Feuer Software GmbH

Privacy Policy

Last updated: March 2026

This privacy policy is intended to be easy to understand. We therefore largely dispense with legal jargon and paragraphs. Our aim is to explain to you in a clear and concise manner what data we process, why we do it and what your rights are.

The statement is divided according to our products and areas of application:

- Website
- Connect Portal
- Deployment Monitor
- ApplicationTablet
- ApplicationApp
- Operations Manager
- PartnerApp
- Helper App

General safety measures

Feuer Software GmbH encrypts all data traffic transmitted over the Internet. All databases are protected against unauthorized access by encryption or equivalent measures. Data backups are carried out regularly.

All data is generally hosted in Germany by certified service providers. We use modern EDR security technology, VPN connections, minimum length password managers, disk encryption, and multi-factor authentication. Access to data is logged. There is an internal data protection management system that is reviewed at least annually.

Customers and users at Feuer Software GmbH

Feuer Software GmbH distinguishes between customers and users. Our customers are our contractual partners and organisation owners – mostly cities, municipalities, districts and associations. Users, on the other hand, are the end users within an organizational account. The services provided to the users are carried out as order processing for the respective customers. Use by consumers is excluded by the terms and conditions.

Responsible for data processing

Feuer Software GmbH

Karlsbader Str. 16, 65760 Eschborn

E-mail: info@feuersoftware.com

Phone: 06196 / 5255697

Managing Director: Dirk Koch

Website

Our website can be accessed freely from the Internet. The transmission is secured by means of encryption technology (HTTPS). This means that a third party cannot read the information exchanged.

Our website is divided into several sections: the information page, the documentation page, the forum and a web shop for invoicing without payment options.

Forum

In the forum, voluntary registration with name and e-mail address is possible. The forum is used for the exchange of ideas, wishes and questions between users. There is no connection with the contractual performance. The e-mail addresses provided are only used for normal forum use, such as notifications of new messages. The forum is hosted by netcup GmbH in Germany. The legal basis is your consent (Art. 6 para. 1 lit. a GDPR).

Web shop and ordering process

In the webshop, information about the billing address is necessary to process a purchase contract and register you as a customer. As part of the sales process, the email address provided is matched with the Connect service to assign licenses. Invoice data is processed by our accounting service provider Billomat (Germany) and stored according to the statutory retention periods (10 years). The legal basis is the performance of the contract (Art. 6 para. 1 lit. b GDPR).

Cloudflare

Our website uses the Cloudflare service via our web hosting provider 1&1 IONOS SE for load balancing and security. Cloudflare ensures high availability of the website and protects against attacks. Technical data such as IP addresses are processed. The legal basis is our legitimate interest in the secure provision of our website (Art. 6 para. 1 lit. f GDPR).

Google Analytics

We use Google Analytics to optimize our website. The tool will only be activated after your consent in the cookie banner. Without consent, no data is collected for website optimization. The service provider is Google Ireland Limited (Ireland). The legal basis is your consent (Art. 6 para. 1 lit. a GDPR).

Connect Portal

The Connect portal is the central administration and information portal for the processing of operational information. It is used in conjunction with EinsatzMonitor, EinsatzApp, EinsatzTablet and external interfaces.

Registration

Registration is required to use the Connect portal. A distinction is made between the creation of an organization account and the registration of individual users within an organization. We require surname, first name and e-mail address as mandatory information. Users can also voluntarily provide information about their place of residence and accessibility (telephone numbers). This voluntary information is only displayed within your own organization. In principle, it is possible to specify pseudonyms as names. The legal basis is the performance

of a contract (Art. 6 para. 1 lit. b GDPR), for voluntary information consent (Art. 6 para. 1 lit. a GDPR).

Operational data

The Connect portal processes mission-related data that is transmitted by the control center in the event of an emergency. Depending on how processed by the respective control center, these may also contain personal data (e.g. names, addresses, telephone numbers of reporters or affected persons). In individual cases, health data may also be included. The lawfulness of the collection and transmission of this data lies with the respective client. As a rule, this data is processed within the framework of the public interest, legal obligations or life-saving measures.

Organization administrators can restrict the visibility of the deployment data via an authorization concept. Deployment data can be individually configured by the customer with their own deletion deadlines.

Email notifications

Administrators and moderators can post information in the portal, which can also be received by e-mail according to individual user settings. Name and e-mail address are processed. Shipping is done via AWS Europe (Germany). The legal basis is the performance of the contract.

Push notifications

For the delivery of alarms and notifications to end devices, push notifications are sent via Apple and Google. Technical device identifiers (push tokens) are processed. The push messages themselves do not contain any personal data – the data is pseudonymised. The legal basis is the fulfilment of the contract (technically necessary for the alert).

Interfaces (WDX, Alamos, Public-API)

The Connect portal has interfaces to third-party systems (e.g. WDX, Alamos). These make it possible to transfer or retrieve operational data to Connect. All interfaces communicate exclusively in encrypted form. Approval is explicitly done by the organization administrator. These interfaces generate log data that is stored in AWS CloudWatch (Germany) for maintenance and troubleshooting purposes.

ApplicationApp

The EinsatzApp is an application for mobile devices (smartphones). It allows users to receive information about current operations and processes in the organization. The login is done with the Connect Portal account.

Data collected

Mandatory information is surname, first name and e-mail address. Optionally, residential address and telephone numbers can be provided. For technical reasons, device IDs and IP addresses are processed. Availability information is transmitted to the Connect portal along with the name when the user manually initiates this process.

GeoLocation (GeoFence)

The EinsatzApp offers an optional location function for availability detection. This function calculates the distance to the equipment shed locally on the end device. No location data is transmitted to Feuer Software GmbH – only the distance to the equipment shed in meters. The function must be actively activated by the user. The legal basis is consent in the form of activating the feature.

Tetra radio connection

It is possible to connect the account with an identification number from the Tetra wireless network. This can be linked to the user data in order to use the feedback function via radio message receivers.

Bug Reports and Log Data

The EinsatzApp can automatically send technical log data to the developers in the event of errors. This data contains technical metadata (e.g. device ID) and is stored at AWS CloudWatch (Germany) for 7 days and then automatically deleted. The legal basis is the fulfilment of the contract and the legitimate interest in the stability of the software.

Beta Feedback

A beta feedback form allows users to voluntarily provide feedback on beta versions of the app. Name, e-mail address and telephone number can optionally be entered. The form can also be used without personal information. The data is processed by Microsoft (M365) and Zendesk. IP addresses are deleted after 30 days. The legal basis is consent.

Support Protocol

As part of support activities, locally stored logs of the EinsatzApp can be voluntarily transmitted to support by e-mail. This can include email addresses, device IDs, IP addresses, and location data.

Deployment Monitor

The EinsatzMonitor is a central display and input system for operational data. It can receive mission data in various ways (e-mail, SDS, fax, sFTP, own scripts). Components of operational data can be personal data such as addresses, names and registration images. Since this data is used to rescue people, anonymization is not possible.

The EinsatzMonitor also receives the feedback from the alarmed users and, via Tetra-Control, the feedback from digital radio BOS pagers, which are assigned to the users.

The EinsatzMonitor sends service information to the Connect server at regular intervals to ensure that the latest software version is available. IP addresses are transmitted in the process. As a rule, the device is located in a public authority, so there is no direct personal reference.

Database upload for support

In individual cases, customers can transmit databases from the EinsatzMonitor to Feuer Software GmbH for error checking. These will be deleted immediately after completion of the support activity.

ApplicationTablet

The EinsatzTablet is an application for mobile devices (tablets) that is used in emergency vehicles. The tablet is basically assigned to a vehicle. It displays operational information and feedback from the emergency services.

Person assignment

People can be recorded on the Operational Tablet and assigned to the vehicle (vehicle crew). This information is passed to the Connect deployment log. The surname, first name and qualification are processed. The assignment remains in place in the deployment report until the deletion deadline set by the customer. The legal basis is the fulfilment of the contract (documentation obligation in the deployment report), and the clients regularly act to fulfil public tasks. Data can be passed on to investigating authorities on request.

Vehicle locations

Vehicles are identified by their ISSI (Tetra identifier) and these can be located via radio and tablet. Basically, vehicles are objects without a personal reference. A personal reference can arise if persons have been assigned to the vehicle or the vehicle is personally assigned to a person. A maximum of the last 3 to 10 positions are stored.

Operations Manager

The EinsatzManager is an application for operational documentation and for the creation of mission diaries. It is now also available as a portal solution (cloud-based), which replaces the previous on-premises application. The EinsatzManager can be connected to the Connect portal and transfer assignment information.

Recording of participants

In the EinsatzManager, external participants (e.g. those affected during operations) can be recorded by users or customers. Name, address, telephone number and, in certain cases, health data may also be processed. The processing is carried out within the framework of legal obligations, public interest and life-saving measures. Storage is carried out in accordance with the statutory retention periods (up to 10 years). All mission logs are archived in encrypted form if required.

PartnerApp

The PartnerApp is a stand-alone app that can be connected to the EinsatzApp by means of a QR code scan. In the event of an alarm, the user's feedback status is transmitted to the partner. No other personal information is transmitted – only technical device metadata for assignment. The legal basis is the performance of the contract.

In the event of app crashes, technical log data can be automatically sent to AWS CloudWatch (Germany). These are automatically deleted after 30 days. No log data is stored locally on the device. The legal basis is the legitimate interest in operational stability (Art. 6 para. 1 lit. f GDPR).

Helper App

The HelferApp works similarly to the EinsatzTablet, but is optimized for use on smartphones. It makes it possible to coordinate foot squads at events and to process operations through smaller feedback. For this purpose, the device is also used to determine the location for the

duration of the operation. The legal basis for the location transfer is contractual performance in accordance with Art. 6 (1) (b) GDPR. The activity is carried out for the client.

Name, age information and, in certain cases, health data of those affected can be recorded. The legal basis depends on the respective client and the country-specific regulations for rescue services, fire brigades and aid organisations. The HelferApp can only be used after activation by Feuer Software GmbH, for which a separate order processing agreement (AVV) for health data must be available. Data is automatically deleted after the end of the requirement.

Other interfaces

The Connect portal has other interfaces that allow third-party providers to pass or retrieve data to Connect. All interfaces require explicit approval by the organization administrator and the respective user. All interfaces communicate exclusively via encrypted transfer points. It is a transfer according to instructions within the framework of the contractual relationship by the respective customer.

Bug Reports (Sentry)

For the automatic detection of errors on our products, we use the Sentry service. IP addresses are processed and automatically deleted after 90 days. Sentry is based in the USA. Data is transferred on the basis of standard contractual clauses (SCCs). Only technical telemetry data is transmitted. The legal basis is the legitimate interest in improving the stability of the services (Art. 6 para. 1 lit. f GDPR).

Support

Ticket system (Zendesk)

We use Zendesk's ticket system to handle support requests. Name, e-mail address and, if applicable, telephone number are processed. Zendesk is based in the US and is certified under the EU-US Data Privacy Framework. User data will be deleted after 3 years, ticket content after 10 years in accordance with statutory retention periods. The legal basis is the performance of the contract.

Support via email, phone and forum

As part of our support activities, our employees are not able to access user data directly. Access may need to be granted through remote support tools by the customer or user. Our administrators can perform error analysis on database-level escalation – these accesses are logged under strict organizational requirements.

Newsletter (in planning)

It is planned to introduce a newsletter about the MailerLite service to inform administrators and users about operational security, updates and new features. MailerLite is based in the USA and is classified as a safe third country according to the EU-US Data Privacy Framework. Participation will be voluntary. The legal bases are consent, performance of a contract and legitimate interest.

Beta Tester Program

Users can voluntarily participate in the beta tester program for new program features. Name and address data are processed. Participation can be terminated at any time by one's own actions. Data will be deleted upon termination of the contract or termination. The legal basis is consent and performance of the contract.

Data transfer to third countries

In principle, your data will be processed in Germany or within the European Economic Area. Data will be transferred to the USA in the following cases:

- Zendesk (support ticket system) – certified according to the EU-US Data Privacy Framework
- Sentry (bug reports) - Standard Contract Clauses (SCCs), telemetry data only
- MailerLite (newsletter, in planning) – EU-US Data Privacy Framework

In all cases, there are appropriate safeguards for the protection of your data in accordance with the requirements of the GDPR.

Our service providers (processors)

We work with the following service providers who process personal data on our behalf:

- Microsoft Corp. (Germany) – Infrastructure, Databases, M365
- AWS Europe (Germany) – Emailing, Diagnostic Data
- 1&1 IONOS SE (Germany) – Website Hosting, Cloudflare
- netcup GmbH (Germany) –Hosting
- Billomat GmbH & Co. KG (Germany) – Accounting and Billing
- Joekel.dev (Germany) – Freelance work in development
- DPMS (Germany) – Data Protection Management
- Google Ireland Limited (Ireland) – Push notifications, website statistics
- Zendesk (US) Support Ticketing System
- Sentry (USA) Bug Reports
- MailerLite (USA) – Newsletter (in planning)
- Apple - Push notifications, App Store

Your rights

The European General Data Protection Regulation gives you the following rights:

- Right to withdraw: You can revoke your consent at any time. The previous processing remains unaffected.
- Right of access: You can request information about your data stored by us, including processing purposes, data categories, recipients and storage period.
- Right to rectification: You can request the correction of inaccurate data.
- Right to erasure: You can request the deletion of your data, provided that there are no legal retention obligations or legitimate interests to the contrary.

- Right to restriction: You can request the restriction of processing, for example if you contest the accuracy of the data.
- Right to data portability: You can receive your data in a structured, commonly used format or request that it be transferred to another controller.
- Right to lodge a complaint: You can complain to a data protection supervisory authority, usually the authority of your place of residence or workplace.

Right to object

If your personal data is processed on the basis of legitimate interests, you have the right to object to the processing if there are grounds relating to your particular situation.

If you would like to exercise your right to object, an e-mail to info@feuersoftware.com

Contact Now

Managing Director of Feuer Software GmbH

Dirk Koch

Karlsbader Str. 16

65760 Eschborn

info@feuersoftware.com

Phone: +49 6196 5255 697