FOCUS FAMILY

Handbuch für das Admin-Panel

Verwaltung, Leitung und Datenschutz – Schritt für Schritt erklärt

Version 1.3.0 · Stand November 2026 · Software Notion

Inhaltsverzeichnis

1. **Willkommen**
    1. Wofür das Panel da ist
    2. Was das Panel ausdrücklich nicht ist
2. **Anmelden und Grundlagen**
    1. Suchen und filtern
3. **Rollen und Rechte**
    1. Die zwei Ebenen
    2. Einzelne Rechte
    3. Leitungsbereich
4. **Benutzer verwalten**
    1. Neuen Benutzer anlegen
    2. Rechte vergeben
    3. Konten ohne Rechte
    4. Bearbeiten, deaktivieren, Passwort ändern
    5. Einrichtung per QR-Code
    6. Zwei-Faktor-Anmeldung (MFA) einrichten
    7. Passkey-Anmeldung (passwortlos)
    8. Anmeldung über die Organisation (SSO)
5. **Teams und Fallzuweisung**
6. **Bereiche (bereichsorientiertes Arbeiten)**
    1. Grundregeln
    2. Einrichten
    3. Organisation im Bereichsmodus
    4. Ausschalten
    5. Bewegungen
7. **Fälle**
    1. Fall anlegen und zuweisen
    2. Beteiligte und Anschriften
    3. Roadmap, Ziele und Prüfpunkte
    4. Vertretung
    5. Fall übertragen
    6. Termine, Aufgaben und Medien im Fall
    7. Verlauf eines Falls
8. **Schnittstellen: Eingänge und Übergabe**
    1. Eingänge prüfen
    2. Herkunft eingelieferter Dokumente
    3. An Zielsystem übergeben

4. Kalender-Abo

9. **Planung**
10. **Zeiterfassung**
11. **Tätigkeitsnachweise**
    1. Abschließen und wieder öffnen
    2. Kennzeichnung und Nachweis-Archiv
12. **Geräte**
    1. Lizenzplätze
13. **Richtlinien**
14. **Hilfe & Kontakt**
15. **Verwaltete Einstellungen**
    1. Abrechnungsbasis
16. **Rechnungssteller**
17. **Vorlagen und Export-Profile**
18. **Textbausteine**
19. **Kataloge: Institutionen, Maßnahmen, Tätigkeitsarten**
    1. Institutionen
    2. Maßnahmenkatalog
    3. Tätigkeitsarten
20. **Kalender & Belegungen im Fall**
21. **Kontaktkarten und Vertretungen**
    1. Wer darf was?
    2. Träger-Kontaktdaten
    3. Kontaktkarten der Fachkräfte
    4. Vertretungen
22. **Löschanfragen**
23. **Datenschutz: Betroffenenanfragen und Dokumente**
    1. Einrichtung
    2. Vor der ersten Anfrage: Dokumente erzeugen
    3. Eine Anfrage bearbeiten
24. **Sicherheits-Audit**
25. **Absturzberichte und Desktop-Downloads**
26. **Datenschutz und Grenzen des Panels**
27. **Häufige Fragen**

Willkommen

Das **Admin-Panel** ist die Web-Verwaltung des Focus-Family-Servers Ihres Trägers. Sie erreichen es im Browser unter der Adresse Ihres Servers mit dem Zusatz `/admin`.

Dieses Handbuch richtet sich an **Verwaltung, Leitung und Datenschutzbeauftragte**. Es setzt keine technischen Vorkenntnisse voraus. Die Einrichtung und der Betrieb des Servers selbst stehen im **technischen Handbuch**.

Wofür das Panel da ist

Sie verwalten hier die organisatorische Seite Ihrer Arbeit:

- Fachkräfte, deren Zugänge und Rechte,
- Teams und die Zuweisung von Fällen,
- die gemeinsame Planung (Termine und Aufgaben),
- Zeiterfassung und Tätigkeitsnachweise,
- Geräte, Richtlinien und zentrale Einstellungen,
- Vorlagen, Textbausteine und Kataloge,
- Löschanfragen und Datenschutz-Vorgänge.

Was das Panel ausdrücklich nicht ist

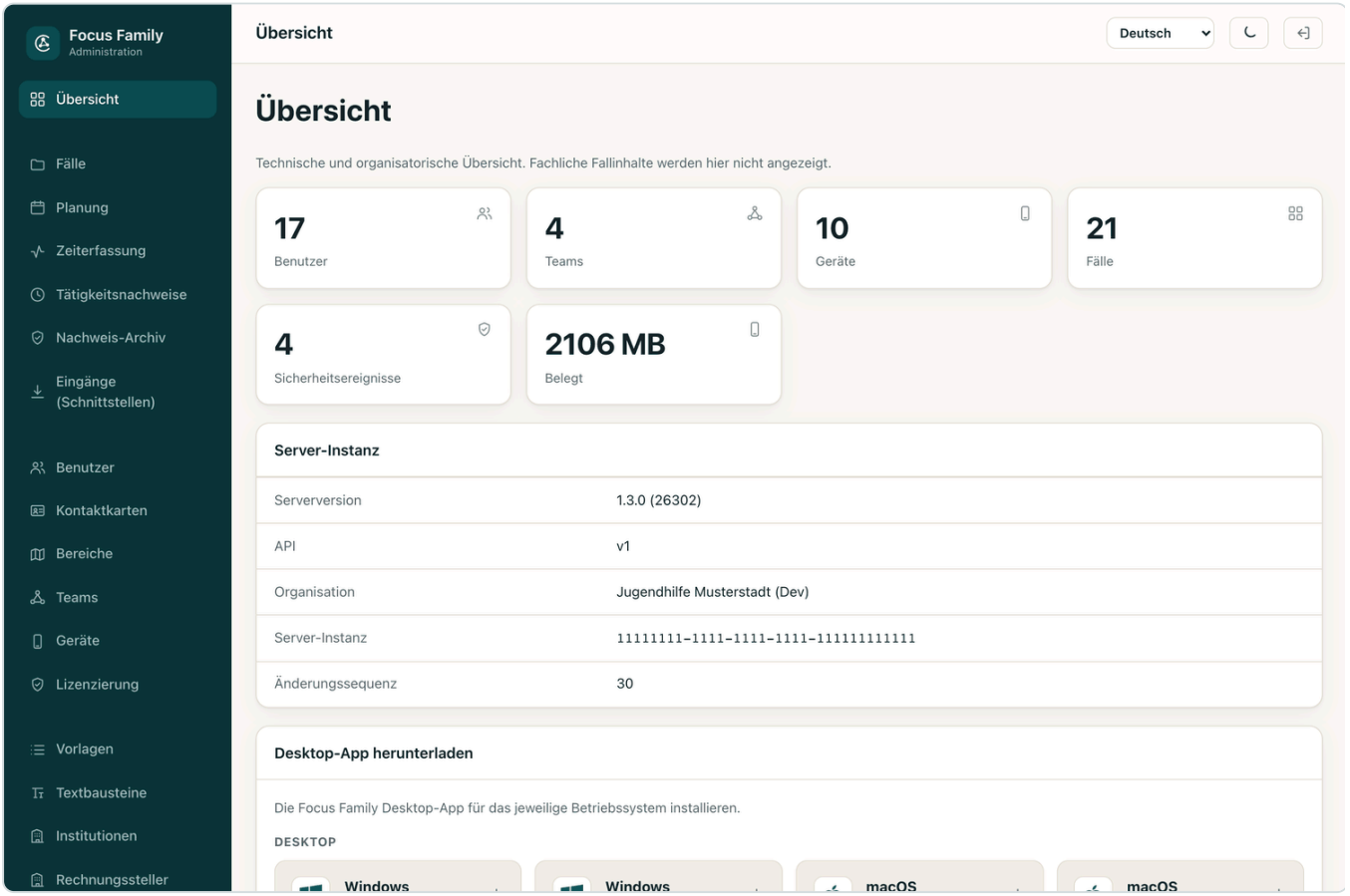
- Es ist **keine zweite Fachdokumentation**. Die fachliche Arbeit – Notizen, Einschätzungen, Verläufe – findet in der App der Fachkräfte statt.
- Administratorinnen und Administratoren sehen **keine privaten Inhalte**. Als „privat" markierte Einträge bleiben ausgeblendet.
- **Technische Administration** sieht **keine** Fälle und keine Termine.

Anmelden und Grundlagen

1. Öffnen Sie im Browser die Adresse Ihres Servers mit dem Zusatz `/admin`.
2. Geben Sie **E-Mail** und **Passwort** ein und klicken Sie auf **Anmelden**.
3. Ist für Ihr Konto die Zwei-Faktor-Anmeldung (MFA) aktiv oder per Richtlinie Pflicht, fragt das Panel zusätzlich den **6-stelligen Code** aus Ihrer Authenticator-App ab.
4. Nutzt Ihr Konto die **Passkey-Anmeldung**, bestätigen Sie stattdessen mit Fingerabdruck, Gesicht oder Sicherheitsschlüssel.
5. Verwendet Ihr Konto noch ein **Startpasswort** – etwa bei den bei der Installation angelegten Admin-Konten oder nachdem ein Admin Ihr Passwort mit Änderungspflicht gesetzt hat –, öffnet sich zuerst **Passwort ändern**. Geben Sie das bisherige und zweimal ein neues Passwort ein; vorher ist keine andere Seite erreichbar. Melden Sie sich in der App an, setzt sie die Anmeldung dafür im Browser fort.

Oben rechts schalten Sie die **Sprache** um (Deutsch, English, Español, Français), wechseln zwischen **hellem und dunklem** Erscheinungsbild und melden sich ab.

> **Wichtig: Technische Admin-Konten** können sich **nicht in den Apps anmelden**. Für die App-Nutzung braucht jede Person ein **Fachkraft-Konto**.



Die Übersicht zeigt Kennzahlen, Angaben zur Server-Instanz und die Downloads der Desktop-App. Links steht die Navigation; welche Punkte sichtbar sind, hängt von Ihren Rechten ab.

Suchen und filtern

Alle längeren Listen haben oberhalb der Einträge dieselbe **Filterleiste**: links ein Suchfeld, daneben die passenden Auswahlfelder. Die Auswahl wirkt sofort; Suchbegriffe bestätigen Sie mit **Filtern** oder der Eingabetaste. **Filter zurücksetzen** zeigt wieder alles. Findet der Filter nichts, steht dort **Keine Treffer.** Die Filter stehen in der Adresszeile, Sie können eine gefilterte Ansicht also als Lesezeichen speichern oder weitergeben. Gefiltert wird nur innerhalb dessen, was Sie ohnehin sehen dürfen.

Seite	Suche	Filter
Fälle	Bezeichnung, Aktenzeichen, Schlagworte, Amt, ASD-Fachkraft	Status, Hilfeart, Fachkraft (Eigentümer oder zugewiesen), Team
Planung	Titel, Ort, Fall, Fachkraft	Fachkraft, Fall; bei Terminen Terminart, Status, Zeitraum; bei Aufgaben Status, Priorität, Fälligkeit (überfällig, heute, nächste 7 Tage, ohne Datum), Zeitraum
Zeiterfassung	Notiz, Tätigkeit, Fall, Fachkraft	Fachkraft, Fall, Art, Abrechnungsstatus, Zeitraum
Benutzer	Name, E-Mail	Status, Kontoart
Geräte	Gerätename, Person, Version, IP	Freigabe, Plattform
Audit	Aktion, Ziel, Korrelation	Aktion, Person, Ergebnis, Zeitraum
Kontaktkarten	Name, Funktion, Telefon, E-Mail	–
Absturzberichte	Fehlertyp, Kontext	Gerät, Version, Plattform

Textbausteine, Institutionen, Maßnahmenkatalog, Tätigkeitsarten, Tätigkeitsnachweise und das Datenschutz-Protokoll haben eigene Filter in derselben Leiste.

Rollen und Rechte

Focus Family trennt die Verwaltung in zwei Bereiche. So kann die IT die Technik betreuen, ohne fachliche Fallinhalte zu sehen – und die Fachleitung kann fachlich verwalten, ohne Servertechnik anfassen zu müssen.

Die zwei Ebenen

Ebene	Darf	Sieht
System-Admin (Technik)	alle technischen Rechte nutzen und vergeben	keine Fälle, keine Termine
Fach-Admin (fachlich)	alle fachlichen Rechte nutzen und vergeben	Fallinhalte, außer privaten Einträgen

Wer beide Ebenen hat, kann alles vergeben.

Einzelne Rechte

Zusätzlich lassen sich **einzelne Rechte** gezielt vergeben. Zwei Regeln gelten immer:

- **„Bearbeiten" schließt „Ansehen" ein.**
- Sie können **nur Rechte aus Ihrem eigenen Bereich** vergeben. Die **allgemeinen Rechte** dürfen Fach- und System-Admins vergeben.
- **Rechte-Obergrenze:** Konten, die Rechte außerhalb des eigenen Vergaberahmens besitzen, lassen sich weder bearbeiten noch deaktivieren, noch lassen sich ihr Passwort, MFA, Passkeys, Einrichtungs-QR oder Anmeldeverfahren ändern. Das Panel meldet dann „Dieses Konto hat

Berechtigungen außerhalb des eigenen Vergaberahmens und kann deshalb hier nicht geändert werden.“ Technische Konten ändert nur, wer *Technische Admins verwalten* hat.

Fachliche Rechte

Recht	Bedeutung
Fälle ansehen / bearbeiten	Fälle einsehen bzw. anlegen und ändern
Kalender ansehen / bearbeiten	Termine einsehen bzw. verwalten
Aufgaben ansehen / bearbeiten	Aufgaben einsehen bzw. verwalten
Zeiterfassung ansehen / erfassen	Zeiteinträge einsehen bzw. eigene anlegen und ändern
Nachweise verwalten	Zeiteinträge und Nachweise **anderer** Fachkräfte im eigenen Leitungsbereich bearbeiten (schließt „Zeiterfassung ansehen" ein)
Nachweise abschließen	vergangene Monate/Jahre abschließen und mit Begründung wieder öffnen (schließt „Nachweise verwalten" ein)
Verwaltete Einstellungen ansehen / bearbeiten	zentrale, in der App gesperrte Werte pflegen
Fachkräfte verwalten	Benutzerkonten anlegen und pflegen
Teams verwalten	Teams und Mitglieder pflegen
Anderen zuweisen	Fälle anderen Personen zuweisen, Vertretungen anlegen
Notfallzugriff (Break-Glass)	zeitlich begrenzter Ausnahmezugriff auf einen Fall
Vorlagen & Export-Profile verwalten	zentrale DOCX-Vorlagen und Export-Profile pflegen
Textbausteine ansehen / erstellen / verwalten	zentrale Textbausteine pflegen
Beträge sehen	Geldbeträge in Rechnungsentwürfen einsehen
Löschanfragen prüfen	über gelöschte Daten entscheiden
Eingänge aus Schnittstellen prüfen und übernehmen	Seite **Eingänge (Schnittstellen)** nutzen: Eingänge prüfen und ablehnen, mit zusätzlich „Fälle bearbeiten“ auch Fällen zuordnen und übernehmen (schließt „Fälle ansehen“ ein; im Fach-Admin enthalten)
Setup-QR anzeigen	Einrichtungs-QR für Fachkräfte erzeugen
Bereiche verwalten	Bereichsmodus ein- und ausschalten, Bereiche pflegen, Fachkräfte und Teams zuordnen, Verwaltungsumfang vergeben (nur mit organisationsweitem Umfang; im Fach-Admin enthalten)
Rechnungsdaten verwalten	zentrale Rechnungssteller-Daten für E-Rechnungen pflegen (Seite *Rechnungssteller*; im Fach-Admin enthalten)
E-Rechnungen erstellen	reines App-Recht: in der App E-Rechnungen erstellen und dafür die zentralen Rechnungsdaten erhalten (öffnet kein Panel; im Fach-Admin enthalten)

Technische Rechte

Recht	Bedeutung
System-Konfiguration	technische Grundeinstellungen
Richtlinien ansehen / bearbeiten	Organisationsrichtlinien pflegen
Geräte ansehen / verwalten	Geräteverbindungen einsehen, freigeben, sperren
Technische Admins verwalten	IT-Administration pflegen – regelt auch das **Entfernen von MFA und Passkeys**
Sicherheits-Audit ansehen	Sicherheitsprotokoll einsehen
System-Status ansehen	technische Auslastung einsehen
Monitoring konfigurieren	Überwachungsschnittstelle einschalten, Zugriffsschlüssel erzeugen und auf Adressbereiche begrenzen
Absturzberichte ansehen	technische Fehlerberichte der Apps einsehen
Absturzberichte verwalten	einzelne oder alle Absturzberichte löschen (schließt Ansehen ein)
Desktop-App herunterladen	Installationspakete im Panel herunterladen
Single Sign-On verwalten	Anmeldung über den Identitätsanbieter der Organisation einrichten, testen und erzwingen (im System-Admin enthalten)
Schnittstellen verwalten (REST-Clients, CMIS, XÖV, Webhooks, SCIM, SIEM)	Anbindung an Fachverfahren, Dokumentenmanagement, XÖV-Empfänger, Webhooks, SCIM, Kalender-Abos und SIEM einrichten (im System-Admin enthalten; Freigabe von Datenflüssen mit Falldaten durch die Datenschutzrolle)

> Das Entfernen der Zwei-Faktor-Anmeldung oder eines Passkeys ist **nur mit dem Recht „Technische Admins verwalten"** möglich.

Allgemeine Rechte

Recht	Bedeutung
Lizenzierung verwalten (zuweisen)	Lizenzplätze Fachkräften zuweisen und entziehen, Lizenzgeräte entfernen und wiederherstellen
Lizenzierung erwerben	Plätze und Abo verwalten – Plätze dazukaufen oder reduzieren, Zahlungsintervall ändern, kündigen (schließt „verwalten" ein)

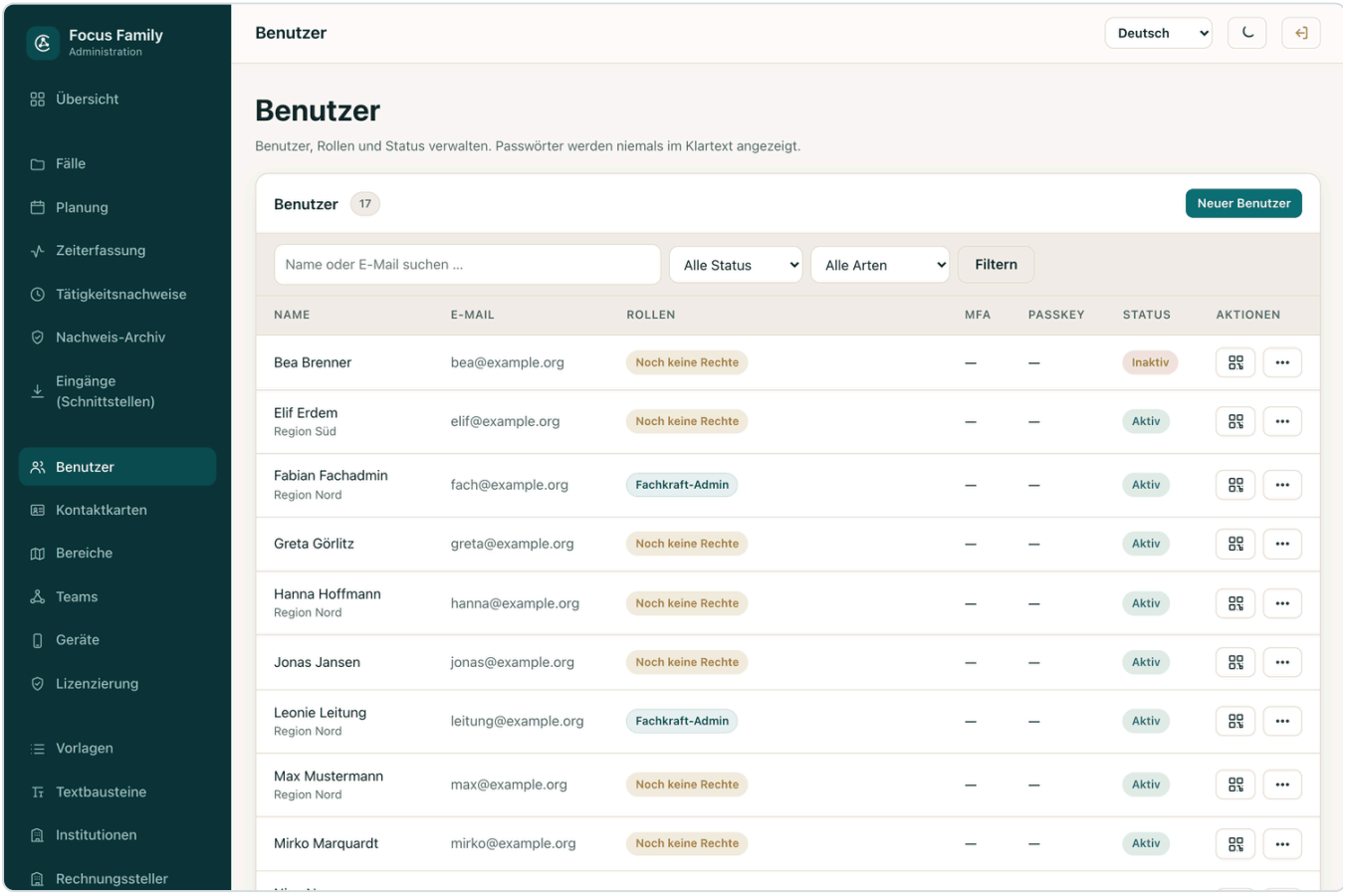
Die bei der Installation angelegten Fach- und technischen Admins erhalten beide Lizenzrechte. Wer im Rechte-Dialog **Fach-Admin** oder **System-Admin** anhakt, bekommt sie vorausgewählt und kann sie bei Bedarf wieder abwählen.

Leitungsbereich

Die beiden Nachweis-Rechte wirken nur im **Leitungsbereich** der Person: in den Teams, in denen sie als **Teamleitung** eingetragen ist, mit deren Mitgliedern und zugewiesenen Fällen. Ein **Fach-Admin** hat automatisch die ganze Organisation als Leitungsbereich; im eingeschalteten Bereichsmodus beschränkt sich das bei bereichsgebundenen Konten auf deren Bereiche (siehe „Bereiche“). Lesen bleibt für alle mit „Zeiterfassung ansehen" organisationsweit möglich.

Benutzer verwalten

Menüpunkt **Benutzer** (Recht *Fachkräfte verwalten*). Passwörter werden nie im Klartext angezeigt.



Die Benutzerliste mit Name und Bereichen, E-Mail, Rollen, Status und Passkey-Zustand. Über das Menü rechts erreichen Sie alle Aktionen zu einer Person.

Neuen Benutzer anlegen

1. **Neuer Benutzer** klicken.
2. **Anzeigename**, **E-Mail** und ein **Passwort** eintragen. Das Passwort braucht mindestens 12 Zeichen mit Groß- und Kleinbuchstaben, einer Ziffer und einem Sonderzeichen; **Passwort erzeugen** füllt beide Felder.
3. Optional **Bei der nächsten Anmeldung Passwortänderung verlangen** anhaken (standardmäßig aus) – dann ersetzt die Person das Passwort bei der ersten Anmeldung durch ein eigenes.
4. **Rechte** festlegen (siehe unten). Ob sich die Person in der App anmelden darf, ergibt sich aus den Rechten: Ohne fachliche Rechte bleibt es bei der reinen Verwaltung.
5. **Anlegen**.

Rechte vergeben

1. Benutzer öffnen und zum Bereich **Rechte** gehen.
2. Die Rechte sind in **Fachlich**, **System / Technik** und **Datenschutz** gruppiert. Sie sehen nur die Gruppen und Rechte, die Sie selbst vergeben dürfen; ein technischer Admin sieht zum Beispiel keine fachlichen Rechte.

3. **Vorlagen** setzen mehrere Häkchen auf einmal: **Fachkraft** und **Teamleitung** erscheinen nur, wenn Sie alle enthaltenen Rechte vergeben dürfen; **Nur Lesen** umfasst die Leserechte aus Ihrem Bereich. **Zurücksetzen** stellt den Stand beim Öffnen wieder her – bei einem bestehenden Konto dessen aktuelle Rechte, bei einem neuen Konto keine.
4. Häkchen setzen und **Speichern**.

Konten ohne Rechte

Konten ganz ohne Rechte – typischerweise nach der ersten SSO-Anmeldung mit automatischer Kontoanlage – tragen in der Benutzerliste das Badge **Noch keine Rechte**. In der Auswahl **Kontoart** zeigt **Ohne Rechte** nur diese Konten.

Solange ein Konto keine Verwaltungsrechte hat (auch Fachkräfte mit reinen App-Rechten wie *Textbausteine lesen*), sieht die Person nach der Anmeldung eine **Willkommensseite**: Anmeldung erfolgreich, noch keine Verwaltungsrechte, eigene Kontaktdaten hier pflegbar. Das Menü enthält nur **Start**, **Meine Kontaktdaten** und **Hilfe & Kontakt**, oben Sprache und Abmelden; lokale Konten finden auf der Willkommensseite außerdem **Kontosicherheit** (MFA, Passkey). Alle anderen Seiten und Aktionen weist der Server ab und zeigt **Zugriff verweigert** mit dem Link **Zur Startseite**. MFA-Pflicht und Passwortwechsel gelten unverändert. Sobald Sie Rechte vergeben, erscheinen die zugehörigen Menüpunkte beim nächsten Seitenaufruf.

Bearbeiten, deaktivieren, Passwort ändern

- **Bearbeiten** – Anzeigename und Einstellungen anpassen.
- **Aktivieren / Deaktivieren** – ein deaktiviertes Konto kann sich nicht mehr anmelden. Der Zugriff endet sofort: Panel-Sitzungen und App-Anmeldungen werden widerrufen, die Synchronisation weist die Geräte der Person ab dem nächsten Kontakt ab. Ihr eigenes Konto können Sie nicht deaktivieren.
- **Passwort ändern** – neues Passwort zweimal eingeben. **Bei der nächsten Anmeldung Passwortänderung verlangen** ist bei anderen Konten voreingestellt; dann vergibt die Person beim nächsten Anmelden ein eigenes Passwort. Ohne Haken gilt das gesetzte Passwort unverändert weiter. Bestehende Panel-Sitzungen der Person werden innerhalb einer Minute beendet. Bei Ihrem **eigenen** Konto ist die Option nicht angehakt und Sie bleiben angemeldet; setzen Sie den Haken, meldet das Panel Sie ab und verlangt die Änderung bei der nächsten Anmeldung.

Einrichtung per QR-Code

Damit eine neue Fachkraft weder Serveradresse noch Zugangsdaten abtippen muss (Recht *Setup-QR anzeigen*):

1. Benutzer öffnen und **Setup-QR anzeigen** wählen.
2. Der QR-Code ist **zeitlich begrenzt** gültig und **nur einmal** verwendbar. Beim Ausstellen wird das bisherige Passwort in einem Schritt durch ein Einmalpasswort ersetzt.
3. Die Fachkraft scannt den Code in ihrer App unter **Server verbinden**.
4. Die App richtet Verbindung und Anmeldung automatisch ein; danach vergibt die Person ein eigenes Passwort.

> **Sicherheitshinweis:** Der Setup-QR ist sensibel. Zeigen Sie ihn nur der richtigen Person, versenden Sie ihn nicht über unsichere Kanäle und lassen Sie ihn nicht offen liegen. Er verfällt nach kurzer Zeit von selbst.

Zwei-Faktor-Anmeldung (MFA) einrichten

Die Focus-Family-App und die Authenticator-App laufen meist auf **demselben Telefon** – und ein Gerät kann seinen eigenen Bildschirm nicht abfotografieren. Deshalb zeigen Sie den Einrichtungs-Code im Panel auf einem zweiten Bildschirm an.

1. **Benutzer** öffnen und **MFA einrichten** wählen.
2. Es erscheinen ein **QR-Code** und ein **Schlüssel** zur manuellen Eingabe.
3. Die Fachkraft scannt den Code mit ihrer Authenticator-App (z. B. Google oder Microsoft Authenticator).
4. Den angezeigten **6-stelligen Code** im Feld **Code** eintragen und auf **Bestätigen & aktivieren** klicken.

Ob MFA **verpflichtend** ist, legen Sie zentral unter **Richtlinien** fest. Die Pflicht gilt für Apps **und** für das Admin-Panel.

Passkey-Anmeldung (passwortlos)

Alternativ kann ein Konto auf **Passkeys** umgestellt werden – Anmeldung mit Fingerabdruck, Gesichtserkennung oder Sicherheitsschlüssel.

1. Im Menü der Person **Passkey-Anmeldung aktivieren**. In der Spalte **Passkey** steht danach **Ausstehend**.
2. Beim nächsten Login wird die Person zur Seite **Passkey einrichten** geführt. Danach steht dort **Aktiv**.
3. Sobald ein Passkey hinterlegt ist, **funktioniert das Passwort für dieses Konto nicht mehr**.
4. **Passkeys anzeigen** listet alle hinterlegten Passkeys. Ein weiterer Passkey (z. B. für ein zweites Gerät) verlangt die Bestätigung mit einem vorhandenen.
5. Bei aktivem Passkey sind **Passwort setzen** und **MFA einrichten** ausgegraut – sie wirken erst nach einem Passkey-Reset.

> **Passkey zurücksetzen** und das Entfernen einzelner Passkeys sind – wie das Entfernen von MFA – nur mit dem Recht **Technische Admins verwalten** möglich, etwa bei Geräteverlust. Beide melden die Sitzungen der Person sofort ab; setzen Sie danach am besten gleich ein neues Passwort.

Anmeldung über die Organisation (SSO)

Ist Single Sign-On eingerichtet (siehe technisches Handbuch), zeigt die Anmeldeseite zusätzlich die Schaltfläche **Mit … anmelden** (mit dem Namen des Identitätsanbieters). Konten, die sich so anmelden, tragen in der Benutzerliste das Badge **SSO**; in den Spalten MFA und Passkey steht **beim Identitätsanbieter**.

1. **Neues SSO-Konto** legt ein Konto ohne Passwort an (Name, E-Mail bzw. UPN, Rechte, Bereich). Rechte und Lizenzplatz können Sie sofort vergeben. Bis zur ersten Anmeldung steht am Badge **ausstehend**; dann wird das Konto über die vom Identitätsanbieter bestätigte E-Mail-Adresse verknüpft. Bestätigt der Anbieter die Adresse nicht, gibt eine Administration mit den Rechten „Single Sign-On verwalten“ und Benutzerverwaltung die Erstanmeldung unter **Single Sign-On → Erstanmeldung freigeben** für 24 Stunden frei.
2. Bestehende Konten stellen Sie im Menü der Person unter **Anmeldeverfahren → Auf SSO umstellen** um. Passwort, MFA, Passkeys und offene QR-Codes werden entfernt, alle Sitzungen beendet;

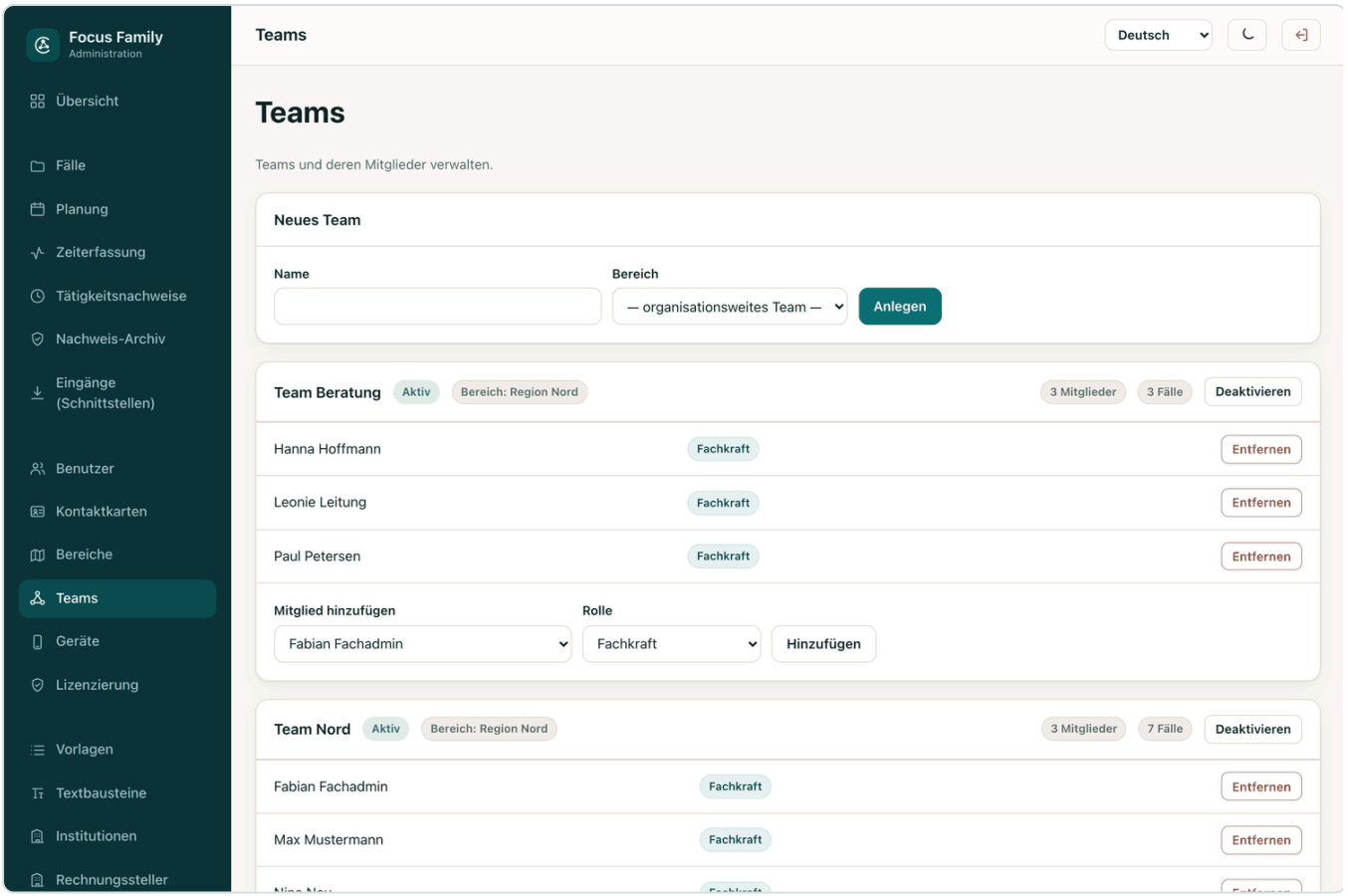
Rechte und Lizenzplatz bleiben.

3. Für SSO-Konten gibt es kein **Passwort setzen**, kein **MFA einrichten**, keine Passkeys und keinen Einrichtungs-QR-Code – das verwaltet der Identitätsanbieter.
4. **Verknüpfung lösen** hilft nach einem Wechsel des Identitätsanbieters; **Auf lokale Anmeldung umstellen** macht das Konto wieder zu einem Passwortkonto (danach Passwort vergeben).
5. Ist die automatische Kontoanlage eingeschaltet, erscheinen neue Personen nach ihrer ersten Anmeldung ohne Rechte und ohne Lizenzplatz in der Liste (Badge **Noch keine Rechte**, Filter **Ohne Rechte**). Bis dahin erreichen sie im Panel nur die Willkommensseite und **Meine Kontaktdaten** (siehe *Konten ohne Rechte*). Vergeben Sie Rechte und Lizenzplatz, bevor die Person die App nutzt.
6. Ist **SSO erzwingen** eingeschaltet, werden beim Einschalten alle lokalen Sitzungen und App-Anmeldungen beendet. App und Desktop bieten danach nur noch **Mit Organisationskonto anmelden** an; Adressen aus den SSO-Domains werden immer zum Identitätsanbieter geleitet.

> Ihr eigenes Anmeldeverfahren können Sie nicht selbst umstellen. Mindestens ein lokales Systemadministrationskonto mit Passwort bleibt immer erhalten (Notfallzugang). Auch bei erzwungenem SSO meldet es sich mit Passwort an – ausschließlich im Admin-Panel, nicht in den Apps.

Teams und Fallzuweisung

Menüpunkt **Teams** (Recht *Teams verwalten*). Teams bündeln Fachkräfte, damit Fälle bequem an mehrere Personen gleichzeitig zugewiesen werden können.



Teams mit ihren Mitgliedern. Die Rolle „Teamleitung" legt zugleich den Leitungsbereich für die Nachweis-Rechte fest.

1. **Neues Team** anlegen und benennen.
2. Über **Mitglied hinzufügen** Fachkräfte aufnehmen, über **Entfernen** wieder herausnehmen.
3. Die Rolle **Teamleitung** wirkt über die Teamverwaltung hinaus: Sie bestimmt den **Leitungsbereich** für „Nachweise verwalten" und „Nachweise abschließen".

Fälle können Sie einem **Team** oder einzelnen **Fachkräften** zuweisen. Eine App zeigt immer nur die Fälle, die der jeweiligen Person zugewiesen sind.

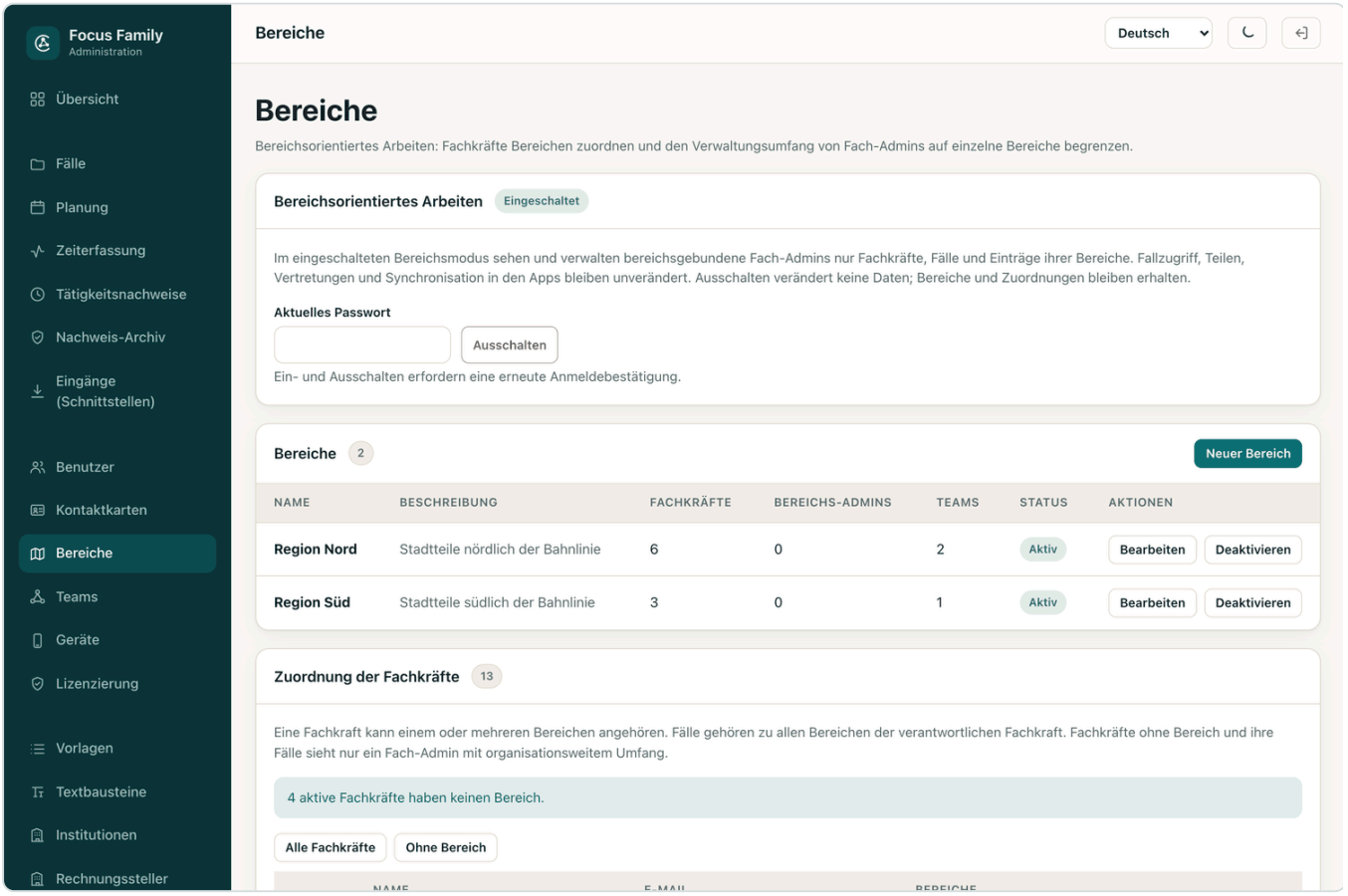
Gibt es **Bereiche** (siehe unten), kann ein Team einem Bereich angehören. Ein solches **Bereichs-Team** nimmt nur Fachkräfte desselben Bereichs auf; Teams ohne Bereich sind organisationsweite Teams. Beim Anlegen wählt ein Gesamt-Admin den Bereich optional aus, ein bereichsgebundener Admin legt Teams immer in seinem Bereich an.

> Entfernen Sie jemanden aus einem Team, verliert dessen Gerät beim **nächsten Sync** den Zugriff auf Fälle, die es nur über dieses Team erreicht hat.

Bereiche (bereichsorientiertes Arbeiten)

Menüpunkt **Bereiche** – sichtbar für Konten mit dem Recht **Bereiche verwalten** und **organisationsweitem Umfang** (das Recht ist im Fach-Admin enthalten und lässt sich in der Rechteliste unter **Bereiche** auch einzeln vergeben). Große Träger können ihre Fachkräfte in **Bereiche** (z. B. Regionen, Abteilungen, Standorte) gliedern und Fach-Admins auf einzelne Bereiche beschränken. Ein Bereich ist eine reine

Verwaltungsgrenze: Fallzugriff, Teilen, Vertretungen und die Synchronisation in den Apps ändern sich dadurch nicht.



Bereichsmodus, Bereiche und die Zuordnung der Fachkräfte; eine Fachkraft kann mehreren Bereichen angehören.

Grundregeln

- **Bereichsmodus**: Organisationseinstellung, **standardmäßig aus**. Solange er aus ist, verhält sich das Panel für alle Konten wie ohne Bereiche.
- **Fachkraft**: gehört **einem oder mehreren** Bereichen an; einer davon ist ihr **Hauptbereich**. Ein **Fall** gehört zu allen Bereichen seiner **verantwortlichen Fachkraft**; eine Übertragung an eine Fachkraft anderer Bereiche verschiebt den Fall mit. Die Admins jedes dieser Bereiche sehen die Fachkraft und ihre Fälle.
- **Verwaltungsumfang** eines Kontos mit fachlichen Verwaltungsrechten: **Gesamt** (organisationsweit) oder **ein oder mehrere Bereiche**. Ein bereichsgebundenes Konto sieht in Fällen, Fallansicht, Benutzerliste und Dashboard nur Fachkräfte und Fälle seiner Bereiche (plus sich selbst); fremde Datensätze verhalten sich wie nicht vorhanden. Aktionen auf fremde Ziele werden mit „nicht gefunden“ abgelehnt und im Audit als „Zugriff außerhalb des Bereichs abgelehnt“ vermerkt.
- **Fail-closed**: Fachkräfte ohne Bereich und deren Fälle sieht nur ein Gesamt-Admin. Ein Konto mit Verwaltungsrechten **ohne** Verwaltungsumfang sieht keine fachlichen Daten; das Panel zeigt dazu einen Hinweis.
- **Bereichsgebundene Admins** ändern nur Konten, deren Bereiche und bereichsgebundene Teams **vollständig** im eigenen Umfang liegen und die keine Rechte über die eigenen hinaus besitzen; zum bloßen Ansehen genügt ein gemeinsamer Bereich. Sie vergeben nie **Fach-Admin** oder **Bereiche verwalten** – Fach-Admins legt nur ein Gesamt-Admin an.

- **Fachkräfte ohne Admin-Rolle** (weder Fach- noch System-Admin), die Panel-Rechte wie *Fälle ansehen* haben und keinen eigenen Verwaltungsumfang erhalten haben, sind automatisch für ihre **eigenen aktiven Bereiche** zuständig; ohne Bereich sehen auch sie nichts.
- Bereichsgebundene Konten können **keine** Rechte für **Audit-Protokoll**, **Lizenz** oder **Datenschutz** erhalten. Technische Admins und Datenschutz-Admins ohne fachliche Rechte sind vom Bereichsmodus nicht betroffen.
- Seiten, die für den Bereichsmodus noch nicht eingerichtet sind, blenden sich für bereichsgebundene Konten mit einem Hinweis aus.

Einrichten

1. **Bereiche** anlegen (**Neuer Bereich**; Name eindeutig, Beschreibung optional). Bearbeiten, Deaktivieren und Löschen stehen in der Liste; gelöscht werden kann nur ein Bereich ohne Fachkräfte, Admins und Teams. Ein deaktivierter Bereich gewährt keinen Verwaltungsumfang mehr.
2. Unter **Zuordnung der Fachkräfte** Fachkräfte auswählen, einen Bereich wählen und **Zum Bereich hinzufügen** oder **Aus Bereich entfernen** (Filter **Ohne Bereich** zeigt noch offene Fachkräfte). Hinzufügen ist immer möglich; bestehende Bereiche bleiben erhalten. Bei eingeschaltetem Bereichsmodus lassen sich die Bereiche einer Person auch im Benutzerdialog unter **Bearbeiten** → **Bereiche** ändern; dort wird auch der **Hauptbereich** gewählt (ohne Auswahl der zuerst zugeordnete Bereich). Ist die Person aktives oder künftig gültiges Mitglied in Teams eines Bereichs, der entfernt werden soll, wird das Entfernen abgelehnt und die Meldung nennt diese Teams. Mit der Option **Mitgliedschaften in Teams entfernter Bereiche beenden** werden diese Mitgliedschaften – auch abgelaufene und künftig gültige – im selben Schritt beendet (Audit je Mitgliedschaft); abgelaufene Mitgliedschaften blockieren nicht und wirken nicht mehr auf Einstellungen; Fälle, die nur über diese Teams erreichbar waren, verschwinden beim nächsten Sync vom Gerät. Teams ohne Bereich bleiben unberührt.
3. **Einschalten** in der Karte **Bereichsorientiertes Arbeiten**: Dazu ist eine **erneute Anmeldebestätigung** nötig (aktuelles Passwort, bei aktivierter Zwei-Faktor-Anmeldung zusätzlich der Code; bei Passkey-Konten die Passkey-Bestätigung). Beim Einschalten erhalten **alle** aktiven Konten mit Verwaltungsrechten, die noch keinen Umfang haben, automatisch **Gesamt** – im Moment des Einschaltens ändert sich also für niemanden etwas. Die Karte nennt die Anzahl vorab.
4. Unter **Verwaltungsumfang der Admins** einzelne Konten auf **Nur ausgewählte Bereiche** umstellen (Mehrfachauswahl möglich). Den eigenen Umfang kann niemand selbst ändern; der letzte Fach-Admin mit Gesamtumfang kann nicht beschränkt werden.
5. Fachkräfte mit Panel-Rechten (z. B. *Fälle ansehen* oder *Zeiterfassung ansehen*) behalten nach dem Einschalten zunächst den Gesamtumfang. Die Sammelaktion **Auf eigenen Bereich beschränken** in derselben Karte stellt alle aktiven Fachkräfte, die mindestens einem aktiven Bereich zugeordnet sind und nur den Gesamtumfang haben, in einem Schritt auf ihre eigenen Bereiche um. Die Karte nennt Anzahl und Namen vorab. Konten mit dem Recht *Fach-Admin* oder *Bereiche verwalten* und das eigene Konto bleiben unverändert.
6. Unter **Teams** jedem Team optional einen Bereich zuordnen oder es in einen anderen Bereich verschieben. Mitglieder, die dem neuen Bereich noch nicht angehören, werden ihm dabei zusätzlich zugeordnet (die Seite nennt die Anzahl); ihre bisherigen Bereiche bleiben erhalten.

Bei eingeschaltetem Bereichsmodus bietet der Dialog **Neuer Benutzer** eine Bereichsauswahl (mehrere möglich, der erste wird Hauptbereich); bei ausgeschaltetem Modus ist sie ausgeblendet. Neue Konten, die

ein bereichsgebundener Admin anlegt, landen automatisch in dessen Bereich (bei mehreren Bereichen mit Pflichtauswahl im Dialog). Konten mit Verwaltungsrechten erhalten beim Anlegen keinen Umfang; diesen vergibt ein Gesamt-Admin.

Organisation im Bereichsmodus

Für bereichsgebundene Konten gilt auf den Organisationsseiten:

- **Teams**: nur Teams der eigenen Bereiche; neue Mitglieder nur aus dem eigenen Bereich.
- **Kontaktkarten und Vertretungen**: nur Karten der eigenen Fachkräfte; Vertretungen erscheinen, wenn die abwesende Person bzw. der Fall im eigenen Bereich liegt. Eine bereichsübergreifende Vertretung legt ein Gesamt-Admin an. Die **Träger-Kontaktdaten** pflegt nur ein Gesamt-Admin.
- **Verwaltete Einstellungen**, **Textbausteine** und **Vorlagen**: organisationsweite Einträge sind **nur lesend**; Einträge für eigene Bereiche, Teams, Fachkräfte und Geräte lassen sich pflegen.
- **Institutionen**, **Maßnahmenkatalog** und **Tätigkeitsarten** gelten organisationsweit und sind **nur lesend**.
- **Geräte**: nur Geräte der eigenen Fachkräfte.
- **Admin-API** (`/api/v1/admin/…`): Anmeldungen eines Benutzerkontos unterliegen demselben Umfang; fremde Ziele antworten mit „nicht gefunden“. Der Dienst-Client (Client Credentials) bleibt organisationsweit.

Ausschalten

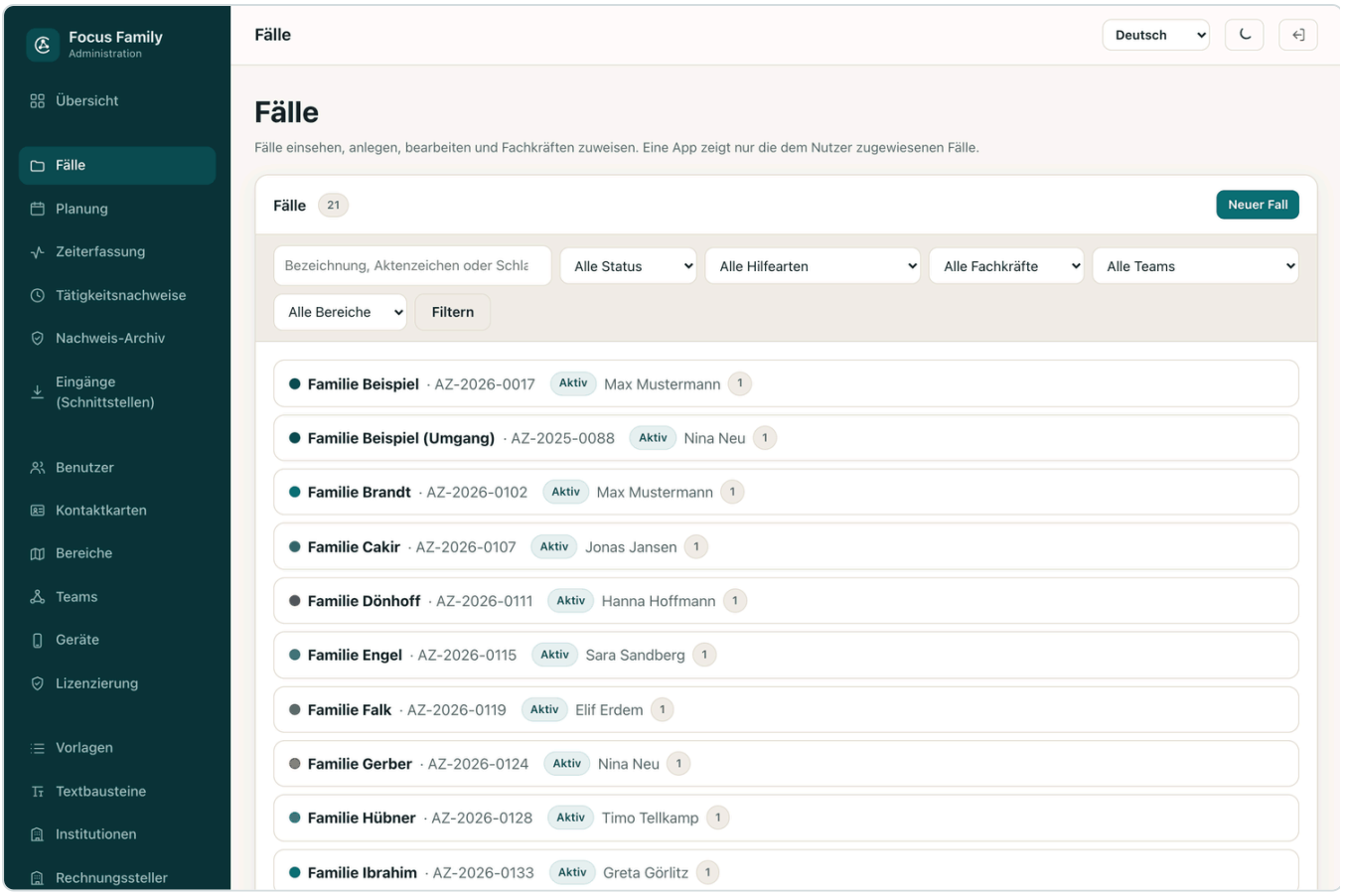
Ausschalten (ebenfalls mit Anmeldebestätigung) setzt nur den Schalter zurück. Bereiche, Zuordnungen und Verwaltungsumfänge bleiben gespeichert und gelten beim erneuten Einschalten wieder; Fälle und Einträge werden nie verändert.

Bewegungen

Die Liste **Bewegungen** zeigt die letzten Bereichsereignisse (Modus, Bereiche, Zuordnungen, Umfänge, abgelehnte Zugriffe) mit Zeitpunkt, handelnder Person und Ziel. Das vollständige Protokoll steht im **Sicherheits-Audit**.

Fälle

Menüpunkt **Fälle** (Recht *Fälle ansehen* bzw. *bearbeiten*). Denken Sie daran: Hier geht es um Verwaltung und Zuweisung, nicht um die inhaltliche Fallarbeit.



Die Fälle der Organisation mit Status, Hilfeart und zugewiesenen Fachkräften.

Fall anlegen und zuweisen

1. **Neuen Fall anlegen** klicken und die Felder ausfüllen: **Bezeichnung / Kürzel**, **Aktenzeichen**, **Status**, **Hilfeart** (unter anderem **Schulbegleitung**), **Zuständiges Amt**, **ASD-Fachkraft**, **Bewilligte Minuten** und **Farbe**.
2. **Fall anlegen**.
3. Unter **Zugewiesene Fachkräfte** mit **Zuweisen** die Personen hinzufügen.

Das Fallformular führt alle Fachfelder – unter anderem verantwortliche Fachkraft, eigene Hilfeart, Schlüsselinformationen, Ressourcen und Tags.

Über die Filterleiste der Fallliste finden Sie Fälle nach Bezeichnung oder Aktenzeichen und grenzen nach Status, Hilfeart, Fachkraft oder Team ein.

Beteiligte und Anschriften

Im Fall listet die Karte **Beteiligte & Anschriften** alle Personen, gruppiert nach ihrer **Anschrift** (früher „Haushalt“). Eine Anschrift fasst die Personen zusammen, die unter derselben Adresse wohnen.

- **Beteiligte hinzufügen** öffnet den Dialog mit Vor- und Nachname, **Rolle**, **Geschlecht**, **Geburtsdatum**, **Geburtsort**, **Sterbedatum**, **Staatsangehörigkeit**, **Familienstand**, **Krankenversicherung**, **Kindergeldnummer** und **Institution / Dienststelle**. Das Sterbedatum darf nicht vor dem Geburtsdatum liegen.
- Zu den Rollen gehören neben Kind, Eltern, Pflegeperson und Netzwerkpartnern auch **Geschwister, Halbgeschwister, Großmutter, Großvater, Tante, Onkel, Stiefelternteil, Partner:in eines**

Elternteils, Cousin:e, sonstige Angehörige und **Jugendhilfeträger**. Bei Halbgeschwistern, Großeltern, Tante, Onkel und Cousin:e erscheint zusätzlich **Verwandtschaftsseite** (mütterlicherseits/väterlicherseits); in der Ansicht steht dann z. B. „Großmutter (mütterlicherseits)“.

- **Ist minderjährig** kennzeichnet Kinder und Jugendliche; bei der Rolle „Kind“ wird es automatisch gesetzt.
- **Anschrift** ordnet die Person einer vorhandenen Anschrift zu. Mit **Neue Anschrift …** legen Sie im selben Dialog eine neue Anschrift mit Bezeichnung und Adresse an; beim Speichern entstehen Anschrift und Person gemeinsam.
- Solange **Adresse der Anschrift übernehmen** angehakt ist, gilt die Adresse der Anschrift und die Felder für eine eigene Adresse sind ausgeblendet. Entfernen Sie den Haken, um eine abweichende Adresse einzutragen.
- Telefonnummern haben die Arten **Handy (privat)**, **Festnetz (privat)**, **Festnetz (dienstlich)**, **Handy (dienstlich)** und **Sonstige**.

Felder, die das Panel nicht anzeigt (etwa Notizen aus der App), bleiben beim Speichern unverändert erhalten.

Roadmap, Ziele und Prüfpunkte

Im geöffneten Fall zeigen zwei Karten den Hilfeverlauf:

- **Roadmap** – eine Zeitachse vom Fallbeginn bis heute: Zielspuren, Prüfpunkte als Marken und darunter die erfasste Zeit je Woche oder Monat mit Kontingentlinie.
- **Ziele & Prüfpunkte** – die Liste der Ziele (Status, Zieltermin, Vorgänger-Ziel, Erreicht am) und der Prüfpunkte (Datum, Art, Titel, nächster Termin, Status). Mit *Fälle bearbeiten* legen Sie Prüfpunkte an; die Änderungen synchronisieren zu den Geräten.

Vertretung

Jeder Fall hat die Karte **Vertretung (zeitlich begrenzt)**:

- **Kolleg:in** wählen, **Von** und **Bis** festlegen, **Vertretung anlegen**. Der Zugriff beginnt und endet automatisch; Urlaubsvertretungen lassen sich im Voraus planen und jederzeit vorzeitig beenden.
- Eine Vertretung erhält für ihre Dauer normalen Lese- und Bearbeitungszugriff. **Private Einträge bleiben geschützt**, dauerhafte Zuweisungen bleiben unverändert.
- Jeder Schritt (angelegt, aktiviert, beendet, abgelaufen) wird protokolliert.

Fall übertragen

Wechselt die Zuständigkeit dauerhaft, übertragen Sie den Fall vollständig an eine andere Fachkraft. Im Fall unter **Zugewiesene Fachkräfte** öffnet **Fall übertragen** einen Dialog (Rechte *Fälle bearbeiten* und *Anderen zuweisen*):

1. **Neue zuständige Fachkraft** wählen (nur aktive Fachkräfte der Organisation).
2. Optional **Bisherige Fachkraft behält Zugriff** anhaken – dann bleibt sie als geteilte Person am Fall.
3. **Übertragen** und die Rückfrage bestätigen.

Die neue Fachkraft wird Eigentümerin des Falls und übernimmt alle Einträge, die bisher der abgebenden Fachkraft gehörten – auch private und eingeschränkt sichtbare Einträge sowie Dateien. Zeiteinträge,

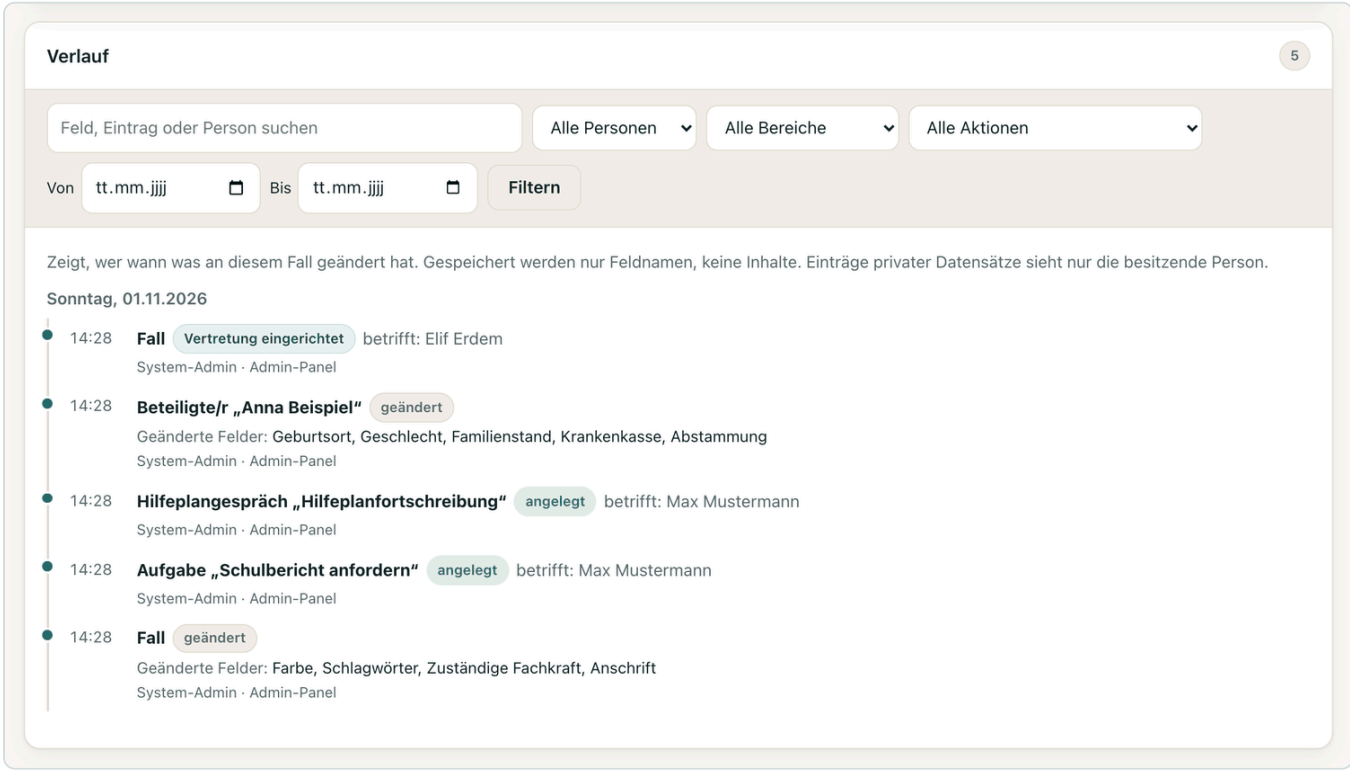
Unterschriften und Abschlüsse bleiben der Person zugeordnet, die sie erfasst hat. Offene Vertretungen für die abgebende Fachkraft enden. Ohne „Zugriff behalten“ verliert die abgebende Fachkraft den Fall beim nächsten Sync, sofern sie ihn nicht über ein Team weiterhin sieht. Die Übertragung steht im **Audit** als „Fall übertragen“.

In der App kann nur die aktuelle Eigentümerin bzw. der aktuelle Eigentümer einen Fall übertragen.

Termine, Aufgaben und Medien im Fall

- Über **Termin hinzufügen** und **Aufgabe hinzufügen** legen Sie beides direkt im Fall an.
- Im Bereich **Medien** sehen Sie Fotos, Videos, Audio-Memos und Skizzen – aber nur, wenn Sie Fach-Admin oder dem Fall zugewiesen sind, und **nur nicht-private** Einträge. Ist eine Datei noch nicht übertragen, erscheint der Hinweis „Datei noch nicht auf dem Server".
- Die **E-Akte** listet die Dokumente je Abschnitt (z. B. Verträge & Einwilligungen) mit Erzeugung, Version, Vorlage und Unterschriften. Ein Klick auf den Titel oder auf **Öffnen** lädt die Datei; Dateiname und Größe stehen im Tooltip. In schmalen Fenstern blendet das Panel die Spalten Vorlage und Unterschriften aus.

Verlauf eines Falls



Der Verlauf nennt je Änderung Uhrzeit, betroffenen Eintrag, Aktion, Person, Gerät und Quelle – nur Feldnamen, nie Inhalte.

Ganz unten in der Fallansicht zeigt der Bereich **Verlauf**, wer wann was am Fall geändert hat – neueste Einträge zuerst, nach Tagen gruppiert. Erfasst werden alle Wege: Synchronisation aus App und Desktop (mit Gerät), Änderungen im Admin-Panel, die App-Funktionen Teilen, Freigabe entziehen, Vertretung und Übertragen sowie Löschanträge, Aufbewahrungsentscheidungen und Einschränkungen der Verarbeitung. Nicht in den Verlauf gehören rein technische Datensätze: Abschlüsse von Tätigkeitsnachweisen (Zeitraum-Momentaufnahmen), importierte Personenkalender und daraus übernommene externe Termine. Zeiteinträge, Fahrten und Unterschriften erscheinen dagegen, weil sie im Fall geleistete Arbeit belegen.

- Jeder Eintrag nennt Uhrzeit, Bereich (z. B. „Beteiligte/r „Anna B.““, „Termin vom 12.03.2026“ oder „Zeiteintrag vom 03.10.2026“), Aktion, Person bzw. „System“, Gerät und Quelle (z. B. „über App/Desktop synchronisiert“).
- Bei Änderungen stehen nur die **Namen der geänderten Felder** (z. B. „Geburtsdatum, Hauptanschrift“). Inhalte, alte oder neue Werte speichert der Verlauf nie. Technische Felder wie Zeitstempel, Versionen oder Prüfsummen zählen nicht als Änderung.
- Namen von Einträgen erscheinen nur, wenn sie ohnehin in der Fallansicht sichtbar sind; Termine, Zeiteinträge und Fahrten zeigen stattdessen ihr Datum. Fehlt beides (etwa bei privaten oder gelöschten Einträgen), steht nur der Bereich, z. B. „Telefonnummer“ – ohne technische Kennung.
- Mit den Filtern grenzen Sie nach Person, Bereich, Aktion und Zeitraum ein; die Suche durchsucht Bereich, Feldnamen und Personen. Je Seite erscheinen 50 Einträge, **Ältere** und **Neuere** blättern.
- Sichtbar ist nur, was Sie auch in der Fallansicht sehen dürfen: Termine nur mit Kalender-Recht, Aufgaben nur mit Aufgaben-Recht, Zeiteinträge und Fahrten nur mit Zeiterfassungs-Recht, Rechnungssätze nur mit Abrechnungsrecht, E-Akte und Medien nur für Fach-Admins und zugewiesene Personen. Einträge zu privaten Datensätzen sieht nur die besitzende Person. Bei einem privaten Fall sehen andere nur Verwaltungsschritte wie Teilen, Übertragen oder Vertretungen.
- Wird ein Fall nach der Löschprüfung endgültig gelöscht, verschwindet sein Verlauf vollständig. Bei einem einzelnen endgültig gelöschten Eintrag bleibt nur der Vermerk „endgültig gelöscht“.

Schnittstellen: Eingänge und Übergabe

Ist der Server an Fachverfahren, ein Dokumentenmanagement, eine E-Akte oder Jugendämter angebunden, richtet das die technische Administration ein; Einzelheiten stehen im **Schnittstellenhandbuch**. In der fachlichen Arbeit zeigt sich das an mehreren Stellen.

Eingänge prüfen

Die Seite **Eingänge (Schnittstellen)** sammelt Dokumente, Stammdatenänderungen und Termine aus angebundenen Systemen, die geprüft werden sollen. Sie steht Konten mit dem Recht **Eingänge aus Schnittstellen prüfen und übernehmen** zur Verfügung (im Fach-Admin enthalten, unter **Fachlich** in der Rechteliste) und zeigt wie die Fallansicht nur Eingänge zu Fällen im eigenen Verwaltungsumfang, die nicht gelöscht, nicht zur Löschung vorgemerkt und nicht in der Verarbeitung eingeschränkt sind; dieselben Fälle bietet die Fallauswahl beim Zuordnen an. **Zuordnen** und **Übernehmen** schreiben in Fälle und erscheinen nur, wenn das Konto zusätzlich **Fälle bearbeiten** hat; ablehnen genügt das Recht für die Eingänge. „Fälle bearbeiten“ allein öffnet die Seite nicht, weil hier auch Unterlagen landen können, die einer anderen Fachkraft zugeordnet sind. Wird ein Fall zum Beispiel in der Verarbeitung eingeschränkt, verschwinden seine Eingänge aus der Liste und lassen sich nicht mehr übernehmen, zuordnen oder ablehnen.

- Jede Zeile nennt Zeitpunkt, **Quelle** (Name der Schnittstelle), **Art** (Dokument, Stammdaten, Termin, Katalog), **Inhalt**, **Fall** und **Status**.
- **Zu prüfen: Übernehmen** legt das Dokument in der E-Akte an bzw. trägt die Stammdaten in den Fall ein. **Ablehnen** verwirft den Eingang.
- **Fall zuordnen:** Das angebundene System hat keinen eindeutigen Fall genannt. Wählen Sie den Fall aus und klicken Sie **Zuordnen**. Danach wird die Datei auf Schadsoftware geprüft und steht unter **Zu prüfen** bereit. Eingänge ohne Fall sehen nur Konten mit organisationsweitem Verwaltungsumfang.

- **Konflikt:** Eine Fachkraft hat ein Feld seit der letzten Übernahme aus diesem System geändert; unter dem Status stehen die betroffenen Felder. **Übernehmen** überschreibt die Werte der Fachkraft erst nach einer Rückfrage, **Ablehnen** lässt sie stehen.
- Übernommene und abgelehnte Eingänge bleiben am Ende der Liste sichtbar.
- Wird ein Fall oder ein Datensatz endgültig gelöscht, behalten seine Eingänge nur technische Angaben; Inhalt, Dateiname sowie Fallreferenz und externe ID des angebundenen Systems werden entfernt.

Je nach Einrichtung übernimmt der Server Dokumente auch direkt; Termine aus angebundenen Systemen legt er immer direkt im Fall an. Freitexte der Fachkräfte ändert keine Schnittstelle, und von außen wird nichts gelöscht.

Herkunft eingelieferter Dokumente

Übernommene Dokumente erscheinen in der **E-Akte** des Falls als finale Dokumente; als Autorin bzw. Autor steht der Name der Schnittstelle. Der **Verlauf** des Falls nennt als Quelle „Schnittstelle“. Auf den Geräten der Fachkräfte kommen die Dokumente mit der nächsten Synchronisation an.

An Zielsystem übergeben

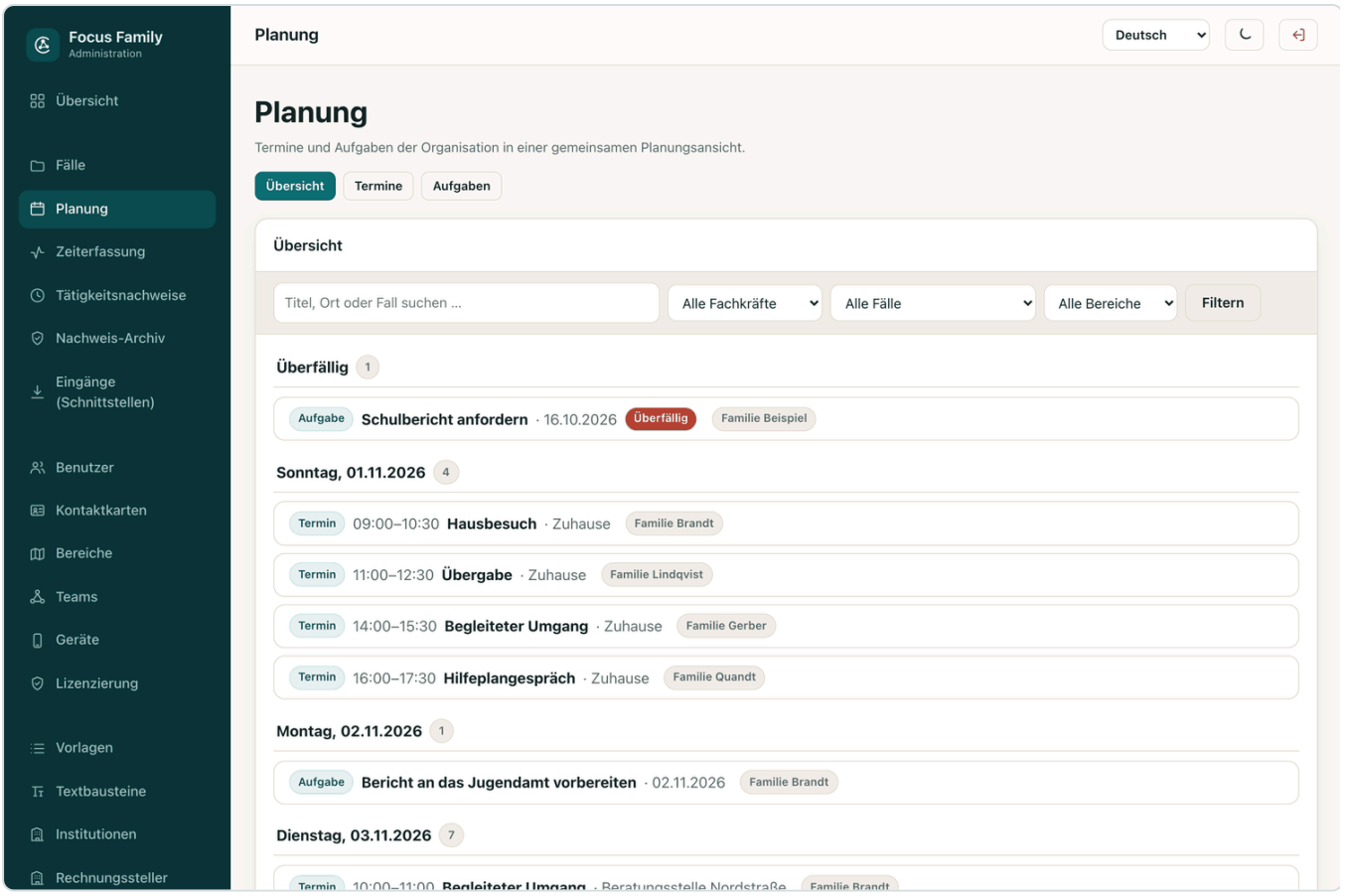
Ist eine Schnittstelle für die manuelle Übergabe eingerichtet, zeigt die Fallansicht Konten mit **Fälle bearbeiten** die Schaltfläche **An Zielsystem übergeben**. Wählen Sie das **Zielsystem** (z. B. die E-Akte oder ein Jugendamt über XÖV) und bestätigen Sie mit **Übergabe starten**. Übergeben wird die Akte mit den freigegebenen Dokumenten. Es gelten die Datenschutz-Einstellungen der Schnittstelle; gesperrte Dokumenttypen und private Einträge bleiben zurück. Die Übergabe erscheint im Übertragungsprotokoll der technischen Administration.

Kalender-Abo

Sind Kalender-Abos freigeschaltet, erzeugt jede Person unter **Kalender-Abo** eine persönliche Abo-Adresse für Outlook, Thunderbird oder den iPhone-Kalender. Die Adresse wird nur einmal angezeigt und ist geheim; **Neue Adresse erzeugen** macht die bisherige ungültig, **Abo beenden** widerruft sie. Wie viel ein Termin im Abo zeigt (nur „Belegt“, Terminart und Fallalias, dazu der Ort), legt die Organisation fest; private Termine erscheinen immer nur als „Belegt“.

Planung

Menüpunkt **Planung** – eine Seite mit drei Ansichten:



Übersicht, Termine und Aufgaben der gesamten Organisation an einer Stelle.

- **Übersicht** – zuerst überfällige Aufgaben, dann Termine und Aufgaben nach Tagen gruppiert, zum Schluss Aufgaben ohne Datum. Ein Klick auf einen Eintrag öffnet ihn unter **Termine** bzw. **Aufgaben** zum Bearbeiten. Überfällig sind geplante Termine, deren Endzeit vorbei ist, und Aufgaben, deren Fälligkeitstag bzw. -uhrzeit überschritten ist – auch am selben Tag; sie tragen das Kennzeichen **Überfällig**.
- **Termine** (Recht *Kalender ansehen*) – die organisationsweite Terminliste. **Neuer Termin** legt Termine an; im Abschnitt **Wiederholung** entsteht eine **Terminserie** (täglich, wöchentlich mit Wochentagen und „Alle N Wochen", monatlich; Ende per Datum oder Anzahl; höchstens 180 Termine über höchstens 3 Jahre). Serienvorkommen tragen ein **Serie**-Kennzeichen; das Bearbeiten ändert nur dieses Vorkommen, **Serie löschen** entfernt die ganze Serie. Vergangene und dokumentierte Termine bleiben erhalten.
- **Aufgaben** (Recht *Aufgaben ansehen*) – die organisationsweite Aufgabenliste mit **Neue Aufgabe**. Aufgaben ohne Fall lassen sich bearbeiten und entfernen; neue Aufgaben brauchen einen Fall.

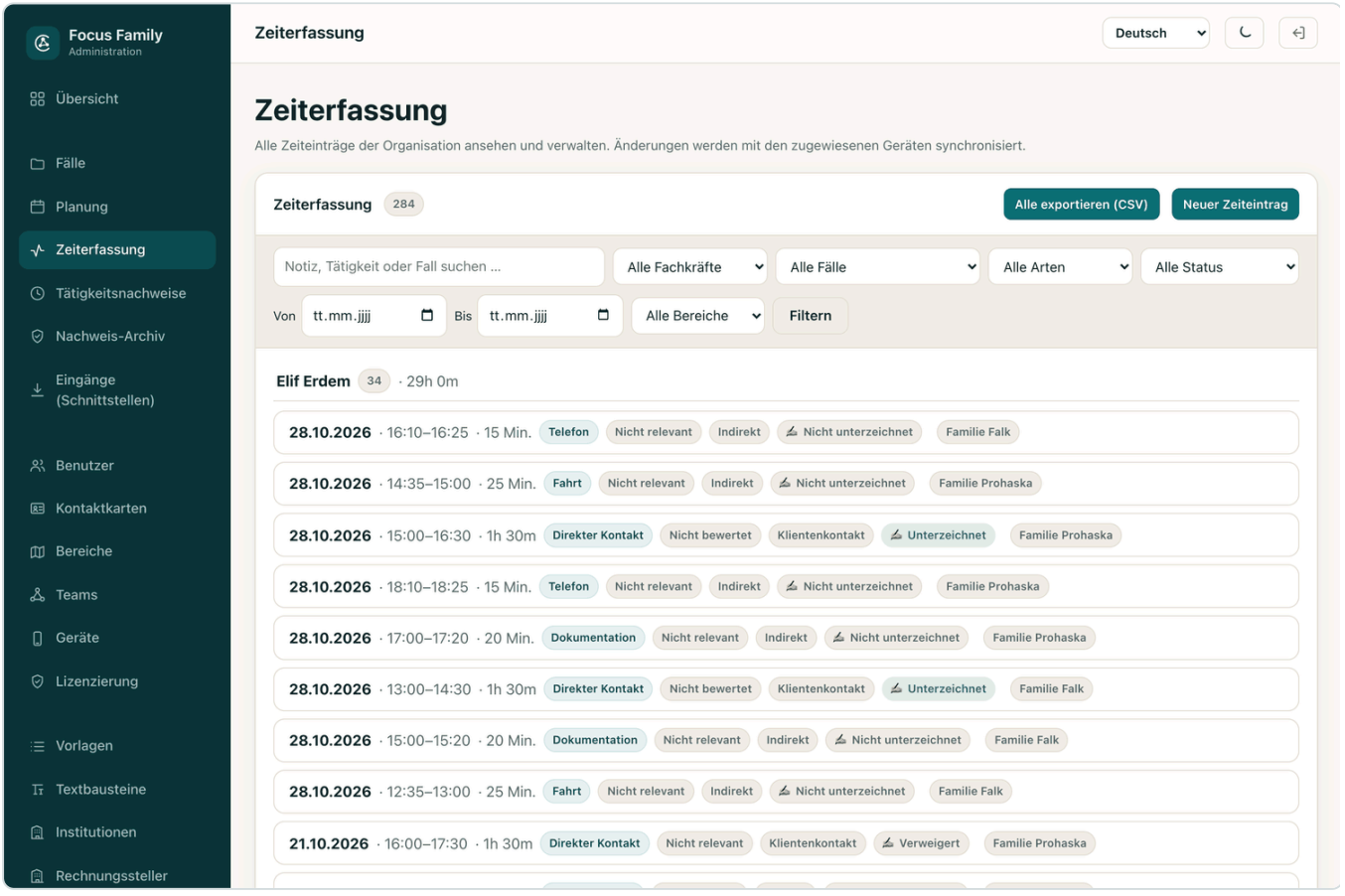
Bearbeiten und Entfernen setzen die Rechte *Kalender bearbeiten* bzw. *Aufgaben bearbeiten* voraus. Termine mit Unterschrift, Zeiteinträgen oder Dokumentation lassen sich nicht entfernen; das Panel nennt den Grund. **Serie löschen** behält solche Vorkommen ebenfalls. Schlägt eine Änderung fehl, zeigt das Panel eine Fehlermeldung statt „Gespeichert“.

Mit dem Recht *Zeiterfassung erfassen* bietet jeder Termin zusätzlich **Als Zeiteintrag übernehmen** – höchstens ein Zeiteintrag pro Termin.

Jede Ansicht hat eine Filterleiste: in allen Ansichten Suche, Fachkraft und Fall, bei **Termine** zusätzlich Terminart, Status und Zeitraum, bei **Aufgaben** Status, Priorität, Fälligkeit und Zeitraum.

Zeiterfassung

Menüpunkt **Zeiterfassung**.



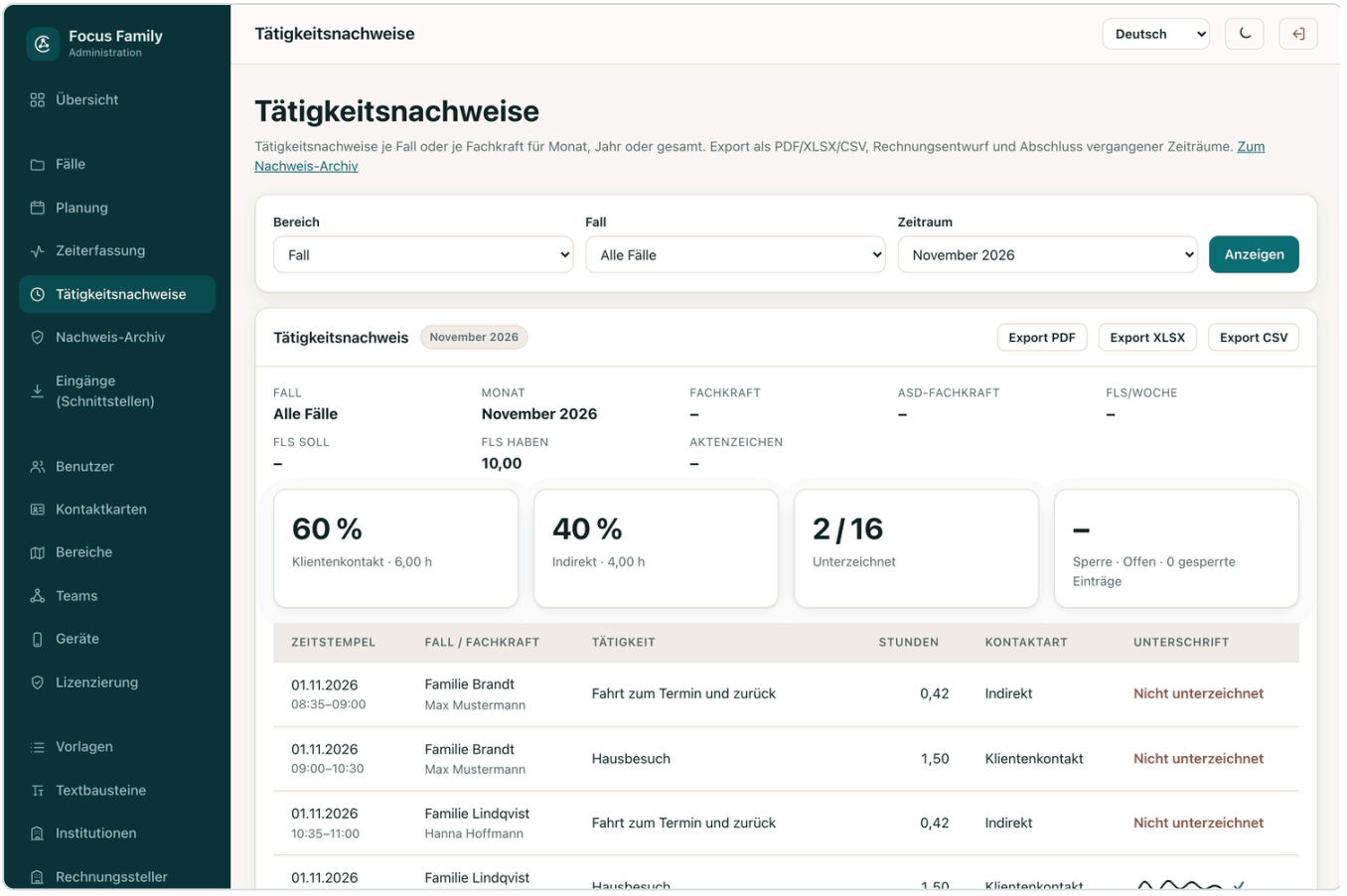
Alle Zeiteinträge der Organisation mit Sperr- und Unterschriftsstatus; über Filter grenzen Sie auf eine Fachkraft ein.

- Mit **Zeiterfassung ansehen** sehen Sie alle Zeiteinträge der Organisation mit Datum, Dauer, Art und Fall sowie den Spalten **Sperre** (Schloss = Zeitraum abgeschlossen) und **Unterschrift** (Unterzeichnet, Nicht unterzeichnet, Verweigert).
- Mit **Zeiterfassung erfassen** legen Sie über **Neuer Zeiteintrag** eigene Einträge an.
- Einträge **anderer** Fachkräfte ändern oder löschen Sie nur mit **Nachweise verwalten** und nur in Ihrem **Leitungsbereich**. Solche Änderungen werden als Leitungsänderung protokolliert.
- Über die Filterleiste grenzen Sie nach Fachkraft, Fall, Art, Abrechnungsstatus und Zeitraum ein oder suchen in Notizen und Tätigkeiten; mit **Alle exportieren (CSV)** holen Sie die Daten für die Weiterverarbeitung heraus.
- Fahrten, die in der App mit **Jetzt losfahren** und **Angekommen** aufgezeichnet wurden, erscheinen als Fahrtzeit-Eintrag mit einem Kilometer-Hinweis. In den Details zeigt der Abschnitt **Aufgezeichnete Fahrt** Kilometer, Dauer, Abfahrt und Ankunft, Ziel und Zweck sowie eine Streckenskizze als Nachweis. Die Skizze wird im Panel ohne Kartendienst gezeichnet; die Streckenpunkte sind Bewegungsdaten der Fachkraft und werden deshalb nicht in Auskünfte und Datenexporte für Klient:innen übernommen.

> Vom Gerät aus kann niemand die Zeiteinträge oder Unterschriften einer anderen Fachkraft ändern. Leitungskorrekturen sind ausschließlich hier im Panel möglich.

Tätigkeitsnachweise

Menüpunkt **Tätigkeitsnachweise** (Recht *Zeiterfassung ansehen*).



Nachweis je Fall oder Fachkraft mit Kennzahlen, Einzelzeilen, Exporten und dem Abschluss vergangener Zeiträume.

1. **Fall** oder **Fachkraft** wählen und den **Zeitraum** (Monat, Jahr, Gesamt), dann **Anzeigen**.
2. Die Seite zeigt die **Kennzahlen**: Stunden, Soll/Haben aus dem Kontingent, Anteil Klientenkontakt und Indirekt, Unterschriftsquote und Sperrstatus – darunter die Tabelle mit Datum, Fall bzw. Fachkraft, Zeit, Tätigkeit, Stunden, Kontaktart und Unterschrift. Jahres- und Gesamtnachweise sind nach Monaten gruppiert, Fachkraft-Nachweise nach Fällen. **Private Einträge sind nie enthalten.**
3. **Unterschriften** erscheinen direkt in der Tabelle mit Bild, Name, Rolle und Zeitpunkt. Daneben steht ein Prüfsymbol: - ✓ – die Prüfsumme passt zu Bild und eingefrorener Zusammenfassung; die Unterschrift ist unverändert. - ⚠ – die Prüfsumme stimmt **nicht**; Bild oder Zusammenfassung wurden verändert oder sind beschädigt. Klären Sie das mit der Fachkraft. Eine fehlende Unterschrift ist **kein Fehler** – sie ist freiwillig.
4. **Export** als **PDF**, **XLSX** oder **CSV**.
5. **Rechnungsentwurf** erzeugt aus einem Fall-Nachweis eine JSON-Vorbereitung mit Kostenträger, Positionen je Tätigkeitsart und offenen Unterschriften. Beträge erscheinen nur mit dem Recht *Beträge*

sehen. Die E-Rechnung selbst (XRechnung oder ZUGFeRD-PDF) erstellen die Fachkräfte in App oder Desktop, weil nur dort die Rechnungsstellerangaben (Steuernummer, IBAN, Umsatzsteuer-Regelung) gepflegt werden.

Abschließen und wieder öffnen

Nötig ist das Recht *Nachweise abschließen*, und zwar nur im eigenen Leitungsbereich.

- **Abschließen** friert einen **vergangenen** Monat oder ein **vergangenes** Jahr ein (optional mit Notiz). Danach sind alle Zeiteinträge des Zeitraums auf allen Geräten **gesperrt**: Änderungen, Löschungen und das Verschieben in den Zeitraum werden abgewiesen; lesen bleibt möglich. Der Nachweis erhält eine Prüfsumme, und der vollständige Stand wird gespeichert.
- **Abgeschlossener Stand:** Beim Öffnen eines abgeschlossenen Zeitraums zeigt die Seite den Hinweis „Abgeschlossener Stand (Prüfsumme gesichert)". Tabelle und Exporte stammen dann aus dem gespeicherten Stand. Erscheint zusätzlich das Warnzeichen **„Achtung: aktuelle Daten weichen vom abgeschlossenen Stand ab"**, wurden Einträge nach dem Abschluss verändert – etwa, weil ein Gerät später synchronisiert hat. Angezeigt und exportiert wird weiterhin der abgeschlossene Stand.
- Der **laufende Monat** und das **laufende Jahr** lassen sich nie abschließen.
- **Wieder öffnen** hebt die Sperre auf und verlangt eine **Begründung**. Beides steht im Sicherheits-Audit.
- Fachkräfte selbst können nichts abschließen oder öffnen; sie sehen gesperrte Einträge mit einem Schloss.

Kennzeichnung und Nachweis-Archiv

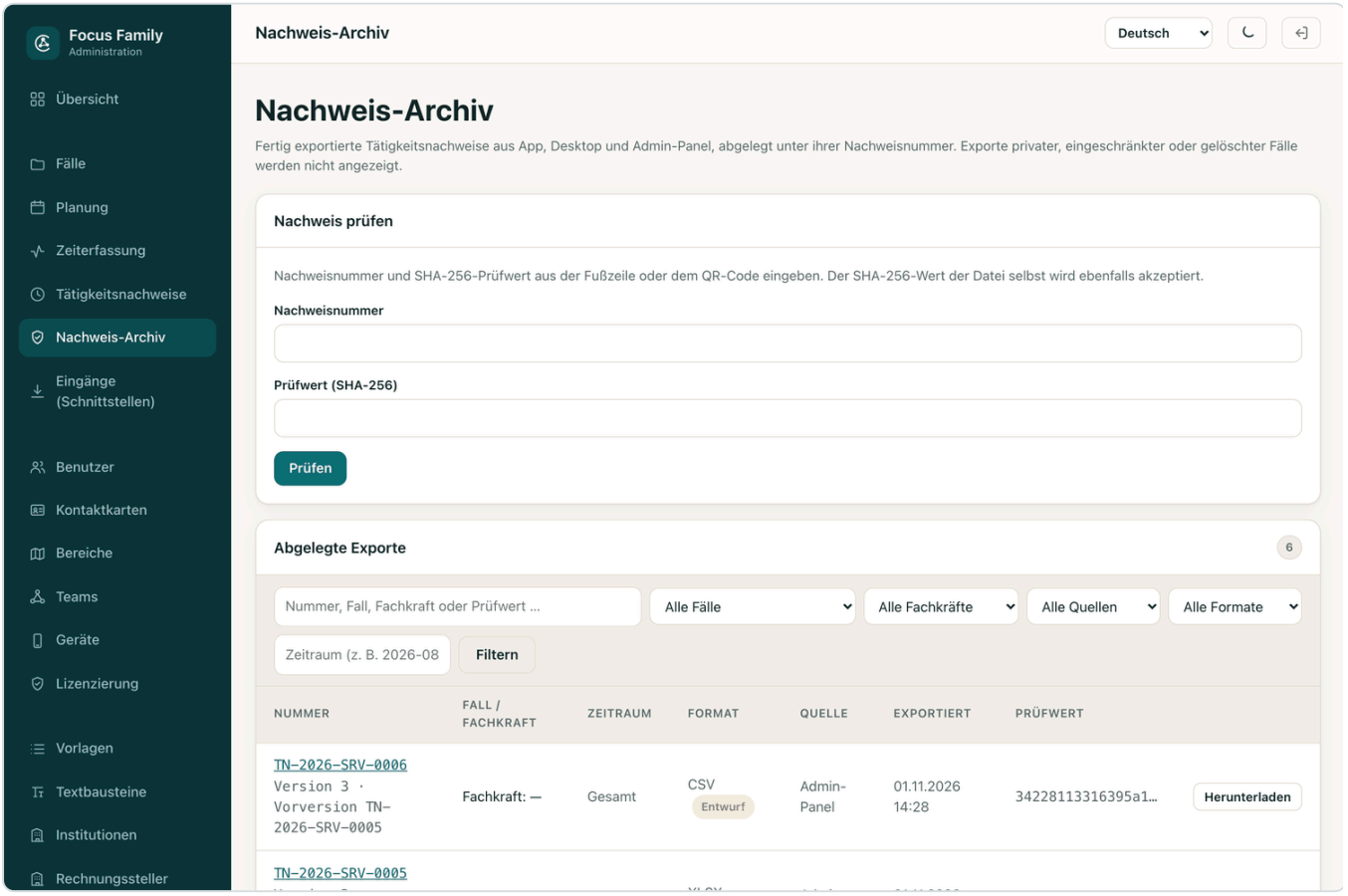
Jeder exportierte Tätigkeitsnachweis – aus App, Desktop oder Panel, in jedem Format – ist eindeutig gekennzeichnet:

- **Nachweisnummer** im Format `TN-<Jahr>-<Gerätekürzel>-<laufende Nummer>`, z. B. `TN-2026-7KQ2-M9XA-0042`. Das achtstellige Gerätekürzel wird auf jedem Gerät einmalig zufällig erzeugt; die laufende Nummer zählt je Gerät und Jahr. So entstehen auch offline auf mehreren Geräten derselben Person keine doppelten Nummern. Exporte aus dem Panel erhalten Nummern mit dem Kürzel `SRV` (z. B. `TN-2026-SRV-0007`), die der Server fortlaufend vergibt.
- **Exportzeitpunkt** und **Version**: Wird derselbe Nachweis (gleicher Fall bzw. gleiche Fachkraft und gleicher Zeitraum) erneut exportiert, steigt die Version, und das Dokument nennt die Nummer der Vorversion.
- **SHA-256-Prüfwert** über den Inhalt des Nachweises einschließlich Nummer, Version und Exportzeitpunkt. Jede nachträgliche Änderung am Inhalt ergibt einen anderen Wert.
- **QR-Code** mit Nummer und Prüfwert; bei mit dem Server verbundenen Geräten führt er direkt auf die Prüfseite.

PDF und Word zeigen diese Angaben in der Fußzeile jeder Seite, Excel auf dem Blatt **Kennzeichnung** und in der Druckfußzeile, CSV im Block **Kennzeichnung** am Dateiende (nach einer Leerzeile; die Spaltenüberschriften bleiben in der ersten Zeile) und JSON im Abschnitt `identification`.

Ablage: Ist ein Gerät mit dem Server verbunden, lädt es jeden Export nach dem Speichern verschlüsselt hoch – ohne Netz zwischengespeichert, sobald wieder eine Verbindung besteht. Exporte aus dem Panel werden sofort abgelegt. Menüpunkt **Nachweis-Archiv** (Recht *Zeiterfassung ansehen*) listet alle abgelegten

Exporte mit Suche und Filtern (Fall, Fachkraft, Quelle, Format, Zeitraum) und bietet den **Download** der Originaldatei. Exporte, die einen privaten, eingeschränkten oder gelöschten Fall enthalten, erscheinen nicht.



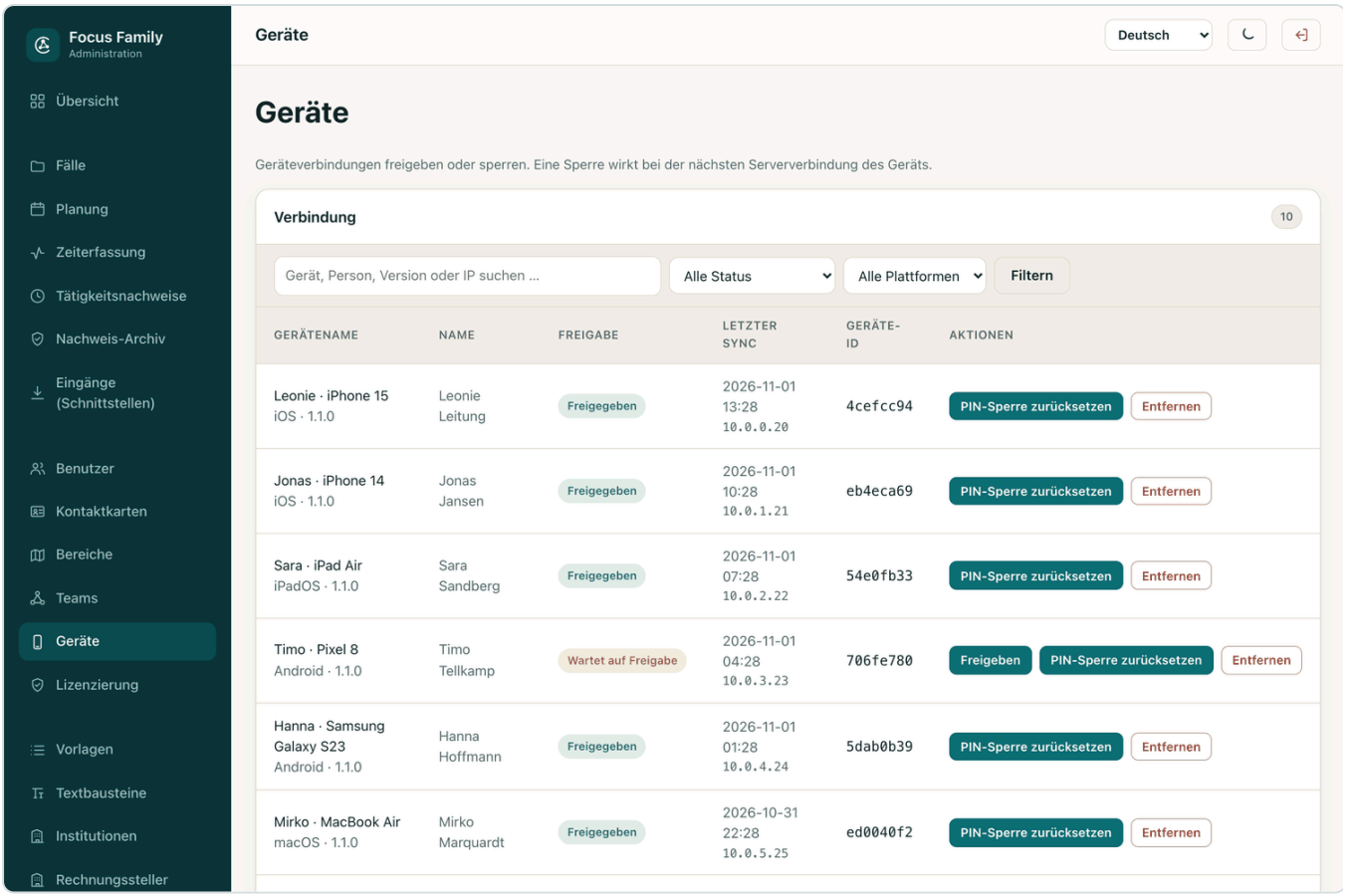
Das Nachweis-Archiv listet jeden abgelegten Export mit Nachweisnummer, Version, Quelle, Format und Prüfwert.

Prüfen: Unter **Nachweis prüfen** Nachweisnummer und Prüfwert aus Fußzeile oder QR-Code eingeben (der QR-Code öffnet die Seite nach der Anmeldung direkt). Das Ergebnis lautet *Echt*, *Abweichung* (der Prüfwert passt nicht – das vorgelegte Dokument wurde verändert) oder *Nicht gefunden*. Statt des Inhalts-Prüfwerts kann auch der SHA-256-Wert der Datei eingegeben werden. Die Prüfseite verlangt eine Anmeldung und zeigt keine Inhalte gesperrter Fälle.

Löschung: Wird ein enthaltener Zeiteintrag gelöscht oder ein Fall endgültig entfernt, wird die archivierte Datei mitgelöscht. Nummer, Version und Prüfwerte bleiben als Nachweis bestehen („Datei gelöscht“).

Geräte

Menüpunkt **Geräte** (Recht *Geräte ansehen* bzw. *verwalten*).



Registrierte Geräte mit Plattform, Version, letztem Sync und Status. Hier geben Sie Geräte frei, sperren sie oder trennen die Verbindung.

Die erste Zeile nennt das Gerätemodell, etwa **iPhone Duo**. Hat das Gerät einen eigenen Namen, steht er in der Zeile darunter. iPhones und iPads melden ihren Namen nur mit Freigabe durch Apple; ohne sie steht dort nur das Modell. Desktop-Geräte zeigen den Rechnernamen.

- **Freigeben / Sperren** – eine Sperre wirkt, sobald das Gerät das nächste Mal Kontakt zum Server aufnimmt.
- **PIN-Sperre zurücksetzen** – hat sich eine Fachkraft ausgesperrt oder die PIN vergessen, heben Sie die App-Sperre hier auf. Sie wird beim nächsten Sync gelöst; die Person vergibt dann eine neue PIN.
- **Entfernen** – trennt die Serververbindung. Das Gerät verliert den Zugriff und muss neu eingerichtet werden; der belegte **Lizenzplatz wird wieder frei**. Fachkräfte können die Verbindung **nicht selbst** trennen.
- **Re-Enrollment-Code** – muss ein bekanntes Gerät neu eingerichtet werden (z. B. nach einer Neuinstallation), stellen Sie einen Code aus. Das Gerät verbindet sich wieder mit seiner bestehenden Registrierung, ohne einen neuen Platz zu belegen.

Lizenzplätze

Lizenzplätze (Seats) werden **ausschließlich von der Administration zugewiesen** – Geräte oder Fachkräfte können sich keinen Platz selbst nehmen. Ohne Platz kann ein Gerät nicht synchronisieren. Den Überblick über Ihre Organisationslizenz gibt der Menüpunkt **Lizenzierung** (Recht *Lizenzierung verwalten*); die Schaltfläche zum Verwalten von Plätzen und Abo erscheint nur mit dem Recht *Lizenzierung erwerben*.

Die Kachel **Seats zugewiesen** zeigt „zugewiesen / gesamt“; die Gesamtzahl ist die Summe aus gekauften (bei laufendem Abonnement) und gesponserten Plätzen.

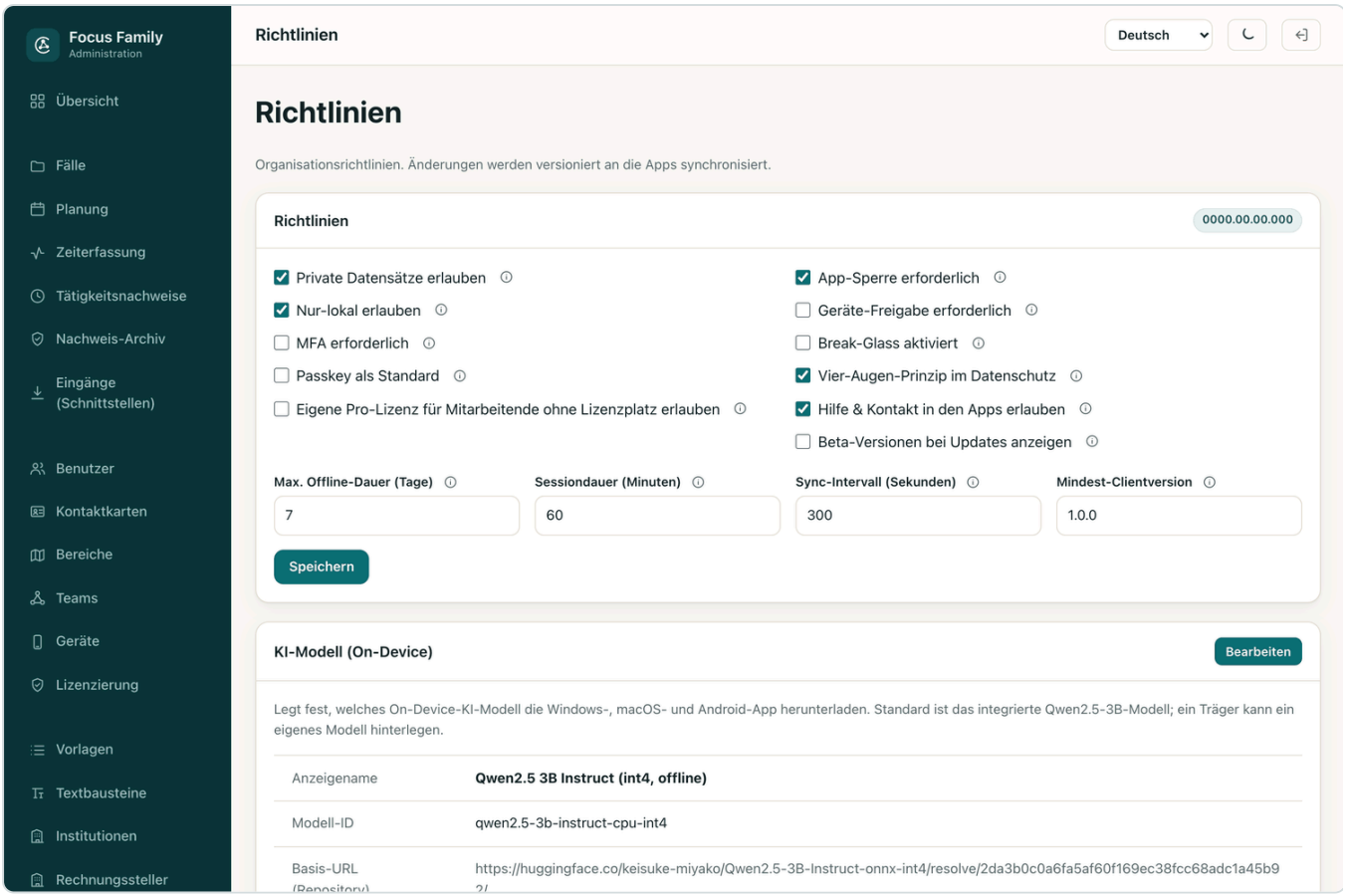
Gesponserte Plätze: Der Hersteller kann einer Organisation zusätzlich kostenlose Plätze zur Verfügung stellen. Sie zählen zur Gesamtzahl und lassen sich wie gekaufte Plätze zuweisen, auch ohne Abonnement; die Kachel **Abonnement** zeigt dann **Gesponsert**. Unter den Kacheln steht der Hinweis „Gesponserte Seats: *Anzahl* – kostenlos und nicht Teil der Abrechnung (bis *Datum*). Zuweisbar wie gekaufte Seats, im Abonnement aber nicht änderbar.“ Sie lassen sich im Admin-Panel weder hinzufügen noch entfernen. Beim Dazukaufen oder Reduzieren gekaufter Plätze werden sie nicht berücksichtigt; reduziert werden kann bis auf die Zahl zugewiesener Plätze abzüglich der gesponserten.

Zugewiesen, ohne Lizenz: Gibt es kein laufendes Abonnement und weniger gesponserte Plätze als Zuweisungen (etwa nach dem Ende eines Sponsorings), gelten nur die zuerst zugewiesenen Plätze bis zur Zahl der gesponserten. Die übrigen Fachkräfte tragen in der Liste das Kennzeichen **Zugewiesen, ohne Lizenz**, darüber nennt ein Hinweis ihre Zahl. Sie können nicht synchronisieren, bis Plätze gebucht oder Zuweisungen entzogen werden; entziehen lässt sich ein Platz jederzeit, auch ohne gültige Lizenz.

> **Lizenz-Erinnerungen in der App:** Kostenpflichtige Lizenzen müssen regelmäßig online bestätigt werden. Bleibt das aus, erinnert die App ab **Tag 3** höchstens einmal täglich, ab **Tag 5** stündlich, und ab **Tag 10** verlangt sie die Bestätigung (Sperre bis zur erfolgreichen Prüfung – die Daten bleiben unangetastet).

Richtlinien

Menüpunkt **Richtlinien** (Recht *Richtlinien ansehen* bzw. *bearbeiten*). Richtlinien gelten organisationsweit, werden **versioniert** und an alle Apps verteilt.



Organisationsweite Vorgaben – von der Pflicht zur App-Sperre bis zur maximalen Offline-Dauer.

Richtlinie	Bedeutung
Private Datensätze erlauben	Fachkräfte dürfen einzelne Einträge privat führen
Nur-lokal erlauben	Inhalte, die bewusst nur auf dem Gerät bleiben
MFA erforderlich	Zwei-Faktor-Anmeldung ist Pflicht (Apps und Panel)
App-Sperre erforderlich	die App muss mit PIN oder Biometrie gesperrt sein
Max. Offline-Dauer (Tage)	wie lange ein Gerät ohne Serverkontakt weiterarbeiten darf
Sessiondauer (Minuten)	nach dieser Zeit ohne Aktivität ist eine erneute Anmeldung nötig
Sync-Intervall (Sekunden)	wie oft die App im Hintergrund synchronisiert
Mindest-Clientversion	ältere App-Versionen werden bei der Synchronisation abgewiesen
Geräte-Freigabe erforderlich	neue Geräte müssen erst freigegeben werden
Break-Glass aktiviert	Notfallzugriff ein- oder ausschalten
Vier-Augen-Prinzip im Datenschutz	Freigabe von Auskünften durch eine zweite Person
Hilfe & Kontakt in den Apps erlauben	Fachkräfte können aus App und Desktop Fehlerberichte, Funktionswünsche, allgemeine Anfragen und Sicherheitsmeldungen an Software Notion senden – nie mit App-Daten; ausgeschaltet ist der Bereich in den Apps nach der nächsten Synchronisation und im Panel ausgeblendet; im Panel behalten ihn nur Konten mit dem Recht *Richtlinien bearbeiten*; Standard an
Beta-Versionen bei Updates anzeigen	nur für die Systemadministration sichtbar: der Update-Hinweis bietet auch Vorabversionen an; nur für Testinstallationen empfohlen, Standard aus

Break-Glass (Notfallzugriff): In Ausnahmefällen – etwa bei akuter Kindeswohlgefährdung – kann eine berechtigte Person zeitlich begrenzt (höchstens 120 Minuten), mit Zwei-Faktor-Bestätigung und protokolliertem Grund auf einen Fall zugreifen, auch ohne reguläre Zuweisung. Jeder Zugriff steht im Audit.

KI-Modell: Ebenfalls unter Richtlinien wählen Sie das **Sprachmodell**, das die Apps für die lokale KI-Unterstützung verwenden. Die Modellgröße bestimmt den Download in der App. Die KI läuft weiterhin vollständig auf dem Gerät.

Hilfe & Kontakt

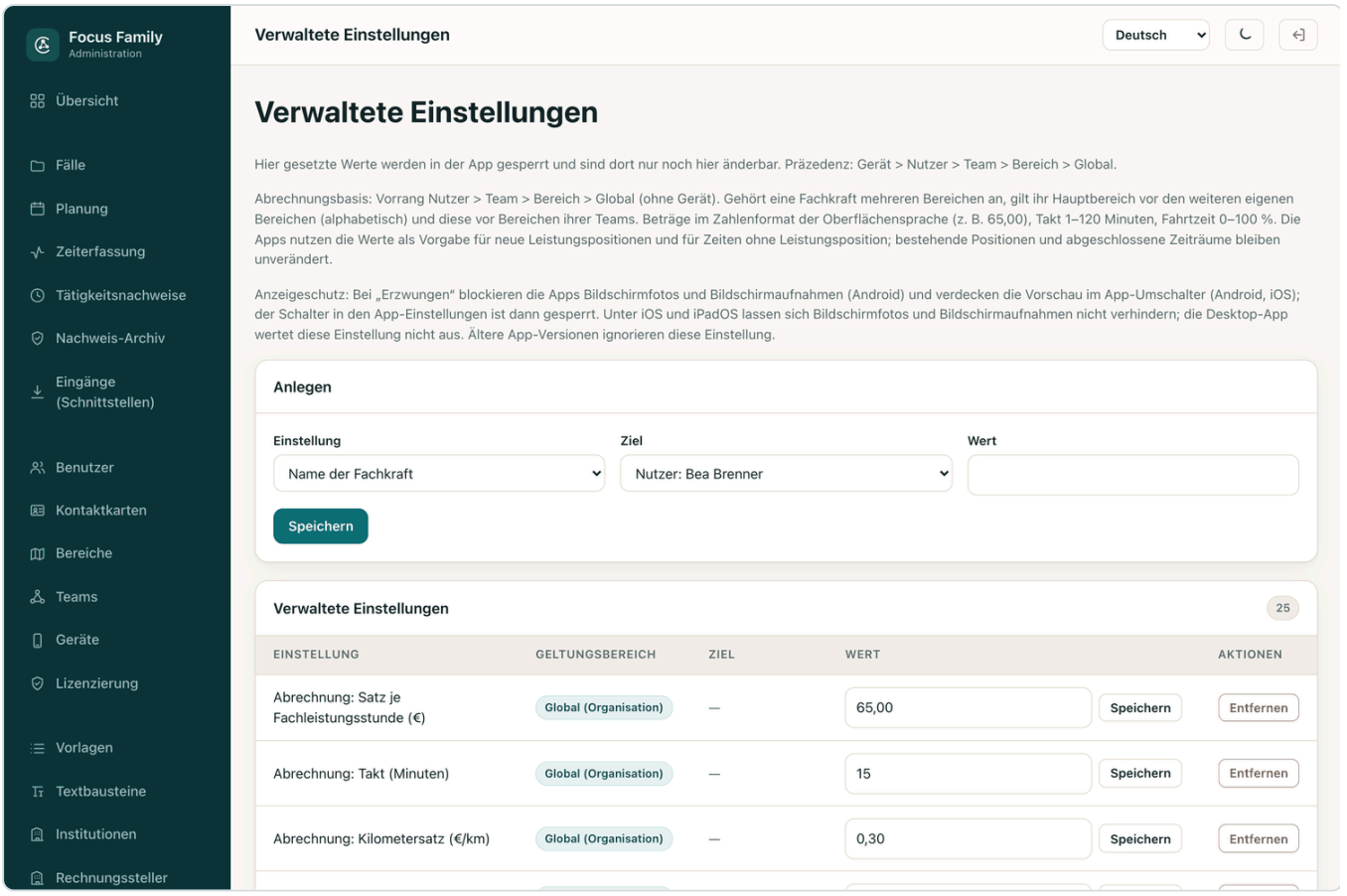
Menüpunkt **Hilfe & Kontakt** (für alle angemeldeten Konten, solange die Richtlinie **Hilfe & Kontakt in den Apps erlauben** an ist; Konten mit dem Recht *Richtlinien bearbeiten* sehen ihn immer). Hier senden Sie aus dem Admin-Panel einen **Fehlerbericht**, einen **Funktionswunsch**, eine **allgemeine Anfrage** oder eine **Sicherheitsmeldung** an Software Notion.

- Es werden **keine Daten aus dem Panel** übertragen – keine Fälle, Termine, Aufgaben, Dokumente oder Personen. Beschreiben Sie das Anliegen deshalb möglichst genau (Seite, Schritte, erwartetes und tatsächliches Ergebnis).
- **Prüfen** kontrolliert den Text auf Namen und Anschriften aus der Datenbank und entfernt Telefonnummern, E-Mail-Adressen und ähnliche Angaben. Die **Vorschau** zeigt danach genau, was gesendet wird: technische Angaben (Referenz, Panel-Version, Lizenzart, Focus-Family-ID, Server-Instanz) sowie Betreff und Text, die Sie noch korrigieren können. Beim **Absenden** wird der Text erneut geprüft.
- Antworten gehen an die angegebene E-Mail-Adresse (vorbelegt mit der Adresse Ihres Kontos).
- Das Panel sendet die Meldung selbst über HTTPS an `software-notion.de`. Hat der Server keinen Internetzugang, bietet die Seite **Text kopieren** und **Per E-Mail senden** an.
- Erfolgreich gesendete Meldungen stehen mit Art und Referenz – ohne Text – im Sicherheits-Audit.

Welche Daten übertragen und wann sie gelöscht werden, steht unter focusfamily.software-notion.de/support. Ob Fachkräfte den Bereich auch in den Apps sehen, legt die Richtlinie **Hilfe & Kontakt in den Apps erlauben** fest.

Verwaltete Einstellungen

Menüpunkt **Verwaltete Einstellungen** (Recht *Verwaltete Einstellungen ansehen* bzw. *bearbeiten*).



Zentral gesetzte Werte erscheinen in der App gesperrt. Jeder Wert gilt für einen Geltungsbereich.

Hier legen Sie Werte fest, die in der App **gesperrt** sind und nur noch hier geändert werden können – zum Beispiel **Träger-Name**, **Träger-Anschrift**, **Träger-Kontakt**, **Name der Fachkraft** oder das **Blob-Speicherlimit**.

Jeden Wert setzen Sie für einen **Geltungsbereich**: **Global (Organisation)**, **Bereich**, **Team**, **Nutzer** oder **Gerät**. Gilt für dieselbe Einstellung mehr als ein Wert, greift die Präzedenz:

> **Gerät > Nutzer > Team > Bereich > Global** – der speziellere Wert gewinnt.

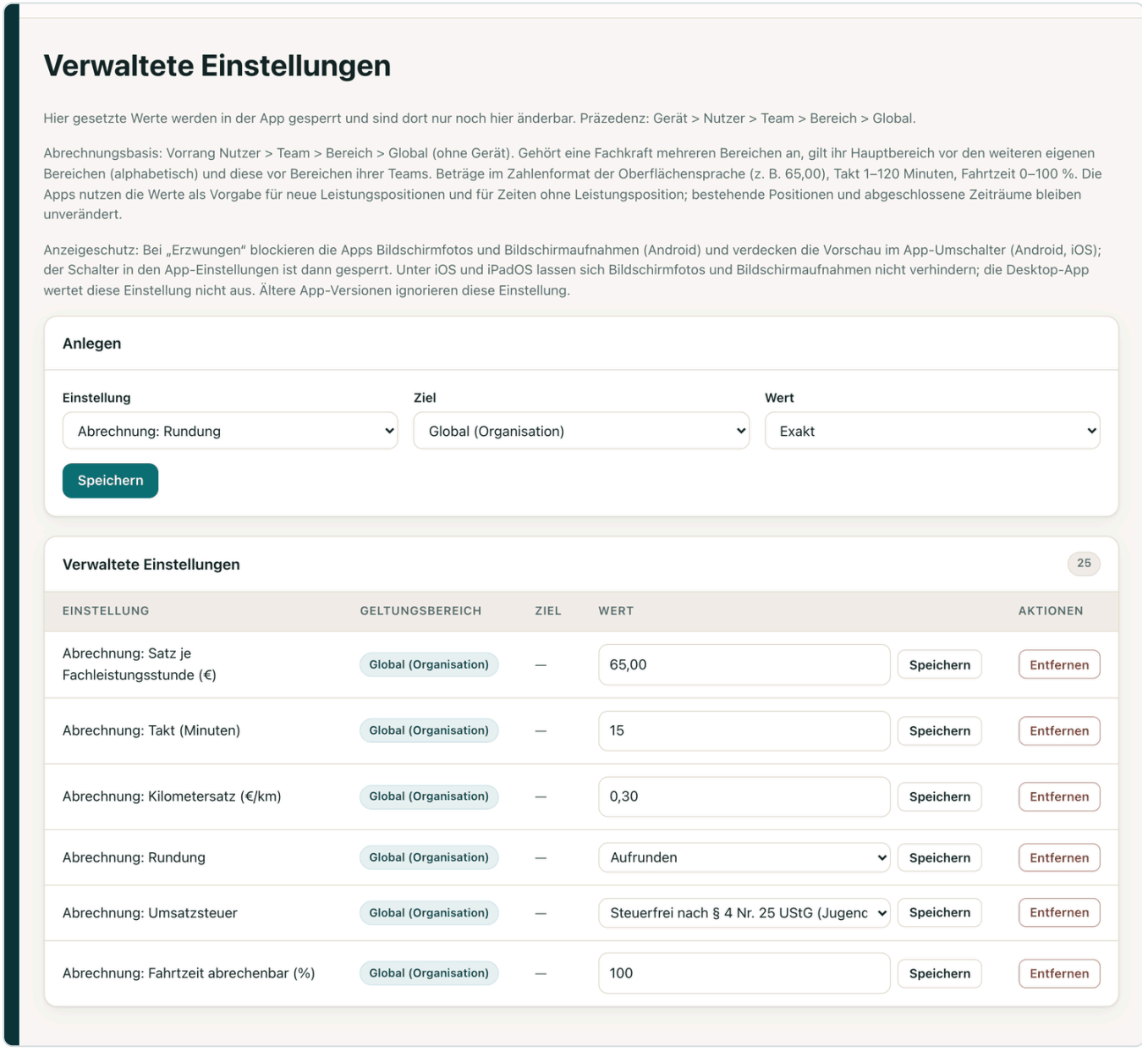
Ein Wert für einen **Bereich** gilt für die Fachkräfte dieses Bereichs und für die Mitglieder der Teams, die diesem Bereich angehören, solange der Bereich aktiv ist. Gelten für eine Fachkraft Werte mehrerer Bereiche, gewinnt der **Hauptbereich**, danach die weiteren eigenen Bereiche in alphabetischer Reihenfolge, danach Bereiche, die nur über Teams gelten (ebenfalls alphabetisch). Er wirkt unabhängig davon, ob der Bereichsmodus eingeschaltet ist. Bereichsgebundene Admins können Werte nur für ihre eigenen Bereiche, Teams, Fachkräfte und Geräte setzen; globale Werte sehen sie nur lesend.

Das **Blob-Speicherlimit** wird in **MB** angegeben und gilt **je Fachkraft** für alle ihre Dateien auf dem Server zusammen (kein Tageslimit). 512 GB entsprechen dem Wert `524288`. Unter **System** zeigt die Kachel „Speicherlimit je Fachkraft (global)“ den globalen Wert.

Abrechnungsbasis

Die Abrechnungsbasis besteht aus sechs Einstellungen, die einzeln **global, je Bereich, je Team oder je Nutzer** festgelegt werden (nicht je Gerät). Es gilt **Nutzer > Team > Bereich > Global**; jede Einstellung wird

für sich aufgelöst, ein Team oder Bereich kann also nur den Stundensatz abweichend festlegen und übernimmt alles andere global.



Die sechs Werte der Abrechnungsbasis; Beträge erscheinen im Zahlenformat der Oberflächensprache.

Einstellung	Vorgabe (branchenüblich)	Erlaubte Werte
Abrechnung: Satz je Fachleistungsstunde (€)	65,00	größer 0 bis 1000
Abrechnung: Takt (Minuten)	15	1–120
Abrechnung: Rundung	Aufrunden	Exakt, Aufrunden, Abrunden, Kaufmännisch
Abrechnung: Kilometersatz (€/km)	0,30	0 bis 5
Abrechnung: Fahrtzeit abrechenbar (%)	100	0–100
Abrechnung: Umsatzsteuer	Steuerfrei nach § 4 Nr. 25 UStG	Steuerfrei § 4 Nr. 25, Kleinunternehmer § 19, 19 %, 7 %

Die Vorgaben orientieren sich an ambulanten Hilfen der Kinder- und Jugendhilfe (z. B. SPFH). Sie werden für jede Organisation einmalig als globale Werte angelegt und lassen sich wie jeder andere Wert ändern. Bereits gesetzte Werte werden nie überschrieben; ein gelöschter Wert wird nicht erneut angelegt. Rundung und Umsatzsteuer wählen Sie aus einer Auswahlliste. Beträge zeigt das Panel im Zahlenformat der Oberflächensprache (Deutsch: `0,30`); bei der Eingabe werden Komma und Punkt erkannt, auch mit Tausendertrennzeichen (`1.000,00` oder `1,000.00`). Ein einzelnes Trennzeichen gilt immer als Dezimaltrennzeichen. Ungültige Werte lehnt das Panel ab.

So nutzen die Apps die Abrechnungsbasis:

- **Neue Leistungspositionen** in Rechnungssätzen werden mit Stundensatz, Takt und Rundung vorbelegt (bei der Einheit Kilometer mit dem Kilometersatz) und bleiben anpassbar. Das gilt auch für neue Positionen im Panel (Fallseite → Rechnungssätze, Abrechnungsbasis der zuständigen Fachkraft).
- **Zeiten ohne passende Leistungsposition** werden im Rechnungsentwurf und in der E-Rechnung als „Fachleistungsstunde (Vorgabe)“ bzw. „Fahrtzeit (Vorgabe)“ bepreist. Fahrtzeit wird mit dem eingestellten Anteil des Stundensatzes berechnet; bei 0 % ist sie nicht abrechenbar.
- **Kilometer** aus aufgezeichneten Fahrten werden genau einmal abgerechnet: im Fall der Fahrt, zum Fahrtdatum, für die Fachkraft, der die Fahrt gehört. Gilt am Fahrtdatum eine Kilometer-Position des Rechnungssatzes, wird sie verwendet, sonst die „Kilometerpauschale (Vorgabe)“ aus der Abrechnungsbasis dieser Fachkraft. Fahrten ohne Fall werden nicht abgerechnet.
- Die **Umsatzsteuer** für E-Rechnungen (XRechnung, ZUGFeRD) ist in den Apps gesperrt und als „Vom Träger festgelegt“ markiert.

Bestehende Leistungspositionen bleiben maßgeblich. Abgeschlossene Zeiträume behalten die Preise, die beim Abschluss galten; spätere Änderungen der Abrechnungsbasis wirken nur auf offene Zeiträume. Auch die Kilometer aus Fahrten und der Kilometersatz werden beim Abschluss festgehalten, sodass der Rechnungsentwurf vor und nach dem Abschluss denselben Betrag ergibt.

Rechnungssteller

Menüpunkt **Rechnungssteller** im Konfigurationsbereich (Recht *Rechnungsdaten verwalten*). Hier werden die Angaben gepflegt, die als Rechnungssteller auf jeder E-Rechnung (XRechnung, ZUGFeRD) stehen,

solange die Apps mit diesem Server verbunden sind. Es gibt genau einen Datensatz je Organisation.

Abschnitt	Felder
Rechnungssteller und Kontakt	Name (Pflicht), Ansprechperson, Telefon, E-Mail, Straße, Hausnummer, PLZ, Ort, Land
Steuerangaben	Steuernummer, Umsatzsteuer-Identifikationsnummer
Bankverbindung	IBAN, BIC, Kontoinhaber
Rechnungsnummern und Zahlungsziel	Präfix der Rechnungsnummer, Zahlungsziel in Tagen (0–365, Vorgabe 30)

Beim Speichern prüft das Panel die Angaben: Name vorhanden, Anschrift vollständig und Postleitzahl passend zum Land, gültige E-Mail-Adresse, **IBAN mit korrekter Prüfziffer**, **USt-IdNr. im gültigen Format** (`DE` und neun Ziffern, andere Länder zwei Buchstaben und 2–12 Zeichen), BIC mit 8 oder 11 Zeichen. IBAN, USt-IdNr. und BIC werden ohne Leerzeichen in Großbuchstaben gespeichert. Für eine gültige E-Rechnung ist zusätzlich die Steuernummer oder die USt-IdNr. nötig; das prüft die App beim Erstellen. Jede Änderung erscheint im Sicherheits-Audit als „Rechnungsdaten geändert“ mit den geänderten Feldern. Bereichsgebundene Admins sehen die Seite nur lesend.

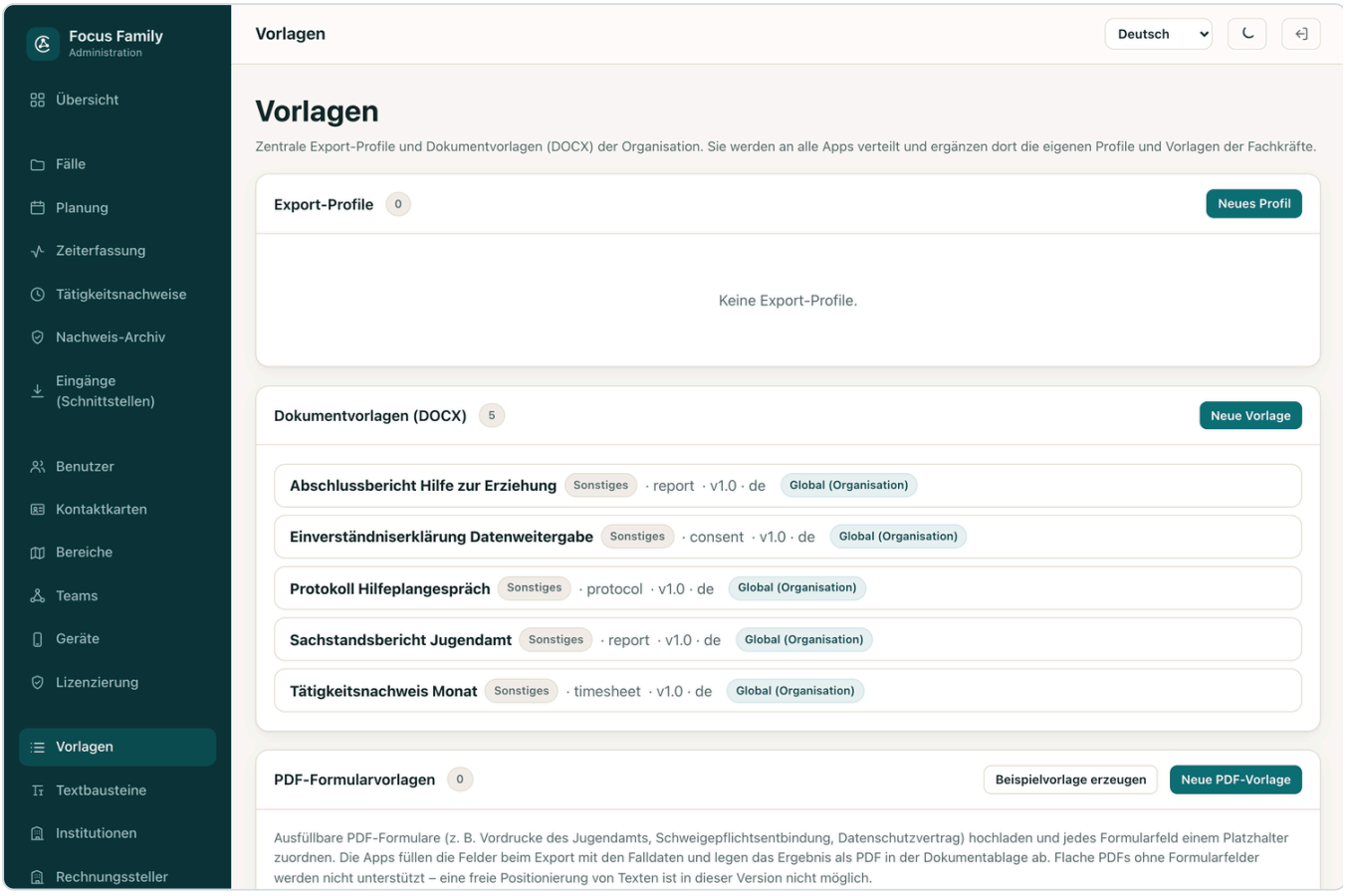
So nutzen die Apps die Rechnungsdaten:

- Ausgeliefert werden sie **nur an Konten mit dem App-Recht *E-Rechnungen erstellen*** – nicht über die verwalteten Einstellungen, die jedes Gerät erreichen. Die Apps speichern sie verschlüsselt, aktualisieren sie bei jeder Synchronisation und löschen sie, sobald das Recht fehlt, die Daten hier entfernt wurden oder das Gerät vom Server getrennt wird.
- In verbundenen Apps sind die eigenen Rechnungssteller-Einstellungen ausgeblendet; sie lassen sich dort weder ansehen noch ändern.
- Ohne das Recht ist die Schaltfläche für E-Rechnungen ausgeblendet, mit dem Hinweis „Für E-Rechnungen ist eine Berechtigung erforderlich.“ Sind hier noch keine Daten hinterlegt, meldet die App „Rechnungsdaten sind noch nicht hinterlegt.“
- Das Präfix gilt für alle Geräte. Rechnungsnummern sind organisationsweit eindeutig, auch ohne Verbindung beim Erstellen: Der Server weist jedem Gerät beim ersten Abruf der Rechnungsdaten eine feste **Nummernserie** zu (nie wiederverwendet, auch nicht nach dem Entfernen eines Geräts). Format: Präfix + Serie (mindestens zwei Ziffern) + `-` + vierstelliger Zähler, z. B. `TR-07-0001`, mit dem Standardpräfix `RE-2026-07-0001`. Die Rechnungsnummer wird automatisch aus der Serie des Geräts vergeben und lässt sich nicht von Hand ändern („Die Rechnungsnummer wird automatisch vergeben.“). Zähler und vergebene Nummern führt das Gerät verschlüsselt; eine Nummer gilt erst nach dem erfolgreichen Export als vergeben – ein abgebrochener oder fehlgeschlagener Export verbraucht keine Nummer. Vor jedem Export prüft die App, dass die Nummer zur eigenen Serie gehört und in dieser Serie noch nicht vergeben wurde; eine vergebene Nummer wird nie erneut verwendet, auch nicht nach einem Neustart oder bei Rückkehr zu einer früheren Serie. Der Zähler läuft nur vorwärts und beginnt nur bei einer neuen Serie (etwa nach erneuter Registrierung) wieder bei 1. Ohne zugewiesene Serie lassen sich keine E-Rechnungen erstellen („Rechnungsdaten sind noch nicht hinterlegt.“). Berechtigung und Rechnungsdaten werden unmittelbar vor jedem Export erneut geprüft. Die Umsatzsteuer kommt weiterhin aus der **Abrechnungsbasis**.

Beim Update von 1.0.0 erhalten alle bestehenden Fach-Admins beide neuen Rechte; alle anderen Konten bekommen sie bei Bedarf über die Rechte-Checkliste (Zeile „E-Rechnungen“).

Vorlagen und Export-Profile

Menüpunkt **Vorlagen** (Recht *Vorlagen & Export-Profile verwalten*).



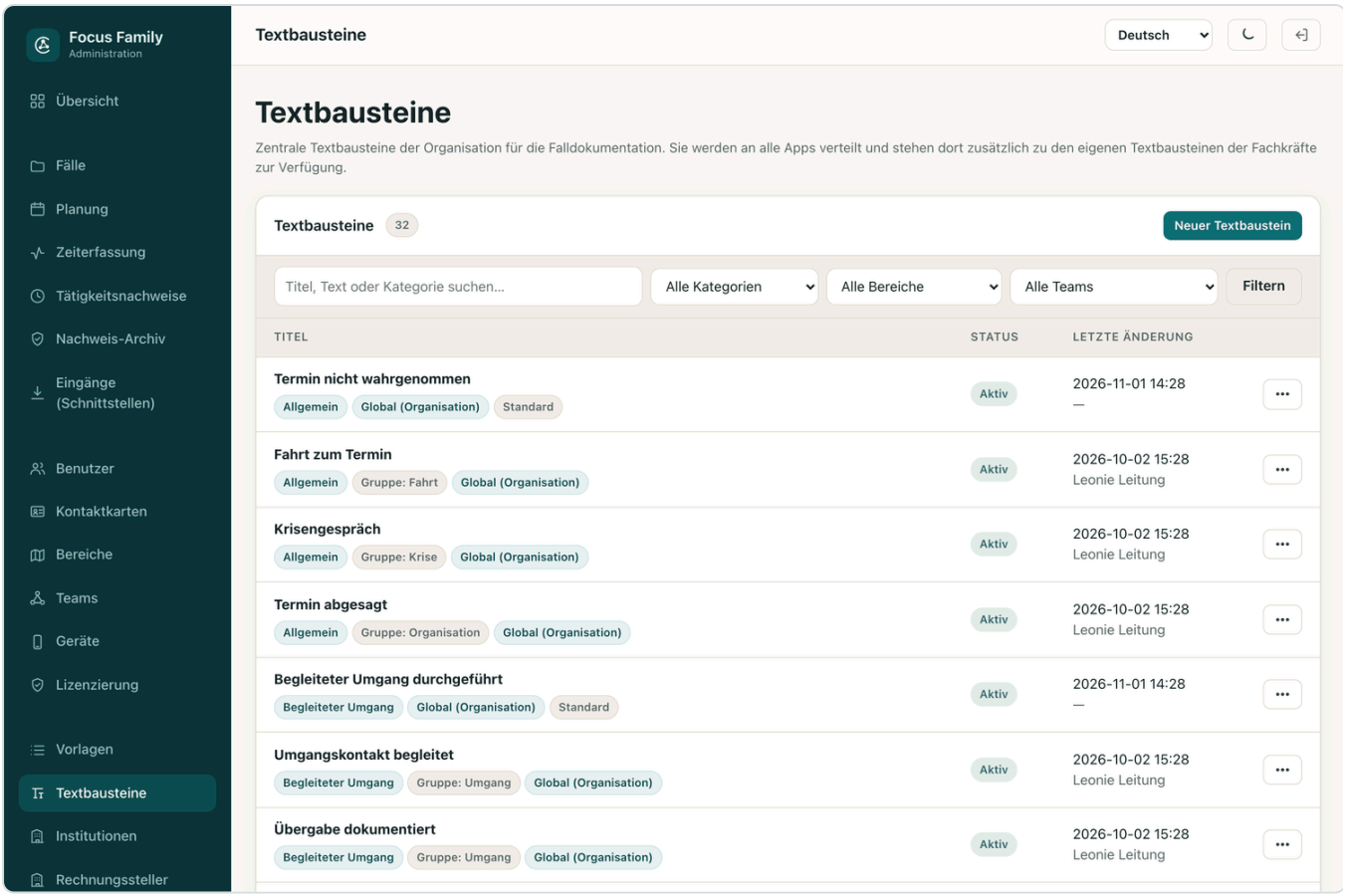
Zentrale Export-Profile und Word-Vorlagen werden an alle Apps verteilt.

- **Export-Profile** – Vorgaben für den Export: Formate, Deckblatt, Logo, Unterschriftsfelder und Datensparsamkeit („Namen pseudonymisieren", „Anschrift entfernen").
- **Dokumentvorlagen (DOCX)** – Word-Vorlagen mit Platzhaltern, höchstens 5 MB je Datei.
- **PDF-Formulare** – ausfüllbare Formulare Ihres Trägers, die die Fachkräfte in der E-Akte direkt am Gerät ausfüllen können. PDF-Dateien mit Berechtigungsschutz (etwa amtliche Formulare, die sich ohne Kennwort öffnen lassen) werden unterstützt; mit einem Kennwort zum Öffnen geschützte PDF-Dateien lehnt das Panel beim Hochladen mit einem Hinweis ab.

Diese zentralen Vorgaben sind eine **Basis**; eigene Profile und Vorlagen der Fachkräfte bleiben weiterhin möglich.

Textbausteine

Menüpunkt **Textbausteine** (Rechte *Textbausteine ansehen* / *erstellen* / *verwalten*).



Bausteine auf Organisations-, Team- und persönlicher Ebene, mit Kategorien und Standardvorlagen.

Textbausteine sind wiederverwendbare Textschnipsel für Dokumentation und Tätigkeitsnachweis. Sie werden an alle Apps verteilt und stehen dort zusätzlich zu den eigenen Bausteinen der Fachkräfte zur Verfügung.

- **Neuer Textbaustein** legt einen Baustein an; **Bearbeiten** passt ihn an; **Deaktivieren** nimmt ihn aus dem Umlauf.
- Es gibt die Ebenen **Organisation**, **Team** und **persönlich**. Persönliche Bausteine gehören der jeweiligen Fachkraft und können nur von ihr geändert werden.
- Der Server bringt **Standard-Textbausteine** mit, damit Sie nicht bei null anfangen. Sie lassen sich anpassen oder deaktivieren.
- **Titel sind eindeutig:** Innerhalb der Organisation, eines Teams und der persönlichen Bausteine einer Fachkraft darf jeder Titel nur einmal vorkommen; Groß- und Kleinschreibung sowie zusätzliche Leerzeichen zählen nicht als Unterschied. Organisations- und Teambausteine dürfen einander nicht gleichen. **Duplizieren** vergibt fortlaufende Titel („(Kopie)", „(Kopie) 2" …). Bereits doppelte Titel markiert die Liste mit **„Titel doppelt – bitte umbenennen"**; in den Apps erscheinen gleichnamige Bausteine mit ihrer Herkunft, z. B. „Anrede · Organisation".

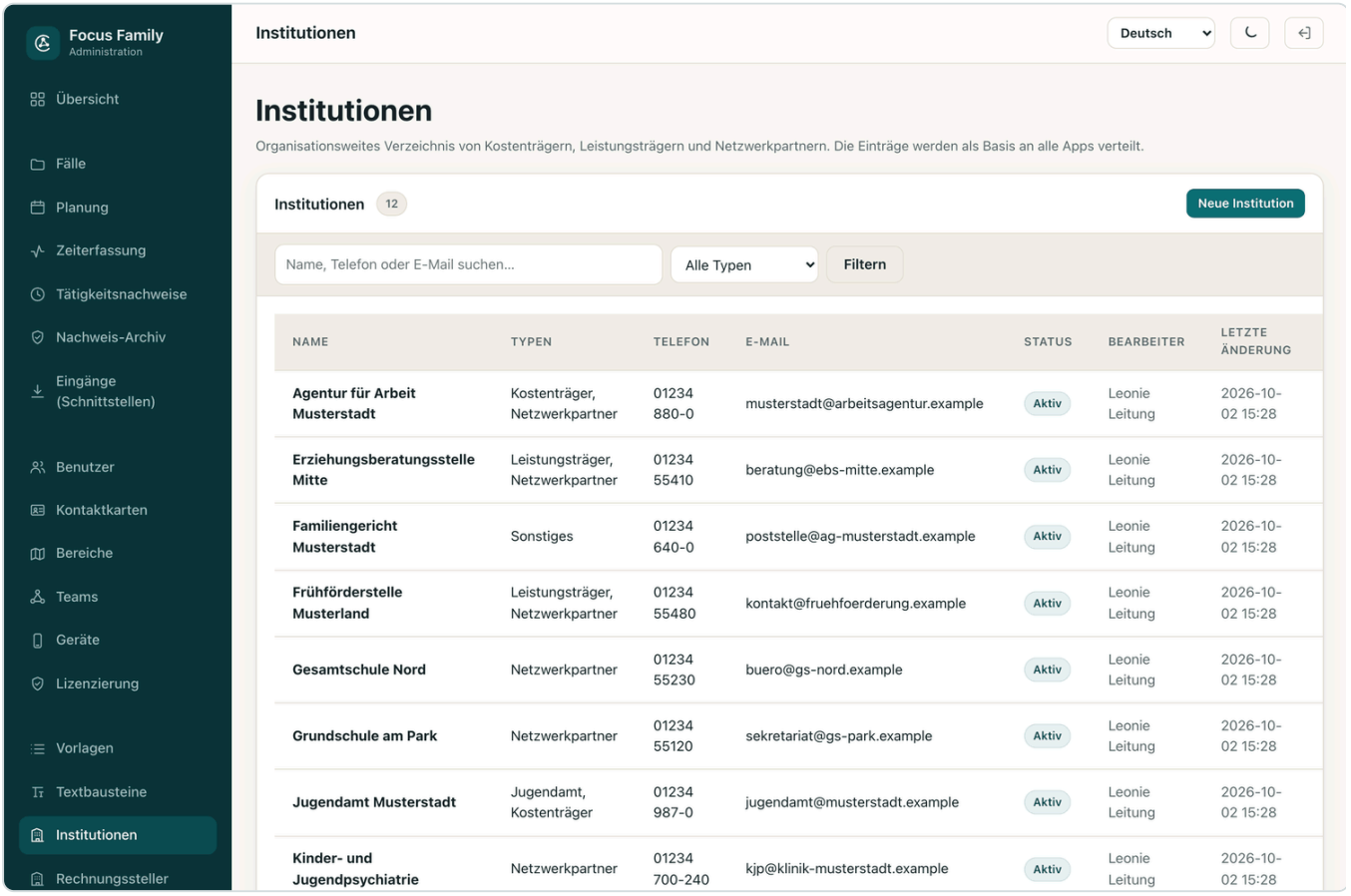
Kataloge: Institutionen, Maßnahmen, Tätigkeitsarten

Drei Kataloge sorgen dafür, dass alle Fachkräfte mit denselben Begriffen arbeiten.

In allen drei Katalogen bietet das Menü ⋯ einer Zeile **Bearbeiten**, **Deaktivieren/Aktivieren** und **Löschen**. **Deaktivieren** nimmt einen Eintrag aus der Auswahl, er bleibt aber in der Liste; **Löschen** entfernt ihn endgültig. Tätigkeitsarten, die in Zeiteinträgen oder Rechnungssätzen verwendet werden, lassen sich nicht löschen, nur deaktivieren – auf den Geräten bleiben sie für bestehende Einträge erhalten. Ist eine Suche oder ein Filter gesetzt, führt **Filter zurücksetzen** zur ungefilterten Liste zurück.

Adressen werden geprüft: Das Land ist ein zweistelliges Kürzel (z. B. DE, AT), die PLZ passt zum Land (Deutschland: fünf Ziffern), zu einer Straße gehören PLZ und Ort, zu einer Hausnummer eine Straße. Dieselbe Prüfung gilt für Personen, Anschriften und Kontaktkarten.

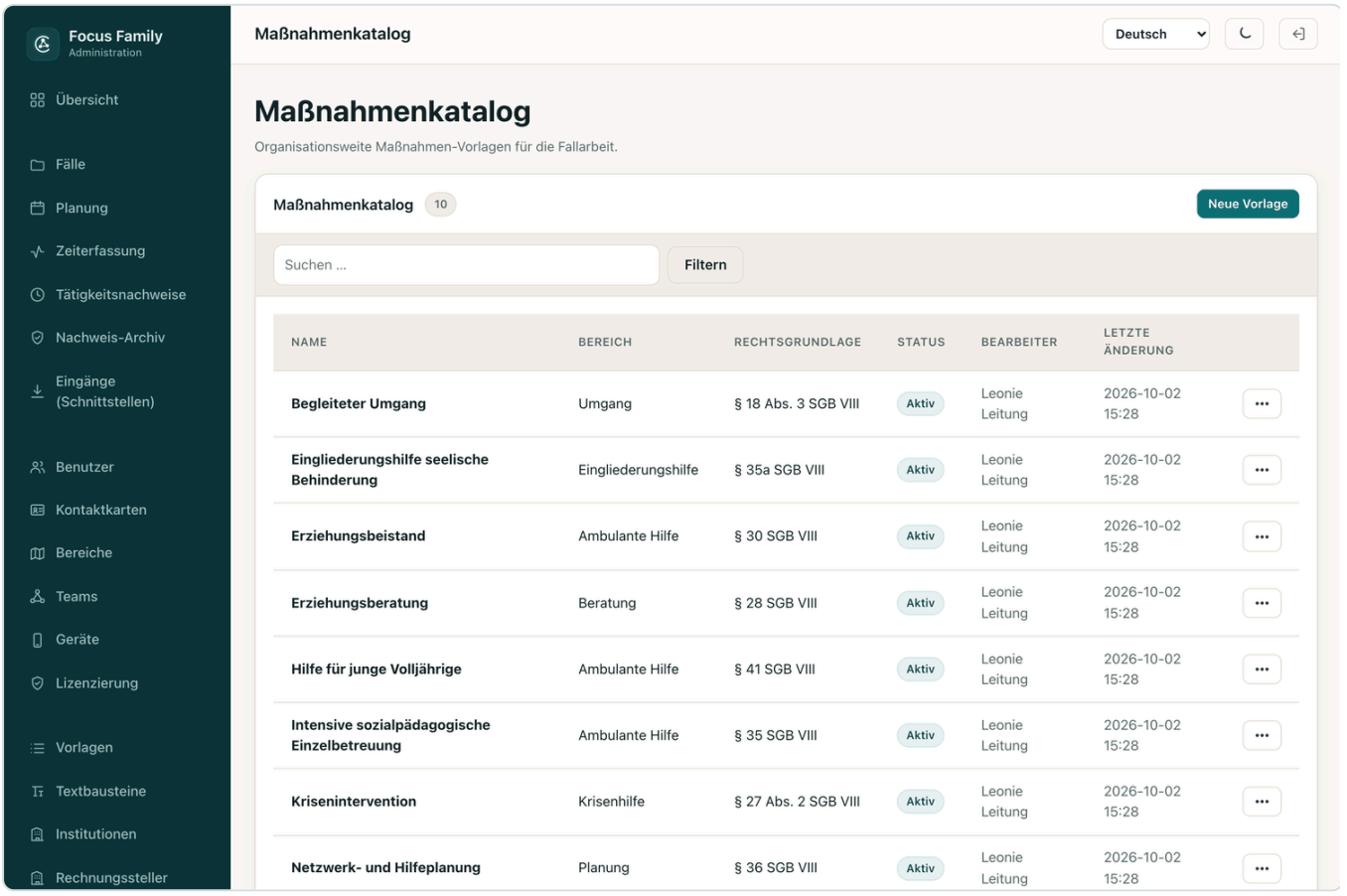
Institutionen



Jugendämter, Schulen, Kitas, Beratungsstellen und Kostenträger zentral gepflegt.

Im Menüpunkt **Institutionen** pflegen Sie die Einrichtungen, mit denen Ihr Träger zusammenarbeitet – mit Art, Anschrift und Kontaktdaten. In der App stehen sie beim Anlegen von Fällen und Netzwerkkontakten zur Auswahl.

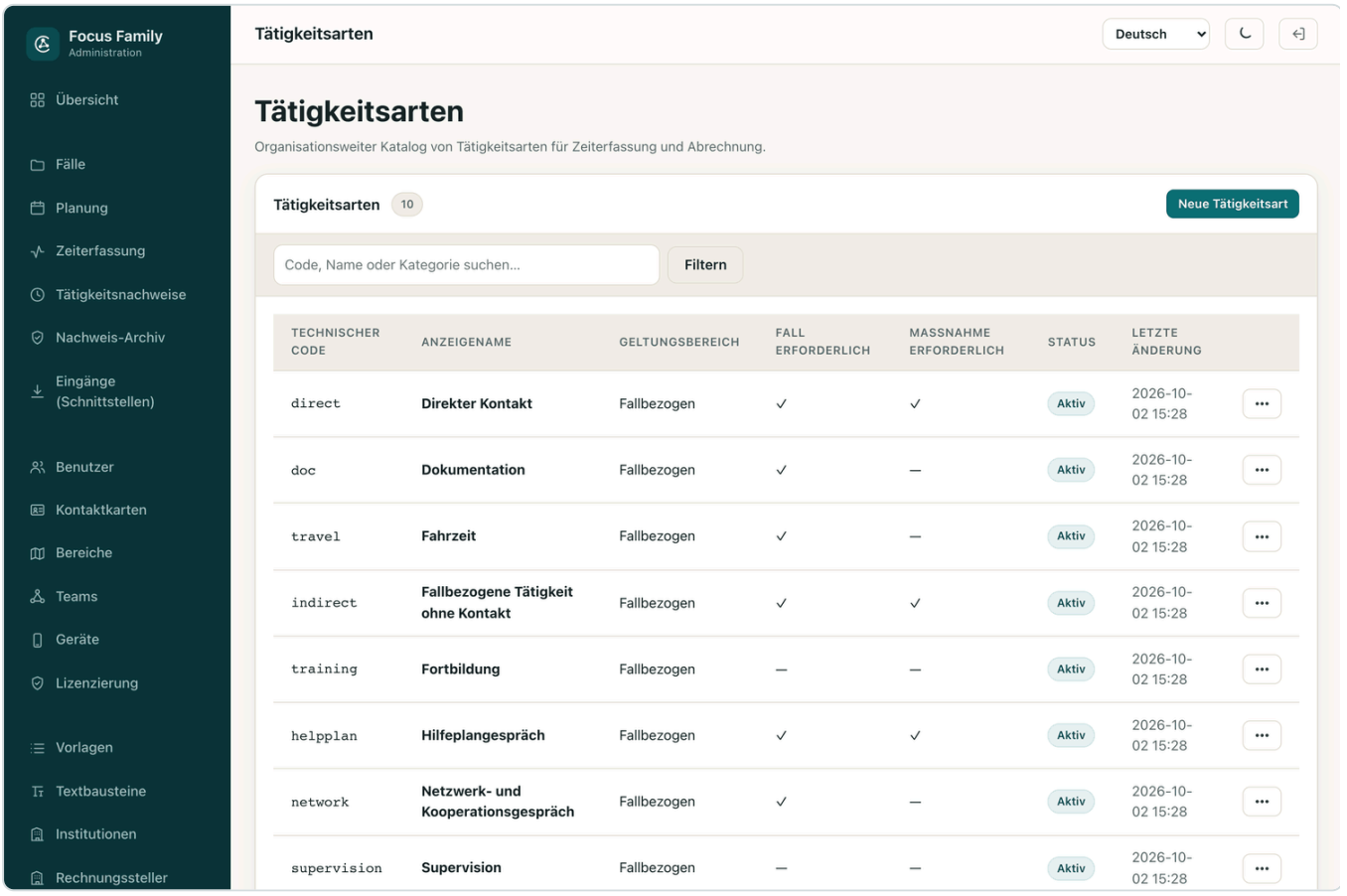
Maßnahmenkatalog



Die Hilfearten und Leistungen Ihres Trägers – Grundlage für Fälle und Abrechnung.

Der **Maßnahmenkatalog** enthält die Hilfe- und Leistungsarten Ihres Trägers (z. B. SPFH, Begleiteter Umgang, Erziehungsbeistandschaft) mit Bezeichnung, Kürzel und den Angaben, die für Nachweis und Abrechnung gebraucht werden.

Tätigkeitsarten



Tätigkeitsarten steuern, wie Zeiten erfasst und im Nachweis gewertet werden.

Tätigkeitsarten bestimmen, welche Kategorien in der Zeiterfassung zur Auswahl stehen – etwa Klientenkontakt (persönlich), Fahrtzeit, Dokumentation oder Telefonat – und ob eine Tätigkeit als **direkter Kontakt** oder **indirekt** zählt. Daraus berechnet der Tätigkeitsnachweis die Kontaktquote.

Kalender & Belegungen im Fall

Liest eine Fachkraft einen geteilten Kalender einer beteiligten Person ein oder erfasst Termine, die ohne sie stattfinden, erscheint das in der Fall-Detailseite im Abschnitt **Kalender & Belegungen**: je Kalender die Person, der Zeitpunkt der Einlesung und die Anzahl der Einträge, darunter die Belegungen mit Datum, Zeitfenster und Herkunft (manuell erfasst oder aus einem Kalender). Der Abschnitt erscheint nur, wenn Einträge vorliegen, und setzt das Recht zum Ansehen des Kalenders voraus.

Kontaktkarten und Vertretungen

Menüpunkt **Kontaktkarten** – für Fachkräfte ohne besondere Rechte heißt er **Meine Kontaktdaten**.

Hier entsteht, was die Fachkräfte in der App an Familien weitergeben: eigene Erreichbarkeit und die der Vertretung.

Wer darf was?

- **Jede Fachkraft** pflegt ihre **eigene** Kontaktkarte selbst – im Panel, in der App und auf dem Desktop. Dafür ist kein Recht nötig.
- Das Recht *Kontaktkarten anderer Fachkräfte & Vertretungen verwalten* (im **Fach-Admin** enthalten) ergänzt die Träger-Kontaktdaten, die Karten aller Fachkräfte und die Vertretungen.

Träger-Kontaktdaten

Einmal zentral gepflegt – Träger/Einrichtung, Telefon, E-Mail, Web, Anschrift und ein Notfallkontakt. Diese Angaben gelten für **jede** Kontaktkarte, solange die Fachkraft das jeweilige Feld nicht selbst füllt. Der Schalter **Fachkräfte dürfen ihre Kontaktkarte in der App selbst bearbeiten** entscheidet, ob Selbstpflege erlaubt ist; ist er aus, sind die Karten in App und Desktop schreibgeschützt und werden ausschließlich hier gepflegt.

Kontaktkarten der Fachkräfte

Die Tabelle zeigt alle aktiven Fachkräfte mit Funktion, Telefon, Mobil, E-Mail, Erreichbarkeit und der Freigabe zur Weitergabe. **Bearbeiten** öffnet die vollständige Karte:

- **Funktion**, **Bereich / Team**, **Träger / Einrichtung**
- **Telefon (dienstlich)**, **Mobil**, **E-Mail**, **Web**
- **Anschrift** für postalische Themen
- **Erreichbarkeit**: je Wochentag bis zu zwei Zeitfenster im Wochenraster, dazu ein freier Hinweis
- **Im Notfall**, **Notiz** und der Schalter **Karte darf weitergegeben werden**

Leere Felder erben die Träger-Angaben. Eine Karte ohne Kontaktmöglichkeit wird in der App gar nicht erst zum Teilen angeboten.

Vertretungen

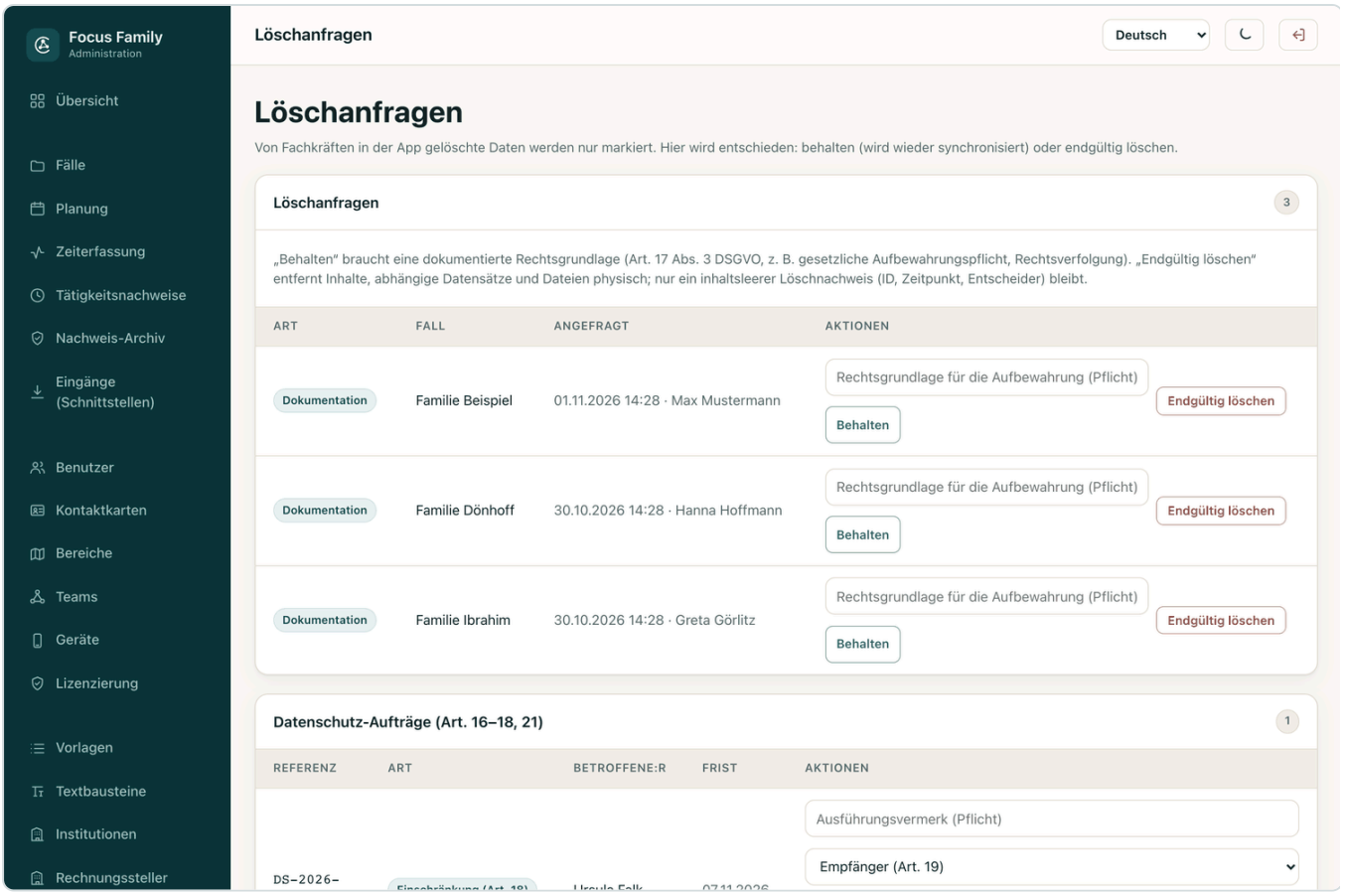
Vertretung eintragen hält fest, wer welche Fachkraft von wann bis wann vertritt, mit optionalem Hinweis (zum Beispiel „Urlaub"). Die Vertretung erscheint danach in der App der abwesenden Fachkraft und kann von ihr direkt an Familien weitergegeben werden. Regeln:

- Zwei verschiedene, aktive Fachkräfte; Zeitraum in der Zukunft, höchstens ein Jahr.
- Überschneidende Vertretungen derselben Paarung werden abgelehnt.
- **Beenden** stoppt eine laufende Vertretung sofort.
- Die Liste zeigt auch die **Fall-Vertretungen** aus der App. Die Spalte **Geltungsbereich** unterscheidet „Ganze Organisation“ von „Fall: …“, und **Beenden** funktioniert für beide Arten. In den Apps sehen Fall-Vertretungen nur die Fachkräfte des jeweiligen Falls.

Jede Änderung an Karten, Träger-Daten und Vertretungen steht im Audit-Log.

Löschanfragen

Menüpunkt **Löschanfragen** (Recht *Löschanfragen prüfen*).



Von Fachkräften gelöschte Daten werden zunächst nur markiert und hier zur Entscheidung vorgelegt.

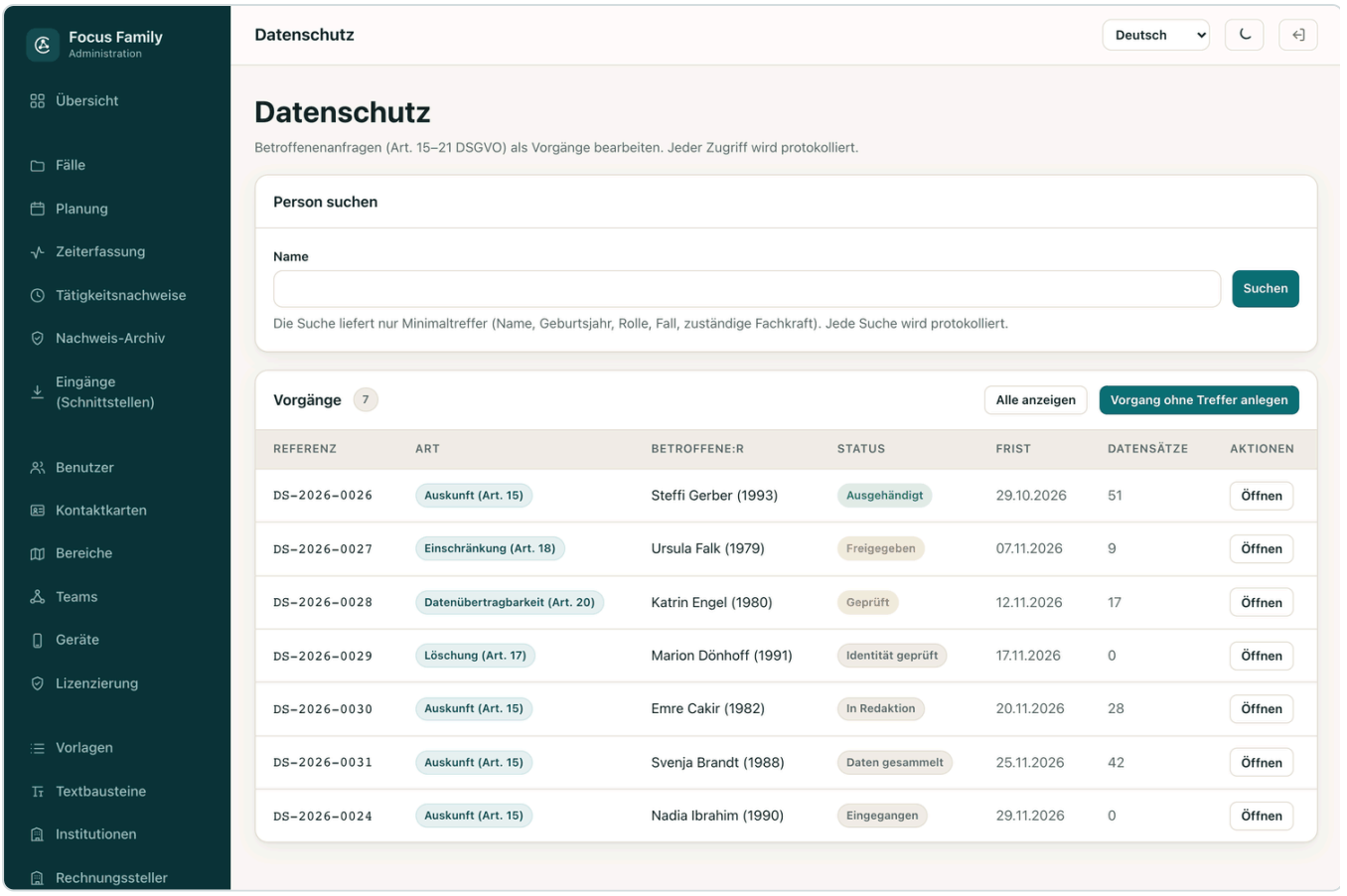
Löscht eine Fachkraft in der App Daten, werden diese zunächst **nur markiert**. Sie entscheiden je Eintrag:

- **Behalten** – die Daten bleiben erhalten und werden wieder zu den Geräten synchronisiert. Sie geben die **Rechtsgrundlage** für die Aufbewahrung an (z. B. gesetzliche Aufbewahrungspflicht, laufendes Verfahren); sie wird am Datensatz gespeichert.
- **Endgültig löschen** – Inhalte, abhängige Datensätze und Dateien werden **physisch und unwiderruflich** entfernt; es bleibt nur ein inhaltsleerer Löschnachweis. Bei einem Fall entfernen die Geräte den Fall beim nächsten Sync. Es erscheint eine Sicherheitsabfrage.

Auf derselben Seite sehen Sie **eingeschränkte Datensätze** (Art. 18/21 DSGVO). Eine Einschränkung lässt sich nur aufheben, wenn Sie **Datum und Weg** der vorherigen Information an die betroffene Person sowie die **Rechtsgrundlage** der Aufhebung eintragen.

Datenschutz: Betroffenenanfragen und Dokumente

Der Bereich **Datenschutz** ist für Ihre Datenschutzbeauftragte beziehungsweise Ihren Datenschutzbeauftragten (DSB).



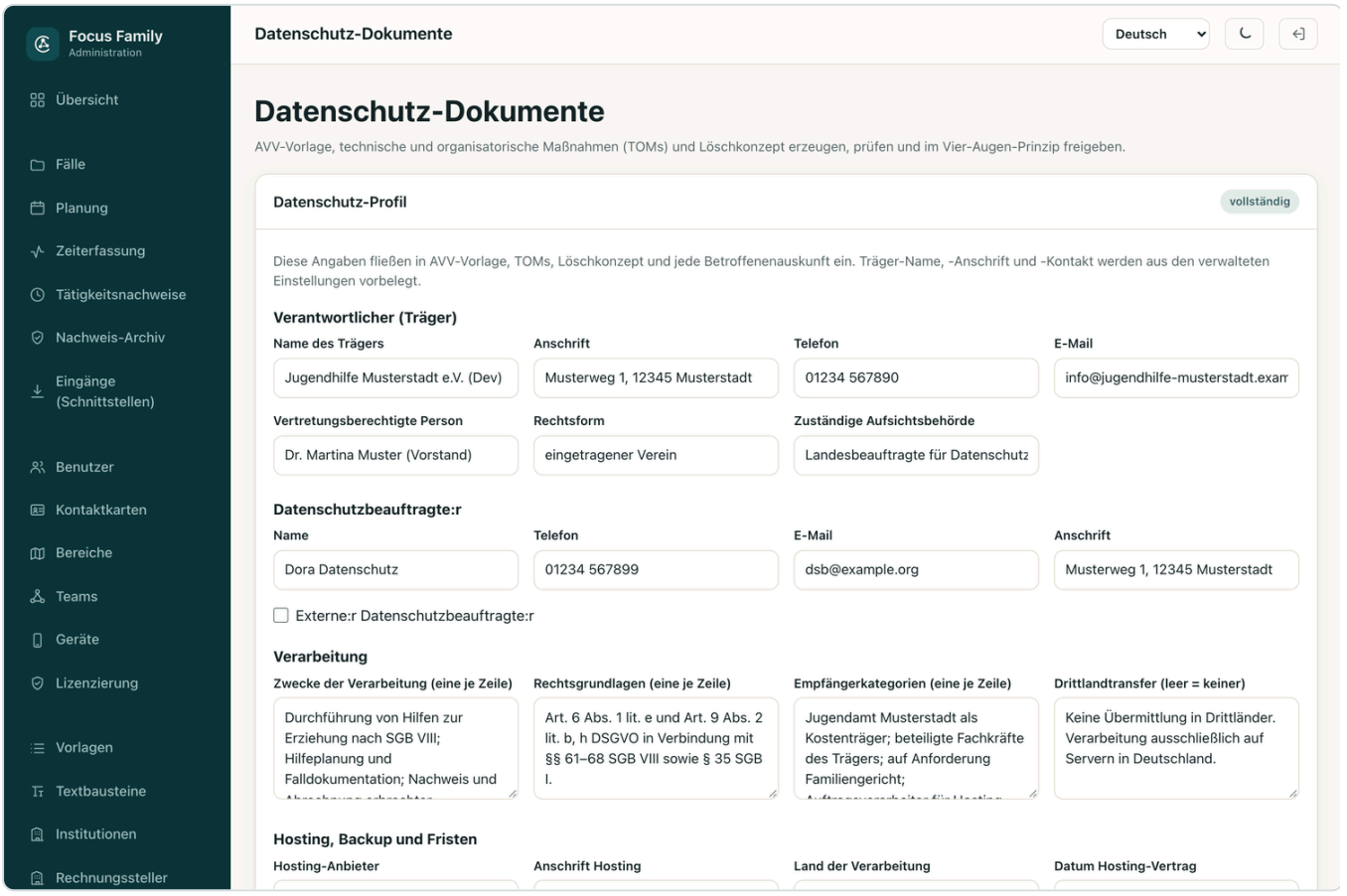
Vorgänge zu Betroffenenrechten – von der Identitätsprüfung über die Redaktion bis zur Freigabe.

Einrichtung

Legen Sie das Konto mit der Art **Datenschutzbeauftragte:r** an und setzen Sie die Häkchen im Block **Datenschutz**. Ein solches Konto kann sich **nicht in den Apps anmelden**, sofern es keine fachlichen Rechte hat.

Weil die endgültige Freigabe standardmäßig durch eine **zweite Person** erfolgt (Vier-Augen-Prinzip), brauchen Sie ein zweites Konto mit dem Recht **Freigabe (Vier-Augen)**. Kleine Träger ohne zweite Person schalten das Vier-Augen-Prinzip unter **Richtlinien** ab – protokolliert wird trotzdem jeder Schritt.

Vor der ersten Anfrage: Dokumente erzeugen



Datenschutz-Profil sowie AVV-Vorlage, TOMs und Löschkonzept als Entwurf, geprüft und final.

1. **Datenschutz-Dokumente** öffnen und das **Datenschutz-Profil** ausfüllen: Träger, DSB-Kontakt, Aufsichtsbehörde, Zwecke, Rechtsgrundlagen, Hosting und Löschfristen.
2. Die drei Dokumente erzeugen: **AVV-Vorlage**, **TOMs** und **Löschkonzept**.
3. Jedes Dokument entsteht als **Entwurf** mit Wasserzeichen, wird als **geprüft** markiert und von einer **zweiten Person finalisiert**. Ein neuer Entwurf verwirft ältere, noch nicht finalisierte Versionen.

Nur **finale** Versionen werden Auskünften beigelegt. Passen die Dokumente nicht mehr zum Profil oder zu den Richtlinien, zeigt die Seite „Veraltet" – dann ist eine neue Finalisierung nötig.

Eine Anfrage bearbeiten

1. **Datenschutz** öffnen und die Person per Name suchen. Sie sehen nur Minimaltreffer (Name, Geburtsjahr, Rolle, Fall, zuständige Fachkraft). **Vorgang anlegen** – die Monatsfrist beginnt mit dem eingetragenen Eingangsdatum und lässt sich bei komplexen Anfragen einmalig um zwei Monate verlängern.
2. **Identität bestätigen** und festhalten, wie Sie sie geprüft haben.
3. **Daten sammeln** – das Panel stellt alles zusammen, was zu dieser Person gespeichert ist. Andere Familienmitglieder bleiben außen vor.
4. **Redigieren** – jeden Datensatz mit Freitext öffnen und Angaben zu Dritten entfernen. Das System markiert mögliche Nennungen anderer Personen; Sie entscheiden: entfernen, mit Begründung ausschließen oder mit Begründung belassen. Jede Ansicht wird protokolliert.

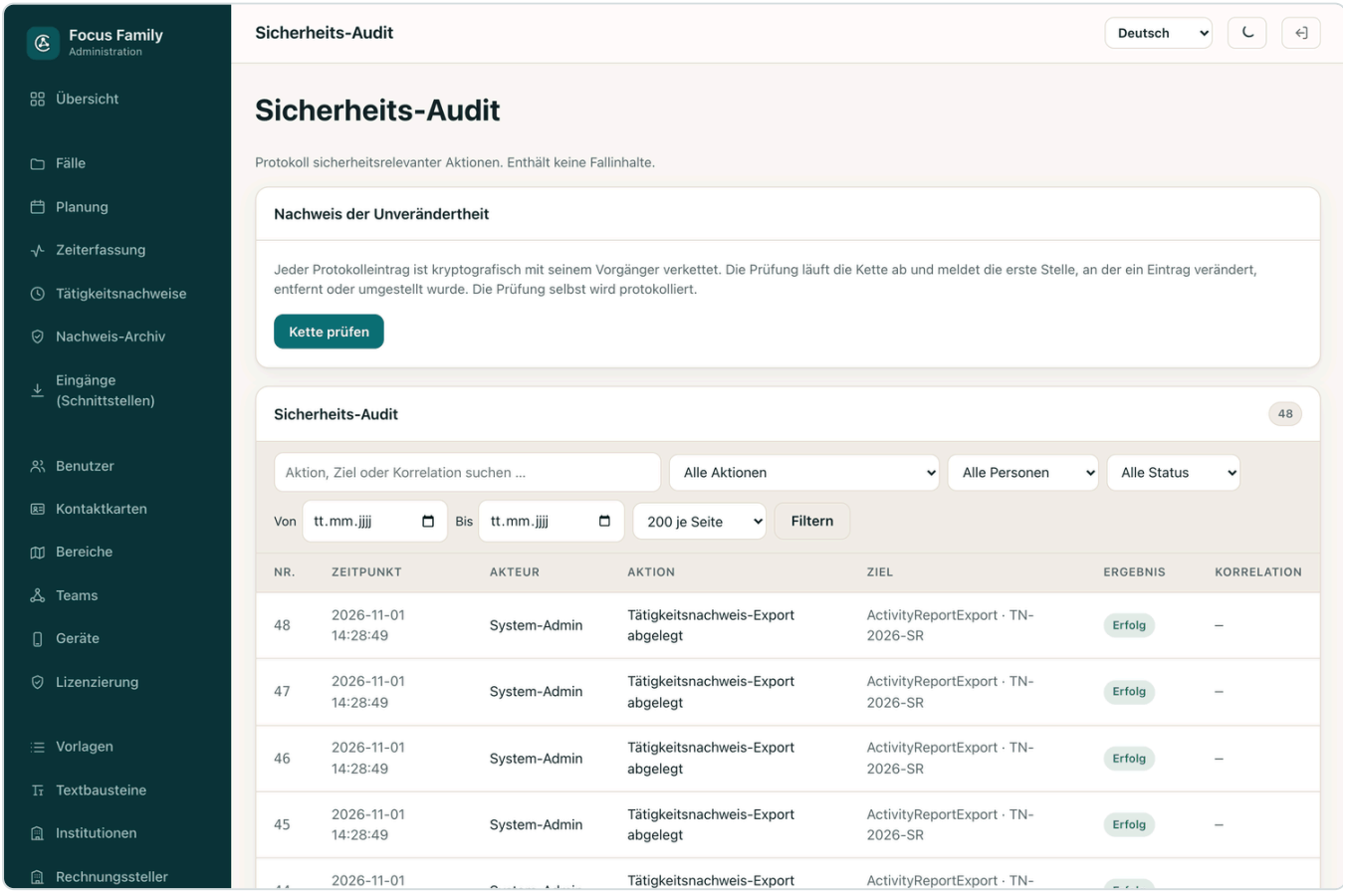
5. **Als geprüft markieren**, sobald die Checkliste vollständig ist.
6. Eine **zweite Person** gibt im Tab **Freigabe** frei. Das Panel erzeugt das Paket (Auskunft als PDF und DOCX, maschinenlesbares JSON, die drei Dokumente und eine Prüfsummendatei) und zeigt das **Passwort einmalig**. Laden Sie das Paket sofort herunter – der Link funktioniert nur einmal – und übermitteln Sie das Passwort **getrennt** (telefonisch oder per Brief).
7. Den Vorgang als **ausgehändigt** und später als **abgeschlossen** markieren.

> Das verschlüsselte Archiv öffnen Sie mit 7-Zip, WinRAR, Keka oder PeaZip – nicht mit den eingebauten Entpackern von Windows und macOS.

Weitere Betroffenenrechte: Einschränkungen (Art. 18) und stattgegebene Widersprüche (Art. 21) sperren die gewählten Datensätze sofort technisch – kein Sync, keine Änderung, die Speicherung bleibt. Berichtigungen (Art. 16) führt die Fach-Administration anhand Ihrer Anweisung durch. Ein Übertragbarkeits-Antrag (Art. 20) liefert den JSON-Export der selbst bereitgestellten Stammdaten.

Sicherheits-Audit

Menüpunkt **Sicherheits-Audit** (Recht *Sicherheits-Audit ansehen*).



Protokoll sicherheitsrelevanter Aktionen mit Zeitpunkt, Aktion, Ziel und Ergebnis.

Das Audit protokolliert, **wer wann was** getan hat – zum Beispiel: Benutzer angelegt, Passwort zurückgesetzt, Teammitglied hinzugefügt oder entfernt, Fall zugewiesen, Gerätefreigabe geändert, Richtlinie

geändert, Notfallzugriff geöffnet oder geschlossen, Speicher bereinigt, Nachweis abgeschlossen oder wieder geöffnet, Zeiteintrag durch die Leitung geändert.

> Das Audit enthält **keine Fallinhalte**.

Absturzberichte und Desktop-Downloads

Absturzberichte (Recht *Absturzberichte ansehen*): Stürzt eine App ab, kann sie einen technischen Bericht an den Server melden. Sie sehen Zeitpunkt, Plattform und technische Details. Absturzberichte enthalten **keine Falldaten, Namen oder Notizen**. Mit dem Recht *Absturzberichte verwalten* entfernen Sie Berichte über **Bericht löschen** (Detailseite) oder **Alle Berichte löschen** sofort; ansonsten löscht der Server sie nach der eingestellten Aufbewahrungsfrist (Standard 90 Tage) automatisch.

Desktop-App herunterladen (Recht *Desktop-App herunterladen*): Hier liegen die Installationspakete der Desktop-App – **.pkg** für macOS (Apple Silicon und Intel) und der **MSI**-Installer für Windows (x64 und ARM64). Geben Sie sie an Ihre Fachkräfte weiter.

Datenschutz und Grenzen des Panels

- Administration sieht **keine privaten Inhalte**.
- **Technische Administration** sieht **keine** Fälle und Termine.
- Das Panel ist **Verwaltung, keine Fachdokumentation**.
- Passwörter werden **nie im Klartext** angezeigt; Dateien liegen auf dem Server verschlüsselt.
- Sicherheitsrelevante Aktionen sind im **Audit** nachvollziehbar.

Häufige Fragen

Eine Fachkraft hat ihre PIN vergessen. Öffnen Sie **Geräte** und wählen Sie beim betreffenden Gerät **PIN-Sperre zurücksetzen**. Die Sperre löst sich beim nächsten Sync.

Eine Fachkraft hat ihr Telefon verloren. Entfernen Sie das Gerät unter **Geräte** – damit ist die Verbindung getrennt und der Lizenzplatz frei. Setzen Sie bei Bedarf MFA oder Passkey zurück und stellen Sie einen neuen Setup-QR aus.

Warum sehe ich einen bestimmten Menüpunkt nicht? Die Navigation zeigt nur, wozu Sie berechtigt sind. Lassen Sie sich das nötige Recht von einer Person mit passender Admin-Ebene geben.

Warum fehlen in einem Nachweis Einträge? Private Einträge sind nie enthalten. Außerdem erscheinen Einträge erst, wenn das Gerät der Fachkraft synchronisiert hat.

Ein Nachweis zeigt das Warnzeichen „Daten weichen ab". Nach dem Abschluss sind noch Einträge des Zeitraums eingegangen oder geändert worden. Prüfen Sie sie unter **Zeiterfassung** und entscheiden Sie, ob der Zeitraum wieder geöffnet werden muss.

Kann ich eine Fachkraft aus der Ferne aussperren? Ja – deaktivieren Sie das Konto unter **Benutzer** und/oder sperren beziehungsweise entfernen Sie ihre Geräte unter **Geräte**.

Wer darf MFA entfernen? Nur Konten mit dem Recht **Technische Admins verwalten**.

Focus Family · Handbuch für das Admin-Panel · Version 1.3.0 · Stand Oktober 2026