
Hitobito

Release 0.1

Hitobito contributors

20.01.2025

1 Rollen	3
1.1 Empfehlungen	4
1.2 Eigene Bezeichnungen für Rollen	5
2 Personenfilter	7
2.1 Filtern von Personen	7
2.1.1 Neuen Filter Anlegen	7
2.1.2 Auswahl auf welcher Ebene / Gruppe gesucht werden soll.	8
2.1.3 Auswahl an Personen mit gesuchten Rollen.	9
2.2 Gefilterte Listen speichern	10
3 Events	11
3.1 Anlässe	11
3.2 Kurse	11
3.3 Einladungen	11
4 Tags	13
4.1 Erfassen von Tags	13
4.2 Verwalten von Tags	14
4.3 Personen mit Tags auswählen	14
5 Mailinglisten / Abos	15
5.1 Neues Abo erstellen	15
5.1.1 Absender-Rechte	15
5.2 Empfänger zuweisen	16
5.2.1 Gruppe/Rolle hinzufügen wählen	16
5.2.2 Nach Tags einschränken (optional)	17
5.3 Mailversände	17
5.4 Etiketten drucken	18
5.5 Mailinglisten nach Tags filtern	18
6 Rechnungen	19
6.1 Rechnungseinstellungen	19
6.2 Rechnungsartikel	19
6.3 Rechnungen erstellen	20
6.4 Rechnungen einsehen und bearbeiten	20
6.5 Zahlungen Erfassen	20

6.6	Buchungsbeleg	21
6.7	Häufig gestellte Fragen:	21
7	Berechtigungskonzept	23
7.1	Gruppen / Rollen - Wie funktioniert das?	23
7.1.1	Karin ist Geschäftsleiter direkt im Dachverband	23
7.1.2	Maria hat eine Rolle in der Region	25
7.1.3	Petra leitet ein Gremium in der Region	25
7.1.4	Anna leitet eine Ortsgruppe	26
7.1.5	Franz leitet eine Einheit innerhalb einer Ortsgruppe	27
7.1.6	Jonas ist Mitglied innerhalb einer Gruppe in der Ortsgruppe	27
7.2	Kumulierung von Rollen innerhalb der Struktur	28
7.3	Daten in Anlässen (Lagern, Kursen)	28
7.4	Spezialfall <code>Contact_Data</code>	28
7.5	Spezialfall <code>finance</code>	29
7.6	Spezialfall <code>impersonation</code>	29
7.7	Security: Zugriffsanfragen und manuelle Freigabe	29
8	MailChimp-Export von Mailinglisten / Abos	31
8.1	Grundsatz	31
8.2	Verknüpfen einer Mailingliste mit MailChimp	31
8.3	Exportieren nach MailChimp	33
9	EBICS Schnittstelle	35
9.1	Allgemeines	35
9.2	Wie richte ich die Schnittstelle ein?	35
9.3	Einrichten	36
9.4	Unterstützte Finanzinstitute	36
10	Zwei-Faktor-Authentifizierung	39
10.1	Voraussetzungen	39
10.2	Einrichten	39
10.3	Login mit Zwei-Faktor-Authentifizierung	40
10.4	Zurücksetzen und deaktivieren	40
11	Fragen und Antworten	41
11.1	Hitobito meldet, dass die IBAN Nummer ungültig ist	41
11.2	Die Haupt-E-Mail kann nicht geändert werden	41
11.3	Geänderte Haupt-E-Mail muss bestätigt werden	41
11.4	Wie werden Personen-Duplikate erkannt?	42
11.5	Wann wird welche Referenznummer verwendet?	42
11.6	Über hitobito können verschiedene Mails verschickt werden. Welcher Absender wird da verwendet?	42
11.7	Was bedeutet Hitobito	43

Hier findest du die generische Benutzerdokumentation für Hitobito.

Du kannst selbst deinen Beitrag leisten und Ergänzungen vornehmen, in dem du auf Github: https://github.com/hitobito/user_documentation Korrekturen an den Anleitungsseiten vornimmst. Wenn dir das zu kompliziert ist, kannst du einfach auch Änderungen, Ergänzungen über dieses Formular: https://github.com/hitobito/user_documentation/issues/new vorschlagen.

Rollen sind ein zentrales Konzept in hitobito:

- Jede Person kann beliebig viele Rollen in verschiedenen Kontexten haben. Peter kann z. B. gleichzeitig Leiter eines Gremiums in einem Kantonalverband sein, als auch Mitglied in einer Ortsgruppe.
- Welche Rollen zur Verfügung stehen, hängt davon ab, in welcher Gruppe du die Person zuweist. Z. B. hat eine Gruppe vom Typ Vorstand Rollen wie PräsidentIn und SekretärIn zur Verfügung.
- Die Rolle der Person bestimmt die [Zugriffsrechte](#) dieser Person.

1.1 Empfehlungen

The screenshot displays the Hitobito user interface. At the top, there is a green navigation bar with the Hitobito logo and several menu items: 'GRUPPEN', 'ANLÄSSE', 'KURSE', and 'EINSTELLUNGEN'. On the left side, a sidebar menu is visible, with 'Dachverband' highlighted. Below this, there are sub-menu items: 'Geschäftsstelle', 'Kontakte', 'Vorstand', and 'Ohne Rollen'. Further down, there is a section for 'REGIONEN/KANTONE' with options for 'Region Bern', 'Region Nordost', and 'Region Zürich'. The main content area shows the details for the 'Dachverband' group. It includes a 'Kontaktangabe' section with the following information: 'Dachverband', 'Schellingstr. 8', '5692 Damianburg', and the email 'alta.haley@example.ch'. Above this information, there are buttons for 'Bearbeiten', '+ Gruppe erstellen', and 'CSV Untergruppen'. A dropdown menu is open over the '+ Gruppe erstellen' button, showing a list of roles: 'Vorstand', 'Geschäftsstelle', 'Gremium/Projektgruppe', 'Mitglieder', 'Kontakte', 'Region/Kanton', and 'Lokalgruppe/Sektion'.

Für jede Organisation stellen wir die passenden Rollen bereit. Versuch also möglich die passende Art von Gruppentyp auszuwählen, damit du dort der Person die richtige Rolle zuweisen kannst.

1.2 Eigene Bezeichnungen für Rollen

Rolle für Vivienne Tschirch / Amet erstellen

[Speichern](#) [Abbrechen](#)

Gruppe

Rolle

Bezeichnung

Optionale Bezeichnung der Rolle dieser Person

[Speichern](#) [Abbrechen](#)

Du kannst neben der offiziellen Rollenbezeichnung noch deine eigene ergänzen, indem du im Rollendialog das zusätzliche Feld ausfüllst.

Nach dieser Bezeichnung kann allerdings aktuell noch nicht gefiltert werden.

Auf der Personenliste kann nach unterschiedlichen Kriterien gefiltert werden:

- Rollenfilter
- Qualifikationsfilter
- Felder
- Tags

2.1 Filtern von Personen

2.1.1 Neuen Filter Anlegen

The screenshot displays the 'Geschäftsstelle' interface. On the left, a sidebar lists navigation options including 'Region Bern', 'Geschäftsstelle', 'Kontakte', 'Vorstand', 'Ohne Rollen', and 'LOKALGRUPPEN/SEKTI...'. The main area shows the 'Personen' tab selected, with a sub-tab 'Mitglieder (3)'. A dropdown menu is open over this sub-tab, showing options: 'Gesamte Gruppe' and 'Neuer Filter...'. Below the dropdown, a table lists members with columns for 'Nachname', 'Rollen', and 'E-Mails'. Two members are visible: 'Kopf Milana / Non' and 'Mensah Sam / Nostrum', both with the role 'Leitung'.

Nachname	Rollen	E-Mails
Kopf Milana / Non	Leitung	milana_kopf@hi neil.barton@exa
Mensah Sam / Nostrum	Leitung	admin@hitobito

Unter *weitere Ansichten* *Neuer Filter* wählen.

2.1.2 Auswahl auf welcher Ebene / Gruppe gesucht werden soll.

Personen filtern


Suchen

Suche speichern

[Abbrechen](#)

- In der aktuellen Ebene und allen darunter liegenden Ebenen und Gruppen
- In der aktuellen Ebene und allen ihren Gruppen
- Nur in der aktuellen Gruppe

2.1.3 Auswahl an Personen mit gesuchten Rollen.

 **Rollen**

Welche Rollen sollen angezeigt werden?

Region/Kanton

Vorstand

Präsident Sekretär(in)


Vizepräsident Vorstandsmitglied

Geschäftsstelle

Leitung

Mitglied

Gremium/Projektgruppe

 Leitung

Mitglied

Mitglieder



Aktivmitglied

Passivmitglied

Kontakte

Kontakt

Im Zeitraum (optional)

 bis 

war die Rolle aktiv.

wurde die Rolle erstellt.

wurde die Rolle gelöscht.

26. B. alle Leiter von Gremien/Projektgruppen

Hinweis: Tipp: Beim klicken auf die Gruppe, werden alle Rollen dieser Gruppe ausgewählt.

2.2 Gefilterte Listen speichern

Name

 *

Suchen

Suche speichern

[Abbrechen](#)

Der definierte Filter kann gespeichert werden und, steht allen anderen Benutzern zur Verfügung.

In Hitobito können unterschiedliche Arten von Events geführt werden. Einfache Anlässe und Kurse. Für gewisse Instanzen wurden zusätzliche Eventsarten wie Lager, Ferienlager oder Musikfeste ergänzt.

3.1 Anlässe

In der Organisation von Anlässen unterstützt Hitobito auf eine einfache Weise. Mitglieder können sich mit ihrem Benutzer direkt anmelden, ohne erneut ihre Angaben wie Adressen eingeben zu müssen.

3.2 Kurse

Die Kurse bauen auf den Anlässen auf, sind durch zusätzliche Funktionen ergänzt. So können Anmeldebedingungen definiert werden und Teilnehmer können aufgrund ihrer angegebenen Priorität zugewiesen werden.

3.3 Einladungen

Einladungen sind nützlich, wenn bestimmte Personen an einem Anlass oder Kurs teilnehmen sollten. In diesem Fall können die Verantwortlichen diese Personen auf dem *Einladungen*-Tab hinzufügen. Das *Einladungen*-Tab zeigt den Status aller eingeladenen Personen.

Einladungen

Info [Teilnehmende](#) [Einladungen](#)

[+ Person einladen](#) [Download](#)

Person	Haupt-E-Mail	Teilnehmerrolle	Status	Ablehnungsdatum	Erstellungsdatum	
Vivian Kinzel / Tenetur	kinzel_vivian@hitobito.example.com	Teilnehmer/-in	Abgelehnt	25.03.2023 22:37	25.03.2023 23:05:36.124	
Vivian Kuhlee / Velit	kuhlee_vivian@hitobito.example.com	Teilnehmer/-in	Angenommen		25.03.2023 23:28:19.495	
Hannah Hiebl / Porro		Teilnehmer/-in	Eingeladen		25.03.2023 23:39:51.541	
Simeon Hanenberger / Dicta		Teilnehmer/-in	Angenommen		25.03.2023 23:40:23.792	

Die eingeladenen Personen können sich dann auf der Anlass-Seite für den Anlass an- oder abmelden.

Anlass 157

[Info](#)

Du wurdest zu diesem Anlass eingeladen.

[✓ Anmelden](#) [✗ Abmelden](#)

Die eingeladenen Personen erhalten keine automatische Benachrichtigung, da die Betroffenen wohl in vielen Fällen (z.B. Sitzungen, Generalversammlung) separat ausführlich informiert werden müssen.

Über das Personen-Register der anbietenden Gruppe eines Anlasses oder Kurses können auch mehrere Personen gleichzeitig hinzugefügt werden.

[Info](#) [Personen](#) [Anlässe](#) [Abos](#) [Notizen](#) [Gelöscht](#)

Mitglieder (24)

[Weitere Ansichten](#)

[+ Person hinzufügen](#)

[+ Rec](#)

24 Personen angezeigt.

3 Ausgewählt

[Rollen](#)

[+ Zu Veranstaltung hinzufügen](#)

[+](#)



Bayer Rosario / Iure

Anlass

-in



Blanda Keyon / Eveniet

Anlass (Einladung)

-in



Borer Creola / Occaecati

Kurs

er/-in

Kurs (Einladung)

Mit Tags (engl. für Etikett, Schildchen) lassen sich in hitobito Kategorien oder Merkmale auf Personen abbilden. Tags sind nicht strukturierte Informationen und können frei definiert werden. Um Tags zu vergeben, sind Schreibrechte auf der Person erforderlich.

4.1 Erfassen von Tags

Beim Erfassen der Tags könnt ihr die Kategorie direkt eingeben oder auch Unterkategorien bilden.

Bsp.:

- Tag „Newsletter“ vergeben, falls diese Person einen Newsletter erhalten soll.
- Tag „Mailings: News“ oder „Mailings: Events“ vergeben, wenn es Newsletter für verschiedene Fälle gibt.

Tags

Interesse

Hackathon ✕

Mailing

Community Meeting ✕

Newsletter ✕

Release Notes ✕

Tag hinzufügen...

Ok

4.2 Verwalten von Tags

Als Administrator können die Tags unter Einstellungen für die ganze Instanz erstellt, bearbeitet, gelöscht und zusammengeführt werden.

4.3 Personen mit Tags auswählen

Auf der Personenlisten können nach Tags gefiltert werden. Weiter können bei Mailinglisten/Abo Personen aufgrund der gesetzten Tags ausgewählt werden.

Mailinglisten / Abos

Mit Mailinglisten / Abos können die Empfänger von Zeitschriften / Abos verwaltet werden, man kann sie auch für die interne Kommunikation benutzen.

Für Mailversände und das Verwalten von Abonnementen könnt ihr entsprechende Verteilerlisten erfassen.

5.1 Neues Abo erstellen

Mit den nötigen Berechtigungen könnt ihr im Tab „Abos“ ein neues Abo erstellen. Minimal muss ein Name für das Abo vergeben werden. Falls das Abo für Mailversände verwendet werden soll, muss zudem unter „Mailinglisten Adresse“ eine Adresse eingetragen werden.

5.1.1 Absender-Rechte

Ohne weitere Konfiguration dürfen alle Personen, die das Abo bearbeiten können auch Mails an den Verteiler senden. Kontrolliert wird dabei ob die im Absender eingetragene Mail-Adresse bei den berechtigten Kontakten als Haupt- oder weitere Mailadresse hinterlegt ist.

Die Mailadressen der Gruppe, zu dem das Abo gehört, dürfen ebenfalls jederzeit Mails an den Verteiler senden.

Zusätzliche Absender können mit folgenden Optionen berechtigt werden

1. Das Feld „Zusätzliche Absender“: Mails mit den aufgeführten Absender-Adressen dürfen auf die Liste schreiben.
2. „Abonnenten dürfen auf die Mailingliste schreiben“: Die bei den Abonnenten erfassten Mail-Adressen dürfen auf die Liste schreiben.
3. „Beliebige Absender/-innen dürfen auf die Mailingliste schreiben“: Alle, die die Abo-Adresse kennen, können Mails dorthin senden.

5.2 Empfänger zuweisen

In einem zweiten Schritt gilt es noch, die Empfänger dieses Abos zu bestimmen. Hierfür orientieren wir uns primär an den Organisationsstrukturen und den definierten Rollen.

5.2.1 Gruppe/Rolle hinzufügen wählen



5.2.2 Nach Tags einschränken (optional)

Abonnent erstellen

Speichern [Abbrechen](#)

Gruppe

hitobito AG > Angestellte

Es können nur Gruppen unterhalb der Abogruppe ausgewählt werden

Rollen

Geschäftsstelle

Leitung
 Mitglied

Tags

Nur Person mit einem der untenstehenden Tags hinzufügen:

Mailing:Newsletter

Speichern [Abbrechen](#)

5.3 Mailversände

Wenn ihr für das vorliegende Beispiel eine Einladung an alle Mitglieder der Region Bern versenden möchtet, könnt ihr diese an die gewählte E-Mail-Adresse senden. hitobito wird diese danach an die damit verknüpften Rollen, Anlässe etc. „weiterleiten“.

Im Abo kann definiert werden, wer auf das Abo schreiben darf. Nur Abonnenten auf der Mailingsliste, oder beliebige Absender*innen. Im Feld „Zusätzlicher Absender“ kann definiert werden, wenn von weiteren E-Mail Adressen auf den Mailverteiler geschrieben werden kann. Ein Beispiel: Abo ist ein Präsidiumsverteiler mit sämtlichen Personen mit der Rolle Präsident*in. Da dürfen nur Personen welche im Abo sind drauf schreiben. Zusätzlich soll aber von info@hitobitokunde.ch auf dieses Abo geschrieben werden. In diesem Fall muss die Mailadresse info@hitobitokunde.ch

in das Feld „Zusätzlicher Absender“ eingetragen werden. Mittels Strichpunkt (;) können auch mehrere Adressen erfasst werden.

5.4 Etiketten drucken

Falls ihr ein entsprechendes Etikettenformat definiert habt, könnt ihr diese im Abo unter „Export“ auswählen, damit euch für physische Versände die Adressen der gewählten Mitglieder exportiert werden.

5.5 Mailinglisten nach Tags filtern

Personen können beim hinzufügen via Rolle/Gruppe auch nach Tags gefiltert werden

In Hitobito können Debitoren verwaltet, Rechnungen erstellt und Zahlungen verbucht werden. Hitobito hat keine Buchhaltungsfeatures. Bei Bedarf können die Rechnungs- und Zahlungsdaten exportiert, oder eine Buchhaltungssoftware via Schnittstellen angebunden werden.

Bemerkung: Rechnungen sind ein Feature welches pro Instanz aktiviert werden kann. Ob eine Person Rechnungen verwalten kann hängt davon ab, ob sie eine entsprechende Rolle hat. Welche Rollen *:finance* Berechtigungen haben hängt von der jeweiligen Organisation ab.

6.1 Rechnungseinstellungen

In den Rechnungseinstellungen werden pro Ebene gültige Angaben gemacht. Hier werden die allgemeinen Rechnungseinstellungen verwaltet und Mahnungsfristen und -texte definiert. Zudem können Einstellungen zum Email-Versand und Rechnungslayout vorgenommen werden, sowie Zahlungsschnittstellen eingerichtet werden.

Hinweis: Damit Rechnungen versendet werden können müssen gültige Rechnungseinstellungen vorhanden sein.

6.2 Rechnungsartikel

Häufig verwendete Rechnungspositionen (z.B. Mitgliederbeitrag, Jahresabo, etc.) können hier pro Ebene vordefiniert werden. Diese Artikel können beim Erstellen von Rechnungen ausgewählt und individuell angepasst werden.

Bemerkung: Die Felder Kostenstelle und Konto haben in Hitobito keine Funktion. Sie sind lediglich für einen allfälligen Export in eine Buchhaltungssoftware vorhanden.

6.3 Rechnungen erstellen

Hinweis: Rechnungen werden nicht auf der Ansicht Rechnungen erstellt, sondern ausgehend von Personenlisten oder einer bestimmten Person.

Rechnungen können aus folgenden Ansichten erstellt werden:

- Personenlisten in einer **Gruppe**. Erstellt eine Einzelrechnung an die ausgewählten Personen.
- Teilnehmerlisten von einem **Event**. Erstellt eine Einzelrechnung an die ausgewählten Personen.
- Auf dem Profil einer **Einzelperson**. Erstellt eine Einzelrechnung an die ausgewählte Person.
- In einem **Abo**. Erstellt eine Sammelrechnung an die jeweiligen Empfänger des Abos.
- **Externe Rechnungen** erstellen in der Übersicht Einzelrechnungen. Erstellt eine Einzelrechnung. Diese wird keiner Person in Hitobito zugeordnet.

6.4 Rechnungen einsehen und bearbeiten

Rechnungen können in der Übersicht Rechnungen eingesehen und bearbeitet werden. Hier wird zwischen Einzelrechnungen und Sammelrechnungen unterschieden.

Rechnungen können gestellt, gemahnt und per Email versendet werden. Dabei werden immer sämtliche ausgewählten Rechnungen gestellt oder gemahnt abhängig von ihrem aktuellen Status.

Hier können Rechnungen auch gedruckt oder exportiert werden, und es können Zahlungen erfasst werden.

Sammelrechnungen werden in der Übersicht zusätzlich pro Rechnungslauf zusammengefasst. Dabei wird die Anzahl Empfänger, so wie die Anzahl und der Betrag der bezahlten Rechnungen angezeigt.

Die Rechnungen einer spezifischen Person können auch auf der jeweiligen Personenansicht eingesehen werden.

6.5 Zahlungen Erfassen

Zahlungen können auf drei verschiedene Arten erfasst werden.

Auf jeder Einzelrechnung können manuelle Zahlungen für die jeweilige Rechnung erfasst werden.

In der Übersicht Einzelrechnungen können camt.54 XML-Datei¹ hochgeladen werden. Diese erfassen die jeweiligen Zahlungen auf den dazugehörigen Rechnungen. Die Zahlungen werden auch erfasst, wenn es sich dabei um eine Sammelrechnung handelt.

Ist in den Rechnungseinstellungen eine Zahlungsschnittstelle eingerichtet, werden die Zahlungen nächtlich über die EBICS Schnittstelle mit der Bank abgeglichen. Anleitung zum einrichten der EBICS Schnittstelle: <https://hitobito.readthedocs.io/de/latest/ebics.html>

¹ Eine camt.054 XML-Datei ist die Sammelbuchungs-auflösung und Belastungs- und Gutschriftsanzeige. Diese enthält eine Reihe verschiedene Buchungspositionen welche automatisiert auf Basis der ESR-Nummer bestehenden Rechnungen zugeordnet werden.

6.6 Buchungsbeleg

Unter Buchungsbeleg wird eine rudimentäre Übersicht über die eingegangenen Zahlungen gegeben. Diese werden nach Rechnungsartikel sortiert. Dabei wird davon ausgegangen, dass gleiche Rechnungsartikel auch immer den gleichen Betrag aufweisen.

6.7 Häufig gestellte Fragen:

Q1: Ich kann keine Rechnungen erstellen. Die Gruppe als welche ich Rechnungen stellen möchte ist ausgegraut.

A1: Für die ausgegraute Gruppe sind keine gültigen Rechnungseinstellungen vorhanden. Bitte aktualisiere die Rechnungseinstellungen.

Q2: Ich kann meine Rechnungseinstellungen nicht speichern?

A2: Vermutlich ist in einem anderen Tab der Rechnungseinstellungen noch eine falsche Information vorhanden. Probiere auf den verschiedenen Tabs die Rechnungseinstellungen zu speichern.

Q3: Ich kann eine Rechnung nicht mehr löschen?

A3: Eine Rechnung kann nur gelöscht werden, solange sie noch den Status „Entwurf“ hat. Eine Sammelrechnung kann nur gelöscht werden, wenn noch alle darin enthaltenen Rechnungen den Status „Entwurf“ haben. Hat eine Rechnung bereits einen anderen Status, kann diese nur noch storniert werden.

Q4: Eine Rechnung mit dem Status „Gestellt“ wird nicht gemahnt, obwohl ich diese bei Mahnen ausgewählt hatte.

A4: Rechnungen werden nur gemahnt, wenn das Mahndatum erreicht wird. Schau in den Rechnungseinstellungen nach, wie lange nach Rechnungsdatum hier die Mahnfrist ist.

Q5: Nach dem Speichern meiner Sammelrechnung werden keine Rechnungen erstellt.

A5: Damit Sammelrechnungen erfolgreich erstellt werden können, muss mindestens eine Rechnungsposition einen Betrag aufweisen (Dieser Betrag kann 0 sein).

7.1 Gruppen / Rollen - Wie funktioniert das?

In hitobito können komplexe hierarchische Organisationen abgebildet werden. Alles basiert darauf, dass wir verschiedene Gruppentypen zulassen, welche auch definieren welche Rollen zur Verfügung stehen.

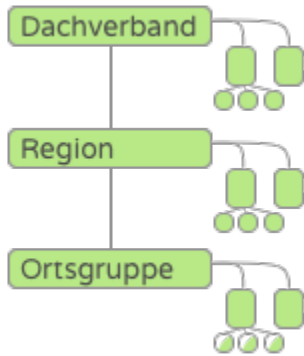
- Jede Organisation kann aus mehreren Ebenen bestehen, z. B. Dachverband, Kantonalverband (, optionale Zwischenstufen wie Regionen) und Ortsgruppen.
- Jede Ebene kann intern wieder ihre innere Struktur haben, es gibt einen Vorstand, Arbeitsgruppen, Mitgliederlisten, Kontaktlisten.
- Jede Person hat eine oder mehrere Rollen. Diese Rollen definieren, wen man sehen kann, und von wem man gesehen wird.

Hier einige Beispiele, wie das aussehen kann.

7.1.1 Karin ist Geschäftsleiter direkt im Dachverband

technisch: `layer_and_below_full` direkt in Dachverband, inkl. `contact_data`

Karin sieht:



Karin hat vollen Zugriff auf ihrer Ebene und auf alle darunter liegenden Ebenen. Dadurch kann sie alle Personen im Dachverband, in Regionen und auf oberster Ebene der Ortsgruppen sehen und ändern. Nicht sichtbar und änderbar sind für sie alle Personen, die innerhalb einer Ortsgruppe, also in einer Untergruppe unter der Ortsgruppe, aufgehängt sind. Da Karin's Rolle als kontaktrelevant geführt ist (sog. ContactData-Flag, siehe unten), kann sie alle anderen Personen mit Kontaktrelevanz sehen, unabhängig von deren Position innerhalb der Struktur.

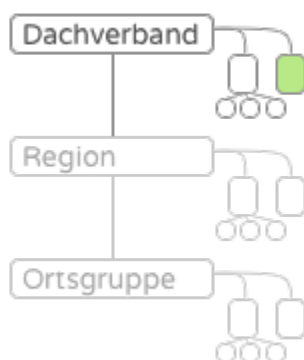
Karin sehen:

Karin ist für alle anderen Personen mit Rechten innerhalb der Ebene des Dachverbands sichtbar. Auf Grund der Kontaktrelevanz von Karin's Rolle ist sie ebenfalls für alle anderen kontaktrelevanten Rollen sichtbar.

Luca ist ein Mitglied in einem Gremium im Dachverband

technisch: `group_read` in Gremium ohne `contact_data`

Luca sieht:



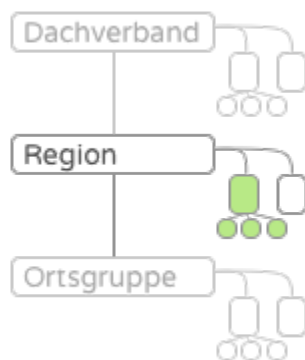
Luca sieht alle Mitglieder und Leitung innerhalb des Gremiums. Sonst sieht er niemanden ausserhalb des Gremiums.

Luca sehen:

Luca ist für Personen mit vollen Rechten (`layer_full` oder `layer_and_below_full`) für die Dachverbandsebene sicht- und änderbar. Zusätzlich kann die Leitung innerhalb seines Gremiums seine Daten einsehen und ändern (`group_full`). Seine Kollegen mit gleicher Rolle im Gremium sehen seine Daten, können diese aber nicht ändern (`group_read`)

7.1.2 Maria hat eine Rolle in der Region

technisch: `group_read` inkl. `contact_data`

Maria sieht

Maria kann alle Mitglieder ihrer Gruppe sehen, also alle Mitarbeitenden auf Regionsebene.

Da Maria's Rolle als kontaktrelevant geführt ist (sog. `ContactData-Flag`, siehe unten), kann sie alle anderen Personen mit Kontaktrelevanz sehen, unabhängig von deren Position innerhalb der Struktur.

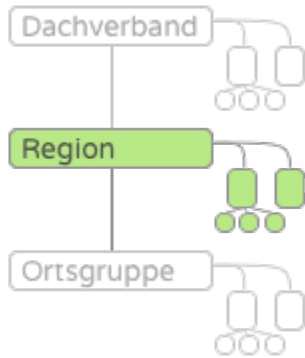
Maria sehen

Maria ist für alle anderen Personen mit Rechten innerhalb der Ebene des Dachverbands sichtbar. Auf Grund der Kontaktrelevanz von Maria's Rolle ist sie ebenfalls für alle anderen kontaktrelevanten Rollen sichtbar.

7.1.3 Petra leitet ein Gremium in der Region

technisch: `layer_read` inkl. `contact_data`

Petra sieht:



Petra sieht alle Personen in der Region inkl. Personen in allfälligen Untergruppen. Sie sieht jedoch keine Personen in Ortsgruppen, welche der Region angehängt sind.

Da Petra's Rolle als kontaktrelevant geführt ist (sog. ContactData-Flag, siehe unten), kann sie alle anderen Personen mit Kontaktrelevanz sehen, unabhängig von deren Position innerhalb der Struktur.

Petra sehen

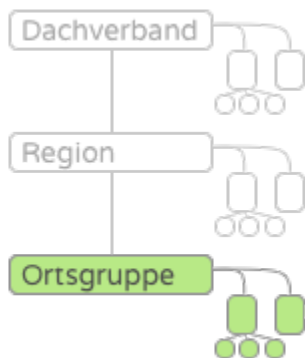
Petra ist für Personen auf kantonaler oder Dachverbandsebene sichtbar, welche eine Rolle mit Zugriff auf untergeordnete Ebenen besitzen (layer_and_below). Zudem sehen alle Personen in der Region, die Rechte innerhalb der Gruppe oder der Ebene besitzen, ihre Daten.

Auf Grund der Kontaktrelevanz von Petra's Rolle ist sie ebenfalls für alle anderen kontaktrelevanten Rollen sichtbar.

7.1.4 Anna leitet eine Ortsgruppe

technisch: layer_full incl. contact_data

Anna sieht



Anna sieht alle Personen innerhalb der Ortsgruppe.

Da Anna's Rolle als kontaktrelevant geführt ist (sog. ContactData-Flag, siehe unten), kann sie alle anderen Personen mit Kontaktrelevanz sehen, unabhängig von deren Position innerhalb der Struktur.

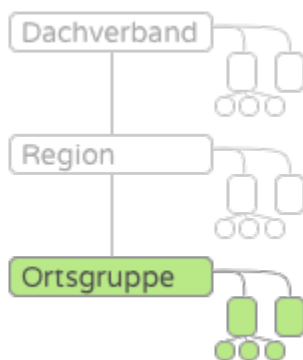
Anna sehen

Anna ist für Personen oberhalb der Ortsgruppe sichtbar, falls diese das Recht besitzen, Personen unterhalb ihrer Ebene zu sehen. Zudem können ihre Kolleginnen und Kollegen innerhalb der Ortsgruppe ihre Daten sehen, falls sie das Recht für die Gruppe oder die Ebene besitzen. Auf Grund der Kontaktrelevanz von Anna's Rolle ist sie ebenfalls für alle anderen kontaktrelevanten Rollen sichtbar.

7.1.5 Franz leitet eine Einheit innerhalb einer Ortsgruppe

technisch: `layer_read` (ohne `contact_data`)

Franz sieht



Franz sieht alle Personen innerhalb der Ortsgruppe, kann diese aber nicht ändern.

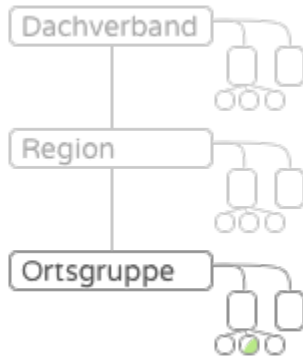
Franz sehen

Franz ist für Personen in der Ortsgruppe sichtbar, falls diese das Recht besitzen, Personen innerhalb der ganzen Ebene zu sehen. Personen oberhalb der Ortsgruppe können Franz nicht sehen.

7.1.6 Jonas ist Mitglied innerhalb einer Gruppe in der Ortsgruppe

technisch: none

Jonas sieht



Jonas sieht keine weiteren Personen.

Jonas sehen

Jonas ist für Personen in der Ortsgruppe sichtbar, falls diese das Recht besitzen, Personen innerhalb der ganzen Ebene zu sehen. Personen oberhalb der Ortsgruppe können Jonas nicht sehen.

7.2 Kumulierung von Rollen innerhalb der Struktur

Die Zugriffe durch mehrere Rollen kumulieren sich. So ist ein Mitglied einer Ortsgruppe, das gleichzeitig in der Region aktiv ist, trotzdem für die Regionsleitung sichtbar.

7.3 Daten in Anlässen (Lagern, Kursen)

Teilnehmer in einem Anlass können die Teilnehmerliste einsehen und sehen dort ihre gegenseitigen Kontaktdaten. Die Daten sind nur im Kontext „Anlass“ sichtbar, wenn über die Teilnehmerliste zur Person navigiert wird. Im Kontext einer „Gruppe“, wenn über die Gruppenhierarchie zur Person navigiert wird, gelten die Zugriffsrechte gemäss den strukturbasierten Rechten oben.

7.4 Spezialfall Contact_Data

Ist die Rolle einer Person als kontaktrelevant markiert, so hat diese Person auf alle anderen Personen mit kontaktrelevanten Rollen Zugriff. Gleichzeitig ist sie auch für alle anderen Personen mit kontaktrelevanten Rollen sichtbar. Dies umfasst Rollen, welche häufig im Austausch mit Personen aus anderen Ortsgruppen stehen.

7.5 Spezialfall finance

Erlaubt auf der entsprechenden Ebene Rechnungen zu erstellen und einzusehen.

7.6 Spezialfall impersonation

Darf andere Accounts temporär übernehmen, z. B. für Support Aufgaben oder für Tests. Dies ist eine sehr mächtige Funktion und sollte nur an klar definierte Rollen vergeben werden.

7.7 Security: Zugriffsanfragen und manuelle Freigabe

Angenommen, Anna möchte unberechtigt Zugriff auf die persönlichen Daten von John bekommen. Dazu kann Anna John einfach in einer Gruppe, einem Anlass oder Abo hinzufügen, in der sie Zugriffsrechte hat. Dieses Datenschutz-Problem kann in hitobito mit den „manuellen Freigaben“ verhindert werden.

Beim Hinzufügen von John in Gruppen, Anlässen und Abos überprüft hitobito Johns Haupt-Rolle (die Rolle die mit einem Stern markiert ist). Falls John keine aktive Rolle mehr hat, überprüft hitobito stattdessen die letzte Rolle die noch aktiv war. Es wird überprüft, ob in der Ebene dieser Rolle die manuellen Freigaben aktiviert sind. Beispiel: John hat seine Haupt-Rolle in der Arbeitsgruppe „Saturn“ des Vereins „Sterngucker Luzern“. Die manuellen Freigaben können bei der Ebene (Verein Sterngucker Luzern) auf dem Anfragen-Tab aktiviert werden.

Sind manuelle Freigaben in der Ebene aktiviert, dann wird John nicht direkt in die neue fremde Gruppe, Anlass oder Abo hinzugefügt, sondern es wird eine Zugriffsanfrage ausgelöst. Anna sieht dann folgende Nachricht:

The screenshot shows the Hitobito interface for a group named 'Lernhilfe'. The left sidebar contains navigation options: Gruppen, Anlässe, Kurse, and Einstellungen. The main content area shows the 'Lernhilfe' group details, including a search bar, user list, and a notification banner. The notification states: 'Wir haben eine Zugriffsanfrage für John Doe versendet. Die Rolle wird erstellt, sobald die Anfrage freigegeben wird. Allfällige Details zur Rolle müssen nach der Freigabe erneut angegeben werden.' Below the notification, a table lists group members, including 'Corkery Janice / Qui' with their roles and contact information.

Nachname Vorname Ceviname	Rollen	E-Mails	Telefonnummern	Adresse PLZ Ort
<input type="checkbox"/> Corkery Janice / Qui	Leiter/-in Adressverantwortliche/-r	janice_corkery@hitobito.example.com rupert@example.org Privat	1-445-989-0926 Privat 1-374-854-2998 x39225 Mutter	599 Luellwitz Freeway 5624 Seanstad

Alle Personen die auf dem Anfragen-Tab ausgewählt sind, sowie John falls er einen Login hat, bekommen ein E-Mail welches darüber informiert dass Anna John an einem neuen Ort hinzufügen will. Von diesem E-Mail aus oder auf dem Anfragen-Tab der Gruppe kann die Zugriffsanfrage akzeptiert oder abgelehnt werden.

The screenshot shows the 'INTEGRATION' section of the Hitobito interface. On the left is a sidebar with navigation options: Gruppen, Anlässe, Kurse, and Einstellungen. The main content area is titled 'Cevi Schweiz' and includes a search bar, a 'Deaktivieren' button, and a table of requests. Below the table is a list of administrators with toggle switches.

Person	Anfrage für	Anfrage von	Datum
Doe John / Earum Angestellte/-r in Geschäftsstelle	Weiteres Arbeitsgebiet Lernhilfe Mitglied	Corkery Janice / Qui Leiter/-in in Lernhilfe Adressverantwortliche/-r in Lernhilfe	02.11.2021 10:56

Buttons: Akzeptieren, ✖Ablehnen

Benachrichtigungen an:

- Siegrist Louis / Löl Administrator/-in
- Beahan Monserrat / Cupiditate Administrator/-in
- Bednar Aiden / Ut Administrator/-in
- Boller Simon / Chinchilla Administrator/-in (LKB ZH-SH-GL)
- Braun Roman / Popcorn Administrator/-in

So bekommt Anna nie unberechtigten Zugriff auf die Personendaten von John. Das Ganze funktioniert aber nur, wenn die manuellen Freigaben auf der Ebene aktiviert sind. Es wird keine Zugriffsanfrage ausgelöst wenn Anna bereits vorher Zugriff auf John hat (z.B. wenn beide eine Rolle mit *contact_data* haben).

MailChimp-Export von Mailinglisten / Abos

Mit dem MailChimp-Export können die Abonnent*innen von Mailinglisten exportiert werden in eine MailChimp-Liste. Bitte beachtet vor Benutzung dieses Features zwei Dinge:

- Die MailChimp-Liste wird durch den Export **überschrieben** (siehe auch folgenden Abschnitt)
- Die MailChimp-Liste wird **regelmässig** (alle 24h) und bei Bedarf zusätzlich **auf Knopfdruck** exportiert

8.1 Grundsatz

Das MailChimp-Feature ermöglicht es, die in Hitobito organisierten Daten zu brauchen, um mit MailChimp gestaltete Newsletter zu versenden. Es kann nicht gebraucht werden, um eine MailChimp-Liste mit einer Hitobito-Mailingliste zu synchronisieren, da es **keine Daten von MailChimp importiert** und **bestehende Daten von MailChimp bei jedem Export überschreibt**.

8.2 Verknüpfen einer Mailingliste mit MailChimp

Mit jeder Mailingliste kann jeweils eine MailChimp-Liste verknüpft werden. Dies geschieht in den Einstellungen der Mailingliste durch die beiden Felder «MailChimp API-Schlüssel» und «MailChimp Listen-ID»:

MailChimp Listen-ID

Abonnenten können an die MailChimp-Liste exportiert werden. Diese Aktion überschreibt die MailChimp-Liste und bestehende Kontakte werden gelöscht.

MailChimp API-Schlüssel

Alle Versandadressen synchronisieren

Hinweis: Standardmässig werden nur die Haupt-E-Mailadressen der Abonnent*innen synchronisiert. Sollen weitere E-Mailadressen, welche die Option „Versand“ haben ebenfalls mit MailChimp synchronisiert werden, ist die Option

„Alle Versandadressen synchronisieren“ anzuwählen.

Die «**MailChimp Listen-ID**» kannst Du in den Einstellungen der gewünschten Liste in MailChimp holen (in gelb unten rechts):

Test-Liste 1

[Switch list](#) ▾

[Stats](#) ▾ [Manage contacts](#) ▾ [Add contacts](#) ▾ [Signup forms](#) [Settings](#) ▾ [Q](#)

List name and campaign defaults

List name

Test-Liste

[Want to change your signup form title?](#)

List ID

Some plugins and integrations may request your
Typically, this is what they want: **test-12345**.

Der «**MailChimp API-Schlüssel**» ermöglicht es einer fremden Applikation wie Hitobito, in deinem Namen Änderungen in MailChimp vorzunehmen. Du kannst einen neuen API-Schlüssel im Menü «Extras / API keys» in den Einstellungen deines Profils erstellen. Auf der entsprechenden Seite kannst Du «Create A Key» drücken (im Bild unten links) und den «API key» aus dem Textfeld (im Bild gelb hinterlegt) in das entsprechende Feld in Hitobito kopieren:

Testprofil

[Overview](#) [Settings](#) ▾ [Billing](#) ▾ [Extras](#) ▾ [Integrations](#) [Transactional](#)

API keys

About the API

The Mailchimp API makes it easy for programmers to integrate Mailchimp's features into other applications.

[Read The API Documentation](#)

Developing an app?

Writing your own application that requires access to other Mailchimp users' accounts? Check out our [OAuth2 API documentation](#), then register your app.

[Register And Manage Your Apps](#)

Your API keys

API keys provide full access to your Mailchimp account, so keep them safe. [Tips on keeping API keys secure](#).

Created	User	Label	API key	QR Code	Status
Aug 24, 2018 4:34 am	Testprofil (owner)	none set	test-12345678901234567890123456	QR	<input checked="" type="checkbox"/>

[Create A Key](#)

[Create A Mandrill API Key](#)

Gratuliere, nach dem Speichern dieser zwei Informationen ist nun deine Mailingliste mit der MailChimp-Liste verknüpft!

8.3 Exportieren nach MailChimp

Um die Abonent*innen einer Mailingliste nach MailChimp zu exportieren, wähle die entsprechende Option im «Export»-Menu des «Abonnenten»-Tabs deiner Mailingliste in Hitobito aus.

Gefahr: Bitte beachte, dass der Export deine verknüpfte Liste in MailChimp überschreiben. Bestehende Kontakte werden in Mailchimp archiviert.

Test-Mailingliste

Info Abonnenten

+ Person hinzufügen + Gruppe/Rollen hinzufügen + Anlass hinzufügen - Person ausschliessen **Export**

Personen
 Keine Einträge gefunden.

Gruppen / Rollen

- CSV
- Excel
- vCard
- PDF
- MailChimp**
- Etiketten
- E-Mail Adressen

Nach dem Auslösen des Exports wird die Liste im Hintergrund in die gewählte MailChimp-Liste exportiert und die Abonent*innen deiner Mailingliste sollten nach einiger Zeit dort erscheinen. Sollten E-Mailadressen in Mailchimp den Status „cleaned“ besitzen, wird in hitobito ein entsprechender Validation Tag gesetzt. (z.B. „Haupt-E-Mail ungültig“)

Bemerkung: Abonent*innen Ihrer Mailingliste, welche sich in der Vergangenheit aktiv bei MailChimp von Ihrer Liste abgemeldet haben (über den Abmelden-Link in Ihrer E-Mail), behalten ihren «Unsubscribed»-Status und erhalten auch nach einem neuerlichen Export aus hitobito keine E-Mails mehr von Ihnen.

EBICS Schnittstelle

9.1 Allgemeines

Hitobito lässt sich mit einem Bank- oder Postkonto verbinden. Dies bedeutet folgendes:

Wird eine Zahlung über hitobito ausgelöst und vom Empfänger bezahlt, ist diese Information nicht mehr nur im Bankkonto ersichtlich, sondern wird auch im hitobito ausgewiesen. Hitobito kann so die Buchhaltung unterstützen, da damit die Zahlungseingänge zentral und personifiziert überwacht werden können.

Als Schnittstelle verwendet hitobito die Technologie EBICS. EBICS ist eine standardisierte Schnittstelle zu Finanzapplikationen und wird in der Schweiz von beinahe allen Banken angeboten (Ausnahmen sind möglich, uns aber nicht bekannt). Mehr Informationen zu EBICS findet ihr auf den Webseiten der verschiedenen Banken.

Über die [EBICS Schnittstelle](#) können camt054 Dateien regelmässig von einem Finanzinstitut bezogen werden. Mittels Referenznummer werden die Zahlungen einer Rechnung von der Ebene zugewiesen. Zahlungen die keiner Rechnung zugewiesen werden können, werden ignoriert

In den Rechnungseinstellungen kann pro Ebene die EBICS Schnittstelle definiert werden. Zugangsdaten werden verschlüsselt in Hitobito abgelegt.

9.2 Wie richte ich die Schnittstelle ein?

1) **Über die eigene Bank/Post muss ein EBICS Vertrag angefordert werden.**

- a) Der Vertrag regelt, welche Konten mit hitobito verknüpft werden. Es können mehrere Konten gleichzeitig über EBICS mit hitobito verknüpft werden.
- b) Im Vertrag muss EBICS als Schnittstelle ausgewählt werden, falls Euch der Vertrag mehrere Optionen gibt.
- c) Im Vertrag muss eine Software angegeben werden, damit ist hitobito gemeint. Angegeben werden soll als Software «hitobito» und als Hersteller «Puzzle ITC»
- d) Die Buchungsart ist Sammelbuchung, die Periodizität ist Euch selbst überlassen.

- 2) Der Vertrag wird der Bank/Post zurückgeschickt. Von Seiten der Bank/Post wird nun ein Dokument mit der Vertrags-ID und der Kunden-ID für EBICS erstellt und Euch zur Verfügung gestellt. (Die genaue Bezeichnung kann variieren und auch als Teilnehmer-ID / Partner-ID o.Ä. bezeichnet sein.)
- 3) Mit diesem Dokument der Bank/Post könnt Ihr in hitobito unter den Rechnungseinstellungen->Zahlungsschnittstellen die Vertrags-ID und die Kunden-ID eingeben. Sobald dies gemacht ist, erscheint in Hitobito ein Button zur generierung des Initialisierungs-Dokuments (INI-Brief).
- 4) Dieses Dokument muss dem Bankinstitut unterschrieben zurückgeschickt werden, damit die Verbindung zwischen Konto und hitobito erstellt werden kann.
- 5) Die Bank informiert Euch, sobald die Schnittstelle eingerichtet und aktiv ist.
- 6) Ist dies der Fall, werden Zahlungen, die in hitobito ausgelöst wurden, auch in hitobito abgebucht.

ACHTUNG: Für die Zuordnung einer Zahlung an eine Person ist die Referenznummer einziges relevantes Merkmal. Macht Eure Mitglieder darauf Aufmerksam, dass Zahlungen nicht mit alten Referenznummern gemacht werden sollen. Fehlerquellen sind hauptsächlich falsch eingegebene oder alte Referenznummern. In solchen Fällen muss über die Bank die Nachforschung zur entsprechenden Zahlung gemacht werden. Weder Puzzle ITC noch Hitobito kann in solchen Fällen unterstützen.

9.3 Einrichten

- Beim Einrichten der Schnittstelle wird ein HTML File generiert das ausgedruckt und per Post an die Bank gesendet wird.
- Anschliessend kann Teilnehmer-ID und Kunden-ID ausgefüllt werden
- Das Passwort wird verwendet um die Kommunikation zu verschlüsseln. Wenn dieses Passwort geändert wird, muss die ganze Einrichtung der Schnittstelle wiederholt werden.

9.4 Unterstützte Finanzinstitute

Folgende Banken können via EBICS angebunden werden.

- Postfinance
- Raiffeisen Schweiz

Vorhanden, jedoch noch keine abschliessende Verifikation:

- Credit Suisse
- UBS
- Luzerner Kantonalbank
- St.Galler Kantonalbank
- Thurgauer Kantonalbank
- Zürcher Kantonalbank
- BancaStato
- BEKB | BCBE
- Valiant
- Zuger Kantonalbank

Gerne ergänzen wir diese Liste mit weiteren Banken.

Zwei-Faktor-Authentifizierung

Hitobito unterstützt die Zwei-Faktor-Authentifizierung mit folgender Methode:

- TOTP mittels Authenticator-App und sechsstelligem Code

10.1 Voraussetzungen

Für die Zwei-Faktor-Authentifizierung wird ein Smartphone und eine Authenticator-App benötigt. Die Zwei-Faktor-Authentifizierung wurde mit der kostenfreien freeOTP App (<https://freeotp.github.io/>) entwickelt und getestet, sollte aber grundsätzlich auch mit anderen ähnlichen Apps wie andOTP (<https://github.com/andOTP/andOTP>) oder Google Authenticator funktionieren.

10.2 Einrichten

Um die Zwei-Faktor-Authentifizierung einzurichten, muss man sich erst in Hitobito anmelden. Auf dem eigenen Profil kann man nun im Dropdown „Login“ den Knopf „Zwei Faktor Authentifizierung einrichten“ sehen. Durch Klicken auf diesen Knopf landet man auf einer Seite mit einem QR-Code.

In der freeOTP App auf dem Smartphone klickt man nun auf den QR-Code-Knopf in der Kopfzeile. Dadurch öffnet sich die Kamera mit einem Quadrat in der Mitte. Der QR-Code in hitobito kann nun mit der Kamera gescannt werden.

Sobald der Code gescannt wurde, schliesst sich die Kamera und ein neues Element in der Liste sollte auf der App ersichtlich sein. Dies erkennt man anhand der Bezeichnung , 'hitobito' und der E-Mail-Adresse. Durch einen Klick auf den Eintrag wird ein sechsstelliger Code wird angezeigt.

Dieser Code ändert sich alle paar Sekunden. Nun tippt man den Code in hitobito ein und klickt auf „Absenden“. Sollte der Code inkorrekt sein, wird eine entsprechende Nachricht angezeigt und man muss es erneut versuchen. Sobald der Code korrekt und rechtzeitig eingegeben wurde, wird man auf das Profil zurückgeleitet, und die Zwei-Faktor-Authentifizierung ist eingerichtet.

10.3 Login mit Zwei-Faktor-Authentifizierung

Sobald die Zwei-Faktor-Authentifizierung eingerichtet ist, muss der Code von der App bei jedem Login eingegeben werden. Nach der Eingabe von E-Mail und Passwort wird man auf eine Seite mit einer Eingabeaufforderung weitergeleitet. Hier tippt man nun wieder den Code aus der freeOTP App ab und klickt auf „Absenden“. Sollte der Code nicht korrekt oder bereits abgelaufen sein, wird eine entsprechende Nachricht angezeigt. Ist der Code jedoch korrekt, wird man authentifiziert und in hitobito weitergeleitet.

10.4 Zurücksetzen und deaktivieren

Administratoren können die Zwei-Faktor-Authentifizierung einer Person auf deren Profil zurücksetzen oder deaktivieren. Dort erscheinen unter dem Dropdown „Login“ zwei Knöpfe „Zwei Faktor Authentifizierung zurücksetzen“ und „Zwei Faktor Authentifizierung deaktivieren“.

Wird die Zwei-Faktor-Authentifizierung zurückgesetzt, wird der Nutzer beim nächsten Login einen neuen QR Code scannen müssen.

Bei der Deaktivierung wird der Nutzer nicht mehr zur Zwei-Faktor-Authentifizierung aufgefordert.

11.1 Hitobito meldet, dass die IBAN Nummer ungültig ist

Falls als Einzahlungsschein QR Rechnungen ausgewählt sind, muss eine spezielle QR-IBAN (<https://www.moneytoday.ch/lexikon/qr-iban/>) hinterlegt werden. Diese unterscheidet sich von der bestehenden IBAN Nummer.

11.2 Die Haupt-E-Mail kann nicht geändert werden

Wenn ein Account beispielsweise bei einer Ortsgruppe und im Dachverband eine aktive Rolle hat, kann die **Haupt-E-Mail** nur von einer Person geändert werden, welche Schreibrechte in beiden Gruppen hat. Folgende Nachricht wird dann jeweils angezeigt: „Die Haupt-E-Mail Adresse einer Person mit mehreren Rollen kann nur von einem über alle diese Rollen übergeordneten Benutzer geändert werden“ Der Account selbst kann seine Haupt-E-Mail immer ändern.

Ein Beispiel: Ich bin in der Ortsgruppe Wabern und habe eher wenig Rechte im System. Ich kann aber in meiner Gruppe einen Admin zu meiner Gruppe hinzufügen, der auf dem Dachverband sehr viele Rechte hat. Dadurch erhalte ich Schreibrechte auf dieser Person. Ich könnte die primäre Mailadresse auf eine mir zugängliche Adresse ändern, ein Passwortreset auf dem User machen und mich anschliessend als Dachverbands-Admin einloggen. Um das Ganze zu vertuschen, könnte ich danach die Mailadresse wieder zurückändern. Aus diesem Grund ist das Ändern der primären Mailadresse nur zugelassen wenn ich die Berechtigung über alle Gruppen des Admins habe.

11.3 Geänderte Haupt-E-Mail muss bestätigt werden

Wird die Haupt-E-Mail einer Person mit Login geändert, so wird ein Mail mit Bestätigungslink an die **neue** E-Mail-Adresse gesendet. So wird sichergestellt, dass die neue Adresse funktioniert und die Person hinter der E-Mail-Adresse mit der Verwendung einverstanden ist. Die Haupt-E-Mail von Personen ohne aktiviertem Login lassen sich sofort ändern.

Die Bestätigung ist wichtig, da Hitobito als OAuth Provider genutzt werden kann und viele OAuth Dienste die E-Mail zur Identifikation nutzen. Ohne Bestätigung würde folgendes Angriffsszenario funktionieren:

1. Eine Person A loggt sich via hitobito bei einem Drittservice ein
2. Der Drittservice merkt sich A anhand der Haupt-E-Mailadresse
3. Eine Person X mit Schreibzugriff auf A bearbeitet A und löscht die Haupt-E-Mailadresse
4. Person X füllt bei sich selber die ehemalige Haupt-E-Mailadresse von Person A ein. *Dieser Schritt wird durch die aktuelle E-Mail-Verifikation verhindert.*
5. Person X verwendet beim Drittservice den „Login via hitobito“ und kann nun den dortigen Account von Person A übernehmen.

11.4 Wie werden Personen-Duplikate erkannt?

Wenn eine Person mehrfach erfasst wurde, dann kann man die Duplikate zusammenführen. Dazu gibt es auf dem „Personen“-Tab einer *Ebene* (z.B. Dachverband, Region, Ortsgruppe) einen Button „Duplikate“. Der Button ist nur für Personen mit sehr hohen Berechtigungen (`layer_and_below_full` oder `admin`) sichtbar.

Hitobito analysiert jede Nacht die Einträge in der Datenbank und ergänzt die Liste von Duplikaten. Zwei Personen zählen als Duplikate, wenn die Felder Vorname, Nachname, Firmenname, Postleitzahl und Geburtsdatum übereinstimmen (bei Postleitzahl und Geburtsdatum zählt es auch, wenn das Feld bei einer der Personen leer ist). Ein Beispiel: Anna Berger (PLZ 1000, Geburtsdatum 01.01.1970) wird als Duplikat von Anna Berger (ohne PLZ oder Geburtsdatum) erkannt. Anna (PLZ 1000, Geburtsdatum 01.01.1970) ohne Nachname ist hingegen kein Duplikat, der Nachname muss zwingend übereinstimmen oder bei beiden Personen leer sein.

Dieselbe Duplikatserkennung wird auch schon direkt während dem Import einer CSV-Datei angewendet. Dort bekommt man gleich während dem Import noch die Möglichkeit, auszuwählen welche Zeilen eine bestehende Person aktualisieren sollen und welche Zeilen wirklich neue Personen sind.

11.5 Wann wird welche Referenznummer verwendet?

Hitobito unterstützt sowohl die QR-Referenz wie die Creditor Reference (SCOR). Die QR-Referenz entspricht im Aufbau der ESR-Referenz (immer 26 numerische Zeichen gefolgt von einer Prüfziffer nach Modulo 10 rekursiv) und kann vom Rechnungssteller als strukturierte Referenz verwendet werden. Creditor Reference ist gemäss ISO-11649-Standard implementiert. Die Prüfziffer der Creditor Reference muss mit Modulo 97-10 berechnet werden. Weitere Infos unter <https://www.paymentstandards.ch/dam/downloads/ig-qr-bill-de.pdf>

Wenn keine QR-IBAN in Hitobito erfasst wurde, wird eine Creditor Reference (SCOR) bei der generierung von Rechnungen verwendet.

11.6 Über hitobito können verschiedene Mails verschickt werden. Welcher Absender wird da verwendet?

Wenn du ein Mail an ein Abo schickst, wirst du beim Empfänger auch als Absender angezeigt. Der technische Absender ist aber eine bounced Mailadresse pro Abo mit der Kundendomaine verwendet. Vom System generierte Mails wie Rechnungen, Passwortresets haben einen pro Instanz definierten Absender. Die Mails werden über den hitobito eigenen Mailserver (`mxout.appuio.puzzle.ch`) verschickt. Mittels SPF Eintrag sorgen wir dafür, dass dieser Mailserver im Namen der Kundendomaine verschicken darf.

11.7 Was bedeutet Hitobito

Hitobito kommt aus dem Japanischen und bedeutet Mensch. Durch die beiden ist die Mehrzahl gemeint: Menschen oder auch Gemeinschaft. Quelle: <https://www.wordsense.eu/%E4%BA%BA%E4%BA%BA/>