte Bemerkung zum Request an

Unterhalb des Bereichs "Request" befinden sich - je nach Request-Modus und Request-Typ - unterschiedliche Informationen, die den Inhalt des Requests genauer beschreiben.

## 8.4 Personensuche

Im Gegensatz zu anderen Stammdaten existiert in tenfold keine gesonderte Verwaltungsmaske für Personen. Stattdessen bietet tenfold Ihnen mehrere unterschiedliche Einstiegspunkte in die Maske zur Bearbeitung von Personen. Eine dieser Einstiegspunkte ist die Maske zur Personensuche. Diese erreichen Sie im Menü unter *Personen > Suche*.

Resultate (3)						
Nachname	Vorname	Benutzername	Personalnummer	Abteilung	Titel	E-Mail
Aachen	Daniel	daachen	11319	Accounting	Manager	
Aachen	Ines	iaachen	10116	Sales		
Aachen	Sabrina	saachen	10435	Human Resources		

### Benötigte Berechtigung

Für die Funktion wird die Berechtigung "Use Person Search (Default)" (2021) benötigt.

#### 8.4.1 Personen suchen (Standardsuche)

Nachdem Sie auf die Maske gelangt sind, können Sie eine Reihe von Filtereinstellungen treffen, um Personen mit bestimmten Eigenschaften zu suchen.

##### Schnellsuche

Für einfache Suchen nach Benutzername, Vor- und/oder Nachname empfiehlt sich die Schnellsuche. Siehe [Schnellsuche\(see page 350\)](#) für Details.

Filter	Beschreibung
Nachname	Der Nachname (LAST_NAME) der Person muss den eingegebenen Text enthalten.
Vorname	Der Vorname (FIRST_NAME) der Person muss den eingegebenen Text enthalten.
Benutzername	Der Benutzername (USERID) muss den eingegebenen Text enthalten.

Filter	Beschreibung
Personalnummer	Die Personalnummer (EMPLOYEE_ID) muss den eingegebenen Text enthalten.
Lifecycle-Phase	Die Person muss sich aktuell in der ausgewählten Lifecycle-Phase befinden.
Abteilung	Der Name der Abteilung (DEPARTMENT) muss den eingegebenen Text enthalten. <b>Achtung:</b> Es handelt sich bei diesem Feld <b>nicht</b> um ein Auswahlfeld. Es handelt sich um einen Textfilter für den Namen der Abteilung.
Niederlassung	Der Name der Niederlassung (OFFICE), in welcher sich die Person befindet, muss den eingegebenen Text enthalten.
Unternehmen	Der Name des Unternehmens der Niederlassung (OFFICE), in welcher sich die Person befindet, muss den eingegebenen Text enthalten.
Kostenstelle	Der Name oder Code der Kostenstelle (COST_CENTER) muss den eingegebenen Text enthalten.
Personenart	Die Person muss die ausgewählte Personenart (IDENTITY_TYPE) haben.
Position	Die Person muss die ausgewählte Position (POSITION) haben.

#### Personenfelder

Die Namen der Personenfelder auf der Maske zur Bearbeitung von Personen können sich von den Bezeichnungen der Felder auf der Suchmaske unterscheiden.

Filter ohne Eingabe werden bei der Suche nicht berücksichtigt. Alle eingegebenen Filter müssen jedoch zutreffen, damit die Person im Suchresultat aufscheint.

#### Groß-/Kleinschreibung

Die Groß-/Kleinschreibung wird bei den Filtereinstellungen nicht beachtet.

## 8.4.2 Personen suchen (Feldregelsuche)

Alternativ zu der Suche mittels Suchfiltern können Personen auch über Feldregeln gesucht werden.

#### Benötigte Berechtigung

Für diese Funktion wird die Berechtigung "Use Person Search (Field Rules)" (2032) benötigt.

Um die Maske in den Modus für Feldregelsuche umzuschalten, betätigen Sie die Schaltfläche "Feldregelsuche" im Kopfbereich der Maske.

### Berechtigung

Verfügen Sie nur über die Berechtigung "Use Person Search (Field Rules)" (2032) wird Ihnen die Maske direkt im Modus für die Feldregelsuche dargestellt. Haben Sie beide Berechtigungen, beginnt die Maske im Modus für Standardfilter.

Benutzen Sie die Schaltfläche "Hinzufügen", um eine bestehende Feldregel als Suchkriterium hinzuzufügen und die Schaltfläche "Neue Feldregel", um zur Maske für die Erstellung von Feldregeln (siehe [Feldregeln \(see page 562\)](#)) zu gelangen, damit Sie eine neue Feldregel für die Suche anlegen können. Wenn Sie die Feldregel speichern gelangen Sie wieder auf diese Maske und können die Feldregel dann zu den Suchkriterien hinzufügen.

Im Feld "Überprüfungsmodus" können Sie auswählen, ob die Suchmenge die Personen enthalten soll, auf welche zumindest eine Feldregel zutrifft oder, ob alle gewählten Feldregeln zutreffen müssen.

Egal, ob Sie die Standardsuche oder die Feldregelsuche benutzen, müssen Sie die Schaltfläche "Suchen" betätigen, um ein Ergebnis mit den getroffenen Suchkriterien zu erhalten. Nachdem Sie ein Suchergebnis haben können Sie die folgend beschriebenen Funktionen verwenden.

### 8.4.3 Angezeigte Felder

In den Suchergebnissen der Personensuche und Schnellsuche werden folgende Felder immer angezeigt:

- Personenart (IDENTITY\_TYPE) (Icon)
- Nachname (LAST\_NAME)
- Vorname (FIRST\_NAME)

- Benutzername (USERID)

Zusätzlich zu diesen Feldern lassen sich in den Systemparametern (siehe [Systemparameter\(see page 484\)](#)) folgende weitere Felder einblenden:

- Abteilung (DEPARTMENT)
- E-Mail (EMAIL)
- Fax (FAX)
- Fax2 (FAX2)
- Mobiltelefon (MOBILE)
- Personalnummer (EMPLOYEE\_ID)
- Position (POSITION)
- Ressourcen
- Stellenbezeichnung (JOB\_TITLE)
- Telefon (PHONE)
- Telefon privat (PHONE\_HOME)
- Telefon2 (PHONE2)
- User Principal Name (USER\_PRINCIPAL\_NAME)

#### **Globale Einstellung**

Die Einstellung der angezeigten Felder wird global für alle Benutzer getroffen. Eine individuelle Einstellung der Anzeige je Benutzer ist nicht möglich.

Um die angezeigten Felder anzupassen, navigieren Sie im Menü zur Maske Einstellungen > System > Parameter und öffnen dort den Knoten Sucheinstellungen und Suchergebnisse > Personensuche.

#### **Benötigte Berechtigung**

Für die Konfiguration ist die Berechtigung "Configuration administration" (8010) erforderlich.

Unterhalb dieses Knotens finden Sie die Einstellungen zur Anzeige der verschiedenen optionalen Felder.

### **8.4.4 Excel-Export**

Sobald Sie ein Suchergebnis erhalten haben, können Sie die Schaltfläche "Excel-Export" im Kopfbereich der Maske verwenden, um eine Excel-Datei mit gefunden Personen zu erhalten. Diese Excel-Tabelle enthält ein oder mehrere Arbeitsblätter - eines für jede Personenart, welche im Suchergebnis aufscheint.

Die Felder welche pro Arbeitsblatt aufscheinen werden in den Einstellungen der Felder für die jeweilige Personenart konfiguriert. Für Details siehe [Personenarten\(see page 81\)](#).

#### **Unsichtbare Felder**

Felder, welche die exportierende Person aufgrund von Berechtigungen nicht anzeigen darf, scheinen auch im Export nicht auf. Selbst wenn für dieses der Export aktiviert wurde.

#### **Dauer**

Je nach Anzahl der gefunden Personen kann der Export eine gewisse Zeit in Anspruch nehmen.

## 8.4.5 Aktionen

Zu jeder gefundenen Person können folgende Aktionen über das jeweilige Aktionsmenü durchgeführt werden:

- Anzeigen**

Wechselt zur Maske für die Anzeige von Personen.

- Bearbeiten**

Wechselt zur Maske für die Bearbeitung von Personen.

- Passwort ändern**

Startet den Passwortänderungsprozess für diese Person.

- Profile**

Öffnet die Maske zur Übersicht und zum Abgleich von Profilen für die gewählte Person.

- Bericht**

Öffnet den Assistenten zur Erstellung eines Berichts für die Person.

### Benötigte Berechtigung

Um die jeweiligen Aktionen angezeigt zu bekommen werden die entsprechenden Berechtigungen benötigt. Siehe [Personenverwaltung](#)(see page 63) und [Berechtigungen](#)(see page 457) für Details.

## 8.5 Dashboard

Das Dashboard von tenfold zeigt Ihnen Probleme in Ihrer Landschaft auf und bietet Ihnen vorgefertigte Lösungen für diese Probleme an.

The screenshot shows the tenfold dashboard interface with a blue header bar containing navigation links like 'Personen', 'Ressourcen', 'Berechtigungen', etc. Below the header is a dark grey sidebar with the title 'Dashboard' and the subtitle 'Existierende Probleme finden und bearbeiten'. The main area consists of a grid of 12 cards, each representing a different type of system issue or audit finding. The cards are arranged in three rows of four. Each card includes a small icon, a category label (e.g., FILESERVER, ACTIVE DIRECTORY, MICROSOFT 365), a numerical value in a yellow box, and a brief description. The categories and their values are:

Category	Value	Description
FILESERVER	0	Verzeichnisse mit 'Jeder'-Berechtigung
FILESERVER	0	Verzeichnisse mit 'Authentifizierte Benutzer'-Berechtigung
FILESERVER	12	Verzeichnisse mit direkt berechtigten Benutzern
FILESERVER	19	Verzeichnisse bei denen Vererbung aufgebrochen wurde
FILESERVER	14	Verwaiste SIDs, die Berechtigungen haben
ACTIVE DIRECTORY	286	Leere Active Directory-Gruppen
ACTIVE DIRECTORY	2239	Niemals genutzte Benutzerkonten
ACTIVE DIRECTORY	54	Verwaiste Benutzerkonten
ACTIVE DIRECTORY	255	Benutzerkonten ohne Gruppenmitgliedschaften
ACTIVE DIRECTORY	64	Benutzerkonten ohne Passwortänderung
ACTIVE DIRECTORY	0	Temporär gesperrte Benutzerkonten
MICROSOFT 365	3	Deaktivierte Benutzer mit Lizenz
MICROSOFT 365	7	Gastbenutzer
MICROSOFT 365	1	Gastbenutzer in Teams
MICROSOFT 365	1	Gastbenutzer mit Lizenz

### Benötigte Berechtigung

Für die Verwendung ist die Berechtigung "Use Dashboard" (8290) erforderlich.

Sie gelangen zum Dashboard über das Menü unter *Berechtigungen > Dashboard*.

Auf der Maske angelangt, finden Sie zunächst eine Reihe von Kacheln vor, welche Ihnen Auskünfte über die Art der behandelten Probleme geben sowie wie häufig das jeweilige Problem auftritt. In der rechten oberen Ecke jeder Kachel finden Sie eine Kategorie, welche angibt, zu welcher Art von System das Problem gehört (z.B. Active Directory, File Server, etc.).

Durch einen Klick auf eine Kachel mit einer Anzahl von Problemen, welche 1 oder größer ist, gelangen Sie zu einer Maske mit einer Auflistung der einzelnen Problemfälle. Die Details, welche zu jedem Problem dargestellt werden, unterscheiden sich von Problemfall zu Problemfall. Für manche Problemfälle bietet tenfold Ihnen eine Behebung an. Haken Sie dafür die gewünschten Problemfälle an und betätigen die Schaltfläche "Beheben".

Verzeichnis	Person	Berechtigung	Fileserver
<input type="checkbox"/>	Administrator	Vollzugriff	
<input checked="" type="checkbox"/>	Administrator	Vollzugriff	
<input checked="" type="checkbox"/>	Administrator	Vollzugriff	
<input type="checkbox"/>	Gustl, Xavier	Ändern	
<input type="checkbox"/>	Administrator	Vollzugriff	
<input type="checkbox"/>	Administrator	Vollzugriff	
<input type="checkbox"/>	Administrator	Vollzugriff	
<input type="checkbox"/>	Administrator	Vollzugriff	
<input type="checkbox"/>	Administrator	Vollzugriff	
<input type="checkbox"/>	Administrator	Vollzugriff	

Welche Aktion für die Behebung durchgeführt wird hängt vom Problemfall ab. Im Folgenden finden Sie eine Übersicht der dargestellten Problemfälle und möglichen Behebungsoptionen:

Problemfall	Beschreibung	Behebung
Kategorie "Fileserver"		

Verzeichnisse mit 'Jeder'-Berechtigung	Listet alle Verzeichnisse auf, auf denen der Account 'Jeder' berechtigt wurde. Dieser spezielle Account gewährt allen Anmeldungen (inklusive anonymen Anmeldungen) Berechtigungen und sollte daher vermieden werden.	Es werden die ausgewählten Berechtigungen von den Fileservern entfernt.
Verzeichnisse mit 'Authentifizierte Benutzer'-Berechtigung	Listet alle Verzeichnisse auf, auf denen der Account 'Authentifizierte Benutzer' berechtigt wurde. Dieser spezielle Account gewährt allen gültigen Anmeldungen Zugriff auf die Verzeichnisse, was ein Sicherheitsrisiko darstellt.	Es werden die ausgewählten Berechtigungen von den Fileservern entfernt.
Verzeichnisse mit direkt berechtigten Benutzern	Listet alle Verzeichnisse auf, auf denen Benutzerkonten direkt, ohne Gruppen, berechtigt wurden. Dies entspricht nicht den Best Practices von Microsoft. Unter anderem führt es zu verwaisten SIDs in den Berechtigungen, wenn die betroffenen Konten gelöscht werden.	Wandelt die Berechtigungen in Gruppen-Berechtigungen um. Falls notwendig werden hier neue Berechtigungsgruppen erzeugt, .
Verzeichnisse bei denen Vererbung aufgebrochen wurde.	Hier finden Sie alle Verzeichnisse aufgelistet, bei welchen die Berechtigungsvererbung deaktiviert wurde. Dies erhöht die Komplexität der Berechtigungsstruktur und sollte vermieden werden. Es entspricht nicht den Best Practices von Microsoft.	Die Vererbung der Ausgewählten Verzeichnisse wird wiederhergestellt.
Verwaiste SIDs, die Berechtigungen haben	Listet alle Verzeichnisse auf, auf denen sich Berechtigungen für SIDs finden, deren zugehörige Konten sich aber nicht mehr im Active Directory befinden. <b>Hinweis:</b> Sollte nicht das gesamte Active Directory gescannt worden sein, finden Sie hier auch alle Berechtigungen für Konten, welche in tenfold nicht vorhanden sind, auch wenn diese im Active Directory existieren.	<i>Keine Behebung vorhanden</i>

#### Kategorie "Active Directory"

Leere Active Directory-Gruppen	Hier finden Sie eine Auflistung aller Active Directory-Gruppen ohne Mitglieder. Es sollte geprüft werden, ob diese noch benötigt werden oder gelöscht werden können.	Die ausgewählten Gruppen werden gelöscht.
--------------------------------	--	---

Niemals genutzte Benutzerkonten	Listet alle Benutzerkonten auf, mit welchen noch nie eine interaktive Anmeldung stattgefunden hat. Nicht genutzte Benutzerkonten werden häufig nicht beobachtet und können daher ein Sicherheitsrisiko darstellen.	Die ausgewählten Konten werden gelöscht.
Verwaiste Benutzerkonten	Listet Benutzerkonten auf, mit welchen seit mehr als 180 Tagen keine interaktive Anmeldung stattgefunden hat. Nicht genutzte Benutzerkonten werden häufig nicht beobachtet und können daher ein Sicherheitsrisiko darstellen.	Die ausgewählten Konten werden gelöscht.
Benutzerkonten ohne Gruppenmitgliedschaften	Es werden alle Benutzerkonten aufgelistet, welche keine Gruppenmitgliedschaften, außer der Primärgruppe (normalerweise "Domänen-Benutzer"), besitzen.	Keine Behebung vorhanden
Benutzerkonten ohne Passwortänderung	Listet alle Benutzerkonten auf, deren Passwörter niemals ablaufen. Diese Konten stellen möglicherweise ein Sicherheitsrisiko dar, wenn deren Passwörter kompromittiert sind, da diese ewig gültig sind.	Keine Behebung vorhanden
Temporär gesperrte Benutzerkonten	Zeigt alle Benutzerkonten an, welche durch mehrfache Falscheingabe der Passwörter temporär gesperrt wurden.	Die Konten werden entsperrt.
<b>Kategorie "Microsoft 365"</b>		
Deaktivierte Benutzer mit Lizenz	Eine Auflistung aller Benutzerkonten, welche deaktiviert sind, jedoch noch Lizizen zugewiesen haben. Diese sollten geprüft werden, da unnötige Kosten entstehen können.	Keine Behebung vorhanden
Gastbenutzer	Listet alle Gastbenutzer in Microsoft 365 auf. Es sollte regelmäßig geprüft werden, ob Gastbenutzer noch benötigt werden.	Keine Behebung vorhanden
Gastbenutzer in Teams	Listet alle Gastbenutzer in Microsoft Teams auf. Es sollte regelmäßig geprüft werden, ob Gastbenutzer noch benötigt werden.	Keine Behebung vorhanden

Gastbenutzer mit Lizenzen	Listet alle Gastbenutzer mit zugewiesenen Lizenzen auf. Es sollte geprüft werden, ob die Gastbenutzer die Lizenzen noch benötigen, um unnötige Kosten zu vermeiden.	Keine Behebung vorhanden
---------------------------	---	--------------------------

Sie können die Auflistung der Problemfälle auch auf jeder Maske mit der Schaltfläche "Export" in eine Excel-Datei exportieren und herunterladen.

## 9 Organisationsstruktur

Im Menü *Organisation* befinden sich mehrere Punkte zur Verwaltung Ihrer Organisationsstruktur innerhalb von tenfold. Mithilfe dieser Struktur können Sie in tenfold steuern wie Benutzer angelegt werden sollen, können die Berechtigungen der Benutzer innerhalb von tenfold einschränken, etc. Im weiteren ist die Organisationsstruktur im wesentlichen dafür gedacht, Personen für eine automatische Zuordnung von Profilen zu identifizieren (Siehe [Profile\(see page 168\)](#)). Im Folgenden werden die einzelnen Einstellungen zur Organisationsstruktur genauer beschrieben.

### 9.1 Abteilungen

Abteilungen bilden die Grundlagen für das Berechtigungskonzept von tenfold (siehe [Abteilungen\(see page 366\)](#)). In tenfold kann eine Person entsprechende Berechtigungen immer entweder für Alle oder für bestimmte Abteilungen besitzen. Dadurch lässt sich der Personenkreis einschränken, für welche ein Benutzer von tenfold Anfragen stellen und/oder Genehmigen kann.

#### 9.1.1 Abteilungen

*Organisation > Abteilungen.*

Eine Person kann einer Abteilung mittels des Personenfeldes *DEPARTMENT* zugeordnet werden (siehe [Personenfelder](#)).

Feld	Beschreibung	Beispielwert
Name	Der Name der Abteilung. In der Standardkonfiguration wird dieses Feld der ausgewählten Abteilung einer Person in das Active Directory Feld <i>Abteilung</i> übertragen.	Information Technology
Kurzname	Ein Kürzel für die Abteilungsbezeichnung. In manchen Fällen ist es wünschenswert dieses Feld in das Active Directory zu übertragen, statt dem vollen Namen, ohne dabei auf einen sprechenden Namen in tenfold verzichten zu wollen.	IT
Typ	Hier kann eine Eingliederung in verschiedene Arten von Abteilungen vorgenommen werden.	Intern, Extern
Beschreibung	Eine Beschreibung der Abteilung zu informativen Zwecken.	

Feld	Beschreibung	Beispielwert
Übergeordnete Abteilung	Hier lässt sich die übergeordnete Abteilung einstellen. Hiermit lassen sich Abteilungshierarchien erstellen. (Siehe <a href="#">Abteilungshierarchie(see page 369)</a> ) Diese ist relevant für die Genehmigung von Requests (siehe <a href="#">Abteilungsverantwortliche(see page 368)</a> ).	Information Technology (Dropdown-Auswahl)
Abteilungsgruppe	Hier lässt sich die Abteilung zu einer Gruppe zuordnen. (Siehe <a href="#">Abteilungsgruppen(see page 368)</a> )	Technology
Region	Hier lässt sich die Region einer Abteilung einstellen. Von der Region einer Person hängt ab, wieviel Services für diese Person kosten.	EU
Standardniederlassung	Hier kann eine Standardniederlassung für die Abteilung eingestellt werden. Diese kann zum Beispiel verwendet werden um in Synchronisationsprozessen von Fremdsystemen welche nur Abteilungen kennen eine Niederlassung für eine Person festzulegen.	Büro Seidengasse
AD-Container	Ein Active Directory Container welcher zum Beispiel benutzt werden kann um Personen anhand ihrer Abteilung in das Active Directory einzugliedern. In der Standardkonfiguration wird dieses Feld jedoch nicht Berücksichtigt sondern nur die Einstellung <i>Container für Benutzer</i> der Domäne.	OU=IT,OU=USR,OU=CERTEX,OU=AT
Berechnungsmodus	Die Art der Berechnung welche für die Kostenumlage einer Person dieser Abteilung herangezogen wird. In der Standardkonfiguration sind folgende 3 Berechnungsvarianten vorhanden: <ul style="list-style-type: none"> <li>• Keine Verrechnung: Die Kosten einer Person sind immer 0.</li> <li>• Normale Verrechnung: Die Kosten einer Person ist die Summe aller Kosten ihrer Services</li> <li>• Maximum Verrechnung: Die Kosten einer Person sind die Kosten des teuersten Services jener Person.</li> </ul>	Normale Verrechnung
Parameter	Hier können Benutzerdefinierte Parameter hinzugefügt werden, welche in Anpassungen herangezogen werden können.	

### Abteilungstypen

Für Abteilungstypen gibt es in der aktuellen Version keine Wartungsmaske. Diese werden manuell in der tenfold-Datenbank angelegt. Bitte wenden Sie sich an Ihren Betreuer.

## 9.1.2 Abteilungsverantwortliche

Um die Verantwortlichen einer Abteilung zu bearbeiten rufen Sie den Menüpunkt *Organisation > Abteilungen* auf und wählen im Anschluss, im Aktionsmenü der entsprechenden Abteilung, den Menüpunkt *Verantwortliche*.

Abteilungsverantwortliche kommen in Genehmigungsworflows zum tragen. Sollte in einem Genehmigungsworflow die Berechtigung *Dateneigentümer* ausgewählt sein und es sich bei einem Request um einen Personenänderungsrequest handeln, so kann dieser Schritt von jeder Person genehmigt werden, welcher ein Abteilungsverantwortlicher für die Abteilung der betroffenen Person ist. Sollte für die entsprechende Abteilung kein Verantwortlicher eingetragen sein, so wird in der übergeordneten Abteilung nach einem Verantwortlichen gesucht, so lange bis jemand gefunden wurde. Sollte in der gesamten Hierarchie kein Verantwortlicher gefunden worden sein, so kann dieser Schritt von einer Person mit der Berechtigung *Default Approve Privilege* genehmigt werden.

### Vererbung von Abteilungsverantwortlichen

Eine Vererbung von Abteilungsverantwortlichen wird in der aktuellen Version nicht unterstützt. Sobald in einer Abteilung Verantwortliche gefunden wurden, werden Verantwortliche von übergeordneten Abteilungen nicht mehr befragt. Sie müssen daher Personen in untergeordneten Abteilungen erneut hinzufügen, wenn Sie möchten, dass eine Person auch in untergeordneten Abteilungen genehmigen darf.

Um einen Verantwortlichen hinzuzufügen, wählen sie im Feld *Person* eine Person aus, und klicken auf *Hinzufügen*. Wenn Sie das Feld *Benachrichtigung* aktiviert haben, so wird der entsprechenden Person immer per E-Mail mitgeteilt, wenn es entsprechende Requests für sie zu genehmigen gibt. Wurde dieses Feld nicht aktiviert, so erhält die Person keine Benachrichtigung per E-Mail. Dies kann nützlich sein, wenn Sie eine Person in sehr vielen Abteilungen als Verantwortlichen eingetragen haben, diese Person jedoch zum Beispiel nur als Vertretung agieren und demnach nicht im Normalfall benachrichtigt werden soll. Im Aktionsmenü des jeweiligen Eintrages lassen sich Personen wieder als Verantwortliche entfernen.

### Nachträgliches Bearbeiten des Feldes Benachrichtigung

Sollten Sie im Nachhinein das Feld *Benachrichtigung* setzen oder löschen wollen, müssen Sie den Eintrag der entsprechenden Person entfernen und anschließend mit/ohne Benachrichtigung neu hinzufügen.

## 9.1.3 Abteilungsgruppen

*Organisation > Abteilungsgruppen*

Abteilungsgruppen sind Gruppierungen von Abteilungen. Eine Abteilung kann dabei immer nur einer einzigen Gruppe angehören. Eine Person gehört daher immer der Abteilungsgruppe der Abteilung an in welcher sie sich befindet. Der Hauptzweck von Abteilungsgruppen besteht darin Profile für mehrere Abteilungen anlegen zu können.

### Gruppe von Abteilungen vs. Abteilungsuntergruppen

Abteilungsgruppen befinden sich in der Hierarchie überhalb der Abteilungen. Es handelt sich hierbei *nicht* um Untergruppen von einzelnen Abteilungen.

Feld	Beschreibung	Beispielwert
Name	Der Name der Abteilungsgruppe. Diese Bezeichnung wird in tenfold angezeigt.	Alle Abteilungen
Kurzname	Ein Kürzel für die Abteilungsgruppe.	ALL
Beschreibung	Eine informative Beschreibung.	

## 9.1.4 Abteilungshierarchie

Organisation > Abteilungshierarchie

Dies ist eine Übersichtsmaske zur Darstellung der Abteilungshierarchie innerhalb Ihrer Organisation. Sie können sich hier in einer Baumstruktur die Gliederung Ihrer Abteilungen anzeigen lassen, sowie sich die einzelnen Verantwortlichen einer jeden Abteilung ansehen. (Siehe [Abteilungsverantwortliche](#)(see page 368))

## 9.2 Kostenstellen

Organisation > Kostenstellen

Kostenstellen können Personen über das Personenfeld *COST\_CENTER* oder *IT\_COST\_CENTER* zugeordnet werden (siehe Personenfelder). In der Standardkonfiguration sind diese Einstellungen rein informativ und haben keine besondere Bedeutung für tenfold.

### Bearbeiten von Kostenstellen

Momentan ist eine Bearbeitung von Kostenstellen mittels eines Schirmes in tenfold nicht vorgesehen. Sie sind gedacht um aus Fremdsystem (z.B. SAP) importiert zu werden. Wenden Sie sich bitte an Ihren Betreuer wenn Sie Kostenstellen aus einem anderen System importieren möchten.

## 9.3 Organisationseinheiten

Organisationseinheiten bieten Ihnen die Möglichkeit Ihre Organisation in verschiedene Bereiche aufzuteilen. Im Gegensatz zu Abteilungen handelt es sich hierbei jedoch nicht um eine Gliederung nach Personalbereichen, sondern um eine Aufteilung innerhalb Ihrer IT-Landschaft.

### 9.3.1 Organisationseinheiten

Organisation > Organisationseinheiten

Ein Benutzer ist über seine Niederlassung zu einer Organisationseinheit zugehörig. In dieser Organisationseinheit können Einstellungen über seine Domänenzugehörigkeit u.Ä festgelegt werden.

Feld	Beschreibung	Beispielwert
Name	Der Name der Organisationseinheit. Der Name dient lediglich zur Anzeige in tenfold.	Certex

Feld	Beschreibung	Beispielwert
 Code	Ein Kürzel, zur Identifizierung der Organisationseinheit. Dieses Feld kann z.B. in Anpassungen verwendet werden um eine Organisationseinheit in Fremdsystemen zu identifizieren.	CER
 Beschreibung	Eine Beschreibung der Organisationseinheit. Hier können Sie Informationen über die Organisationseinheit hinterlegen.	
 Typ	Die Art der Organisationseinheit. Hiermit lassen sich Organisationseinheiten z.B in Physische oder Logische Einheiten untergliedern.	Physical Site
 Domäne	Hier legen Sie fest zu welcher Active Directory Domäne ein Benutzer gehört.	certex (Dropdown-Auswahl)
 Freigabe für "Eigene Dateien"	Hier kann festgelegt werden wo sich der Ordner befindet in welchem Home-Verzeichnisse für Personen angelegt werden sollen. Ist dieses Feld leer, so wird für einen Benutzer dieser Organisationseinheit kein Home-Verzeichnis angelegt. Ist dieses Feld befüllt wird einem Benutzer ein Home-Verzeichnis angelegt wenn er erstellt wird.	\\\fileserver\home
 Gruppenabgleich	Hier kann hinterlegt werden ob Mitglieder dieser Organisationseinheit an Active Directory-Gruppen-Abgleichen teilnehmen. Zum Beispiel lässt sich ein Abgleich einrichten, der allen Mitgliedern einer bestimmten Gruppe gewisse Services zuordnet.	Ja/Nein
 AD-Container	Hier lässt sich ein Active-Directory Container eintragen in welchem Personen dieser Organisationseinheit abgelegt werden. In der Standardkonfiguration wird nur die Einstellung <i>Container für Benutzer</i> der Domäne herangezogen. In Anpassungen kann dieser Wert jedoch herangezogen werden.	OU=USR,OU=CERTEX,O=AT
 Mail-Server	Hier lässt sich Einstellen welcher Mail-Server für die Person zuständig ist.	mail-system.certex.at
 Mail-Domain	Hier lässt sich eine E-Mail Domäne festlegen. Diese kann zum Beispiel verwendet werden um einen Vorschlag für die E-Mail-Adresse neuer Personen zu generieren.	certex.at

Feld	Beschreibung	Beispielwert
 Mailbox-Store	Hier kann für die Anlage einer Mailbox für eine Person die Datenbank hinterlegt werden in welche Personen dieser Organisationseinheit gespeichert werden sollen.	mailstore1.edb
 Externe ID	Hier kann eine alternative ID angegeben werden, welche zur Identifizierung des Mailbox-Stores in Fremdsystemen dient.	
 Parameter	Hier können Benutzerdefinierte Parameter für eine Organisationseinheit hinterlegt werden, welche in Anpassungen herangezogen werden können.	

#### Organisationseinheitstypen

Für die Wartung der Organisationseinheitstypen existiert keine eigenständige Wartungsmaske. Die einzelnen Typen werden in den Nachschlagewerten festgehalten.

### 9.3.2 Organisationseinheitsgruppen

Organisation > Organisationseinheitsgruppen

Unter einer Organisationseinheitsgruppe können Sie eine oder mehrere Organisationseinheiten zusammenfassen. Der Hauptzweck von Organisationseinheitsgruppen ist es die örtliche Verfügbarkeit von Services einzuschränken. In jedem Service lassen sich ein oder mehrere Organisationseinheitsgruppen definieren, in welchen der Service verfügbar ist. Damit können nur Personen, welche in ihrer Hauptniederlassung zu einer Organisationseinheit einer solchen Gruppe gehören, diesen Service bestellen.

Feld	Beschreibung	Beispielwert
 Name	Der Name der Gruppe. Dieser wird in tenfold angezeigt.	Alle, Europa, Deutschland
 Kurzname	Ein Kürzel für den Namen.	ALL, EU, DE
 Organisationseinheiten	Eine Liste aller Organisationseinheiten welche in der Gruppe enthalten sind. Eine Organisationseinheit kann zu mehreren Gruppen gehören.	

#### Services

Services sind nur in der Enterprise Edition von tenfold enthalten.

## 9.4 Stellvertretungen

### 9.4.1 Allgemeines

Die Funktion der Stellvertretung dient dazu, die eigenen Berechtigungen innerhalb eines definierten Zeitfensters einer oder mehreren anderen Personen zu übertragen. In diesem Zeitfenster können die hinterlegten Personen die gleichen Aktionen ausführen, wie die vertretene Person. Das inkludiert auch alle Freigaben für Genehmigungsworkflows und Rezertifizierungen. Die Funktion sollte genutzt werden, um beispielsweise einen Vertreter zu bestimmen, wenn man selbst längerfristig abwesend ist (Urlaub oder Krankenstand).

### 9.4.2 Stellvertreter einstellen

#### Benötigte Berechtigung

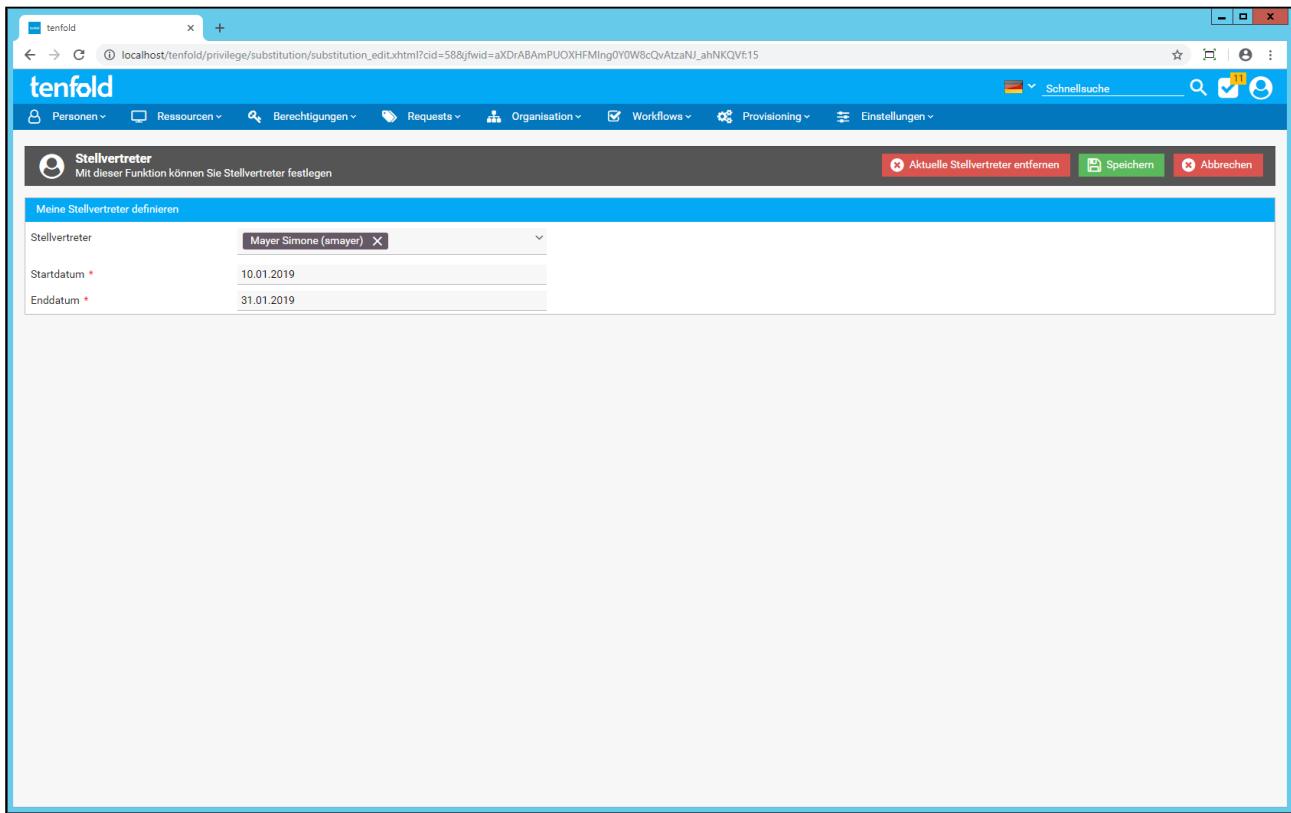
Um einen Stellvertreter für sich selbst einzustellen, benötigt man die Systemberechtigung "Assign Substitute Self" (7050).

The screenshot shows the tenfold software interface. At the top, there is a navigation bar with links for Personen, Ressourcen, Berechtigungen, Requests, Organisation, Workflows, Provisioning, and Einstellungen. Below the navigation bar is a search bar labeled 'Schnellsuche' with a magnifying glass icon. The main area is titled 'Willkommen bei tenfold!' and contains several tiles:

- Ressourcen für mich anfordern**: Shows a computer monitor icon and the text 'Ressourcen für mich anfordern'.
- Meine Personendaten bearbeiten**: Shows a person icon and the text 'Meine Personendaten bearbeiten'.
- Meine Requests**: Shows a tag icon and the text 'Meine angeforderten und genehmigten Requests anzeigen'.
- Meine Stellvertreter**: Shows a purple person icon and the text 'Meine Stellvertreter bearbeiten'. This tile is highlighted with a yellow border.
- Person anlegen**: Shows a person plus icon and the text 'Neue Person anlegen'.
- Daten anderer bearbeiten**: Shows a group of people icon and the text 'Daten anderer bearbeiten'.
- Dateneigentümerbereich**: Shows a green group of people icon and the text 'Bearbeitung der Ressourcen, in denen ich als Dateneigentümer hinterlegt bin'.
- Software**: Shows a yellow square with the number '11' and the text 'Software'.

At the bottom left, there is a section titled 'Gruppierte Kontexte' with two items: 'Gesperrte Personen' (1) and 'Ablaufende Personen' (0).

Um für sich selbst einen Stellvertreter einzustellen, wählt man die Kachel "Meine Stellvertreter" auf der Startmaske.



Anschließend kann man einen oder mehrere Stellvertreter festlegen:

- **Stellvertreter:** Es können eine oder mehrere Personen hinterlegt werden. Diese sind gleichberechtigt und erhalten alle die gleichen Berechtigungen, die Ihnen zugeordnet sind.
- **Startdatum:** Legt fest, wann die Stellvertretung beginnen soll. Die Stellvertreter verfügen erst ab diesem Datum über die zusätzlichen Berechtigungen.
- **Enddatum:** Legt fest, wann die Stellvertretung endet. Die Stellvertreter verfügen ab diesem Datum automatisch nicht mehr über die zusätzlichen Berechtigungen.

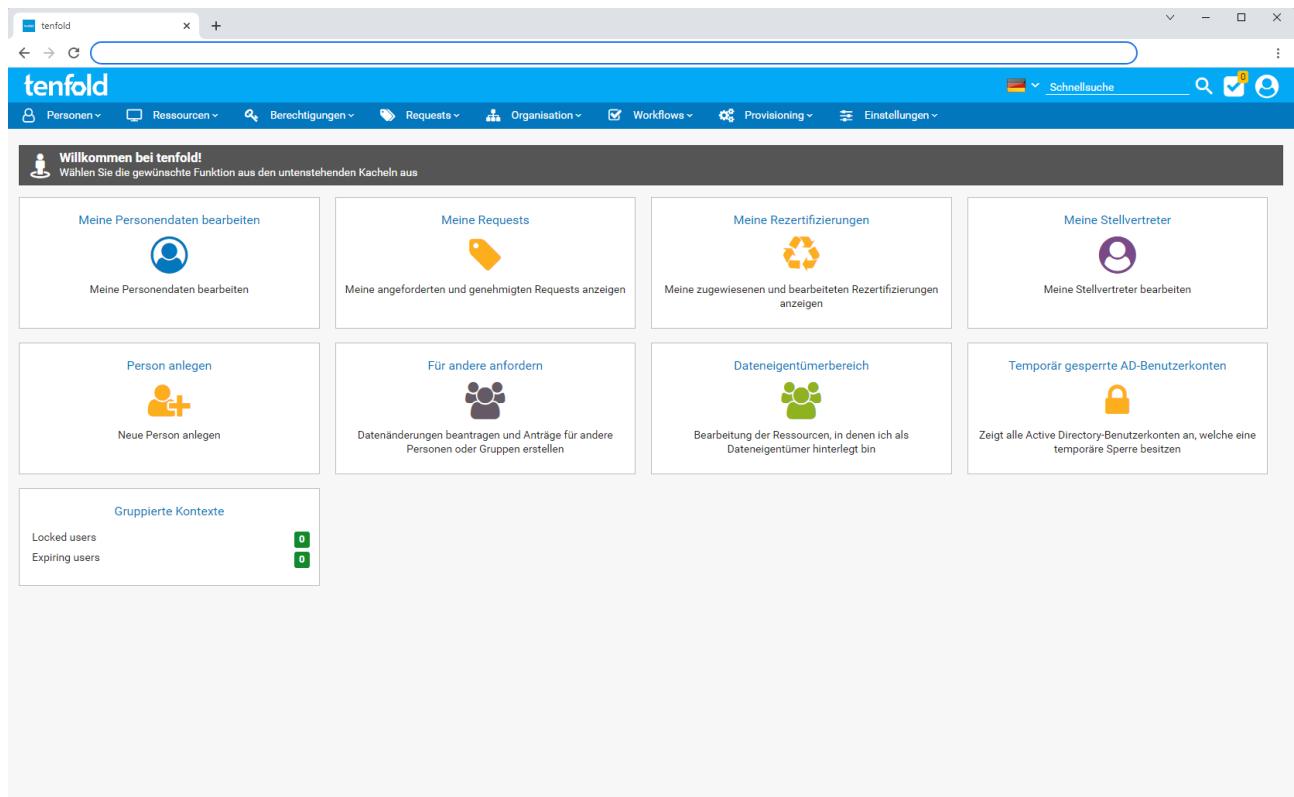
Mit dem Kreuzsymbol neben dem Namen kann ein einzelner Stellvertreter entfernt werden. Über den Button "Aktuelle Stellvertreter entfernen" werden automatisch alle Stellvertreter sowie die Datumsfelder gelöscht.

#### 9.4.3 Stellvertreter für andere

##### **Benötigte Berechtigung**

Um einen Stellvertreter für andere Personen einzustellen zu können, benötigt man die organisationsabhängige Berechtigung "Assign Substitute Others" (7051).

Um für eine andere Person einen Stellvertreter festzulegen, wählt man auf der Startmaske "Daten anderer bearbeiten". Anschließend wählt man die Person aus, welche vertreten werden soll.



Aus den Optionen auf der Maske wählt man anschließend "Stellvertreter" aus. Die Festlegung und Löschung der Stellvertreter erfolgt anschließend analog wie bei der Festlegung der eigenen Stellvertreter.

## 9.4.4 Organisationsabhängige Berechtigungen

Abteilung	Niederlassung	Position	Person	Vorgesetzter	Benachrichtigung
Eigene Abteilung	Alle Niederlassungen	Alle Positionen	Alle Personen	-	-

Wenn einer Person eine Rolle mit organisationsabhängigen Berechtigungen zugeordnet ist und diese Person vertreten wird, so ist das Verhalten wie folgt:

- Ist die Rolle einer bestimmten Organisationseinheit (Abteilung, etc.) zugeordnet, so erhält der Stellvertreter die Berechtigungen für genau diese Organisationseinheit.
- Ist die Rolle allen Organisationseinheiten zugeordnet, so erhält der Stellvertreter die Berechtigungen ebenfalls in allen Organisationseinheiten.
- Ist die Rolle der eigenen Organisationseinheit ("Eigene Abteilung", etc.) zugeordnet, so erhält der Stellvertreter die Berechtigung für die "eigene" Organisationseinheit der vertretenen Person und nicht für seine eigene Organisationseinheit.

## 9.4.5 Anzeige

### Benötigte Berechtigung

Wenn man über die Berechtigung "Assign Substitute Others" (7051) verfügt, dann steht die Anzeigefunktion über das Menü *Berechtigungen > Stellvertreter* zur Verfügung.

Hier können systemweit (im Rahmen der organisationsabhängigen Berechtigung 7051) alle aktuellen Stellvertretungen eingesehen werden. Über die Filteroptionen kann die Liste eingeschränkt werden. Über das Kontextmenü der jeweiligen Zeile können bestehende Stellvertretungen bearbeitet und gelöscht werden.

## 9.4.6 Vererbung

Standardmäßig werden die Stellvertreterberechtigungen an weitere Stellvertreter in einer Kette vererbt. Nehmen Sie hierfür folgendes Beispiel:

- Person A > Person B > Person C

Hier ist "Person C" der Stellvertreter von "Person B" und erbt damit nicht nur sämtliche Berechtigungen von "Person B", sondern auch die Berechtigungen von "Person A".

### Zyklische Vererbung

Eine zyklische Vererbung von Berechtigungen, wie in folgendem Beispiel, ist nicht möglich.

- Person A > Person B > **Person A**

Der Versuch, eine solche Vererbungskette zu speichern, wird mit einer entsprechenden Fehlermeldung unterbunden. Die Tiefe der Vererbungsebene ist hierbei nicht von Bedeutung. Ungeachtet dessen, auf welcher Ebene ein Zirkelbezug auftritt, ist das Speichern eines solchen nicht möglich.

Für die meisten Anwendungsfälle ist dieses Verhalten von Vorteil, um zu verhindern, dass Requests durch Urlaube oder andere Abwesenheiten nicht bearbeitet werden können. Nehmen Sie folgendes Szenario als Beispiel:

- "Person A" ist von 01.01 bis 14.01 auf Urlaub und definiert für diesen Zeitraum "Person B" als Stellvertreter.
- "Person B" ist von 07.01 bis 21.01 auf Urlaub und definiert "Person C" für diesen Zeitraum als Stellvertreter.
- "Person C" ist durchgehend anwesend.

In diesem Fall darf "Person C" im Zeitraum von 07.01 bis 14.01 alle Requests von "Person A" und "Person B" genehmigen. Von 14.01 bis 21.01 dürfen nur noch die Requests von "Person B" durch "Person C" genehmigt werden. Damit ist sichergestellt, dass Requests auch in Abwesenheitszeiten bearbeitet werden können.

In manchen Fällen kann dieses Verhalten jedoch unerwünscht sein. Um es zu unterbinden, können Sie im Menü unter *Einstellungen > Systemparameter* die Einstellung *Stellvertretungen > Berechtigungsvererbung - Aktiv* ändern. Wenn Sie diese Einstellung deaktivieren werden Berechtigungen nur noch an direkte Stellvertreter weitergegeben. In diesem Fall könnte "Person C" aus obigem Beispiel nur die Requests von "Person B" genehmigen. Ist diese Einstellung deaktiviert, so werden, als zusätzliche Konsequenz, Zirkelbezüge zugelassen. Eine Stellvertretereinstellung, wie folgt, wird damit möglich:

- Person A > Person B > **Person A**

Ist die Einstellung aktiviert würde ein solcher Zirkelbezug, wie oben beschrieben, verhindert werden.

#### **Zyklische Vererbung bei Aktivierung der Einstellung**

Sollte der Systemparameter *Stellvertretungen > Berechtigungsvererbung - Aktiv* deaktiviert und zu einem späteren Zeitpunkt wieder aktiviert werden, so werden, an dieser Stelle, zyklische Vererbungen nicht aufgelöst. Diese müssen manuell bereinigt werden. Andernfalls kann es zu Fehlern bei der Anmeldung kommen.

## 9.5 Unternehmen & Niederlassungen

Mit diesen Strukturen lassen sich die einzelnen Orte verwalten, welchen Ihre Benutzer ihrer Arbeit nachgehen. Eine Person kann hierbei einer oder mehreren Niederlassungen zugeordnet sein, wobei immer genau eine Niederlassung als seine Hauptniederlassung herangezogen wird. Über diese Hauptniederlassung wird in tenfold die Zugehörigkeit zu den einzelnen Unternehmen sowie zu einer Organisationseinheit hergestellt.

### 9.5.1 Unternehmen

Organisation > Unternehmen

Bei Unternehmen handelt es sich um Stammdatensätze welche die einzelnen Gesellschaften in Ihrer Organisation abbilden. In der Standardkonfiguration dient dies dazu, die Daten in Ihrem Active Directory einheitlich zu halten. Eine Person erhält seine Zugehörigkeit zu einem Unternehmen über seine Hauptniederlassung. Damit vermeiden Sie Doppel- und Fehleingaben im Feld "Firma" und das Feld wird auch automatisch aktualisiert, sollte der Benutzer in eine andere Niederlassung wechseln.

Feld	Beschreibung	Beispielwert
Name	Der Name des Unternehmens. Dieses Feld wird in der Standardkonfiguration in das Active Directory übertragen. Hierbei wird das Unternehmen der Hauptniederlassung einer Person in das Feld "Firma" geschrieben.	certex Information Technology GmbH

Feld	Beschreibung	Beispielwert
Code	Ein Kürzel für das Unternehmen. Hier kann man zum Beispiel Identifizierer für das Unternehmen eintragen welche in Ihrer IT-Landschaft verwendet werden.	CER
Abteilungsverweis	Hier kann eine Abteilung ausgewählt werden. Dieses Feld hat in der Standardkonfiguration keine Auswirkung, kann aber in Anpassungen berücksichtigt werden.	IT (Dropdown-Auswahl)
Übergeordnetes Unternehmen	Sollten die einzelnen Unternehmen in Ihrer Organisation in einer Mutter-Tochter-Beziehung zueinander stehen, so lässt sich hier die Muttergesellschaft eintragen.	certex Information Technology GmbH (Dropdown-Auswahl)

#### Niederlassung & Unternehmen

In den Personenfeldern einer Personenart kann das Feld *COMPANY* hinzugefügt werden, welches die Auswahl eines Unternehmens bei einer Person erlaubt. Es wird dennoch in der Standardkonfiguration immer das Unternehmen der Hauptniederlassung in das Active Directory übertragen.

## 9.5.2 Niederlassungen

Organisation > Niederlassungen

Bei Niederlassungen handelt es sich um die einzelnen Standorte an welchen die Personen Ihrer Organisation tätig sind. In der Standardkonfiguration werden diese Datensätze dazu verwendet die Daten in Ihrem Active Directory konsistent zu halten. Damit lassen sich Doppel- und Fehleingaben vermeiden. Personen ein und derselben Niederlassung erhalten hierbei immer dieselbe Adresse in derselben Schreibweise im Active Directory.

Eine Niederlassung kann einer Person über das Personenfeld *OFFICE* zugeordnet werden (siehe Personenfelder).

Feld	Beschreibung	Beispielwert
Name	Der Name der Niederlassung. Dieser wird in das Feld <i>Büro</i> , des Active Directory geschrieben.	Wien Seidengasse
Typ	Eine Auswahl des Typs der Niederlassung. In den Einstellungen der Personenarten lässt sich für eine Personenart festlegen, welcher Typus von Niederlassung zulässig ist.	Interne/Externe Niederlassung
Code	Ein Kürzel für die Niederlassung. Hier lässt sich z.B. ein Code eingeben, welcher in Ihrer IT-Landschaft für die Niederlassung verwendet wird.	VIE

Feld	Beschreibung	Beispielwert
Organisationseinheit	Die Organisationseinheit zu welcher die Niederlassung gehört.	Standard
Unternehmen	Das Unternehmen zu welcher die Niederlassung gehört.	certex Information Technology GmbH
Beschreibung	Eine Beschreibung der Niederlassung zu informativen Zwecken.	Dies ist das HQ des Unternehmens.
Telefon	Die Hauptdurchwahl der Niederlassung. Dieses Feld wird nicht zu einer Person in das Active Directory übertragen. In den Personenstammdaten befindet sich hierfür ein eigenes Feld.	+43 (0)1 / 66 50 633
Fax	Die Hauptdurchwahl für das Fax der Niederlassung. Dieses Feld wird nicht zu einer Person in das Active Directory übertragen. In den Personenstammdaten befindet sich hierfür ein eigenes Feld.	+43 (0)1 / 66 50 633
Straße	Die Straße, Hausnummer, etc der Niederlassung. Dieses Feld wird zu einer Person in das Active Directory übertragen.	Seidengasse 9-11, Top 3.4
Stadt	Die Stadt in welcher sich die Niederlassung befindet. Dieses Feld wird zu einer Person in das Active Directory übertragen.	Wien
PLZ	Die Postleitzahl in welcher die Niederlassung zu finden ist. Dieses Feld wird zu einer Person in das Active Directory übertragen.	1070
Bundesland/Kanton	Das Bundesland/der Kanton in welcher/welchem sich die Niederlassung befindet.	Wien
Land	Das Land in welcher sich die Niederlassung befindet. Dieses Feld wird zu einer Person in das Active Directory übertragen.	Austria
Gebäude	Hier lassen sich einzelne Gebäude zu einer Niederlassung zuordnen, falls es sich bei der Niederlassung zum Beispiel um einen Komplex aus mehreren Gebäuden an derselben Adresse handelt.	Produktionshalle, Verwaltungsgebäude

Feld	Beschreibung	Beispielwert
Parameter	Hier lassen sich mehrere vordefinierte Parameter zu der Niederlassung hinzufügen, welche in den Anpassungen Ihrer Installation verwendet werden können.	

### Niederlassungstypen

In der aktuellen Version von tenfold existiert kein Wartungsschirm für die Niederlassungstypen. Diese müssen manuell in der Datenbank gewartet werden. Kontaktieren Sie hierfür bitte Ihren Betreuer.

## 9.5.3 Gebäude

Organisation > Gebäude

Sollten Sie in einer oder mehrere Ihrer Niederlassungen mehrere Gebäude unter einer Anschrift haben, so können Sie hier die Gebäude definieren, welche sie einzelnen Niederlassungen zuordnen können. In der Standardkonfiguration haben Gebäude keine Funktionen, können jedoch in Anpassungen herangezogen werden.

Feld	Beschreibung	Beispielwert
Name	Der Name des Gebäudes	Hauptgebäude, Produktionshalle
EID	Ein Identifizierer, welcher in Ihrer IT-Landschaft für ein Gebäude verwendet wird.	CER-BLD-1
Code	Ein Kürzel welches für dieses Gebäude verwendet wird.	HQ

# 10 Workflows

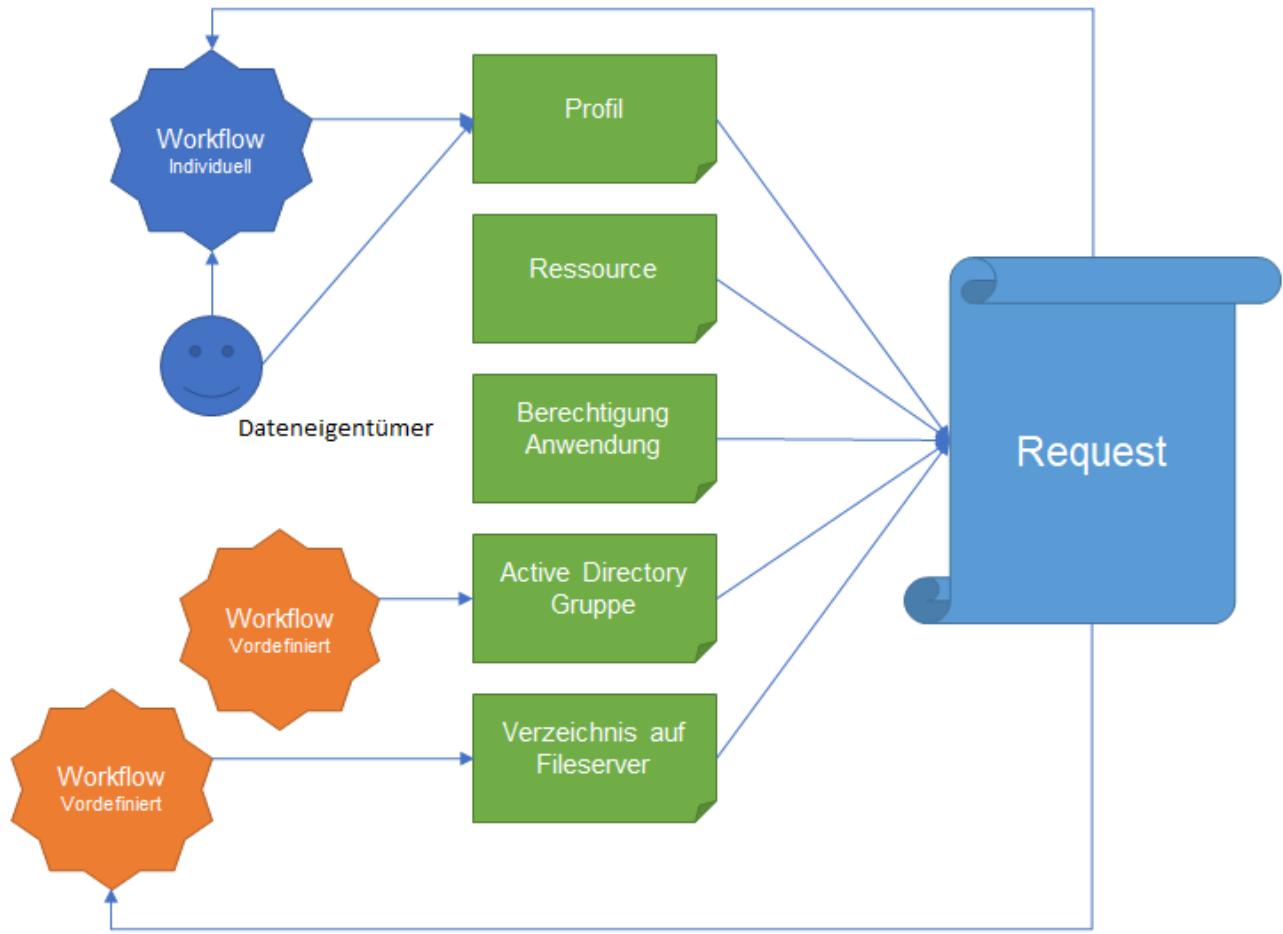
## 10.1 Genehmigungsworflows

### 10.1.1 Zweck

Unter dem Begriff "Genehmigungsworflows" werden in tenfold Genehmigungsverfahren verstanden. Die Workflows steuern, ob eine bestimmte angefragte Änderung (über einen Request) durchgeführt werden soll, oder ob der Request abgelehnt wird und die angefragte Änderung nicht durchgeführt wird. Änderungen, die über Workflows gesteuert werden können, sind im Punkt "Definition" unter [Requests\(see page 352\)](#) zu finden.

### 10.1.2 Auswahl des Workflows

Welcher Workflow für einen bestimmten Request zum Tragen kommt kann durch Hinterlegung des gewünschten Workflows beim jeweiligen Objekt erfolgen. Für Profile, Ressourcen und Anwendungsberechtigungen kann der Workflow individuell definiert werden. Für Active Directory-Gruppen und für Fileserver ist der Workflow jeweils vordefiniert. Das bedeutet, dass festgelegt ist, welcher Workflow für jegliche Active Directory-Gruppenänderungen und Änderungen an Fileservern zum Tragen kommt. Der Inhalt dieses vordefinierten Workflows kann jedoch angepasst werden.



### 10.1.3 Rollen innerhalb eines Workflow

Innerhalb eines Workflows können folgende Personen eine besondere Rolle einnehmen:

- Dateneigentümer des Objekts (Profil, Ressource, Berechtigung, Active Directory-Gruppe, Verzeichnis), auf die sich der Request bezieht
- Direkter Vorgesetzter der Person, auf die sich der Request bezieht
- Dateneigentümer der Abteilung (=Abteilungsverantwortlicher), welcher die Person angehört, auf die sich der Request bezieht
- Inhaber einer im Workflow festgelegten tenfold-Berechtigung (dies bezieht sich anschließend auf alle Personen in tenfold, denen diese tenfold-Berechtigung zugeordnet ist)

Üblicherweise hängt die Genehmigung eines Requests zumindest vom Verantwortlichen der gewünschten Ressource ab (Dateneigentümer des Objekts). In vielen Fällen muss davor oder danach zusätzlich auch die Zustimmung des direkten Vorgesetzten oder des Abteilungsverantwortlichen (=Dateneigentümer der Abteilung) eingeholt werden. In seltenen Fällen muss zusätzliche eine zentrale Stelle (zum Beispiel der Datenschutzbeauftragte) in den Workflow eingebunden werden. In letzterem Fall würde man eine entsprechende tenfold-Berechtigung anlegen (siehe dazu auch [Berechtigungen](#)(see page 457)), diese dann im Workflow verwenden und sie der oder den entsprechenden Personen zuordnen.

## 10.1.4 Requeststatus

Der Status des Request (siehe dazu auch [Requests\(see page 352\)](#)) hängt davon ab, in welchem Zustand sich der Genehmigungsworkflow befindet, der - basierend auf dem jeweiligen Objekt, auf das sich der Request bezieht - ausgewählt wurde. Folgende Situationen sind möglich:

- Ungenehmigt: Der Genehmigungsworkflow ist noch nicht abgeschlossen (es stehen noch Genehmigungen aus).
- Fertig: Der Genehmigungsworkflow wurde erfolgreich durchlaufen und der Request wurde erfolgreich ausgeführt.
- In Bearbeitung: Der Genehmigungsworkflow wurde erfolgreich durchlaufen - im Rahmen der Ausführung des Request sind allerdings noch manuelle Tätigkeiten auszuführen.
- Fehlgeschlagen: Der Genehmigungsworkflow wurde erfolgreich durchlaufen - allerdings ist bei der Durchführung des Request ein Fehler aufgetreten.
- Abgelehnt: Der Genehmigungsworkflow wurde nicht erfolgreich beendet. Eine der beteiligten Personen hat den Request abgelehnt. Eine Wiederaufnahme ist nicht möglich.
- Abgebrochen: Der Request wurde entweder während oder nach dem Durchlaufen des Workflow abgebrochen. Eine Wiederaufnahme ist nicht möglich.

## 10.1.5 Verwendung ermitteln

Objekt	Einschränkungen
Spezialhardware	Request-Typ: Neu - Request-Modus: Ressource - Request-Quelle: Alle

Beim Bearbeiten oder Anzeigen eines Genehmigungsworkflows können Sie im Karteireiter "Verwendung" prüfen, bei welchen Objekten der Workflow hinterlegt wurde. Auf diesem Karteireiter finden Sie eine Tabelle, mit den Informationen zur Verwendung des ausgewählten Workflows. Folgende Informationen finden Sie in der Tabelle:

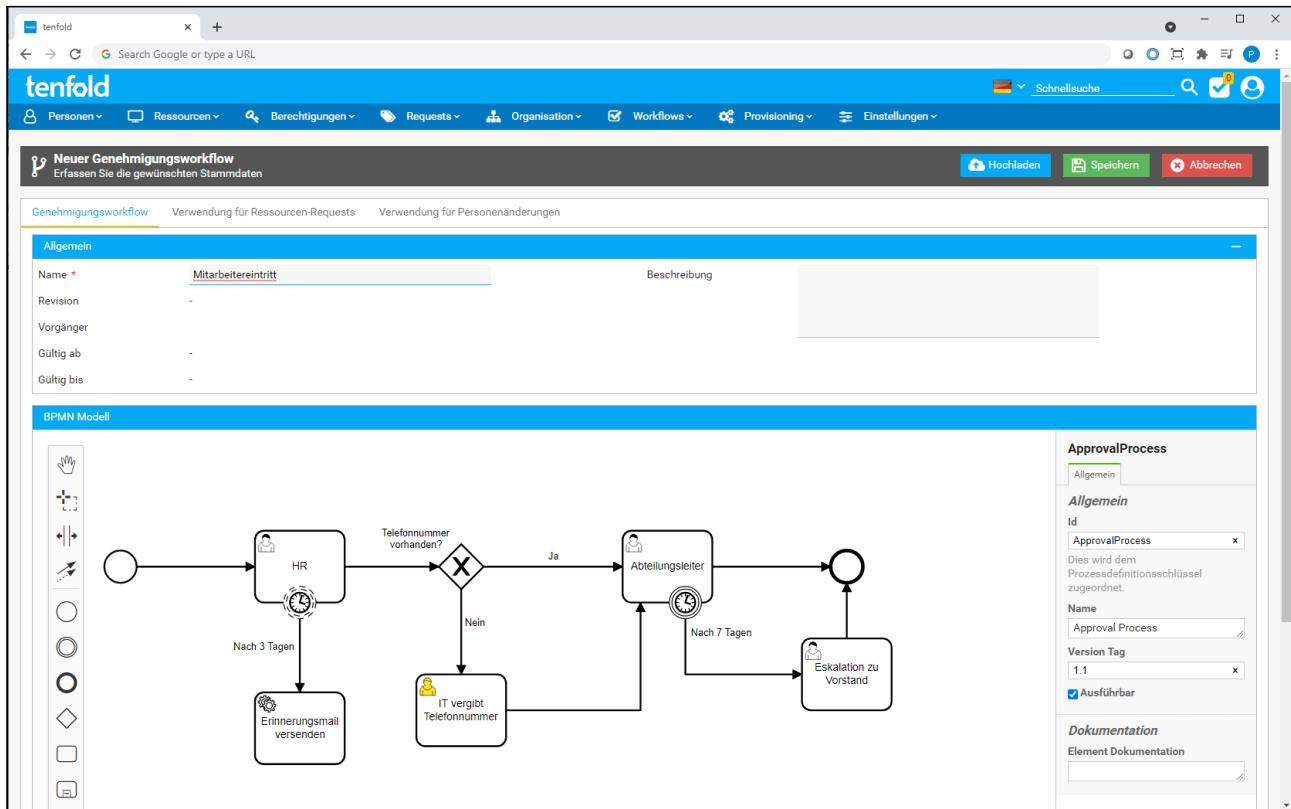
Spalte	Beschreibung
Objekt	In dieser Spalte sehen Sie das Objekt, bei welchem der Workflow hinterlegt wurde. Es wird Ihnen der Name des Objektes angezeigt und ein Icon, welches die Art des Objektes angibt. <b>Hinweis:</b> Im Tooltip des Icons wird Ihnen der Name der Objektart angezeigt.
Einschränkung	Hier finden Sie die Einschränkungen zur Anwendung des Workflows, welche bei dem Objekt hinterlegt wurden. Nähere Informationen zu den möglichen Einschränkungen finden Sie in den Kapiteln zu den jeweiligen Objekttypen.

## 10.2 BPMN-Genehmigungsworkflows

BPMN-Genehmigungsworkflows sind die primäre Methode, um Genehmigungsworkflows in tenfold zu definieren.

### Provisioning

Genehmigungsworkflows dienen nicht zur Steuerung des Provisionings. Das Provisioning findet **nach** dem Genehmigungsprozess statt und kann daher durch Genehmigungsworkflows nicht mehr gesteuert werden.



BPMN steht für "Business Process Model and Notation" und wurde von IBM entwickelt. Es ist eine allgemeine Notationsmethode zur grafischen Abbildung betrieblicher Prozesse. Einen allgemeinen Überblick

über BPMN können Sie sich unter folgendem URL verschaffen: [https://de.wikipedia.org/wiki/Business\\_Process\\_Model\\_and\\_Notation](https://de.wikipedia.org/wiki/Business_Process_Model_and_Notation).

Als Engine zur Automatisierung und Ausführung der BPMN-Prozesse verwendet tenfold Camunda. Für technische Details, wenden Sie sich an <https://camunda.com/>.

Während BPMN ein umfassender Standard zur Darstellung einer Vielzahl verschiedener Prozesse ist, verwendet tenfold nur eine gewisse Untermenge der vorhandenen Symbole. Hierbei handelt es sich um folgende:

Symbol	Name	Beschreibung
○	Startereignis	Dies ist der Startpunkt des Genehmigungsworflows. Jeder Genehmigungsworflow benötigt genau einen Startpunkt.
○	Endereignis	Dies definiert den Endpunkt des Genehmigungsworflows. Ein Genehmigungsworflow kann mehrere Endpunkte oder gar keinen enthalten. Ein Genehmigungsworflow gilt auch als beendet, wenn der Workflow in einem Task landet, von welchem aus keine weiteren Übergänge definiert sind. Dennoch ist es zur besseren Übersicht zu empfehlen, den Workflow mit einem Endereignis abzuschließen. Sind alle begonnenen Pfade an das Ende gelangt, so gilt der Genehmigungsworflow als akzeptiert.
	Benutzeroaufgabe	Benutzeroaufgaben stehen für Teile des Prozesses, welche von Personen durchgeführt werden müssen. In tenfold-Genehmigungsworflows haben User-Tasks eine von folgenden möglichen Bedeutungen: <ul style="list-style-type: none"> <li>• <b>Genehmigungsschritt:</b> Es wird eine Genehmigung in tenfold eröffnet, welche von berechtigten Personen genehmigt oder abgelehnt werden muss. Im Falle von Personendaten-Requests kann die berechtigte Person die angeforderten Daten ändern. Für andere Arten von Requests können an dieser Stelle keine Änderungen vorgenommen werden.</li> <li>• <b>Interaktive Aktivität:</b> Es wird eine Aktivität eröffnet, in welcher eine berechtigte Person Daten eingeben muss. Die Aktivität definiert, welche Daten eingegeben werden müssen (zum Beispiel Personenfelder). Berechtigte Personen sind nicht in der Lage, an dieser Stelle die Anfrage abzulehnen. Optional kann bei der Aktivität jedoch erlaubt werden, dass an dieser Stelle der Request abgebrochen werden kann. <b>Hinweis:</b> Abgebrochene Requests lösen andere Ereignisse aus und werden anders dargestellt, als abgelehnte Requests.</li> </ul>

Symbol	Name	Beschreibung
	Service Aufgabe	<p>Service-Tasks werden verwendet, um automatisierte Tätigkeiten durchzuführen. Bei diesen kann es sich, zum Beispiel, um den Versand einer E-Mail handeln. An dieser Stelle bietet tenfold folgende Möglichkeiten, Automatismen in einem Workflow zu hinterlegen:</p> <ul style="list-style-type: none"> <li>• <b>EXECs:</b> Es wird ein EXEC hinterlegt, welcher die gewünschten Tätigkeiten durchführt. Hierfür ist es notwendig, zuerst einen EXEC vom Typ "Genehmigungsworkflow" anzulegen.</li> <li>• <b>Vordefinierte Aktivität:</b> Hierbei handelt es sich um konfigurierbare Tasks (siehe <a href="#">Aktivitäten(see page 383)</a>), welche hinterlegt werden, um vorgefertigte Aktionen durchführen zu können. Die Auswahl der vordefinierten Aktivitäten hängt von den installierten Plugins ab.</li> </ul>
	Exclusives Gateway	<p>Bei Exclusive Gateways handelt es sich um Verzweigungen mit mehreren möglichen Ausgängen. Es muss jeder ausgehende Pfad mit einer Bedingung verknüpft werden. Hierbei kann es sich um Skript-Ausdrücke oder Provisionierungsbedingungen handeln. Die Bedingungen müssen hierbei so gewählt werden, dass immer exakt eine ausgehende Bedingung zutrifft. Andernfalls führt dies, bei der Durchführung des Workflows, zu einem Fehler.</p>
	Paralleles Gateway	<p>Mit diesem Symbol lassen sich parallele Prozesse abbilden. Sie können damit realisieren, dass zwei Genehmigungsschritte zeitgleich gestartet werden, anstatt hintereinander. <b>Hinweis:</b> Auch wenn mehrere Genehmigungsschritte gleichzeitig offen sind, wird die Anfrage abgelehnt, sobald einer dieser Genehmigungsschritte abgelehnt wird.</p>
	Angeheftete s Zeit-Zwischenereignis	<p>Dieses Symbol können Sie an eine Benutzeraufgabe anhängen, um nach Ablauf einer gewissen Zeit, sollte die Aufgabe noch nicht erledigt sein, einen neuen Pfad aus diesem Ereignis heraus einzuschlagen. Dieses Ereignis existiert in zwei Varianten: Die normale Variante (durchgehende Linien) bricht die Aufgabe ab, während die nicht-unterbrechende Variante (strichlierte Linien) die Aufgabe bestehen lässt. <b>Hinweis:</b> Da Genehmigungsworkflows in tenfold immer durch eine Anfrage gestartet werden ist es nicht möglich, ein (nicht angeheftetes) Zeitereignis als Startpunkt für den Workflow zu verwenden.</p>
	Angeheftete s Nachrichten-Zwischenereignis	<p>Dieses Symbol können Sie an eine Benutzeraufgabe anhängen, um nach Erhalten einer gewissen Nachricht, sollte die Aufgabe noch nicht erledigt sein, einen neuen Pfad aus diesem Ereignis heraus einzuschlagen. Dieses Ereignis existiert in zwei Varianten: Die normale Variante (durchgehende Linien) bricht die Aufgabe ab, während die nicht-unterbrechende Variante (strichlierte Linien) die Aufgabe bestehen lässt. <b>Hinweis:</b> Da Genehmigungsworkflows in tenfold immer durch eine Anfrage gestartet werden ist es nicht möglich, ein (nicht angeheftetes) Nachrichteneignis als Startpunkt für den Workflow zu verwenden.</p>

Symbol	Name	Beschreibung
 Message	Empfangen-Aufgabe	Mit dieser Aufgabe können Sie im Workflow auf den Erhalt einer bestimmten Nachricht warten. Diese Nachricht kann zum Beispiel von einer Unteranfrage gesendet werden. Damit lässt sich erreichen, dass eine Unteranfrage erst bis zu einem gewissen Punkt genehmigt werden muss, damit die Elternanfrage weiter genehmigt werden kann.

#### Ablehnung einer Anfrage

Sollte in einem Genehmigungsschritt die Anfrage abgelehnt werden, so endet an dieser Stelle der Genehmigungsworkflow. Es werden keine weiteren Teile des Genehmigungsworkflows durchgeführt.

#### Wann werden Workflows durchgeführt?

Die Abfolge bei Änderungen in tenfold ist immer: Anfrage > Genehmigung > Durchführung. Dies bedeutet, dass immer zuerst eine Person eine Änderung anfragen muss, damit der eingestellte Genehmigungsworkflow abläuft. Bei erfolgreichem Abschluss des Workflows (oder bei Fehlen dessen) werden die Änderungen durchgeführt. Es lassen sich keine Teiländerungen mitten im Genehmigungsworkflow durchführen.

### 10.2.1 Anlegen eines BPMN-Genehmigungsworkflows

Sie können einen neuen BPMN-Genehmigungsworkflow anlegen, indem Sie im Menü auf die Maske *Workflows > Genehmigungsworkflows* navigieren.

ID	Name	Revision	Vorgänger	Gültig ab	Gültig bis
Q <sub>1</sub>	Ads request approval	1		25.01.2021 15:54:41	-
Q <sub>3</sub>	Ex request approval	1		25.01.2021 15:55:03	-
Q <sub>2</sub>	Fs request approval	1		25.01.2021 15:54:41	-
Q <sub>4</sub>	O365 group request approval	1		26.01.2021 17:12:49	-
Q <sub>5</sub>	O365 license request approval	1		26.01.2021 17:12:49	-

Betätigen Sie dort die Schaltfläche "Neu" und wählen "BPMN-Genehmigungsworkflow" im Drop-Down Menü.

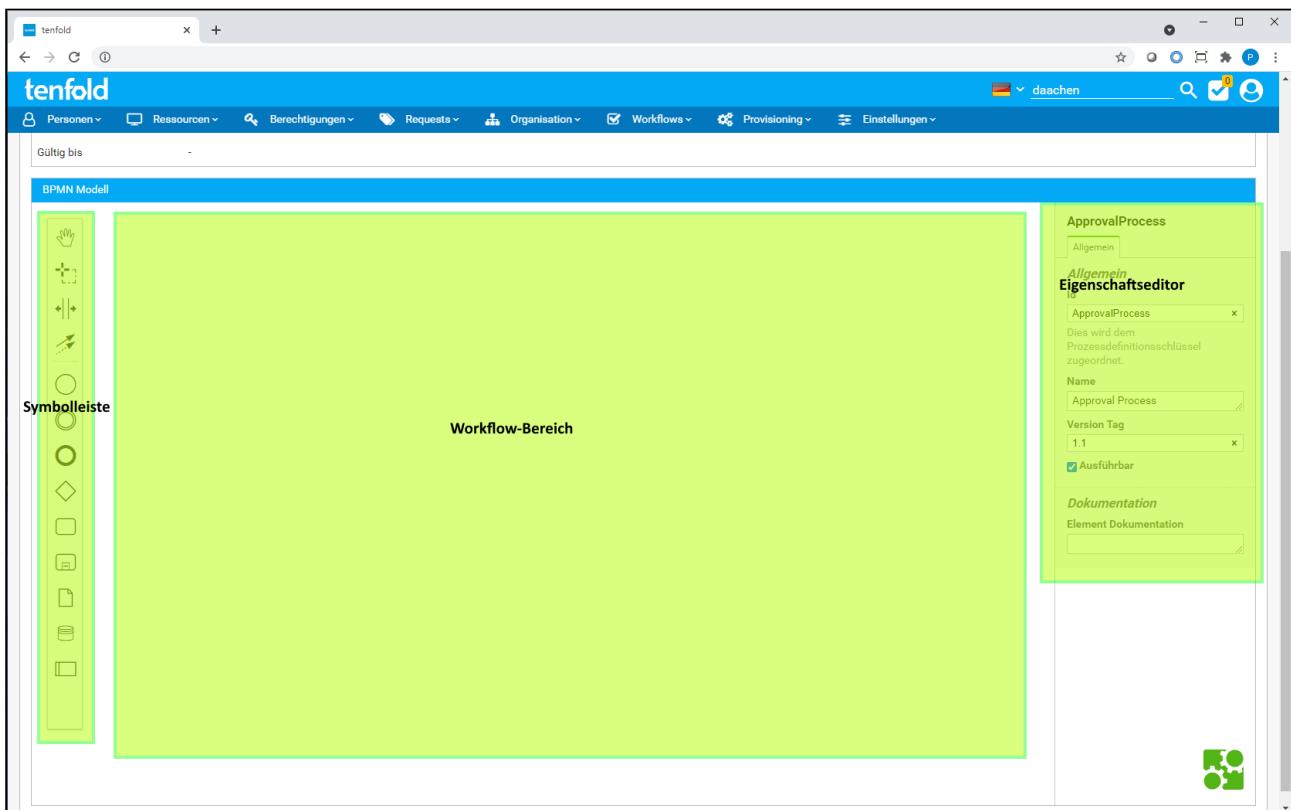
### Berechtigungsbasierte Genehmigungsworkflows

Berechtigungsbasierte Genehmigungsworkflows sind ein Legacy-Feature, welches nur dazu dient, bestehende Installationen zu unterstützen. Nehmen Sie daher bei neuen Genehmigungsworkflows Abstand davon, berechtigungsbasierte Workflows zu verwenden. Sämtliche Prozesse in berechtigungsbasierten Workflows lassen sich besser in BPMN-Workflows abbilden.

Sie gelangen daraufhin auf die Maske zur Bearbeitung von BPMN-Genehmigungsworkflows. Im oberen Bereich "Allgemein", auf dem Tab "Genehmigungsworkflow", können Sie zunächst folgende Einstellungen treffen:

Einstellung	Beschreibung
Name	Der Name des Workflows. Dieser wird auf der tenfold-Oberfläche angezeigt.
Beschreibung	Eine Beschreibung des Workflows zur besseren Übersicht. Beschreiben Sie hier, wofür der Workflow gedacht ist und wie der Ablauf ist.

Im unteren Bereich *BPMN Modell* finden Sie den Editor, mit welchem Sie den Workflow gestalten können.



Auf der linken Seite finden Sie die Symbolleiste. Dort finden Sie die Symbole, welche Sie zu Ihrem Workflow hinzufügen können. Klicken Sie hier auf ein Symbol, welches Sie zum Workflow hinzufügen wollen und klicken anschließend auf den Punkt im Workflow-Bereich in der Mitte, wo Sie das Symbol hinzufügen wollen. Sie können Symbole auch mittels Drag & Drop in den Workflow-Bereich ziehen.

### Nicht unterstützte Symbole

Verwenden Sie keine Symbole für Aufgaben, Gateways oder Ereignisse, welche von tenfold nicht explizit unterstützt werden. Dies kann zu Verwirrungen führen, da tenfold diese bei der Durchführung des Workflows ignoriert. Sie können jedoch Textannotationen und Pools verwenden, da diese nur zu Dokumentationszwecken dienen, um die Übersichtlichkeit zu steigern.

Textannotationen sind Kommentare, welche im Workflow-Diagramm hinterlegt werden können. Mit Pools lassen sich Workflows visuell in verschiedene Abschnitte unterteilen, um z.B. verschiedene Zuständigkeitsbereiche darzustellen.

Mit einem Doppelklick auf hinzugefügte Symbole können Sie den Namen des Elements bearbeiten.

### Namen von Genehmigungsschritten

Die Namen von Benutzeraufgaben wird in der Zeitleiste der Request-Übersicht angezeigt. Verwenden Sie daher Namen, die verdeutlichen, wer für die Genehmigung zuständig ist. Zum Beispiel "Abteilungsleiter", wenn Abteilungsleiter für die Genehmigung zuständig sind.

Wenn Sie ein Symbol im Workflow-Bereich auswählen, können Sie die dazugehörigen Eigenschaften auf der rechten Seite im Eigenschaftseditor bearbeiten. Außerdem erscheint rechts neben dem ausgewählten Symbol eine Auswahl an möglichen Folgeelementen. Sie können einfach auf ein Folgeelement klicken, um dieses dem Workflow hinzufügen. Dadurch wird auch automatisch eine Verbindungsleitung vom gewählten

Symbol zum Folgesymbol gezogen. Verbindungslien definieren die Folge von einem Symbol zum nächsten. Üblicherweise gibt es nur eine Verbindungslien von einem Symbol zum Folgesymbol. Die Ausnahme davon sind Gateways.

Wenn Sie ein Symbol aus dem Workflow entfernen möchten, wählen Sie das Symbol aus und klicken auf das Mülleimer-Icon.

#### **Workflow-Bereich zoomen und scrollen.**

Wenn Sie die STRG-Taste gedrückt halten, während Sie das Mausrad bewegen, können Sie im Workflow-Bereich zoomen. Sie können den Bereich scrollen, indem Sie die Maus bewegen, während Sie die mittlere Maustaste gedrückt halten. Dies kann helfen, wenn Sie Einstellungen erreichen möchten, die unter den angezeigten Bereich hinaus geraten sind.

## **Genehmigungsschritt hinzufügen**

Um einen neuen Genehmigungsschritt zu einem Workflow hinzuzufügen, fügen Sie dem Workflow zunächst ein "Aufgabe"-Symbol, wie im vorhergehenden Abschnitt beschrieben, hinzu. Während das Symbol ausgewählt ist, betätigen Sie die Aktion "Typ ändern" (Schraubenschlüssel-Icon) und wählen dort den Typ "Benutzeraufgabe" aus.

Anschließend wählen Sie im Eigenschaftseditor, im Abschnitt "Benutzeraufgabe", Einstellung "Typ", die Option "Genehmigungsschritt" aus. Sie haben nun folgende Einstellungsmöglichkeiten für den Genehmigungsschritt, welche im Eigenschaftseditor ersichtlich werden:

Einstellung	Beschreibung
Kontext	Der Genehmigungskontext, in welchem der Genehmigungsschritt angezeigt wird. Mittels Genehmigungskontexten können Sie zusammengehörige Genehmigungsschritte gruppieren, um so die Übersicht auf der Genehmigungsliste zu erhöhen.

Einstellung	Beschreibung
Modus	<p>Mit dieser Einstellung konfigurieren Sie, wer den Schritt genehmigen muss. Folgende Optionen stehen zur Auswahl:</p> <ul style="list-style-type: none"> <li>• <b>Vorgesetzter:</b> Der Vorgesetzte der betroffenen Person muss genehmigen. <b>Hinweis:</b> Dieser Modus wird nur von personenbezogenen Requests unterstützt (siehe Kasten "Personenbezogene Requests").</li> <li>• <b>Dateneigentümer (Abteilung):</b> Die Person (oder Personen), welche als Abteilungsverantwortlicher für die Abteilung der betroffenen Person hinterlegt wurde, muss genehmigen. <b>Hinweis:</b> Dieser Modus wird nur von personenbezogenen Requests unterstützt (siehe Kasten "Personenbezogene Requests").</li> <li>• <b>Dateneigentümer (Ressource):</b> Die Person, welche als Dateneigentümer der betroffenen Ressource (tenfold Ressourcen, Active Directory Gruppen, etc.) hinterlegt ist, muss genehmigen.</li> <li>• <b>Berechtigung:</b> Personen mit der ausgewählten tenfold-Berechtigung müssen Genehmigen. Wenn Sie an dieser Stelle eine Organisationsabhängige Berechtigung wählen, kann über die Rollenzuordnung die Berechtigung auf bestimmte Teile der Organisation eingeschränkt werden (siehe <a href="#">Berechtigungen(see page 457)</a>).</li> <li>• <b>Code Snippet:</b> Ein Code Snippet, welches eine einzelne Person oder Berechtigung zurückliefert. Es muss entweder die zurückgelieferte Person oder eine Person mit der zurückgelieferten Berechtigung genehmigen.</li> </ul> <p>Für das Skript stehen folgende Eingabeparameter zur Verfügung:</p> <ul style="list-style-type: none"> <li>• <b>ism:</b> Eine Instanz des IsmConnector. Mit diesem können vor allem die zurückzuliefernden Personen- und Berechtigungsobjekte geladen werden.</li> <li>• <b>delegateTask:</b> Erlaubt es, Variablen für den gesamten Workflow zu setzen oder abzufragen.</li> <li>• <b>requestApproval:</b> Datenobjekt, welches den aktuellen Genehmigungsschritt abbildet.</li> </ul>
Berechtigung	<p>Wurde in der Einstellung "Modus" die Auswahl "Berechtigung" getroffen, so muss die erforderliche Berechtigung hier ausgewählt werden.</p> <p><b>Hinweis:</b> Es werden nur Berechtigungen angezeigt, welche als "Benutzerdefiniert" markiert sind.</p>
Skript	<p>Wurde in der Einstellung "Modus" die Option "Skript" ausgewählt, so muss hier das entsprechende Skript eingetragen werden.</p>

Einstellung	Beschreibung
eSignature (Authentifizierung)	<p>Mit dieser Einstellung können Sie festlegen, ob angemeldete Benutzer, welche den Schritt genehmigen müssen, sich zur Genehmigung noch einmal authentifizieren müssen. Folgende Einstellungen stehen zur Verfügung:</p> <ul style="list-style-type: none"> <li>• <b>Nicht erforderlich:</b> Benutzer müssen ihre Zugangsdaten zur Genehmigung nicht erneut angeben.</li> <li>• <b>Active Directory:</b> Benutzer müssen zur Genehmigung erneut ihre Windows-Zugangsdaten angeben.</li> <li>• <b>Einmalpasswort:</b> Benutzer müssen zur Genehmigung Ihren Authenticator-Token erneut eingeben. Diese Einstellung funktioniert nur für Benutzer, welche die Zwei-Faktor-Authentifizierung aktiviert haben (siehe <a href="#">Zwei-Faktor-Authentifizierung (2FA)</a>(see page 480)).           <ul style="list-style-type: none"> <li>• <b>Active Directory und Einmalpasswort:</b> Es müssen sowohl die Windows-Zugangsdaten als auch ein neues Einmalpasswort eingegeben werden.</li> </ul> </li> </ul>
Dateianhänge	Diese Einstellung regelt, ob Genehmiger Dateianhänge zur Genehmigung hinzufügen können. Dies könnten, zum Beispiel, eingescannte Unterschriften oder Dokumente sein.
Personenänderungen	Mit dieser Einstellung kann geregelt werden, ob Änderungen an den Personendaten im Laufe der Genehmigung vorgenommen werden können.
Einzelgenehmigung Anwendungsberechtigungen	Hier können Sie festlegen, ob bei der Genehmigung von Anwendungsberechtigungen alle Berechtigungen auf einmal oder nur individuell genehmigt/abgelehnt werden können.
Anzeige zugewiesener Anwendungsberechtigungen	Mit dieser Einstellung kann festgelegt werden, ob Genehmiger nur die hinzugefügten/entfernten Berechtigungen einsehen können oder ob sie ebenso die aktuell zugewiesenen Berechtigungen der Person anzeigen können.

### Personenbezogene Requests

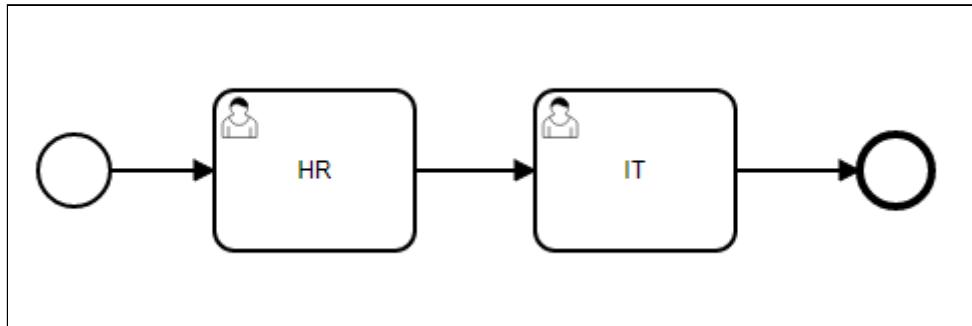
Nicht alle Genehmiger-Einstellungen werden von allen Requests unterstützt. Da sich Requests vom Modus "Active Directory", "Fileserver", "Exchangeserver", "Datenkorrektur", "Microsoft 365-Gruppe" und "Microsoft 365-Lizenz" auf die jeweilig betroffenen Objekte beziehen, statt auf die Personen, können Einstellungen wie "Vorgesetzter" für diese Requests nicht herangezogen werden.

### Speichern

Sie können den Workflow nicht speichern, solange nicht alle erforderlichen Felder der Genehmigungsschritte gesetzt sind.

## Interaktive Aktivität hinzufügen

Bei Anfragen zu Personenänderungen ist es allen Genehmigern möglich, die Daten der betroffenen Person noch einmal zu überarbeiten. Dies reicht in vielen Fällen aus, um Eintrittsszenarien, wie z.B. das folgende, abzubilden:

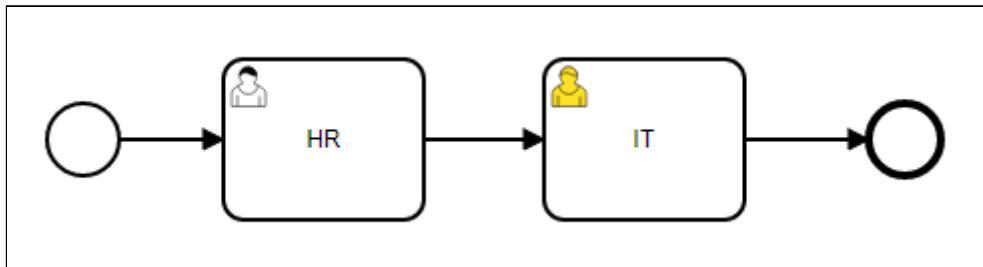


Hier werden die Daten zuerst von der Personalabteilung eingegeben. Die Personalabteilung gibt alle Daten ein, welche ihnen bekannt sind. Nach der Genehmigung geht der Workflow weiter zur IT-Abteilung, welche IT-Relevante Daten eingeben kann, wie zum Beispiel Telefon- oder Faxnummern. Danach ist die Anfrage genehmigt und der Benutzer kann angelegt werden.

Manchmal kann es jedoch erwünscht sein, dass jemand zwar zusätzliche Daten eingeben muss, diese Person den Request aber nicht ablehnen können soll. Auch kann es notwendig sein, zusätzliche Daten einzugeben, wenn es sich nicht um einen Personen-Request handelt. Zum Beispiel kann es sein, dass bei der Beantragung einer Schlüsselkarte die zuständige Person die Nummer der herauszugebenden Schlüsselkarte eintragen muss. Da es sich bei der Schlüsselkarte um eine Ressource handelt, können im Rahmen der Genehmigung jedoch keine Daten eingegeben werden.

In solchen Fällen können interaktive Aktivitäten Abhilfe verschaffen. Wie Sie interaktive Aktivitäten anlegen, erfahren Sie unter [Aktivitäten](#)(see page 628).

Sobald Sie eine interaktive Aktivität angelegt haben, können Sie diese in den Genehmigungsworkflow einbinden. Dazu ziehen legen Sie im Workflow ein neues Aufgaben-Symbol an und geben diesem einen Namen. Wandeln Sie das Aufgaben-Symbol anschließend in eine "Benutzeraufgabe" um. Wenn Sie das getan haben, wählen Sie im Eigenschaftseditor den Typ "Interaktive Aktivität". Das Personen-Icon im Aufgaben-Symbol wird daraufhin gelb dargestellt, um zu verdeutlichen, dass es sich hierbei nicht um einen Genehmigungsschritt handelt.



Anschließend muss im Eigenschaftseditor noch, unter der Einstellung "Interaktive Aktivität", die zuvor angelegte Aktivität ausgewählt werden.

### Speichern

Sie können den Workflow nicht speichern, solange Sie nicht für alle aktivitätsbasierten Benutzeraufgaben eine Aktivität definiert haben.

## Vordefinierte Aktivität hinzufügen

Manchmal kann es erforderlich sein, gewisse Aktionen während des Genehmigungsworkflows durchzuführen. Es ist möglich, solche Aktionen als "Vordefinierte Aktivität" anzulegen und diese dann durch den Genehmigungsworkflow ausführen zu lassen. Zum Beispiel erlaubt es die Aktivität "BPMN-Nachricht senden" des Activity Runner Plugins, Nachrichten an Workflows zu senden, auf welche diese hören können. Wie Sie vordefinierte Aktivitäten anlegen können, erfahren Sie unter [Aktivitäten\(see page 383\)](#).

### Auswahl an vordefinierten Aktivitäten

Welche vordefinierten Aktivitäten Ihnen zur Verfügung stehen, hängt von den installierten Plugins ab. Außerdem lassen sich nicht alle vordefinierten Aktivitäten in BPMN-Workflows einbinden, sondern sind für die Provisionierung gedacht.

Um eine vordefinierte Aktivität zum Workflow hinzuzufügen, fügen Sie zunächst dem Workflow ein neues Aufgaben-Symbol hinzu. Wandeln Sie dieses daraufhin mit der Aktion "Typ ändern" (Schraubenschlüssel-Icon) in eine "Serviceaufgabe" um. Wählen Sie nun im Eigenschaftseditor bei der Einstellung "Typ" die Option "Vordefinierte Aktivität" aus.

Abschließend müssen Sie noch bei der Einstellung "Vordefinierte Aktivität" eine zuvor angelegte Aktivität auswählen.

### Speichern

Sie können den Workflow nicht speichern, solange Sie für eine aktivitätsbasierte Service Aufgabe keine Aktivität festgelegt haben.

## EXEC hinzufügen

### Expertenfunktion

Bei EXECs handelt es sich um eine Expertenfunktion von tenfold, mit welcher mittels Skripten auf interne Objekte zugegriffen werden kann. Verwenden Sie diese Funktion mit Vorsicht!

Manchmal reichen die Möglichkeiten der vordefinierten Aktivitäten nicht aus. In diesen Fällen können Sie einen EXEC ausführen lassen. Dieser EXEC muss vom Typ "Genehmigungsworkflow" sein. In diesem EXEC stehen Ihnen sämtliche Möglichkeiten zur Verfügung, die Sie in anderen EXECs auch haben.

Um in einem Workflow einen EXEC aufzurufen, gehen Sie zunächst wie im vorherigen Abschnitt vor, um eine Service-Aufgabe zum Workflow hinzuzufügen. Wählen Sie bei der Einstellung "Typ" jedoch die Auswahl "EXEC" aus. Zum Schluss wählen Sie im Eigenschaftseditor noch den gewünschten, zuvor angelegten, EXEC aus.

Neben den Connectoren, welche Sie in den EXEC-Einstellungen hinzugefügt haben, stehen Ihnen folgende Variablen zur Verfügung:

Variable	Beschreibung
execution	Hierbei handelt es sich um ein DelegateExecution-Objekt der Camunda-Engine. Mit diesem Objekt können Sie Variablen setzen, welche für die weitere Laufzeit des Workflows gültig sind.

Variable	Beschreibung
request	Das Datenobjekt des aktuellen Requests, für welchen der Workflow ausgeführt wird.
tenfold	Ein Datenobjekt, welches als Workflow-Variable gespeichert wird. Es gewährt Zugriff auf den BpmnService und das Request-Objekt. Mit dem BpmnService lassen sich Abfragen auf aktuell laufende Workflows machen und Nachrichten an diese senden.

### Speichern

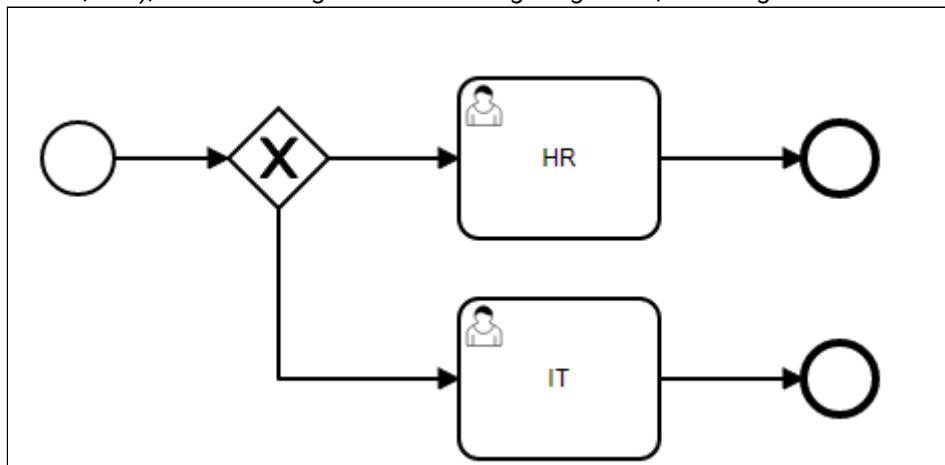
Sie können den Workflow nicht speichern, solange Sie keinen EXEC für eine EXEC-Service-Aufgabe festgelegt haben.

## Verzweigungen hinzufügen

In einigen Fällen kann es notwendig sein, dass für individuelle Vorbedingungen unterschiedliche Pfade im Genehmigungsworkflow verfolgt werden sollen. Da es zum Beispiel bei Personenarten und Ressourcen möglich ist, eine Auswahl des Workflows nach Typ und Modus zu treffen (siehe [Personenarten\(see page 81\)](#) und [Ressourcen\(see page 125\)](#)), ist es meist nicht notwendig, diese Bedingungen im Workflow abzubilden. Manchmal genügen diese Auswahlkriterien jedoch nicht oder es ist einfacher, die Auswahl im Workflow selbst zu treffen. Für diese Fälle können Sie eine Verzweigung mit dem Symbol "Exklusiver Gateway" erzeugen.

Um einen exklusiven Gateway in den Workflow einzufügen, legen Sie über die Symbolleiste ein neues Gateway-Symbol im Workflow an. Nachdem Sie ein Gateway-Symbol angelegt haben, ist dieses automatisch auf den Typ "Exklusiver Gateway" voreingestellt. Sie müssen daher den Typ nicht selber ändern.

Nachdem Sie einen solchen Gateway angelegt haben, können Sie, ausgehend von diesem, mehrere neue Symbole (Aktivitäten, etc.), wie in der folgenden Abbildung dargestellt, hinzufügen.



Um die Bedingungen für die jeweilige Verzweigung festzulegen, wählen Sie einen der ausgehenden Verbindungslien an. Daraufhin können Sie im Eigenschaftseditor, im Abschnitt "Details", die Art der Bedingung auswählen.

Sie haben folgende Möglichkeiten zur Definition der Bedingungen:

Konditionsart	Beschreibung
Bedingungen	Wählen Sie eine oder mehrere zuvor angelegte Provisionierungsbedingung aus und entscheiden, ob zumindest eine oder alle davon zutreffen müssen.
Ausdruck	<p>Ein einzeiliger Ausdruck, welcher auf einfache Weise die Workflow-Variablen verwenden kann. Ausdrücke müssen immer von \${ und } umschlossen werden. Mittels der "tenfold"-Variable kann auf das Request-Datenobjekt zugegriffen werden.</p> <p>Beispiele:</p> <ul style="list-style-type: none"> <li>• <b>`\${tenfold.request.new}`</b>: Trifft zu, wenn der Request ein Neu-Request ist.</li> <li>• <b>`\${tenfold.request.imRequest}`</b>: Trifft zu, wenn der Request ein Personendaten-Request ist.</li> <li>• <b>`\${personId == 10L}`</b>: Trifft zu, wenn der Wert der Variable "personId" den Long-Wert 10 hat. <b>Hinweis</b>: Diese Variable muss zuvor durch einen EXEC gesetzt werden und existiert nicht standardmäßig in einem Workflow. Auf tenfold-Connectoren lässt sich in Ausdrücken nicht zugreifen.</li> </ul>
Skript	<p>Ein (mehrzeiliges) Skript, welches wie EXECs in Groovy geschrieben wird. Das Skript wird jedoch an dieser Stelle eingegeben und muss nicht zuvor als EXEC angelegt werden. Es stehen dieselben Variablen zur Verfügung, wie auch in EXEC-Service-Aufgaben. Connectoren müssen jedoch im Skript bezogen werden und können nicht, wie bei EXECs, konfiguriert werden. Es muss einer der booleschen Werte <i>true</i> oder <i>false</i> zurückgegeben werden.</p>

### Eindeutige Bedingungen

Ein Exclusive Gateway verlangt, dass er durch genau **einen** Pfad verlassen werden muss. Sollten bei der Durchführung keine oder mehr als eine Bedingung erfolgreich zutreffen, so wird der Genehmigungs-Workflow in einen BPMN-Fehler laufen. Dieser wird dem Benutzer auf der Oberfläche angezeigt, der Request ist jedoch weiterhin im Zustand "Ungenehmigt". Der Request kann an dieser Stelle nur abgebrochen werden.

Auch gibt es keine Variante von "else", "otherwise" oder "default". Es muss daher immer eine konträre Bedingung definiert werden. **Beispiel**: Sie möchten, dass Anfragen für Personen der IT-Abteilung einen anderen Pfad einschlagen als Anfragen aus anderen Abteilungen. Sie haben daher für den Pfad der IT-Abteilung folgenden Ausdruck gewählt: \${`tenfold.person.masterdata.department.name == 'IT'`}. Der Pfad für alle anderen Abteilungen benötigt daher eine Bedingung \${`tenfold.request.person.masterdata.department.name != 'IT'`}. Dasselbe gilt auch für Provisionierungsbedingungen und Skripte.

### Speichern

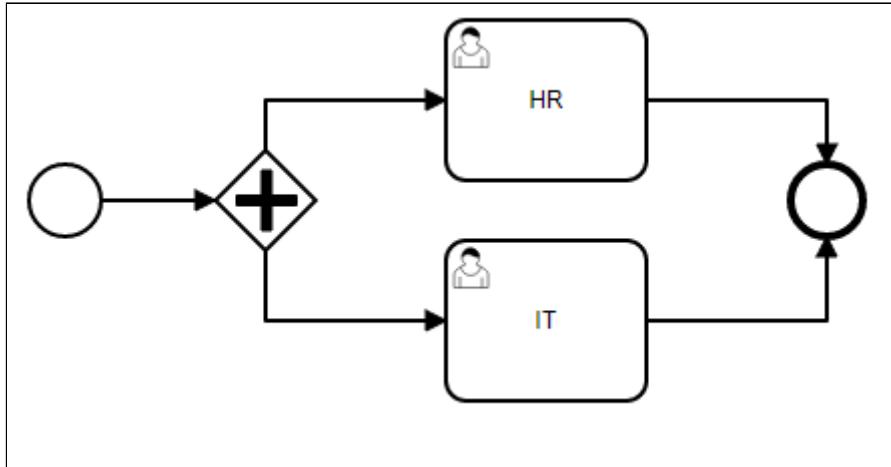
Der Workflow kann nicht gespeichert werden, solange nicht zu allen ausgehenden Verbindungen von Exclusive Gateways eine Bedingung definiert wurde.

## Parallele Genehmigungsworflows hinzufügen

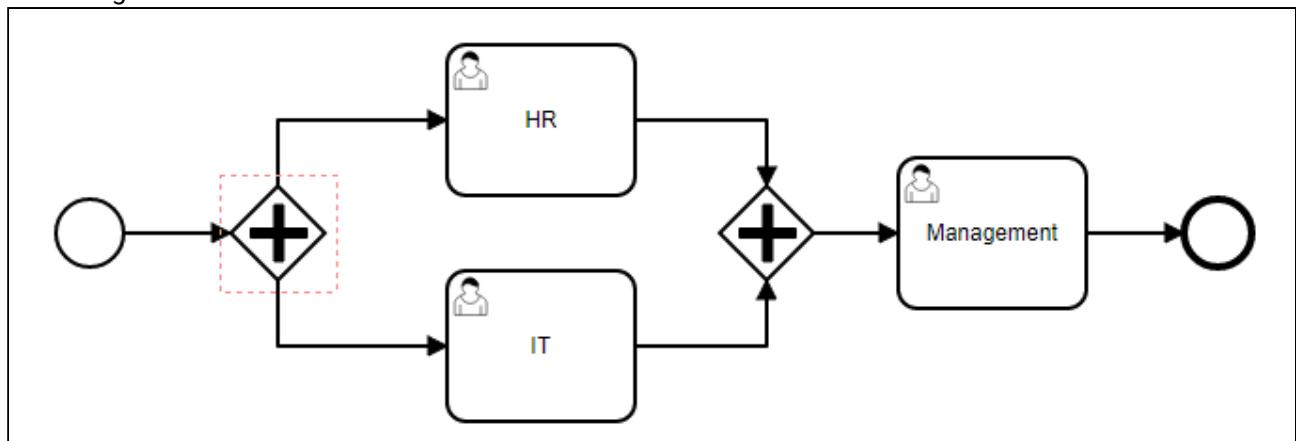
In einigen Fällen möchte man nicht, dass Genehmigungen nacheinander stattfinden, sondern Zeitgleich gestartet werden. Mit einem parallelen Gateway ermöglichen BPMN-Workflows Ihnen, mehrere Pfade im

Workflow zur selben Zeit zu starten. Um Parallelität zu ermöglichen, muss zunächst ein Symbol, "Paralleles Gateway", in den Workflow eingebunden werden. Fügen Sie dazu, wie im vorigen Abschnitt beschrieben, ein Gateway-Symbol in den Workflow ein. Ändern Sie daraufhin den Typ mit der Aktion "Typ ändern" (Schraubenschlüssel-Icon) auf "Paralleles Gateway".

Fügen Sie anschließend, vom Gateway ausgehend, mehrere Symbole über die Symbolleiste hinzu (zum Beispiel einen Genehmigungsschritt) und verbinden das Gateway mit diesen Symbolen. Das Ergebnis könnte dann wie in der folgenden Abbildung aussehen:



Durch das parallele Gateway werden die beiden Genehmigungsschritte sofort gleichzeitig gestartet, anstatt hintereinander. Da beide Pfade in ein End-Ereignis führen, wird dies wie gewünscht funktionieren. Sollten beide Pfade jedoch einen gemeinsamen weiteren Genehmigungsschritt im Anschluss haben, so müssen die Pfade wieder durch ein paralleles Gateway zusammengeführt werden, wie zum Beispiel in folgender Abbildung:



Ein paralleles Gateway wartet darauf, bis sämtliche eingehenden Pfade eingetroffen sind und fährt erst dann mit dem Workflow fort. Hätte man an dieser Stelle die beiden Genehmigungsschritte einfach direkt in den nächsten Genehmigungsschritt geleitet, so wäre dieser zweimal durchgeführt worden: einmal für IT und einmal für HR.

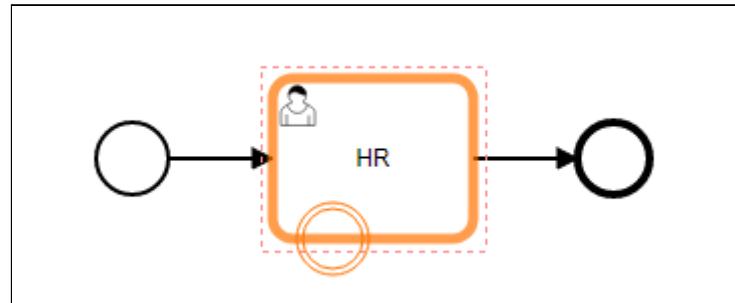
### Automatische Genehmigung

Bei der Anlage eines Requests versucht tenfold alle Genehmigungsschritte zu genehmigen, die der Antragsteller genehmigen darf. Dies geschieht für alle zusammenhängenden Genehmigungsschritte, vom Startereignis ausgehend. Sollte der Antragsteller in einem späteren Schritt noch einmal genehmigen dürfen, wird dieser nicht im Vorfeld bereits genehmigt.

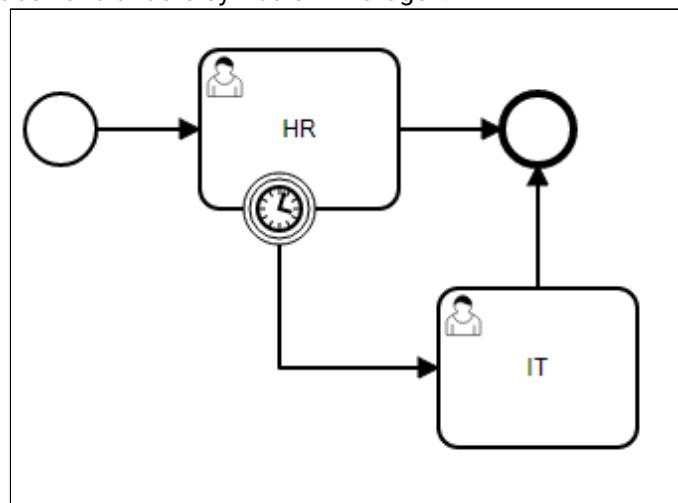
## Zeitliche Beschränkungen hinzufügen

Eine häufige Anforderung ist es, Genehmiger nach einer gewissen Zeit der Inaktivität noch einmal auf die offenen Genehmigungen aufmerksam zu machen. Alternativ könnte auch gewünscht sein, nach einer gewissen Zeit, die Genehmigung an eine andere Stelle zu eskalieren. BPMN-Workflows erlauben dies über sogenannte angeheftete Zeitereignisse.

Wählen Sie hierfür in der Symbolleiste das Symbol "Zwischenereignis" und setzen es an den Rand eines Aufgabensymbols.



Daraufhin ändern Sie den Typ des Zwischenereignisses auf entweder "Angeheftetes Zeit-Zwischenereignis" oder "Angeheftetes Zeit-Zwischenereignis (nicht unterbrechend)". Sie können nun, von diesem Symbol ausgehend, weitere Aufgaben und andere Symbole hinzufügen.



Um zu bestimmen, wann das Zeitereignis eintritt, verwenden Sie die Einstellungen im Eigenschaftseditor. Sie haben folgende Möglichkeiten, die Zeit mit der Einstellung "Timer-Definitionstyp" zu konfigurieren:

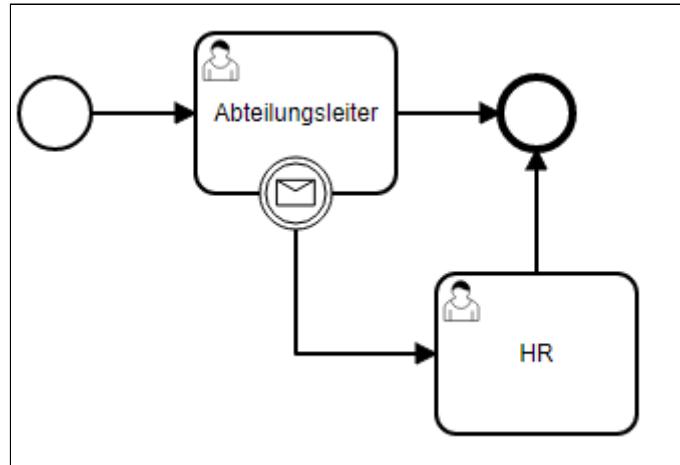
Timer-Definitionstyp	Beschreibung	Beispiel
Datum	<p>Wird verwendet, um feste Datumswerte einzutragen. Tragen Sie hier in der Einstellung "Timer-Definition" ein Datum im ISO 8601-Format ein. Dieses wird zum Beispiel auch in XML-Dateien zur Darstellung von Datumswerten verwendet. Für weitere Informationen, wenden Sie sich an <a href="https://en.wikipedia.org/wiki/ISO_8601">https://en.wikipedia.org/wiki/ISO_8601</a>. <b>Hinweis:</b> Diese Einstellung erlaubt es nicht, dynamische Datumswerte zu verwenden. Sie müssen diese Einstellung daher regelmäßig anpassen. Üblicherweise gibt es kaum Anwendungsfälle für diese Funktion. Sie wird hier jedoch der Vollständigkeit wegen erwähnt.</p>	2999-12-31T00:00:00Z
Zeitspanne	<p>Mit dieser Einstellung tritt das Ereignis ein, sobald eine gewisse Zeit vergangen ist, nachdem das Symbol, an dem dieses Ereignis angeheftet ist, erreicht wurde. Die Definition erfolgt im ISO 8601-Format. Näheres finden Sie unter <a href="https://en.wikipedia.org/wiki/ISO_8601#Durations">https://en.wikipedia.org/wiki/ISO_8601#Durations</a>. <b>Hinweis:</b> Dieses Ereignis tritt nur einmal auf. Wenn Sie die Zeitspanne zum Beispiel auf 3 Tage setzen, dann wird dieses, auch bei nicht unterbrechenden Ereignissen, nur durchgeführt, wenn das erste Mal 3 Tage verstrichen sind.</p>	PT3D
Zyklus	<p>Sie können Zeitintervalle, in welchen das Ereignis ausgelöst wird, in zwei verschiedenen Varianten angeben:</p> <ul style="list-style-type: none"> <li>• ISO 8601 (weitere Informationen finden Sie unter: <a href="http://en.wikipedia.org/wiki/ISO_8601#Repeating_intervals">http://en.wikipedia.org/wiki/ISO_8601#Repeating_intervals</a>)</li> <li>• Cron (weitere Informationen finden Sie unter: <a href="https://www.wikipedia.org/wiki/Cron">https://www.wikipedia.org/wiki/Cron</a>) <b>Hinweis:</b> Im Gegensatz zu Cron stellt das erste Element die Sekunden dar, nicht die Minuten.</li> </ul> <p>Dieses Ereignis wird regelmäßig ausgelöst, solange der Workflow sich im entsprechenden Zustand befindet. <b>Hinweis:</b> Sollten Sie ein unterbrechendes Ereignis gewählt haben, so wird die aktuelle Aufgabe nach dem Ablauf des Intervalls verlassen und damit später nicht noch einmal ausgelöst. Für die Verwendung macht es keinen Unterschied, ob Sie sich für ISO 8601 oder Cron entscheiden. Beide Schreibweisen bilden dieselbe Funktionalität ab, lediglich die Schreibweise unterscheidet sich.</p>	<ul style="list-style-type: none"> <li>• R3/PT10H (ISO 8601)</li> <li>• 0 0/5 * * * ? (Cron)</li> </ul>

### Speichern

Der Workflow lässt sich nicht speichern, solange er Zeiteignisse ohne korrekte Definition enthält.

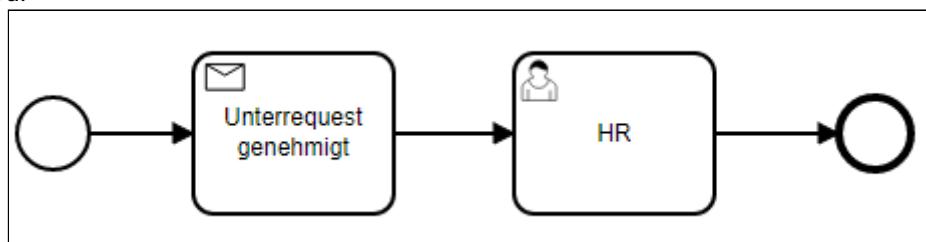
## Nachrichtenempfang hinzufügen

Um die Kommunikation zwischen Workflows (oder anderen Systemen) zu erlauben, unterstützt tenfold zwei Möglichkeiten, um auf den Eingang von BPMN-Nachrichten zu hören. Zunächst können Sie ein "Angeheftetes Nachrichten-Zwischenereignis" verwenden, um einen gerade aktiven Genehmigungsschritt zu unterbrechen. Sie können dies verwenden, um Eskalationsprozesse zu erzeugen oder um einen Workflow auf einen anderen Workflow warten zu lassen.



Gehen Sie hierbei vor, wie unter [Zeitliche Beschränkungen hinzufügen](#)(see page 397) beschrieben, wählen jedoch als Typ "Angeheftetes Nachrichten-Zwischenereignis" oder "Angeheftetes Nachrichten-Zwischenereignis (nicht "Unterbrechend" aus. Wählen Sie daraufhin im Eigenschaftseditor aus, auf welche Nachrichten das Ereignis reagieren soll. Wie auch bei zeitlichen Ereignissen bedeutet "nicht unterbrechend" hier, dass der aktuelle Genehmigungsschritt bestehen bleibt, wenn das Ereignis eintritt.

Die zweite Möglichkeit ist es, den Genehmigungsworkflow zu unterbrechen, bis eine BPMN-Nachricht empfangen wird.



Fügen Sie hierfür ein neues Aufgaben-Symbol zum Workflow hinzu und ändern den Typ in "Empfangen Aufgabe". Wählen Sie dann im Eigenschaftseditor, wie bei den Nachrichten-Zwischenereignissen auch, die Namen der Nachrichten aus, auf welche gewartet werden soll. Daraufhin wird der Genehmigungsprozess an dieser Stelle unterbrochen und wartet solange, bis eine Nachricht vom entsprechenden Typ eingegangen ist. Um zu vermeiden, dass Genehmigungsprozesse potentiell endlos auf den Eingang gewisser Nachrichten warten, können Sie eine "Empfangen Aufgabe", genauso wie an Genehmigungsschritte auch, an Zeitereignisse anheften, um diese, nach einer gewissen Zeit, abzubrechen.

### Senden Aufgabe

In BPMN gibt es, als Gegenstück zur Empfangen-Aufgabe, auch eine Senden-Aufgabe. Mit diesem Symbol lässt sich der Versand von Nachrichten an Prozesse abbilden. In tenfold wird dieses Symbol jedoch **nicht** verwendet und hat keinerlei Funktion. Verwenden Sie stattdessen eine Vordefinierte

Aktivität vom Typ "BPMN-Nachricht senden" (siehe [Vordefinierte Aktivität hinzufügen\(see page 393\)](#)). Diese wird vom Activity Runner Plugin definiert. Installieren Sie daher dieses Plugin, um die Funktion nutzen zu können.

### Speichern

Genehmigungsworkflows, welche "Nachrichten-Zwischenereignisse" oder "Empfangen Aufgaben" ohne Definition der zu empfangenden Nachrichten enthalten, können nicht gespeichert werden.

## Automatische Genehmigung unterbrechen

Wird ein Request erstellt und ein Genehmigungsworkflow gestartet, so wird der Genehmigungsworkflow so weit genehmigt, wie es mit den Berechtigungen des Erstellers möglich ist. Bei der Genehmigung einzelner Schritte wird ebenso so weit genehmigt, wie es mit den Berechtigungen des Genehmigers möglich ist.

Dies dient der erleichterten Abarbeitung von Genehmigungen, so dass Antragsteller und Genehmiger nicht für jeden einzelnen Schritt explizit die Genehmigungsmaske öffnen und bestätigen müssen. Nicht immer ist dies jedoch das gewünschte Verhalten. Manchmal ist es erwünscht, aber für besonders heikle Berechtigungen kann es erwünscht sein, dass die Genehmigung explizit erfolgen muss, um eine versehentliche Vergabe dieser Berechtigungen zu vermeiden. Aus diesem Grund bietet tenfold eine vordefinierte Aktivität, um die automatische Genehmigung zu unterbrechen (siehe [Vordefinierte Aktivitäten\(see page 643\)](#)).

### Activity Runner Plugin

Für die Definition und Verwendung der notwendigen Aktivität ist die Installation des Activity Runner Plugins, in mindestens der Version 2.5, erforderlich.

Legen Sie, wie unter [Vordefinierte Aktivitäten\(see page 643\)](#) beschrieben, eine neue vordefinierte Aktivität an und wählen die Aktion "Verhindern von automatischen Genehmigungen". Geben Sie der Aktivität einen beliebigen Namen und speichern Sie sie ab. Keine weiteren Einstellungen sind für diese Aktivität verfügbar. Sie können daraufhin diese Aktivität, wie unter [Vordefinierte Aktivität hinzufügen\(see page 393\)](#) beschrieben, in einen Genehmigungsworkflow einfügen, um an diesen Stellen die automatische Genehmigung zu unterbinden.

### Manuelle Genehmigung

Diese Aktivität verhindert nicht, dass ein Antragsteller/Genehmiger auf die Genehmigungsmaske einsteigt und den Request manuell weitergenehmigt. Lediglich die automatische Genehmigung wird unterbunden.

## 10.2.2 Workflows bearbeiten und löschen

Um einen bestehenden BPMN-Workflow zu bearbeiten, navigieren Sie zunächst im Menü zu *Workflows > Genehmigungsworkflows*. Dort können Sie einen bestehenden Genehmigungsworkflow bearbeiten, indem Sie, im Aktionsmenü der entsprechenden Zeile, die Aktion "Bearbeiten" auswählen. An dieser Stelle können Sie Genehmigungsworkflows auch löschen, indem Sie die Aktion "Löschen" aus dem Aktionsmenü wählen.

### Standardworkflows