

**Diese Anleitung soll den FF-Agent Anwender durch die wichtigsten Schritte leiten,
wenn dieser seine Organisation einrichtet.**

Voraussetzung: Rechte Administrator

Folgende Schritte sind notwendig, damit ihre Organisation einsatzbereit ist:

1. Datenschutzerklärung prüfen
2. Personen anlegen/ migrieren
3. Alarmierungsart je Person definieren
4. Personengruppen für die Alarmierung anlegen
5. Alarmregeln definieren

Login

Der Login am FF-Agent System kann unter folgender Webadresse erfolgen:
<https://www.ff-agent.com/app>

Bei der Anmeldung muss auf Groß- und Kleinschreibung geachtet werden. Achten Sie darauf, dass weder zu Beginn, noch zu Ende des Kennwortes oder Benutzernamens Leerzeichen stehen. Dies kann sich beim Kopieren der Zugangsdaten aus anderen Dokumenten ergeben.

1. Datenschutzerklärung prüfen

Um den Datenschutz zwischen der Organisation und den Mitgliedern zu regeln, wird über das FF-Agent System bereits eine Datenschutzerklärung, im Sinne der DSGVO, mitgeliefert. Bevor Personen in das System übernommen werden, muss deren Datenschutzerklärung durch den Administrator geprüft und ggf. angepasst werden.

Wichtig:

Die bereitgestellte Datenschutzerklärung im FF-Agent System ist nur eine Vorlage die vom Betreiber der Organisation selbst geprüft und ggf. ergänzt werden muss. Das FF-Agent Team übernimmt keine Haftung, da es keine Rechtsberatung anbietet.

Beim Anlegen der Personen muss der Administrator der Datenschutzerklärung unter Angabe seines PIN-Codes zustimmen und dadurch sicherstellen, dass er selbst bei der anzulegenden Person vorab eine Zustimmung zur Datenschutzerklärung eingeholt hat, dass die angelegte Person die Datenschutzerklärung kennt.

Wird eine Person über eine Account-Anfrage in das System übernommen, muss die Person selbst der Datenschutzerklärung zustimmen. Dies wird auch im System dokumentiert.

Anpassen der Datenschutzerklärung:

Die Datenschutzerklärung kann in der FF-Agent WebUI wie folgt erreicht werden:

Admin > Einstellungen > Datenschutz

Im angezeigten Dialog kann die Datenschutzerklärung angepasst werden, d.h. neue Absätze hinzugefügt oder auch bestehende entfernt werden. Das Format des Dokuments ist in XWiki-Syntax (2.1) erstellt. Eine genauere Beschreibung des Formates finden Sie [hier](#).

Wichtig:

Sollte die Datenschutzerklärung nachträglich geändert werden, so muss jede bereits angelegte Person dieser erneut zustimmen. Der Administrator kann dies über eine Stapelfunktion unter Eingabe seines PIN-Codes durchführen. Dabei hat der Administrator selbst sicherzustellen, dass die Person die geänderte Datenschutzerklärung wirklich gesehen und dieser zugestimmt hat.

Deshalb ist es wichtig, dass die Datenschutzerklärung geprüft wurde, bevor mit dem Anlegen der Personen begonnen wird.

2. Personen anlegen/ migrieren

Es ist auf zweierlei Wegen möglich, Personen in der FF-Agent Organisation anzulegen:

- Personen manuell anlegen
- Personen über eine Account-Anfrage anlegen

Die Anlage der Person über eine Account-Anfrage ist aufgrund nachfolgender Vorteile dem manuellen Anlegen vorzuziehen:

- Jede Person kann die Account-Anfrage selbst ausfüllen.
- Die Zustimmung zur Datenschutzerklärung, sowie der Sichtbarkeitseinstellung der Daten erfolgt bereits im Account-Anfrage-Prozess.
- Die Person erhält ihre Zugangsdaten bereits personalisiert via E-Mail.
- Ein zeitraubendes Anlegen von Personen über den Administrator inklusive Vergabe und Kommunikation der Zugangsdaten entfällt, da hierbei jede Person selbst die notwendigen Daten eintragen muss. Für die Person selbst dauert der Vorgang nur wenige Minuten.

Nachfolgend eine Beschreibung der Erfassungsmöglichkeiten:

2.1 Personen manuell anlegen:

Eine Person kann in der WebUI aus der Personenliste welche wie folgt erreicht werden kann angelegt werden:

Personen > Personen

Über die Schaltfläche „Neu“ eine Person anlegen.

Folgende Felder sind auszufüllen:

- Vorname
- Nachname
- Optional: Geburtsdatum (Format tt.mm.jjjj, z.B. 21.06.1991)
- Optional: E-Mail
- Optional: Mobiltelefon (**notwendig für Alarm SMS und Alarmruf**)
- Rolle bei der Organisation, z.B. bei der Feuerwehr „Commander“
- Rolle im System (Standard oder Admin)

Zugangsdaten:

- Benutzername
- Kennwort
- Kennwort wiederholen (= Kennwort Bestätigung)

Beim nachfolgenden Datenschutzbereich kann definiert werden, wie die Sichtbarkeit der Personendaten für die verschiedenen Personenkreise definiert ist:

- Administrator
- Führungskreis (= Commander)
- Standard (alle Personen die nicht Administrator oder Führungskreis sind)

Zum Abschluss muss der Haken für „Ja, ich habe die Erlaubnis von der Person erhalten, die Datenschutzeinstellungen anzupassen und die Datenschutzerklärung zu akzeptieren.“ gesetzt sein. Daraufhin erscheint ein PIN-Dialog, in der der PIN des Administrators eingegeben werden muss, welcher gerade die Person anlegt (Achtung: nicht der PIN der angelegten Person).

Wichtig:

Wenn eine Person manuell angelegt wird, muss der Administrator selbst sicherstellen, dass die Person die Datenschutzerklärung gelesen und dieser zugestimmt hat und sich diese ggf. auch unterzeichnen lassen. Ebenso muss er der Person ihre Zugangsdaten auf einem vertraulichen Weg zukommen lassen.

2.2 Person über Account-Anfrage anlegen

Eine wesentlich elegantere und auch zeitsparendere Methode Personen im System anzulegen, ist der Weg über die Account-Anfrage.

Hierbei sieht der Prozess wie folgt aus:

1. Administrator gibt eine öffentliche Web-Adresse für das Account-Anfrage-Formular an seine Mitglieder weiter z.B.: über E-Mail.
2. Person ruft die Web-Adresse auf und füllt die notwendigen Daten in die Maske für die Account-Anfrage.
3. Administrator erhält eine E-Mail, dass eine neue Accountanfrage eingegangen ist und kann diese über einen Link aufrufen.
4. Administrator bewertet die Account-Anfrage und wenn diese legitim ist stimmt er dieser zu.
5. Das System legt die Person mit den Daten aus der Account-Anfrage an und versendet eine E-Mail mit allen notwendigen Daten an die Personen inkl. Download Link der App.
6. Person lädt die App, setzt ihr Kennwort und meldet sich an der App an und ist damit bereit für die Alarmierung.

Zum Abschluss des Prozesses sind folgende Punkte gegeben:

- Person ist im System angelegt
- Person hat Benutzername erhalten und selbst ein Kennwort gesetzt
- Person kann die App für Apple iOS und Google Android über einen Link herunterladen
- Person kennt ihren Sicherheits-PIN-Code
- Person ist über die App bereit für die Alarmierung
- Person hat der Datenschutzerklärung zugestimmt, die im System hinterlegt ist und hat die Sichtbarkeit ihrer Daten selbst definiert. Im System wird protokolliert wann und von welcher Person die Datenschutzeinstellungen geändert werden.

In der WebUI kann wie folgt die Account-Anfragen Liste aufgerufen werden:

Personen > Account-Anfragen

In dieser Liste laufen alle Account Anfragen auf. Hier kann der Administrator nach Prüfung der Daten die Account-Anfrage zu einer echten Person im System migrieren (über die Schaltfläche „jetzt migrieren“) oder die Anfrage löschen.

Eine Account-Anfrage hat noch keinerlei Berechtigung im System. Es ist immer eine manuelle Zustimmung eines Administrators notwendig, um eine Anfrage zu einer Person zu migrieren. Gefahrlos können mehrere Account-Anfrage auflaufen, bevor man diese migriert.

Die öffentliche Adresse für das Account-Anfrage-Formular ist auch in der Liste enthalten (beginnt mit: <https://www.ff-agent.com/app/accountRequest/>...).

Sobald die Person migriert wurde, erhält diese an die angegebene E-Mail Adresse eine Nachricht mit folgenden Inhalten:

- Nennung des Benutzernamens
- Link zum Setzen des Kennwortes
- Download Link für Apps (Android oder iOS)
- Anweisung die App zu installieren

Sobald eine Person die FF-Agent App erfolgreich installiert hat und damit auch alarmiert werden kann, wird diese in der Personenliste mit einem blauen Smartphone-Logo dargestellt. Personen mit noch nicht angemeldeter App erhalten ein graues Smartphone-Logo.

Der Benutzername wird durch das FF-Agent-System automatisch generiert. Hierbei wird der erste Buchstabe des Vornamens mit dem Nachnamen verbunden. „Stefan Meier“ wird zu „smeier“. Das System achtet automatisch darauf, dass die Benutzernamen immer eindeutig aufgebaut sind.

Sollte das Benutzernamenformat einem anderen Schema folgen, kann dies auch im FF-Agent unter folgendem Weg definiert werden:

Admin > Einstellungen > Allgemein > Reiter „User“

3. Alarmierungsart für Personen definieren

Wenn eine Person angelegt wurde, so ist diese zuerst über die Alarmierung mittels FF-Agent App eingerichtet. Neben der Push Benachrichtigung über die FF-Agent App kann auch ein Alarmruf über das FF-Agent System erfolgen.

Die Art der Alarmierung kann im Personen Profil unter dem Unterpunkt „Profil“ und dem Reiter „Alarmierung/ Benachrichtigung“ definiert werden.

Wichtig:

Eine Alarmierung über Alarmanruf erzeugt zusätzliche Kosten, die nicht von der Leitstelle übernommen werden. Um diese Funktion zu nutzen, muss die Organisation einen Nutzungsvertrag direkt mit dem FF-Agent Anbieter abgeschlossen haben. Die Nutzung wird per Alarmanruf berechnet.

Der Alarmanruf erfolgt immer über die gleiche Absendernummer und kann somit in einem Handy oder Smartphone mit einem speziellen Klingelton versehen werden.

Neben der direkten Alarmierung kann der Alarmanruf auch als Rückfallebene verwendet werden, wenn die App zum Zeitpunkt der Alarmierung über keine mobile Datenverbindung oder WLAN-Netz verfügt.

Die Rückfallalarmierung kann pro Person definiert werden. Damit diese jedoch überhaupt genutzt werden kann, muss diese unter **Admin > Einstellungen > Alarmierung > Reiter „Alarmierung“** im Bereich „Rückfallalarmierung“ aktiviert werden.

Technisch wird der App über die Push Benachrichtigung mitgeteilt, dass diese beim FF-Agent Dienst den Empfang zu bestätigen hat. Ist dies nicht innerhalb eines bestimmten Zeitraumes erfolgt, ruft der FF-Agent Dienst zusätzlich auf dem Smartphone an.

Eine Rückmeldung ist über den Alarmanruf ebenfalls möglich:

- „1“ – Zusagen zum Einsatz
- „2“ – Absage zum Einsatz

4. Personengruppe für Alarmierung anlegen

Falls Personengruppen abhängig von der Alarmierung alarmiert werden sollen, müssen zuerst die jeweiligen Gruppen hierfür angelegt werden.

Eine Personengruppe kann in der WebUI unter **Personen > Gruppen** angelegt werden. Mit der Schaltfläche „Neu“ wird die Maske zum Anlegen aufgerufen.

Hierbei ist wichtig, darauf zu achten, dass bei Funktionen ein Haken für „Alarmgruppe“ gesetzt ist.

Unter Mitglieder können dann einzelne Personen direkt ausgewählt und hinzugefügt werden.

Wichtig:

Eine Person gilt erst dann als selektiert, wenn diese im Popup ausgewählt und mit „hinzufügen“ der Liste hinzugefügt wurde. Neben dem Personennamen ist dann auch eine rote Schaltfläche mit einem **X** zu erkennen, mit der die Person wieder entfernt werden kann. Ein reines Auswählen der Person *ohne* die „hinzufügen“ Schaltfläche auszuführen selektiert die Person nicht!

Nach dem erfolgreichen Speichern kann die Personengruppe für die Alarmierung herangezogen werden.

5. Alarmregeln definieren

Eine Alarmregel verbindet das Alarmsignal mit der Personengruppe deren Personen den Alarm erhalten sollen.

Eine Alarmregel definiert dabei welche Personengruppe alarmiert werden soll. Dies ist quasi das Ziel der Regel.

Wann die Regel zum Greifen kommt, wird dann über zusätzliche Bedingungen definiert. Die Wichtigsten dabei sind:

- Anschluss (Alarmquelle)

Als Anschluss steht nur der eMID Anschluss zur Verfügung da dieser alle Einsatzdaten bereits beinhaltet.

- Einsatztypen:

Optional kann über die Angaben von Einsatztypen genauer gesteuert werden, ob die Regel greifen soll. So kann z.B. ein THL1 Einsatztyp verwendet werden, um eine begrenzte Personengruppe zu alarmieren. Ist kein Einsatztyp definiert, wird die Regel bei jedem Einsatztyp die hinterlegte Personengruppe alarmieren.

Alarmregel Test

Über den Konfigurationstest lässt sich sehr einfach herausfinden welche Personengruppe bei einem Stichwort alarmiert werden würde. Hierbei wird die Alarmierung nur simuliert, eine tatsächliche Alarmierung erfolgt nicht.

Dieser ist in der WebUI zu finden unter:

Admin > Einsatzplanung/ -konfiguration > Konfigurationstest

Als Stichwort muss eine Kennziffer nach Alarmierungsbekanntmachung, kurz ABek (in der aktuellen Fassung) angegeben werden, beispielsweise „B1017“. Alternativ kann diese auch freigelassen werden. Als Alarmierungsquelle der sogenannte „eMID Anschluss“.

Mit der Schaltfläche „jetzt testen“ wird das Testergebnis angezeigt und ersichtlich, welche Alarmregel verwendet wurde und welche Personengruppen alarmiert worden wären.

Weitergehende Unterstützung

Sollten Fragen zur Einrichtung über die Anleitung hinaus auftreten, können Sie mit unserem FF-Agent Support Team in Kontakt treten.

Dieses erreichen Sie per E-Mail unter: support@ff-agent.com