Privacy Policy

fam. Technologies · Effective date: 16 November 2026

---

1. Who we are

fam. Technologies (KVK 77432525), Biltstraat 335b, 3572AS Utrecht, Utrecht, Netherlands, is the data controller for personal data collected through the fam. platform and our marketing website. You can reach our privacy contact at support@fam.services.

We are subject to the General Data Protection Regulation (EU) 2016/679 (GDPR) and, for users in the United Kingdom, the UK GDPR and the Data Protection Act 2018.

2. What data we collect

2.1 Account data

When you or your Organization registers, we collect:

- First name and last name
- Email address
- Organization name

Users may also optionally provide:

- Phone number
- Location / address
- Profile picture

We collect only the data you choose to provide. Optional fields are never required to use the core Service.

2.2 Content data

As part of normal use of the Service, your Organization and its Users create Content such as tickets, asset records, work orders, comments, and attachments. This Content may contain personal data about third parties. You remain responsible for the lawfulness of processing such data within the Service.

2.3 Usage and activity data

We collect technical and activity data to operate and improve the Service, including:

- Login timestamps and session information
- IP addresses
- Audit logs of actions taken within the application (e.g. ticket creation, updates, deletions)
- Browser type and device information

2.4 Payment data

Stripe Payments Europe, Limited collects and processes your card details directly, and your bank account details (IBAN) if you pay by SEPA Direct Debit. We never receive or store the full number of your card or the full IBAN of the account you pay from.

From Stripe, we store these details of each Organization's payment method: for a card, its brand, last four digits and expiry month and year; for SEPA Direct Debit, the last four digits of the IBAN. For each invoice, we store its number, the amounts due, paid and refunded, its currency, status, billing period and due date, and whether a payment was disputed. We also store the status of the Organization's subscription.

If your Organization chooses to pay by bank transfer, we send Stripe the name, email address, postal address and VAT number you enter for the invoices, so that Stripe can issue them. We do not keep our own copy of these details.

2.5 Ratings and public reviews

When someone in your Organization rates work a provider did for you, the rating counts towards that provider's score and appears on the provider's public page on fam., with the month it was given. Every rating that counts is shown; the provider cannot choose which ones appear. With a rating, you can also write a comment for that page. It is optional, and if you leave it empty, only the stars are shown. The page never shows your name, your Organization's name or the ticket. The comment you leave on the ticket itself stays on the ticket and is never shown on the public page.

2.6 Partner data

If your Organization is a fam. partner, we keep what we need to pay its commission: its legal name, address and VAT number, the IBAN we pay the commission into, and the monthly statements and invoices we issue in its name. If that IBAN changes, we pay into the new account only after we've confirmed the change.

If a partner introduced your Organization to fam., that partner sees your Organization's name and what it paid us and when, because we work out the partner's commission from those payments. The partner never sees the people in your Organization or anything they do in fam.

3. Legal bases for processing

We process personal data on the following legal bases:

- Contract performance: to create and manage your account, process payments, pay partners their commission, and provide the Service.
- Legitimate interests: to maintain security, prevent fraud, operate audit logs, and improve the Service, and to show each provider's ratings on its public page, so organizations looking for a provider can see how its work was rated.
- Legal obligation: to comply with applicable laws, including tax and accounting requirements.
- Consent: for optional profile data, and for a public comment you choose to write with a rating. You may withdraw consent at any time.

4. How we use your data

We use the data we collect to:

- Create and manage accounts and provide access to the Service
- Process payments and manage subscriptions via Stripe
- Send transactional emails (account creation, password reset, system notifications) via Amazon SES
- Maintain security, audit logs, and investigate misuse
- Improve and develop the Service
- Comply with legal obligations

We do not use your data for advertising or sell it to third parties.

5. Data processors and third parties

We share personal data with these processors, only as far as each one needs it:

- Amazon Web Services EMEA SARL: hosting of the Service, its database, files, email and logs, in the European Union (Frankfurt and Ireland).
- Stripe Payments Europe, Limited: payment processing. Stripe may transfer data to Stripe, Inc. in the United States under Standard Contractual Clauses.
- Anthropic, PBC: the AI assistant inside the Service. When someone asks it a question, the question and the records it needs to answer are sent to Anthropic in the United States. When someone asks it to sum up a ticket, their unread notifications or a person's activity, that ticket with its comments, those notifications or that activity are sent the same way. When a search finds nothing and someone presses Enter, the words they typed are sent the same way, so the assistant can work out what they meant. When someone creating a ticket asks it which request fits, what they typed and the names of the requests they can pick are sent the same way. When someone adds a qualification and asks for its details to be filled in from the scan, that scan is sent the same way. Nothing is sent unless someone uses the assistant. The assistant is on for

every Organization until its admins turn it off in the organization settings, and they can turn it back on at any time. While it is off, nothing from that Organization is sent to Anthropic, even when users of another Organization work on its tickets. On our website's demo, the comment a visitor writes on a sample ticket is sent the same way, so a sample colleague can answer it.

- Functional Software, Inc. (Sentry): error reports, stored in the European Union. When a signed-in person runs into a server error, the report includes their name and email address. We don't send Sentry the forms people submit, their cookies, their IP address or their browser's request headers. If they choose to report the error from the error page, Sentry also gets what they write there and which browser they use.
- Google LLC (Cloud Translation): the text someone in your Organization asks us to translate, such as a ticket with its comments and costs, a checklist, or a name or label.
- MapTiler AG: maps and address search. MapTiler receives the address being searched and the IP address of the browser showing a map.

Each processor is bound by a data processing agreement and processes data only on our instructions. We will tell customers 30 days before we add or replace a processor.

6. Data controller vs. data processor

For personal data contained in Content created by your Organization (e.g. employee records, contractor details, ticket data), your Organization is the data controller and we act as a data processor. Our Data Processing Agreement (available on request) governs this relationship.

For account-level data (names, emails, login activity), we are the data controller.

For ratings and public comments shown on a provider's public page (section 2.5), we are the data controller.

For partner data (section 2.6), we are the data controller.

7. International transfers

Some of our processors (Stripe, Anthropic, Functional Software for Sentry, Google and MapTiler's delivery network) operate outside the European Economic Area. Where personal data is transferred outside the European Economic Area or the United Kingdom, we ensure appropriate safeguards are in place, such as the EU Standard Contractual Clauses or the UK International Data Transfer Agreement.

8. Data retention

We retain personal data for as long as your account is active or as needed to provide the Service. When an account is closed or deleted:

- Account and profile data is deleted within 90 days.
- Content data is deleted within 90 days unless a longer retention period is required by law.
- Billing and transaction records are retained for 7 years to comply with Dutch accounting law.
- Anonymised usage statistics may be retained indefinitely.

When an account is closed, we delete it on request or within 90 days of the end of the subscription, whichever comes first.

Ratings stay on the provider's public page for as long as the page exists. A public comment is removed when its author asks us to (section 14), or when we find it breaks our Terms of Use or the law.

9. Your rights

Under the GDPR and UK GDPR, you have the following rights:

- Right of access: request a copy of the personal data we hold about you.
- Right to rectification: request correction of inaccurate or incomplete data.
- Right to erasure: request deletion of your personal data where there is no legitimate reason for us to retain it.
- Right to restriction: request that we limit processing of your data in certain circumstances.
- Right to data portability: receive your data in a structured, commonly used, machine-readable format.
- Right to object: object to processing based on legitimate interests.
- Right to withdraw consent: where processing is based on consent, withdraw it at any time without affecting the lawfulness of prior processing.

To exercise any of these rights, contact us at support@fam.services. We will respond within 30 days. You also have the right to lodge a complaint with your local supervisory authority. In the Netherlands that is the Autoriteit Persoonsgegevens (autoriteitpersoonsgegevens.nl). UK users may contact the Information Commissioner's Office (ico.org.uk).

10. Cookies

fam. sets only the cookies the Service needs to work. We do not use them for tracking, analytics or advertising, so there is nothing to consent to:

- Sign-in cookie: keeps you signed in. It ends when you sign out, or after a day without using the Service.
- Security cookie: stops other websites from sending requests in your name. It lasts 30 days.

- Visitor cookie: when you confirm your email on a public link of an Organization, this browser remembers it for 30 days, so you will not need a new code each time.

You can block or delete cookies in your browser settings, but then you will not be able to sign in.

11. Security

We implement appropriate technical and organisational measures to protect personal data against unauthorised access, loss, or disclosure. These include access controls, encryption in transit, and regular security reviews.

Despite these measures, no internet transmission is completely secure. If you become aware of a potential security problem, please contact us immediately at support@fam.services.

12. Children

The Service is not directed at individuals under the age of 18. We do not knowingly collect personal data from minors. If you believe we have inadvertently collected such data, please contact us and we will delete it promptly.

13. Changes to this policy

We may update this Privacy Policy from time to time. We will notify you of material changes by email or via a notice in the Service. The effective date at the top of this document reflects the most recent version.

14. Contact

Data controller: fam. Technologies, Biltstraat 335b, 3572AS Utrecht, Utrecht, Netherlands

Email: support@fam.services