Privacy Policy

According to the European General Data Protection Regulation requirements, a data protection statement must be easy to understand. The following data protection statement pursues precisely this goal by conveying the necessary information as simply as possible. Therefore, the naming of paragraphs and laws is primarily dispensed with.

Our data protection declaration is subdivided according to the respective products and areas of application to provide a clear introduction. These are

- Website,

- ConnectPortal,

- DeploymentMonitor,

- DeploymentTablet,

- DeploymentAPP, and

- DeploymentManager.

Feuer Software GmbH always encrypts all data traffic transmitted via the World Wide Web (Internet). Furthermore, through encryption, all databases are protected against unauthorized access by third parties. It is ensured that regular backups (data backups) of the information and program contents to be secured are carried out.

All data is hosted in Germany by a certified service provider. Feuer Software GmbH ensures that technical and organizational measures are taken in its area of responsibility to guarantee data security. In addition, Feuer Software GmbH performs its monitoring duties to supervise order processors within the scope of the permissible control options.

Website

Our website is freely accessible from the Internet. Access to this site is secured using encryption techniques (HTTPS). This means that as soon as a connection is established with our site, a third party cannot read information exchanged with this site.

Our website is divided into several sections: the information page, the documentation page, the forum, and a webshop.

In the forum and the webshop, registration is required to participate in the discussions and the exchange of goods. Separate registrations are required for the respective use of the applications mentioned; the data are not linked. A name and e-mail address are required to register as a user in the forum. On the webshop, information on the billing address is also required. These are required to process a possible sales contract and write a customer. As part of the sales process, it is necessary to compare the information provided with the Connect service for the licensee to disclose the e-mail addresses to third parties unless we are legally obliged to do so. The e-mail-address delivered in the forum is only used within everyday forum use, i.e., e.,g. for notification of new messages/entries or administrative purposes.

To optimize the use of our website, we use the tracking tool of Google Analytics; the device is only activated after your consent in the cookie banner on the first call; without this consent, data for the optimization of the website are not collected. Further information on this tool can be found at http://tools.google.com/dlpage/gaoptout?hl=de.

Customers and users at Feuer Software GmbH

Feuer Software GmbH distinguishes between users and customers. Customers are the contractual partners and organization owners, primarily cities, municipalities, and associations. On the other hand, users are the end-users within an organization's account. The services provided to users are performed as order processing by Feuer Software GmbH for the respective customers.

Cloudflare

Our pages use the functions of CloudFlare within the scope of the services offered by the website provider. The provider is CloudFlare, Inc. 665 3rd St. #200, San Francisco, CA 94107, USA. Cloudflare provides a globally distributed content delivery network with DNS. Technically, the transfer of information between your browser and our website is routed through CloudFlare's network. Cloudflare can thus analyze the data traffic between users and our websites, for example, to detect and ward off attacks on our services. In addition, Cloudflare may store cookies on your computer for optimization and analysis. This protects our legitimate interests in the optimal marketing of our offer, which outweigh our interests in the context of a balancing of goods according to Art. 6 para. 1 p. 1 lit. f DSGVO.

Here you can find information on the data collected there and on security & data protection at Cloudflare.

ConnectPortal

Our ConnectPortal is used in conjunction with at least one deployment monitor or an external data interface (see below) and usually with the connection of several deployment APPs and deployment tablets. It is the central administration and information portal for processing information intended to support the emergency forces in their operations.

To join the ConnectPortal, registration is mandatory. A distinction is made between creating an organization account with a user and registering a user as a member of an organization. Surname, first name, and e-mail address are required as personal data. Users can also provide information on their place of residence and availability (telephone numbers). These details are displayed exclusively within the user's organization for all organization participants. Other details are optional and only displayed within the user's organization. It is possible to enter pseudonyms as names.

The ConnectPortal also processes mission-related data (mission data). This data is the data transmitted by the control center in the event of an operation; depending on how the respective control centers process, it may also contain personal data. Third parties collected the data and provided it to Feuer Software GmbH for processing within order processing. The organizational administrators can restrict the visibility of this data to the users of the organization within the framework of an authorization concept. Simplified, this means that managers, for example, could see more deployment information, whereas regular emergency personnel only receive notification of an alarm. It is up to the responsible administrator of the client to make these settings proportionately within the scope of his authority as a client. Operational information data is usually processed to help people whose lives are in acute danger and protect significant material assets as quickly as possible.

The ConnectPortal collects the information from the OperationsAPP, the OperationsMonitor, and the connected interfaces and processes it visually. The names of the users are also displayed with their respective availability statuses. The users themselves set the availability information. (see Deployment App)

The ConnectPortal also displays other data such as news, severe weather warnings, calendar entries, and vehicle information. However, these do not contain any personal data.

Operations Monitor

The Operations Monitor is a central element of Feuer Software GmbH products. The Operations Monitor is often a gateway for

data processing. The operation monitor can read out operation data on the defined alarm path. Information can be initiated in various ways, such as e-mail, SDS, fax, sFTP, custom scripts, etc. The components of operational data can be personal data such as addresses, times, dates, names, alarm images, and active numbers. In context, these data can establish a personal reference and are thus regarded by us as personal data. Since this data is used for human rescue, it is impossible to anonymize it. A government agency usually transfers the data. It may also be data that has not been collected from the data subjects themselves. The collection is not subject to any information obligation in the sense of the GDPR.

The Operations Monitor also receives the user data of the alarmed users in the event of an operation and the available users in standby mode.

Furthermore, the Operations Monitor can be connected to the Tetra radio network via third-party software.

OperationsAPP

The OperationsAPP is an application installed on mobile devices (mobile phones). The purpose of the operations app is to enable users to obtain information about current operations and general processes in the organization. The login is done with the account mentioned above from the ConnectPortal. Here, too, the data to be entered are surname, first name, and e-mail address. Residential addresses and telephone numbers can be entered optionally. In addition, in the form of a beta test, one's availability status is displayed based on location information. This function calculates the mobile devices' position locally, depending on the respective watch location. No location information is transmitted to Feuer Software GmbH. Only the information about whether a person participates in the operation leaves the app. The availability information is transferred to the ConnectPortal and the name if the user has manually triggered this process.

It is possible to link his account with an identification number from the Tetra radio network. This can then be connected to the information above. This makes it possible to use the feedback function on radio message receivers; these replace the individual part in the OperationsAPP.

Deployment tablet

The deployment tablet is an application that can be installed on mobile end devices (tablets). The DeploymentTablet is intended to enable users to obtain information about current deployments and general processes. The Deployment Tablet is designed for use in emergency vehicles. The login is done with a vehicle-specific account, which the respective administration can create. The information released for the organization is then displayed on the monitor. This also includes feedback from the task forces on their participation in the operation. In addition, deployment information on current and past deployments can be viewed, provided that the corresponding releases have been set. Vehicle crews can be recorded on the tablet and transferred to Connect based on the feedback.

Deployment beacons (beta)

Bluetooth beacons ("deployment beacons") can be used with the deployment tablet. These beacons can be assigned to the emergency personnel by the respective organization. This creates a personal reference through the individual identification signals. The use of deployment beacons is optional. The separate IDs of the deployment beacons must be assigned to the person by the administration. The deployment tablet gives the deployment forces to the corresponding vehicle. Currently, the assignments are made for the duration of the deployment. It

is planned to pass on the information later to the deployment manager and the ConnectPortal to document and create deployment reports.

DeploymentManager

The DeploymentManager is an application for Windows computers. It is possible to document a deployment as a deployment diary with the monitor. Data can be entered and are then displayed historically. The deployment manager can be connected to the ConnectPortal. Then the deployment manager can take over and show the deployment information available from the ConnectPortal. Furthermore, data from the radio interface can be transmitted via the ConnectPortal. As far as deployment data is concerned, this data can also contain personal data (data of the person concerned, name, address, report picture).

All mission logs created are archived locally in encrypted form after the end of the respective mission, if required. Unencrypted storage is not possible.

Further interfaces

The ConnectPortal has additional interfaces. These enable third-party providers to receive impulses or even data records from the ConnectPortal or transfer them to the ConnectPortal. If this involves data transfer from third-party providers to the Connect services and Feuer Software GmbH, Feuer Software will process the data as a processor according to instructions.

All interfaces that release data require explicit approval by the organization administrator and the respective user in the Connect portal. All interfaces communicate exclusively via encrypted transfer points. The interfaces only transfer operational data. This is also subject to the individual active setup of the administrator of an organization. This is a transfer according to instructions by the settings of the respective customer.

Support

Our support staff cannot access user data directly within the scope of our support activities. Access may have to be granted to the customer or remote support tools (Anydesk). As part of the error analysis, the employees can escalate the process. Our administrators can then carry out error analyses at the database level, and access is logged under strict organizational requirements.

Bug tracker

Feuer Software GmbH uses an online portal as a "bug tracker application to receive faults, error messages, and feature suggestions." Registration requires the naming of an e-mail address as a means of contact. The IP addresses of the users who use this are also processed as technically necessary information. Names can be entered voluntarily. The entries made there are published and can be viewed publicly by other portal users. The data is deleted after the account is removed. The bug tracker is operated on servers of our order processors.

Rights of users

The European General Data Protection Regulation provides certain rights for our services and homepages users. You are entitled

- to revoke your consent by Art. 7 Para. 3 DSGVO. This means that we may no longer process the data based on this consent in the future;
- to request information about your data processed by us by Art. 15 DSGVO. In particular, you may request information about the processing purposes, the

category of personal data, the types of recipients to whom your data have been or will be disclosed, the planned storage period, the existence of a right to rectification, erasure, restriction of processing or objection, the presence of a right of complaint, the origin of your data if it has not been collected by us, as well as the existence of automated decision-making, including profiling, and, if applicable, meaningful information about its details;

- by Art. 16 DSGVO, to demand the immediate correction of inaccurate or incomplete personal data stored by us;
- by Article 17 of the Regulation, to request the erasure of your data stored by us, unless the processing is necessary for the exercise of the right to freedom of expression and information, for compliance with a legal obligation, for reasons of public interest, or the establishment, exercise or defense of legal claims;
- by Art. 18 DSGVO, to request the restriction of the processing of your data, insofar as the accuracy of the data is disputed by you, the processing is unlawful, but you object to its erasure, and we no longer require the data, but you need it for the assertion, exercise or defense of legal claims or you have objected to the processing by Art. 21 DSGVO;
- by Art. 20 DSGVO, to receive the data that you have provided to us in a structured, standard, and machine-readable format or to request the transfer to another controller; and
- complain to supervisory authority by Art. 77 DSGVO. As a rule, you can contact the supervisory authority of your usual place of residence or workplace or our registered office for this purpose.

Right of objection

Suppose your data is processed based on legitimate interests under Article 6 (1) sentence one lit. f DSGVO, you have the right to object to processing your data under Article 21 DSGVO, provided that there are grounds for doing so which arise from your particular situation.

If you wish to exercise your right of objection, an e-mail to info@feuersoftware.com is sufficient.

Managing Director of Feuer Software GmbH
Dirk Koch
Karlsbader Str. 16
65760 Eschborn
info@feuersoftware.com
Tel: + 49 6196 5255 697
Fax: + 49 6196 5255 696