FOCUS FAMILY

Admin Panel Handbook

Administration, management and data protection – explained step by step

Version 1.0.0 · September 2026 · Software Notion

Contents

Welcome

The **admin panel** is the web administration of your organisation's Focus Family server. You reach it in a browser at your server address followed by `/admin`.

This handbook is written for **administration, management and data protection officers**. It requires no technical knowledge. Setting up and operating the server itself is covered in the **technical handbook**.

What the panel is for

You manage the organisational side of your work here:

- practitioners, their access and permissions,
- teams and case assignment,
- shared planning (appointments and tasks),
- time tracking and activity records,
- devices, policies and central settings,
- templates, text snippets and catalogues,
- deletion requests and data protection cases.

What the panel deliberately is not

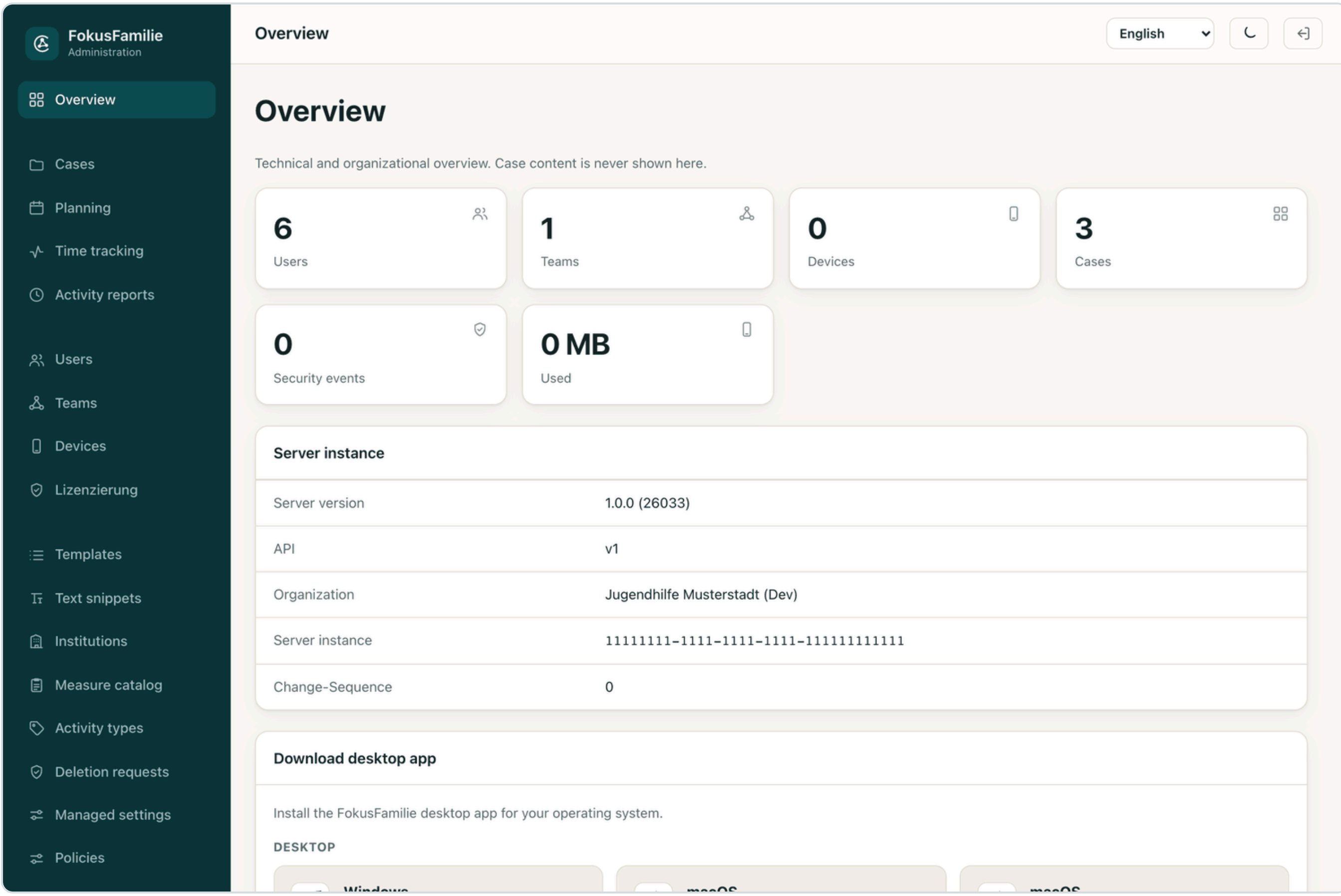
- It is **not a second case documentation**. The professional work – notes, assessments, progress – happens in the practitioners' app.
- Administrators do **not** see private content. Entries marked "private" stay hidden.
- **Technical administration** sees **no** cases and no appointments.

Signing in and basics

1. Open your server address with `/admin` in a browser.
2. Enter **e-mail** and **password** and click **Sign in**.
3. If two-factor sign-in (MFA) is active for your account or required by policy, the panel also asks for the **6-digit code** from your authenticator app.
4. If your account uses **passkey sign-in**, you confirm with fingerprint, face or a security key instead.

At the top right you switch the **language** (Deutsch, English, Español, Français), toggle between **light and dark** appearance and sign out.

> **Important: Technical admin accounts cannot sign in to the apps.** Everyone who uses the app needs a **practitioner account**.



The overview shows key figures, details about the server instance and the desktop app downloads. The navigation on the left only lists what your permissions allow.

Roles and permissions

Focus Family splits administration into two areas. IT can look after the technology without seeing case content – and professional management can administer the content side without touching server technology.

The two levels

Level	May	Sees
System admin (technical)	use and grant all technical permissions	no cases, no appointments
Professional admin	use and grant all professional permissions	case content, except private entries

Anyone holding both levels can grant everything.

Individual permissions

In addition, **individual permissions** can be granted. Two rules always apply:

- **"Edit" includes "view".**
- You can only grant permissions **from your own area**.

Professional permissions

Permission	Meaning
View / edit cases	see cases, or create and change them
View / edit calendar	see or manage appointments
View / edit tasks	see or manage tasks
View / record time	see time entries, or create and change your own
Manage records	edit time entries and records of **other** practitioners within your own management scope (includes "view time")
Close records	close past months/years and reopen them with a reason (includes "manage records")
View / edit managed settings	maintain central values that are locked in the app
Manage practitioners	create and maintain user accounts
Manage teams	maintain teams and members
Assign to others	assign cases to other people, create cover arrangements
Emergency access (break-glass)	time-limited exceptional access to a case
Manage templates & export profiles	maintain central DOCX templates and export profiles
View / create / manage text snippets	maintain central text snippets
See amounts	see monetary amounts in invoice drafts
Review deletion requests	decide about deleted data
Show setup QR	create a setup QR code for practitioners

Technical permissions

Permission	Meaning
System configuration	basic technical settings
View / edit policies	maintain organisation policies
View / manage devices	see device connections, approve or block them
Manage technical admins	maintain IT administration – also governs **removing MFA and passkeys**
View security audit	inspect the security log
View system status	see technical load
View crash reports	see technical error reports from the apps
Download desktop app	download installer packages in the panel

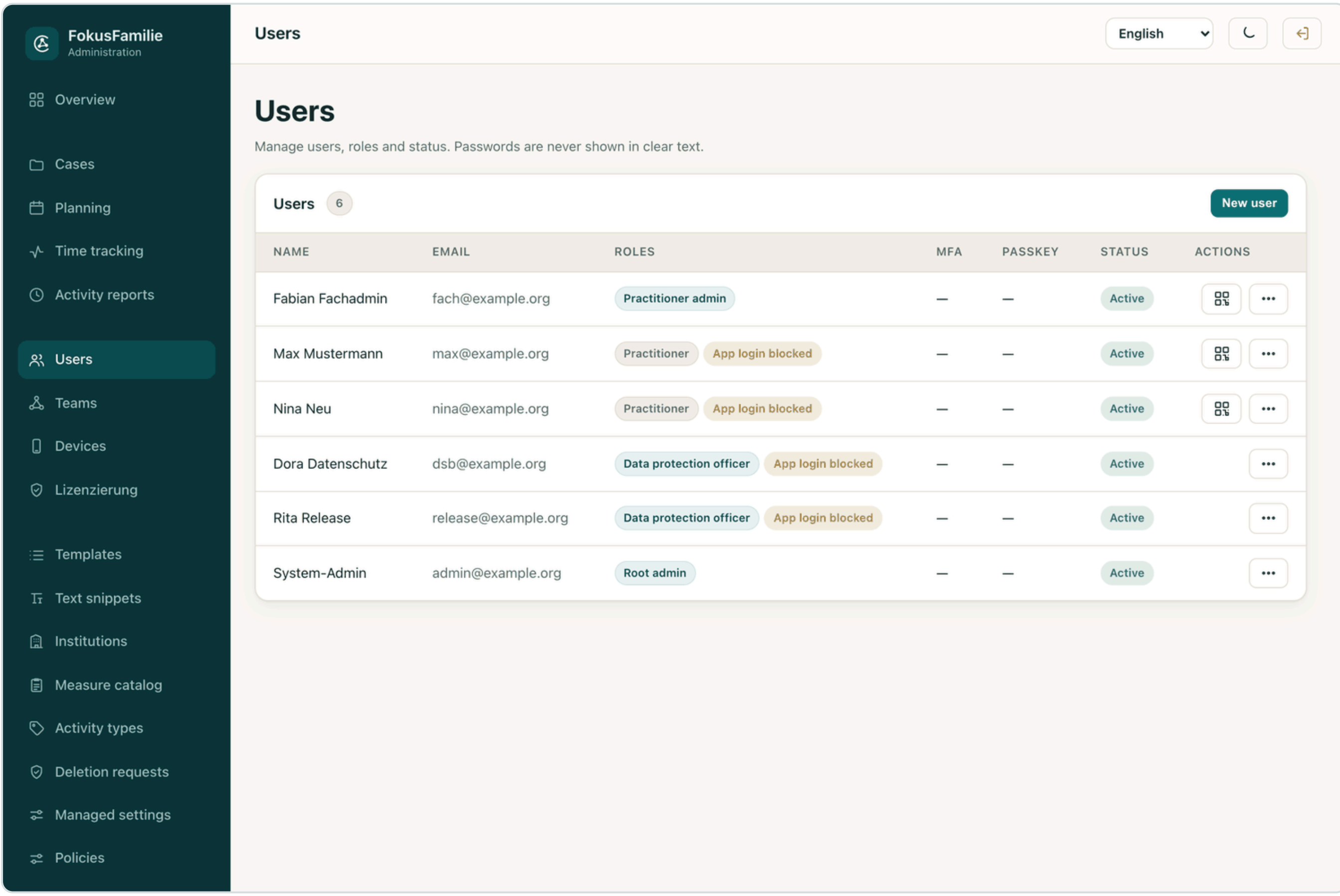
> Removing two-factor sign-in or a passkey requires the permission **Manage technical admins**.

Management scope

The two record permissions only apply inside a person's **management scope**: the teams where they are listed as **team lead**, with those members and assigned cases. A **professional admin** automatically has the whole organisation as their scope. Reading stays organisation-wide for everyone with "view time".

Managing users

Menu item **Users** (permission *Manage practitioners*). Passwords are never shown in clear text.



The user list with name, e-mail, roles, status and passkey state. The menu on the right holds every action for a person.

Creating a user

1. Click **New user**.
2. Enter **display name**, **e-mail** and a **password**. The password needs at least 12 characters with upper and lower case, a digit and a special character.
3. Under **access**, decide whether the person may use the app as a **practitioner** or is **administration only**.
4. Click **Create**.

Granting permissions

1. Open the user and go to the **permissions** area.

2. Permissions are grouped into **professional** and **system / technical**. Preset sets (for example **team lead**) tick several boxes at once.
3. Tick the boxes and click **Save**. You only see permissions you are allowed to grant.

Editing, deactivating, changing passwords

- **Edit** – adjust display name and settings.
- **Activate / deactivate** – a deactivated account can no longer sign in. You cannot deactivate your own account.
- **Change password** – enter the new password twice. Existing panel sessions of that person end within a minute; at their next sign-in they choose their own password.

Setup by QR code

So a new practitioner does not have to type the server address and credentials (permission *Show setup QR*):

1. Open the user and choose **Show setup QR**.
2. The QR code is **time-limited** and can be used **only once**. Issuing it replaces the current password with a one-time password in a single step.
3. The practitioner scans the code in the app under **Connect server**.
4. The app configures the connection and sign-in automatically; afterwards the person sets their own password.

> **Security note:** the setup QR is sensitive. Show it only to the right person, never send it over insecure channels and do not leave it lying around. It expires by itself after a short time.

Setting up two-factor sign-in (MFA)

The Focus Family app and the authenticator app usually run on the **same phone** – and a device cannot photograph its own screen. That is why you show the setup code in the panel on a second screen.

1. Open **Users** and choose **Set up MFA**.
2. A **QR code** and a **key** for manual entry appear.
3. The practitioner scans the code with their authenticator app (for example Google or Microsoft Authenticator).
4. Enter the displayed **6-digit code** in the **code** field and click **Confirm & activate**.

Whether MFA is **mandatory** is decided centrally under **Policies**. The requirement applies to apps **and** the admin panel.

Passkey sign-in (passwordless)

Alternatively an account can be switched to **passkeys** – sign-in with fingerprint, face recognition or a security key.

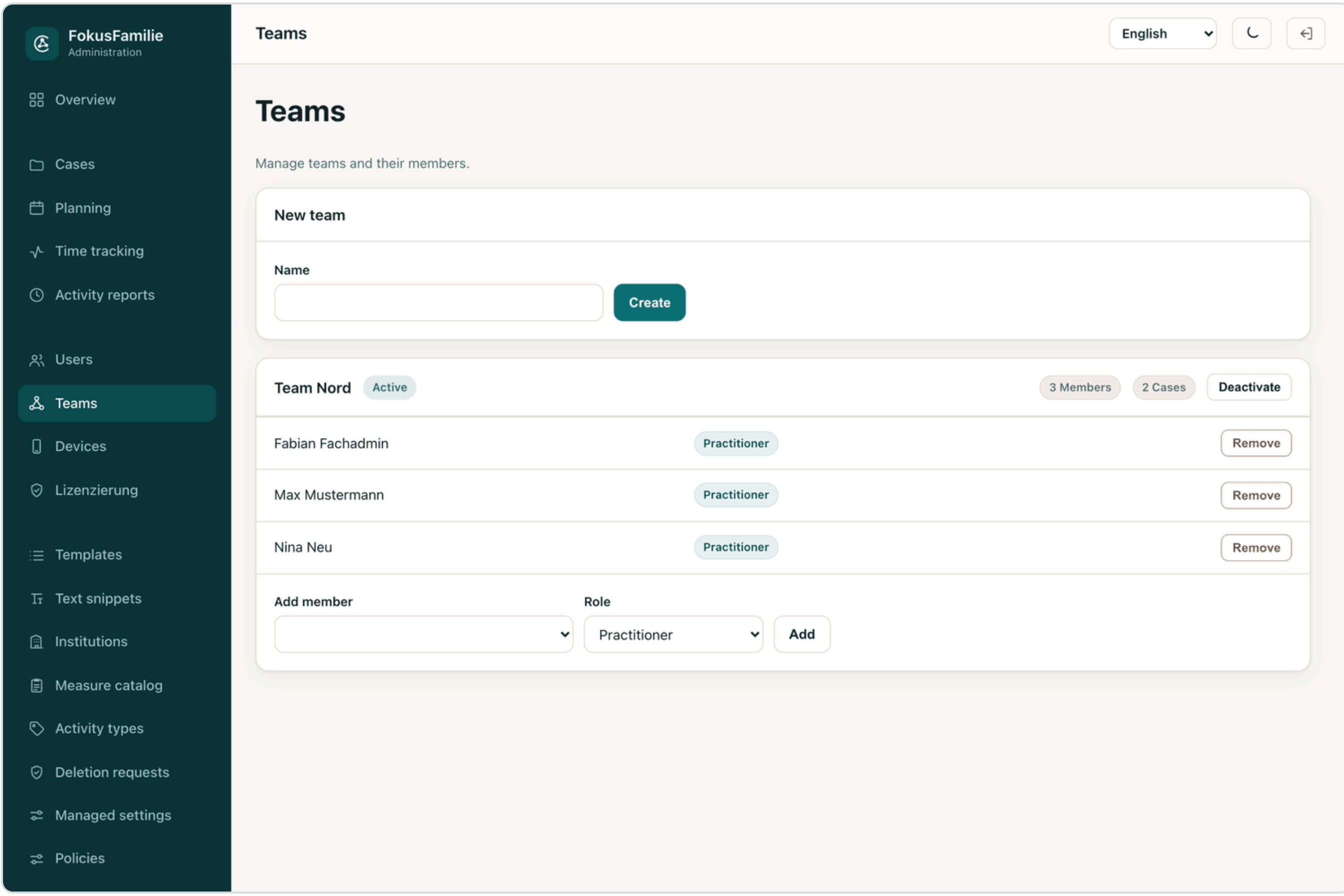
1. In the person's menu choose **Enable passkey sign-in**. The **passkey** column then shows **pending**.
2. At the next sign-in the person is guided to the **set up passkey** page. Afterwards the column shows **active**.

3. Once a passkey exists, **the password no longer works for that account.**
4. **Show passkeys** lists every registered passkey. Adding another one (for a second device, say) requires confirmation with an existing passkey.
5. While a passkey is active, **set password** and **set up MFA** are greyed out – they only take effect after a passkey reset.

> **Resetting passkeys** and removing individual passkeys – like removing MFA – require the permission **Manage technical admins**, for example after a lost device. Both immediately end the person's sessions; set a new password right afterwards.

Teams and case assignment

Menu item **Teams** (permission *Manage teams*). Teams bundle practitioners so cases can be assigned to several people at once.



Teams with their members. The role "team lead" also defines the management scope for the record permissions.

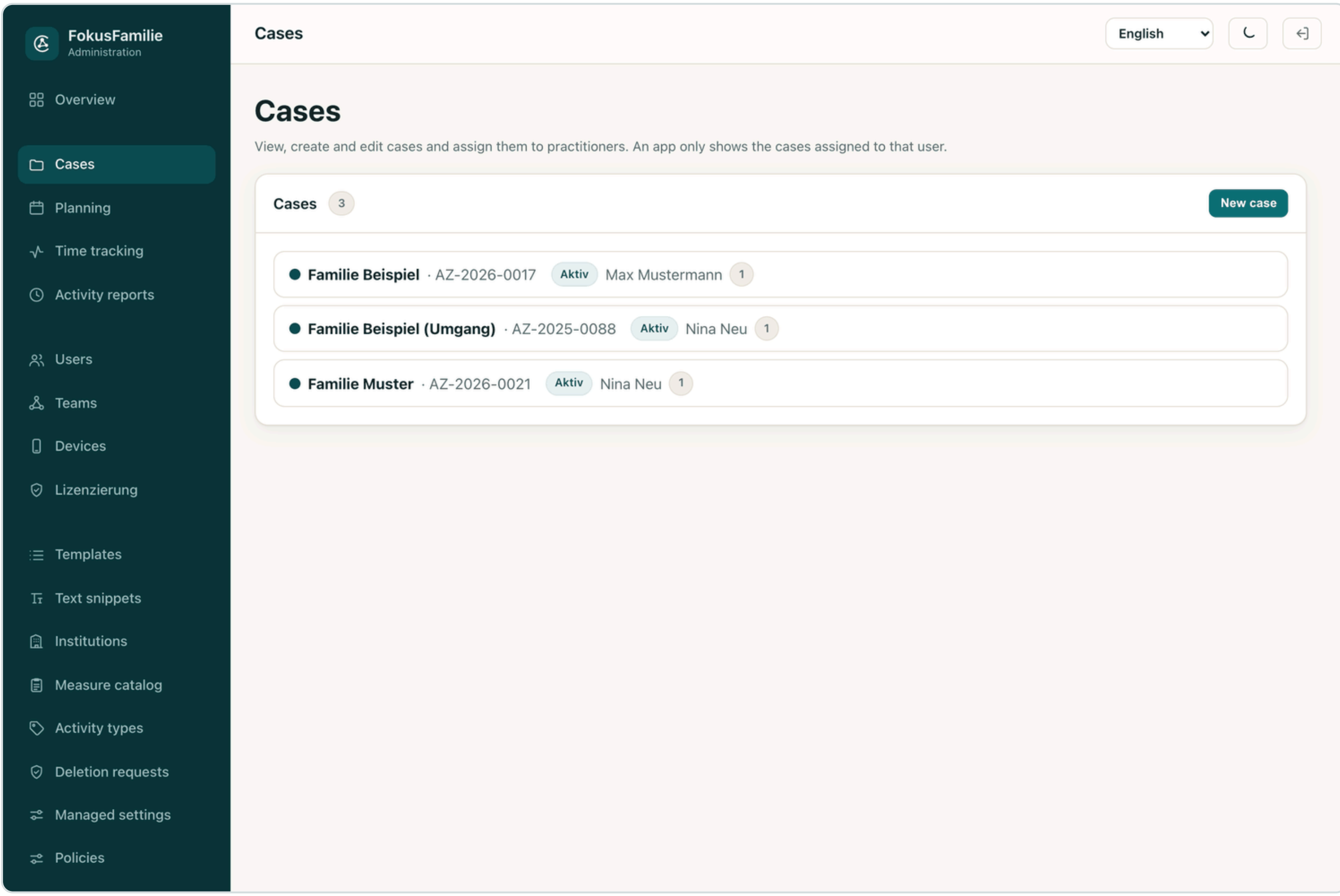
1. Create a **new team** and give it a name.
2. Use **Add member** to include practitioners and **Remove** to take them out.
3. The role **team lead** reaches beyond team administration: it defines the **management scope** for "manage records" and "close records".

Cases can be assigned to a **team** or to individual **practitioners**. An app only ever shows the cases assigned to that person.

> If you remove someone from a team, their device loses access at the **next sync** to cases it only reached through that team.

Cases

Menu item **Cases** (permission *View cases* or *Edit cases*). Remember: this is about administration and assignment, not about the professional case work.



The organisation's cases with status, type of support and assigned practitioners.

Creating and assigning a case

1. Click **Create new case** and fill in the fields: **name / alias**, **file number**, **status**, **type of support**, **responsible office**, **youth welfare officer**, **approved minutes** and **colour**.
2. Click **Create case**.
3. Under **assigned practitioners**, use **Assign** to add people.

The case form contains all professional fields – among them the responsible practitioner, a custom type of support, key information, resources and tags.

Roadmap, goals and review points

Two cards in the open case show how the support is progressing:

- **Roadmap** – a timeline from the start of the case until today: goal tracks, review points as markers and, below, the recorded time per week or month with the quota line.
- **Goals & review points** – the list of goals (status, target date, predecessor goal, achieved on) and review points (date, type, title, next appointment, status). With *Edit cases* you can create review points; changes sync to the devices.

Cover arrangements

Every case has the card **Cover (time-limited)**:

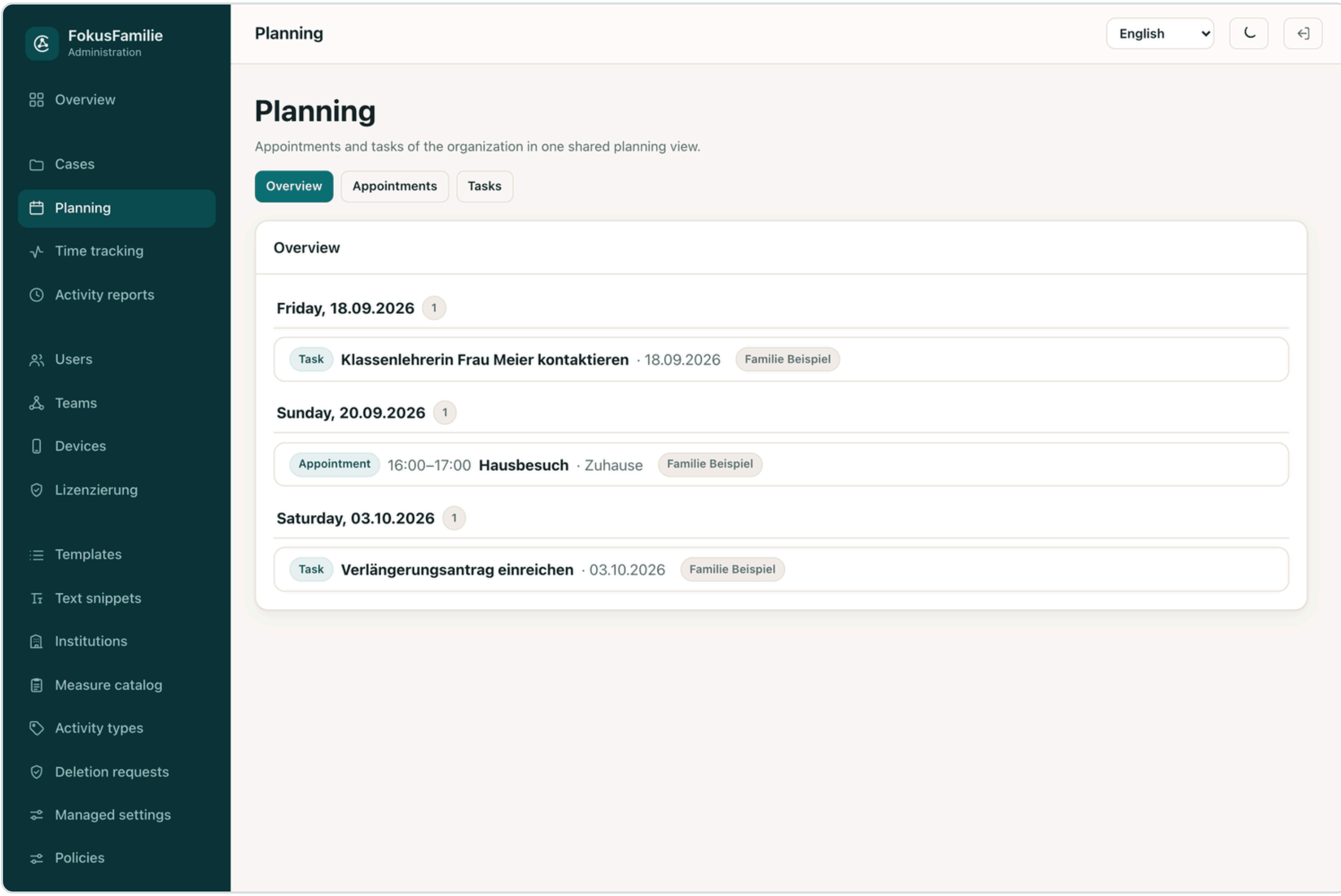
- Choose a **colleague**, set **from** and **to**, then **create cover**. Access starts and ends automatically; holiday cover can be planned in advance and ended early at any time.
- A cover arrangement grants normal read and write access for its duration. **Private entries stay protected**, permanent assignments remain unchanged.
- Every step (created, activated, ended, expired) is logged.

Appointments, tasks and media in a case

- **Add appointment** and **Add task** create both directly inside the case.
- The **media** area shows photos, videos, voice memos and sketches – but only if you are a professional admin or assigned to the case, and only **non-private** entries. If a file has not been transferred yet, the note "file not on the server yet" appears.

Planning

Menu item **Planning** – one page with three views:



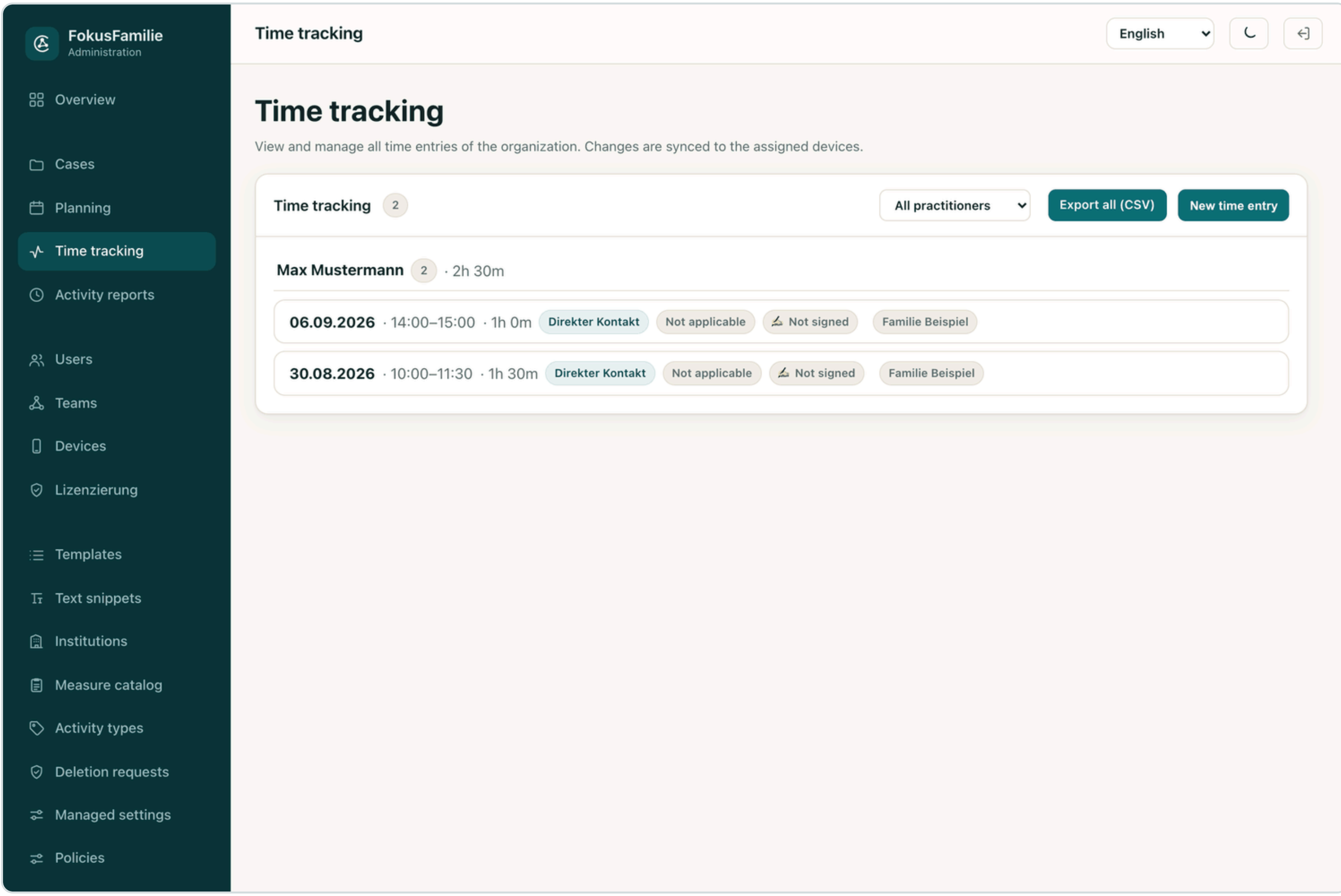
Overview, appointments and tasks for the whole organisation in one place.

- **Overview** – overdue tasks first, then appointments and tasks grouped by day, finally tasks without a date. Read-only.
- **Appointments** (permission *View calendar*) – the organisation-wide appointment list. **New appointment** creates entries; the **repeat** section creates a **series** (daily, weekly with weekdays and "every N weeks", monthly; ending by date or count; at most 180 appointments over at most 3 years). Series occurrences carry a **series** badge; editing changes only that occurrence, while **delete series** removes the whole series. Past and documented appointments are preserved.
- **Tasks** (permission *View tasks*) – the organisation-wide task list with **New task**.

With the permission *Record time*, every appointment additionally offers **Create time entry** – at most one time entry per appointment.

Time tracking

Menu item **Time tracking**.



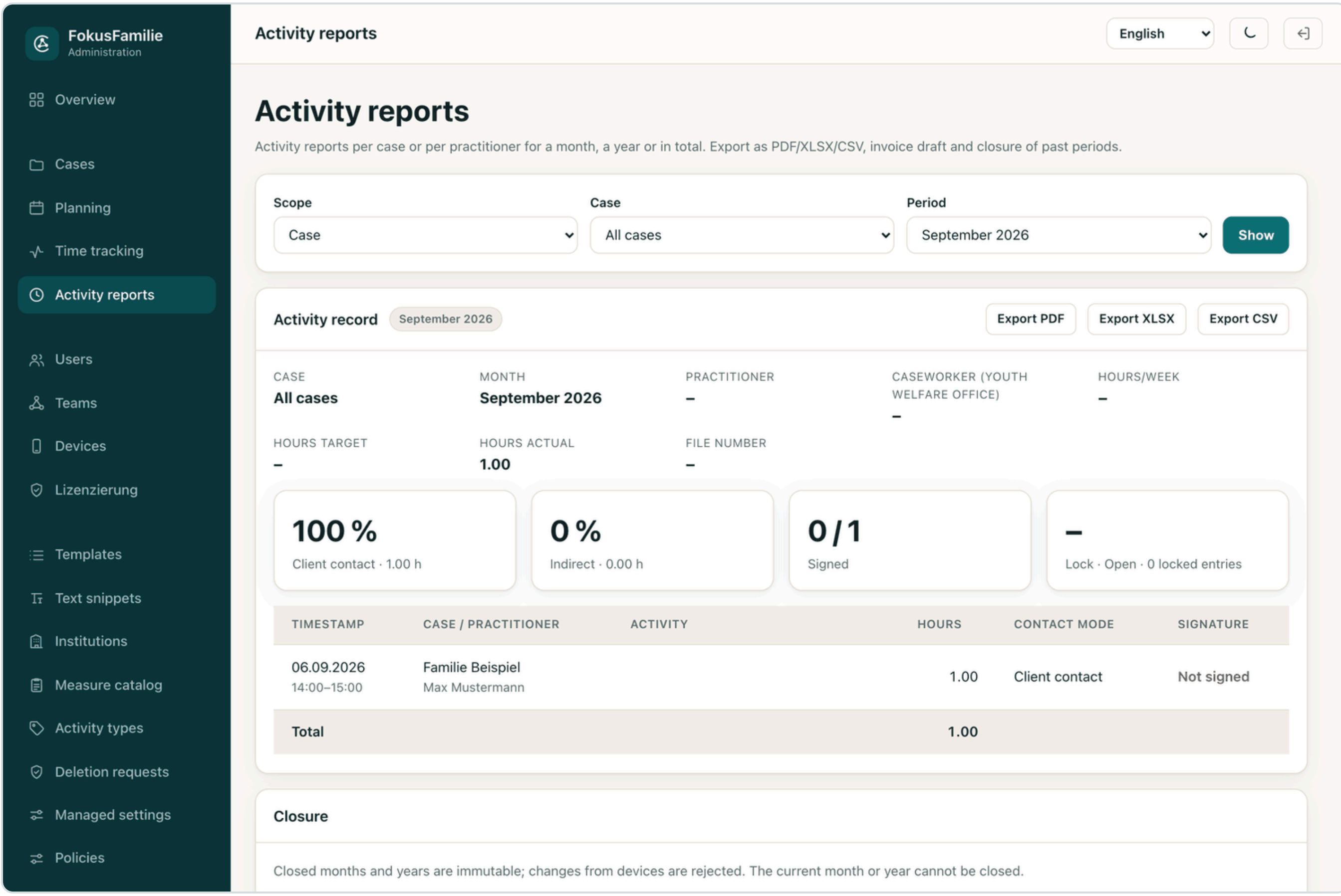
All time entries of the organisation with lock and signature status; filters narrow the list down to one practitioner.

- With **View time** you see all time entries of the organisation with date, duration, type and case, plus the columns **lock** (a padlock means the period is closed) and **signature** (signed, not signed, refused).
- With **Record time** you create your own entries via **New time entry**.
- Entries of **other** practitioners can only be changed or deleted with **Manage records** and only within your **management scope**. Such changes are logged as management corrections.
- **Filter** narrows the view; **Export all (CSV)** extracts the data for further processing.

> No one can change another practitioner's time entries or signatures from a device. Management corrections are only possible here in the panel.

Activity records

Menu item **Activity records** (permission *View time*).



Records per case or practitioner with key figures, individual lines, exports and the closing of past periods.

1. Choose **case** or **practitioner** and the **period** (month, year, total), then **show**.
2. The page shows the **key figures**: hours, target/actual from the quota, share of client contact and indirect work, signature rate and lock status – followed by the table with date, case or practitioner, time, activity, hours, contact type and signature. Yearly and total records are grouped by month, practitioner records by case. **Private entries are never included.**
3. **Signatures** appear directly in the table with image, name, role and time. Next to each image sits a check symbol: - ✓ – the checksum matches the image and the frozen summary; the signature is unchanged. - ⚠ – the checksum does **not** match; image or summary were changed after signing or are damaged. Clarify this with the practitioner. A missing signature is **not an error** – it is voluntary.
4. **Export** as **PDF**, **XLSX** or **CSV**.
5. **Invoice draft** turns a case record into a JSON preparation with funding body, items per activity type and open signatures. Amounts only appear with the permission *See amounts*.

Closing and reopening

This requires the permission *Close records*, and only within your own management scope.

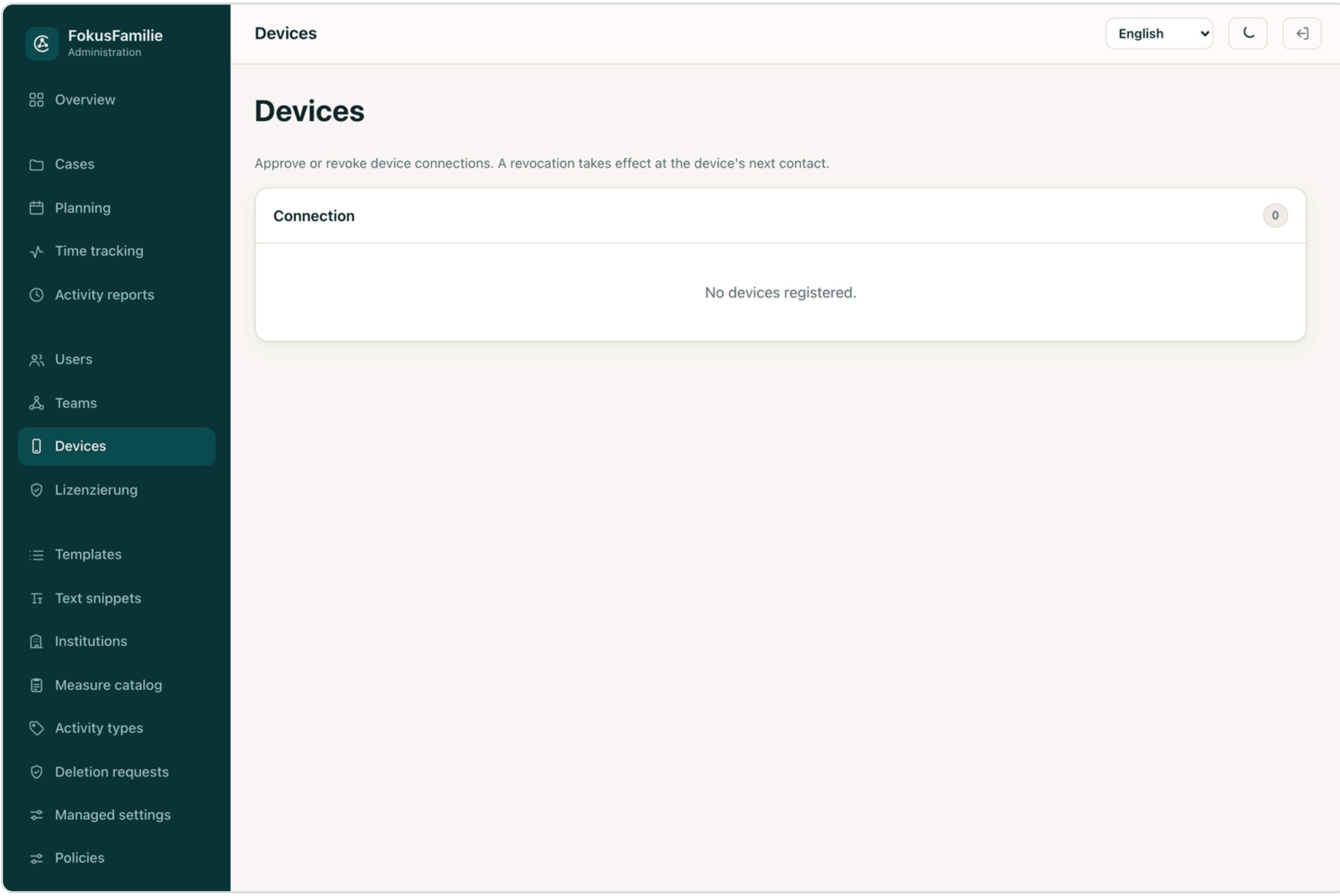
- **Close** freezes a **past** month or year (optionally with a note). From then on all time entries of the period are **locked** on every device: changes, deletions and moving entries into the period are rejected; reading stays possible. The record receives a checksum and the complete state is stored.
- **Closed state:** opening a closed period shows the note "closed state (checksum secured)". Table and exports then come from the stored state. If the yellow warning **"attention: current data differs from**

the closed state" appears as well, entries were changed after closing – for example because a device synced later. The closed state is still what is shown and exported.

- The **current month** and the **current year** can never be closed.
- **Reopen** lifts the lock and requires a **reason**. Both end up in the security audit.
- Practitioners cannot close or open anything themselves; they see locked entries with a padlock.

Devices

Menu item **Devices** (permission *View devices* or *Manage devices*).



Registered devices with platform, version, last sync and status. This is where you approve, block or disconnect devices.

- **Approve / block** – a block takes effect the next time the device contacts the server.
- **Reset PIN lock** – if a practitioner locked themselves out or forgot the PIN, lift the app lock here. It is released at the next sync and the person sets a new PIN.
- **Remove** – disconnects the device from the server. It loses access and must be set up again; the **licence seat becomes free** again. Practitioners cannot disconnect themselves.
- **Re-enrolment code** – if a known device has to be set up again (after a reinstall, say), issue a code. The device reconnects to its existing registration without consuming a new seat.

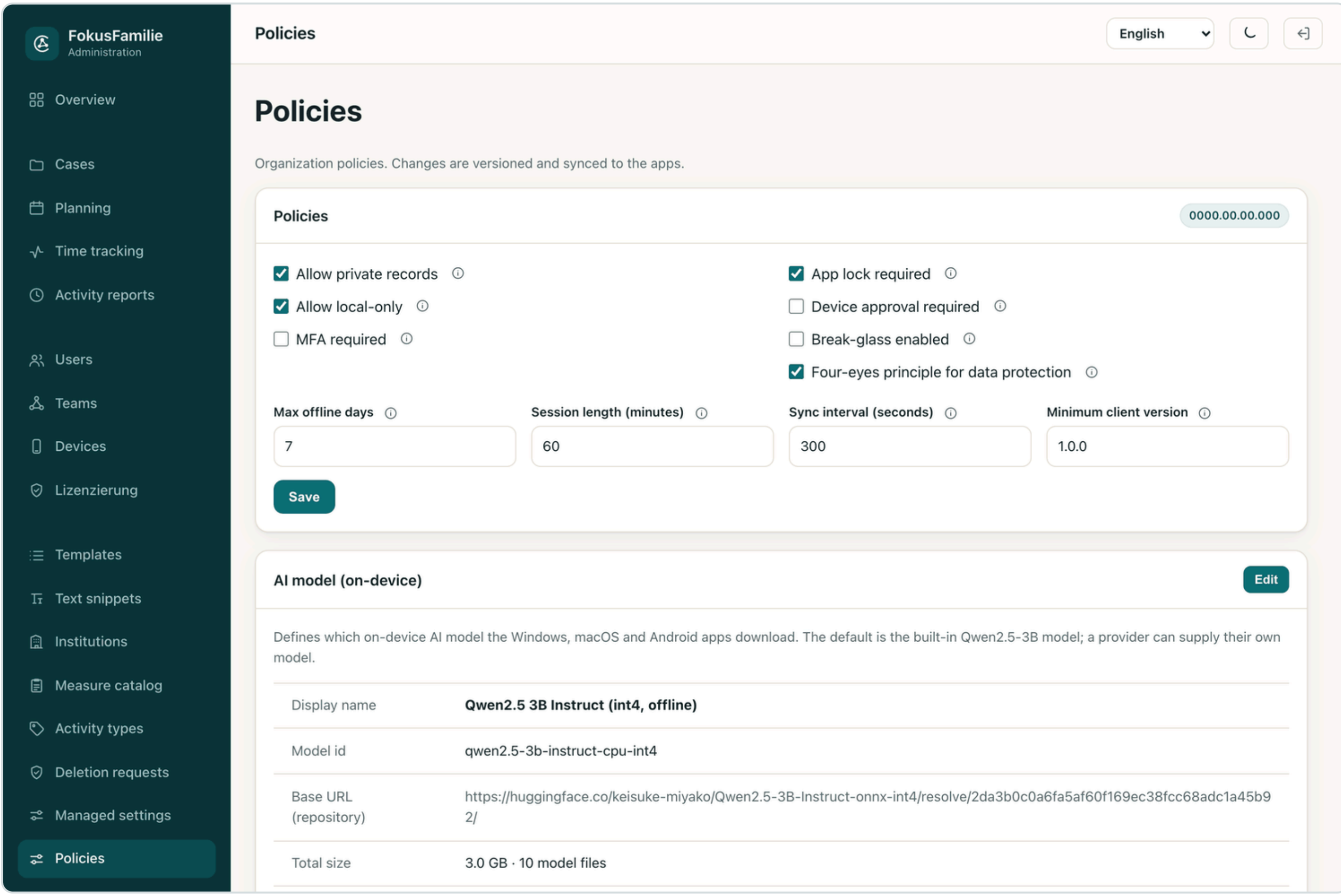
Licence seats

Seats are assigned **exclusively by administration** – devices and practitioners cannot claim one themselves. Without a seat a device cannot sync. The menu item **Licensing** gives an overview of your organisation licence.

> **Licence reminders in the app:** paid licences must be confirmed online regularly. If that does not happen, the app reminds the practitioner from **day 3** at most once a day, from **day 5** hourly, and from **day 10** it requires confirmation (locked until the check succeeds – data stays untouched).

Policies

Menu item **Policies** (permission *View policies* or *Edit policies*). Policies apply organisation-wide, are **versioned** and distributed to all apps.



Organisation-wide rules – from mandatory app locks to the maximum offline period.

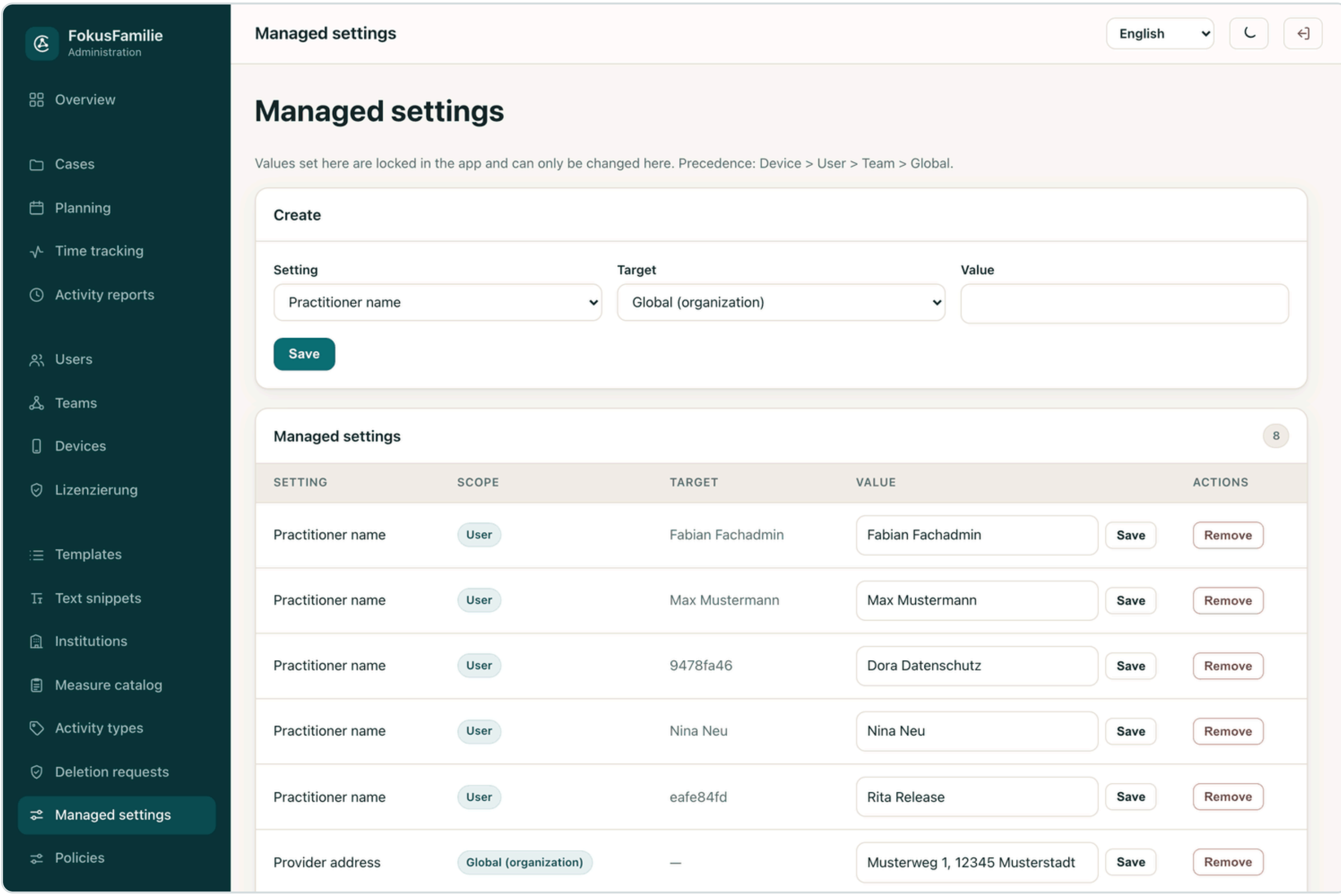
Policy	Meaning
Allow private records	practitioners may keep individual entries private
Allow local-only	content that deliberately stays on the device
MFA required	two-factor sign-in is mandatory (apps and panel)
App lock required	the app must be locked with a PIN or biometrics
Max. offline period (days)	how long a device may work without server contact
Session duration (minutes)	after this time without activity a new sign-in is needed
Sync interval (seconds)	how often the app syncs in the background
Minimum client version	older app versions are rejected during synchronisation
Device approval required	new devices must be approved first
Break-glass enabled	switch emergency access on or off
Four-eyes principle for data protection	release of subject access packages by a second person

Break-glass (emergency access): in exceptional cases – acute risk to a child's welfare, for example – an authorised person can access a case for a limited time (at most 120 minutes), with two-factor confirmation and a logged reason, even without a regular assignment. Every access appears in the audit.

AI model: policies also decide which **language model** the apps use for local AI support. The model size determines the download in the app. The AI still runs entirely on the device.

Managed settings

Menu item **Managed settings** (permission *View managed settings* or *Edit managed settings*).



Centrally set values appear locked in the app. Each value applies to a scope.

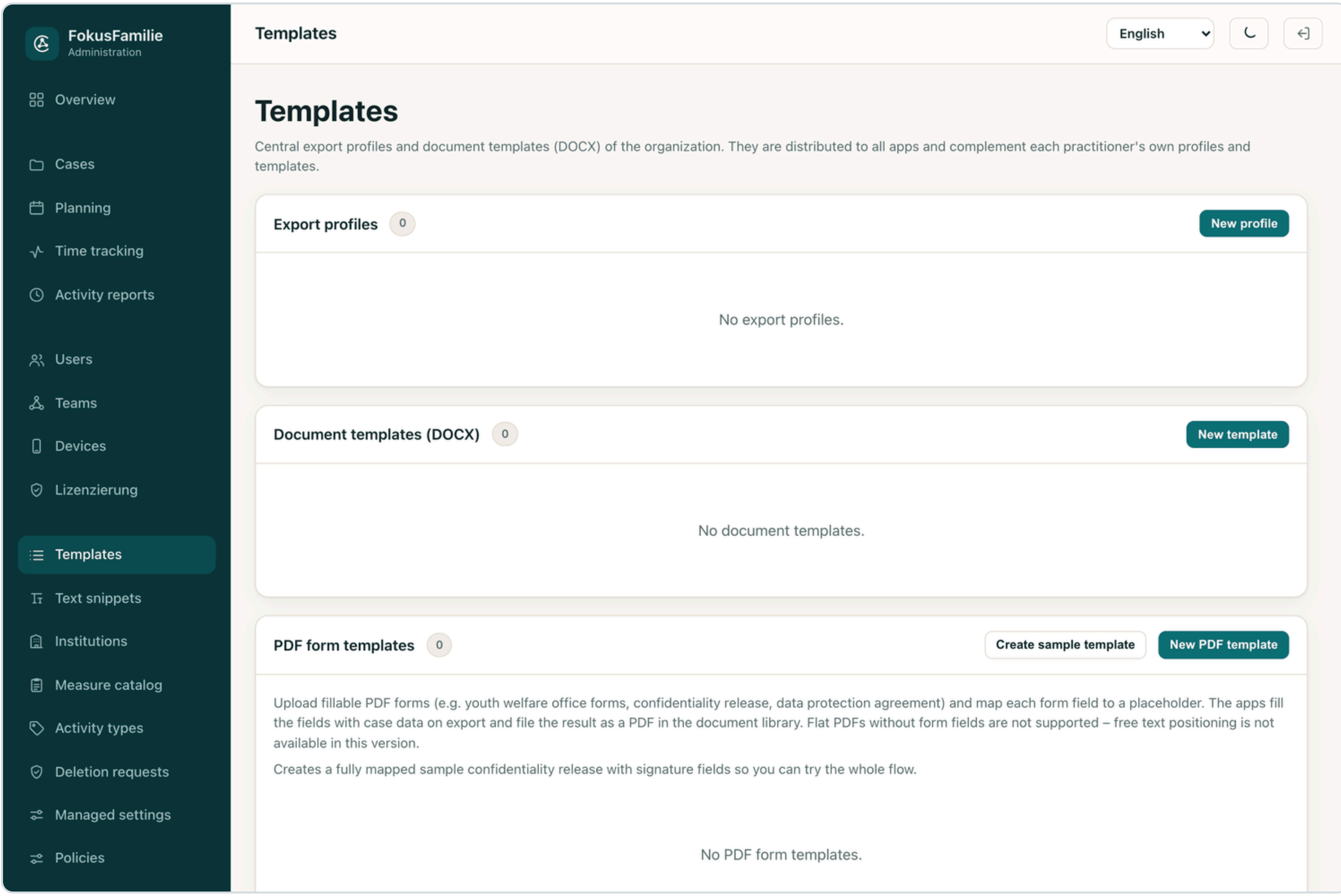
Here you define values that are **locked** in the app and can only be changed here – for example the **organisation name**, **address**, **contact**, the **practitioner name** or the **blob storage limit**.

Each value is set for a **scope**: **global (organisation)**, **team**, **user** or **device.** If more than one value applies to the same setting, precedence decides:

> **Device > user > team > global** – the more specific value wins.

Templates and export profiles

Menu item **Templates** (permission *Manage templates & export profiles*).



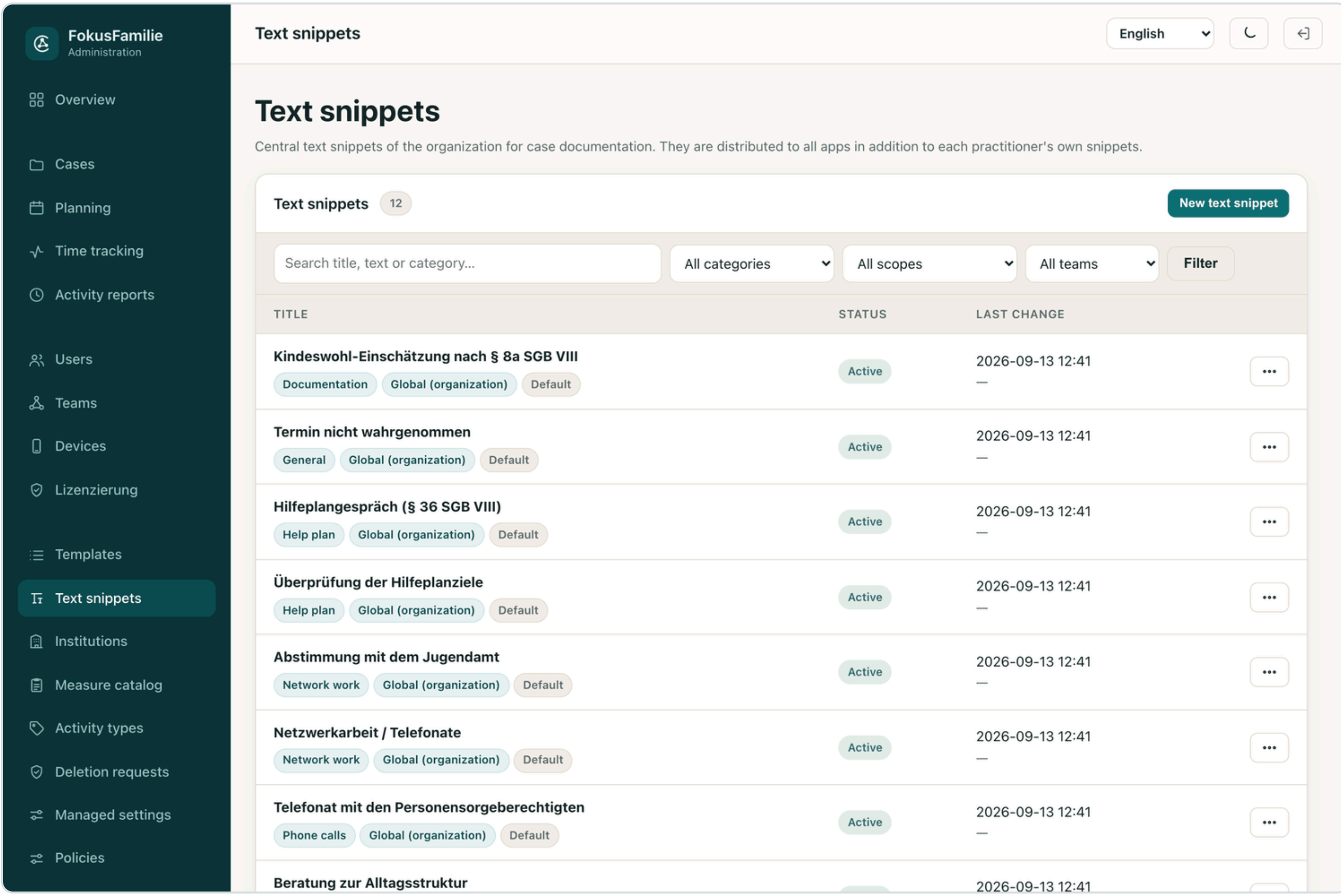
Central export profiles and Word templates are distributed to all apps.

- **Export profiles** – defaults for exporting: formats, cover page, logo, signature fields and data minimisation ("pseudonymise names", "remove address").
- **Document templates (DOCX)** – Word templates with placeholders, at most 5 MB each.
- **PDF forms** – fillable forms of your organisation that practitioners can complete on the device inside the case file.

These central defaults are a **basis**; practitioners can still use their own profiles and templates.

Text snippets

Menu item **Text snippets** (permissions *View / create / manage text snippets*).



Snippets at organisation, team and personal level, with categories and built-in defaults.

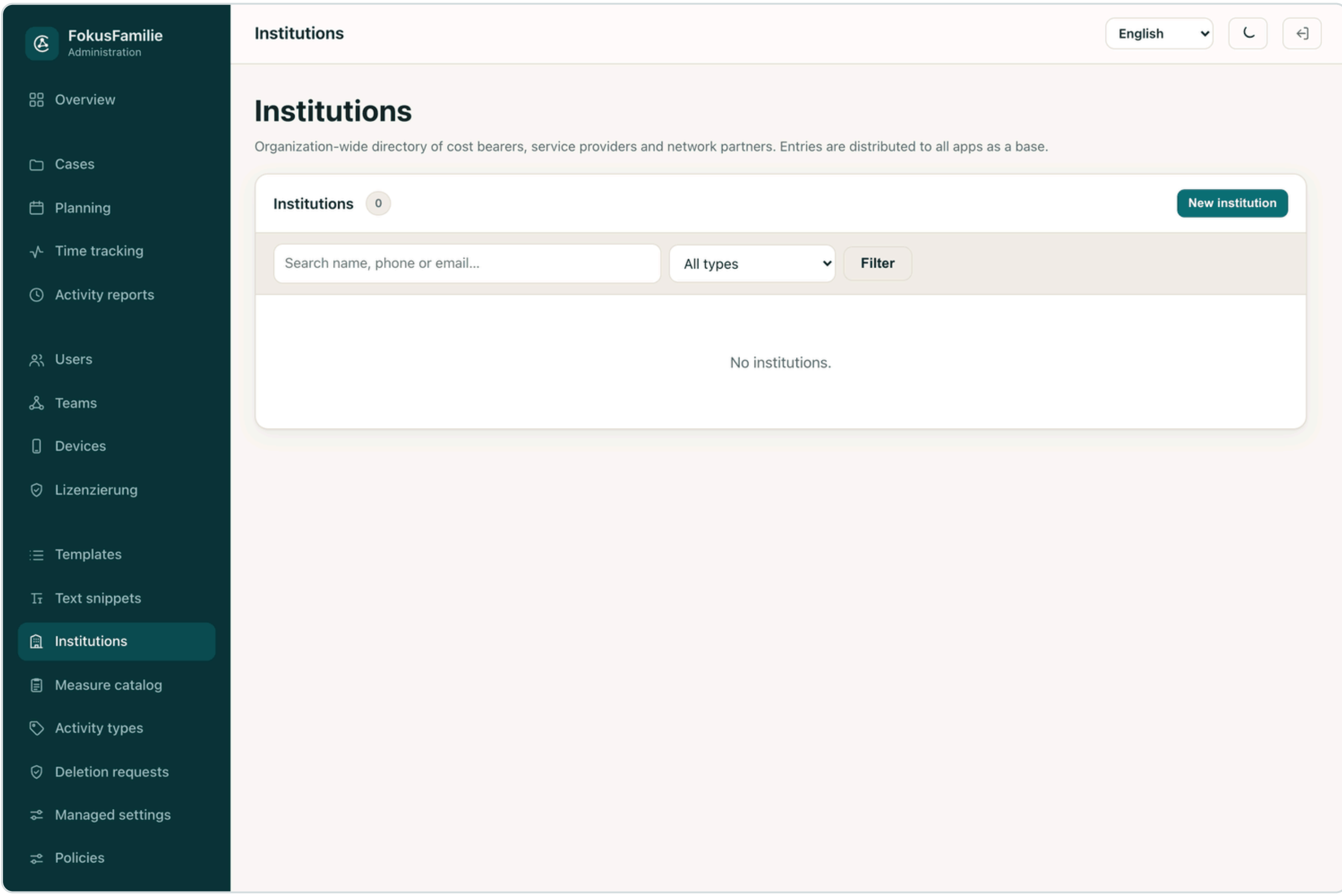
Text snippets are reusable pieces of text for documentation and activity records. They are distributed to all apps and appear there in addition to the practitioners' own snippets.

- **New text snippet** creates one; **edit** adjusts it; **deactivate** takes it out of circulation.
- There are **organisation**, **team** and **personal** levels. Personal snippets belong to the practitioner and can only be changed by them.
- The server ships with **default text snippets** so you do not start from zero. They can be adjusted or deactivated.

Catalogues: institutions, measures, activity types

Three catalogues make sure all practitioners use the same terms.

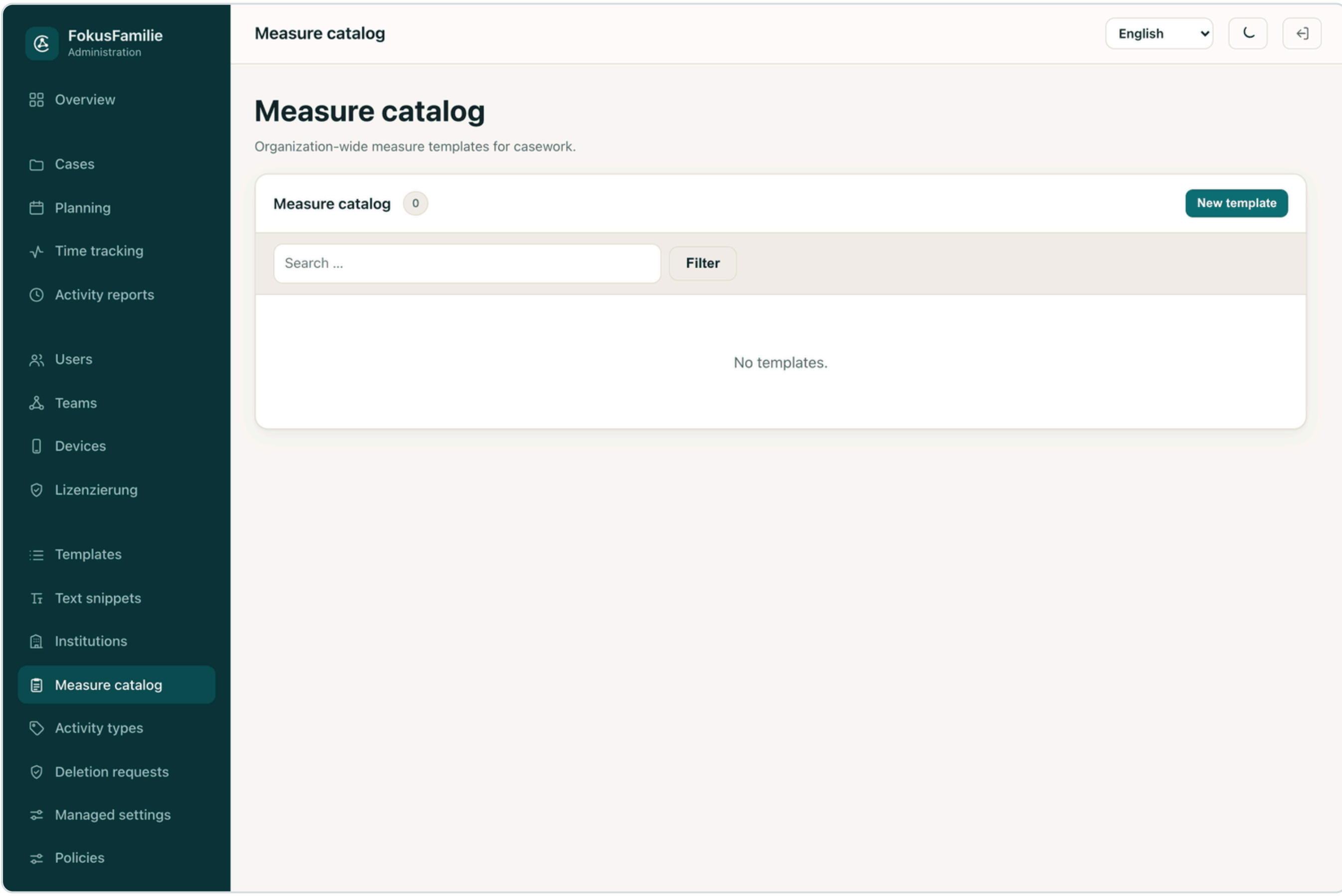
Institutions



Youth welfare offices, schools, day-care centres, counselling services and funding bodies maintained centrally.

The menu item **Institutions** holds the organisations you work with – with type, address and contact details. In the app they are offered when creating cases and network contacts.

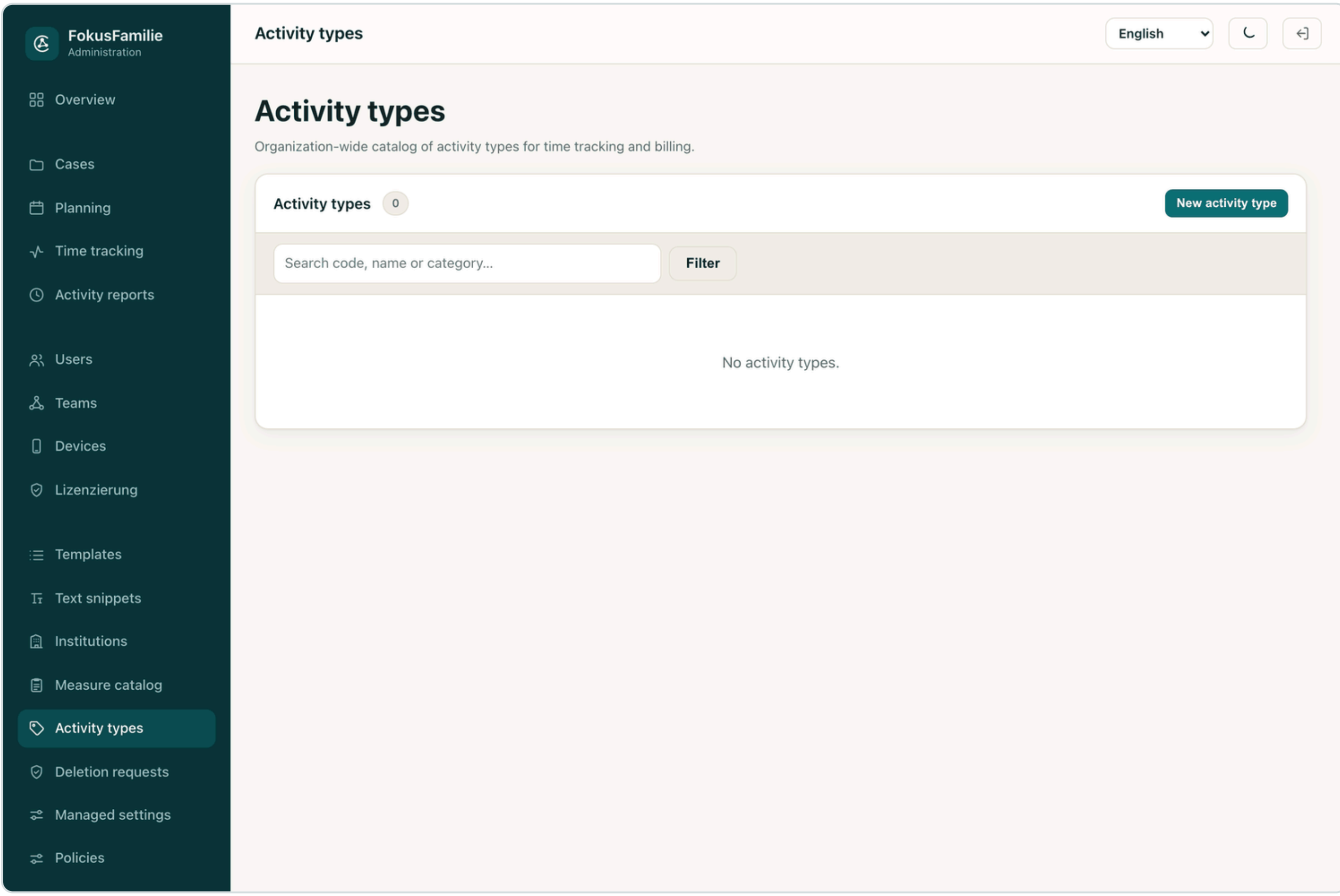
Measure catalogue



The types of support and services of your organisation – the basis for cases and billing.

The **measure catalogue** contains your organisation's types of support and services with name, abbreviation and the details needed for records and billing.

Activity types

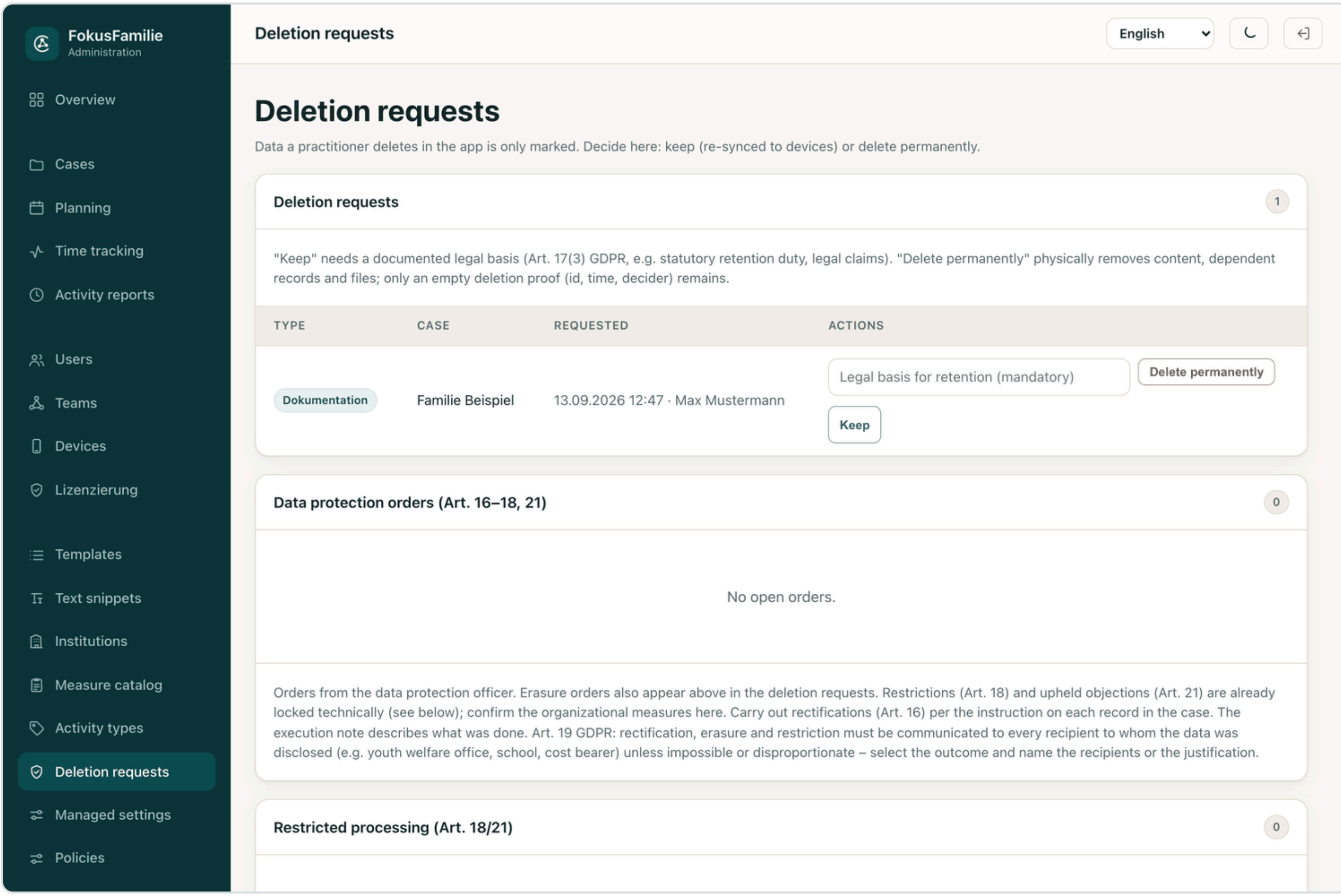


Activity types govern how time is recorded and counted in the activity record.

Activity types determine which categories appear in time tracking – such as client contact (in person), travel time, documentation or phone calls – and whether an activity counts as **direct contact** or **indirect**. The activity record uses this to calculate the contact ratio.

Deletion requests

Menu item **Deletion requests** (permission *Review deletion requests*).



Data deleted by practitioners is only marked at first and presented here for a decision.

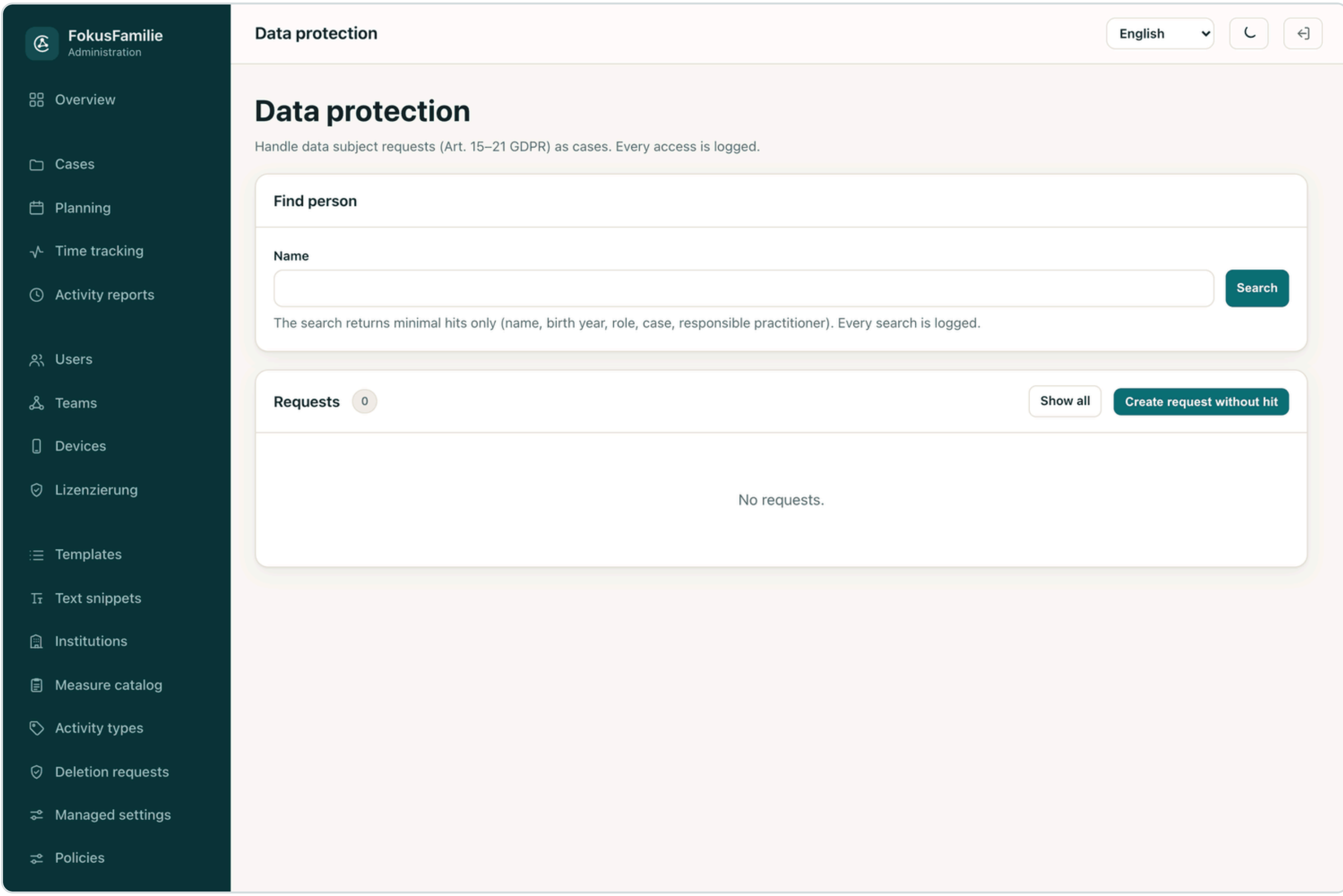
When a practitioner deletes data in the app, it is initially **only marked**. You decide per entry:

- **Keep** – the data remains and syncs back to the devices. You state the **legal basis** for keeping it (for example a statutory retention obligation or ongoing proceedings); it is stored with the record.
- **Delete permanently** – content, dependent records and files are removed **physically and irreversibly**; only an empty deletion receipt remains. For a case, the devices remove it at the next sync. A confirmation prompt appears.

The same page shows **restricted records** (Art. 18/21 GDPR). A restriction can only be lifted if you enter the **date and channel** of the prior information to the data subject and the **legal basis** for lifting it.

Data protection: subject requests and documents

The **data protection** area is for your data protection officer (DPO).



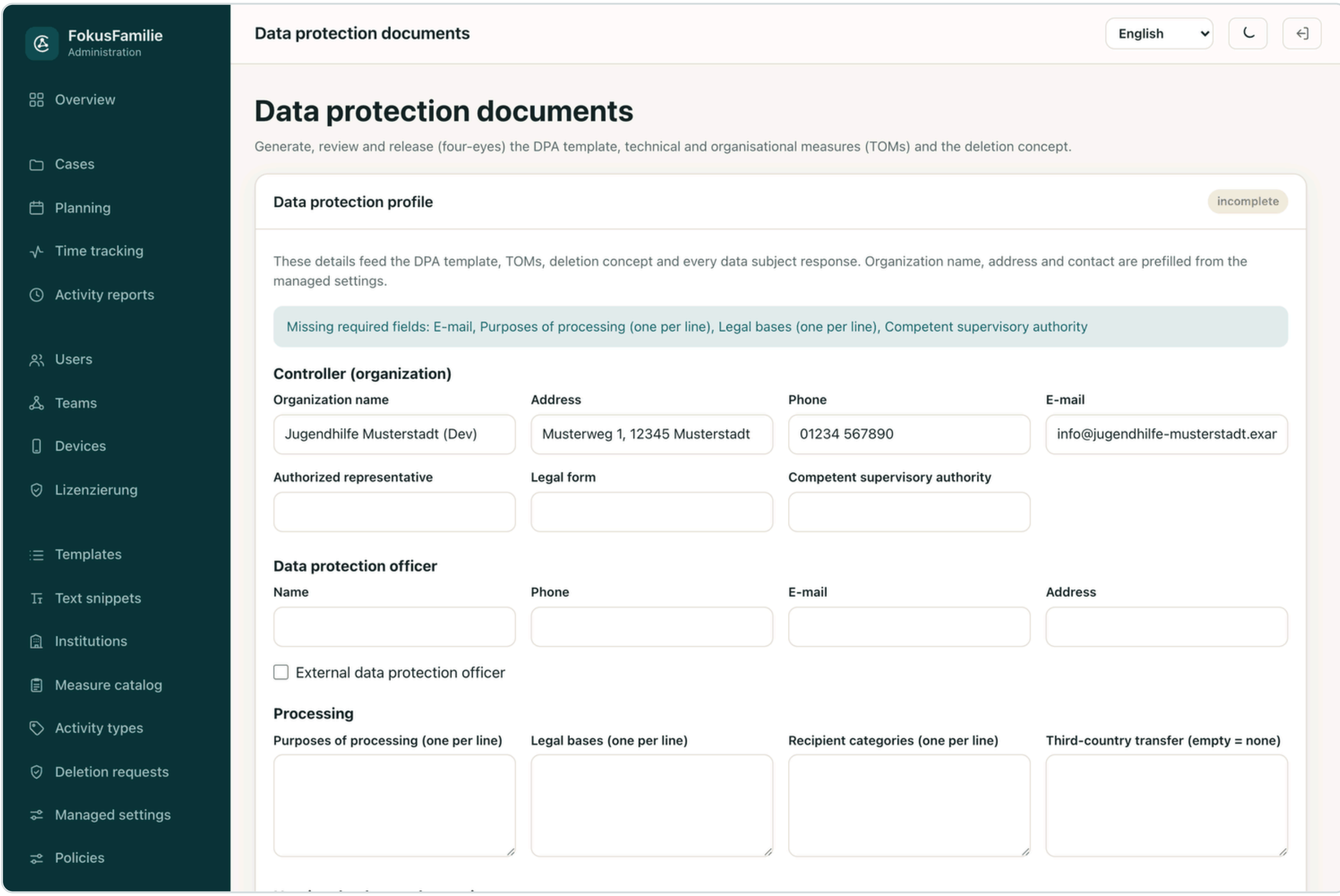
Cases for data subject rights – from identity verification through redaction to release.

Setting it up

Create the account with the type **data protection officer** and tick the permissions in the **data protection** block. Such an account **cannot sign in to the apps** unless it also holds professional permissions.

Because the final release is normally done by a **second person** (four-eyes principle), you need a second account with the permission **release (four eyes).** Small organisations without a second person can switch the four-eyes principle off under **policies** – every step is still logged.

Before the first request: create the documents



The data protection profile plus the processing agreement template, technical and organisational measures and the deletion concept as draft, reviewed and final.

1. Open **data protection documents** and fill in the **data protection profile**: organisation, DPO contact, supervisory authority, purposes, legal bases, hosting and retention periods.
2. Generate the three documents: **processing agreement template**, **technical and organisational measures** and **deletion concept**.
3. Each document starts as a **draft** with a watermark, is marked as **reviewed** and is **finalised by a second person**. A new draft discards older, not yet finalised versions.

Only **final** versions are attached to subject access packages. If the documents no longer match the profile or the policies, the page shows "outdated" – a new finalisation is then required.

Handling a request

1. Open **data protection** and search for the person by name. You only see minimal matches (name, year of birth, role, case, responsible practitioner). **Create case** – the one-month deadline starts with the date of receipt you enter and can be extended once by two months for complex requests.
2. **Confirm identity** and record how you verified it.
3. **Collect data** – the panel assembles everything stored about that person. Other family members stay out of it.
4. **Redact** – open every record containing free text and remove details about third parties. The system marks possible mentions of other people; you decide: remove, exclude with a reason, or deliberately keep with a reason. Every view is logged.

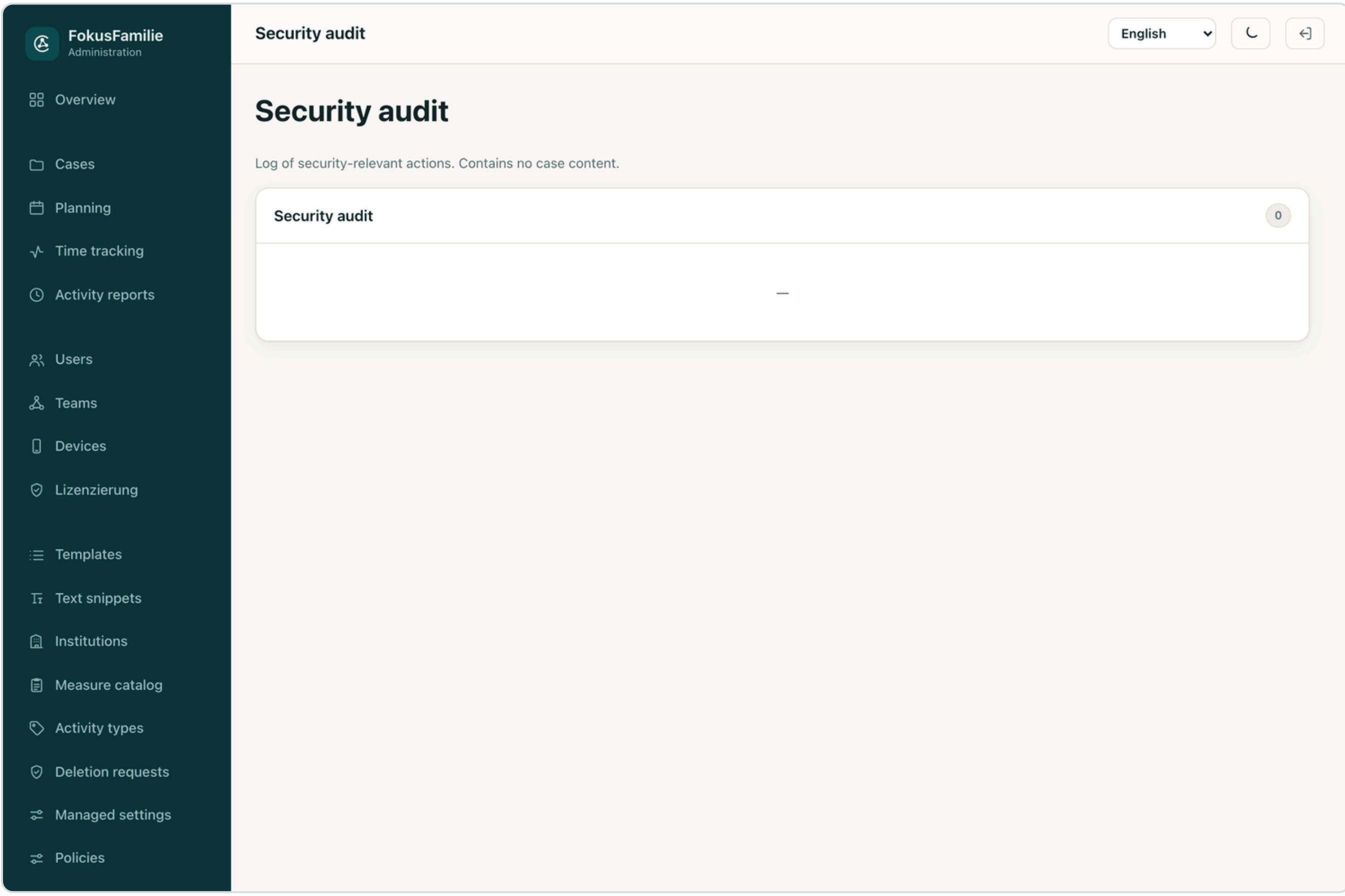
5. **Mark as reviewed** once the checklist is complete.
6. A **second person** releases it in the **release** tab. The panel produces the package (access information as PDF and DOCX, machine-readable JSON, the three documents and a checksum file) and shows the **password once.** Download the package immediately – the link works only once – and transmit the password **separately** (by phone or letter).
7. Mark the case as **handed over** and later as **closed.**

> Open the encrypted archive with 7-Zip, WinRAR, Keka or PeaZip – not with the built-in extractors of Windows and macOS.

Other data subject rights: restrictions (Art. 18) and upheld objections (Art. 21) immediately lock the selected records technically – no sync, no changes, storage remains. Rectifications (Art. 16) are carried out by professional administration on your instruction. A portability request (Art. 20) delivers the JSON export of the master data provided by the person themselves.

Security audit

Menu item **Security audit** (permission *View security audit*).



A log of security-relevant actions with time, action, target and result.

The audit records **who did what and when** – for example: user created, password reset, team member added or removed, case assigned, device approval changed, policy changed, emergency access opened or closed, storage cleaned, record closed or reopened, time entry changed by management.

> The audit contains **no case content**.

Crash reports and desktop downloads

Crash reports (permission *View crash reports*): after a crash an app can send a technical report to the server. You see the time, platform and technical details. Crash reports contain **no case data, names or notes**.

Download desktop app (permission *Download desktop app*): here you find the installer packages of the desktop application – **.pkg** for macOS (Apple Silicon and Intel) and the **MSI** installer for Windows. Pass them on to your practitioners.

Data protection and the limits of the panel

- Administration sees **no private content**.
- **Technical administration** sees **no** cases and appointments.
- The panel is **administration, not case documentation**.
- Passwords are **never** shown in clear text; files are stored encrypted on the server.
- Security-relevant actions are traceable in the **audit**.

Frequently asked questions

A practitioner forgot their PIN. Open **Devices** and choose **Reset PIN lock** for that device. The lock is released at the next sync.

A practitioner lost their phone. Remove the device under **Devices** – this disconnects it and frees the licence seat. Reset MFA or passkeys if needed and issue a new setup QR.

Why can I not see a particular menu item? The navigation only shows what you are entitled to. Ask someone with the matching admin level to grant you the permission.

Why are entries missing from a record? Private entries are never included. Entries also only appear once the practitioner's device has synced.

A record shows the warning "data differs". Entries of the period arrived or changed after closing. Check them under **Time tracking** and decide whether the period needs to be reopened.

Can I lock out a practitioner remotely? Yes – deactivate the account under **Users** and/or block or remove their devices under **Devices**.

Who may remove MFA? Only accounts with the permission **Manage technical admins**.

Focus Family · Admin Panel Handbook · Version 1.0.0 · September 2026