DATA PROTECTION INFORMATION SAFEDI (SAFE DISTANCE Control)

We process your data exclusively in accordance with the provisions of the General Data Protection Regulation (GDPR) and the Austrian Data Protection Act (DSG). The GDPR is an EU regulation that ensures that your personal data is protected.

We make every effort to keep this privacy policy up to date. We therefore reserve the right to change it from time to time and to take changes in the collection, processing or use of your data into consideration accordingly. The current version of the current data protection information is always available at https://safedi.com/datenschutz-app/ and within the SAFEDI app.

In the following we inform you about us and the type, extent and purpose of the data collection and data use, on which legal basis they are based and which rights you have as a data subject when using SAFEDI.

About us

The data controller is SAFEDI Distance Control GmbH, Dr. Walter Zumtobel Straße 2, A-6850 Dornbirn, Austria.

Whenever in this text "we" or "us" is used, then this refers to SAFEDI Distance Control GmbH .

What is the purpose of SAFEDI?

SAFEDI is helping to counteract COVID-19 infection, relieve the burden on the health system and strengthen the economy. In order to achieve this, SAFEDI has two functions:

1. SAFEDI serves as a **distance warning device**. It uses Bluetooth to measure the distance to other SAFEDI devices and helps people who wear a SAFEDI to maintain a greater and safer distance. As soon as people approach each other, SAFEDI triggers an optical signal as an advance warning. If the distance between two people falls below the minimum distance, optical and acoustical signals are continuously released.

SAFEDI does not require Internet or smartphone for this function. No data is stored, transmitted or processed in any other way.

2. SAFEDI **stores contacts** with other SAFEDI devices. A contact log is used to record which SAFEDI devices have come close to each other. The contact log is only active if you log in with a unique SAFEDI ID or QR code, which are included in the package. SAFEDIs can even be used without this function. The activation of the anonymous contact log is voluntary.

If an infection of a SAFEDI user is detected and notified, those SAFEDI devices which, according to the contact log, were in close contact with the infected person, are notified. This gives the users of these devices the opportunity to quarantine, get tested or take other protective measures.

Both reporting an infection and deciding what action a notified person takes are voluntary. However, please note that other legislation may require you to notify employers or health authorities of infections. We also expressly point out that the use of a SAFEDI does not replace recommended hygiene measures or the advice of a doctor.

What is personal data?

Personal data is information that relates to an identified or identifiable natural person. Personal data are protected in accordance with the GDPR.

Health data is personal data relating to the physical or mental health of a natural person, including the provision of health services, from which information on his/her state of health is derived. These are specially protected under the GDPR.

Pseudonymous data is personal data that can no longer be assigned to a specific data subject without the use of additional information. SAFEDI processes pseudonymous data. An assignment of these data to a specific person can only be made by this person him/herself.

Data processed in your SAFEDI

Each SAFEDI has a unique ID. This consists of the MAC address, which is a unique hardware address of your device (also called the "physical address"), and a signature.

In your SAFEDI the MAC address of your own SAFEDI as well as MAC addresses of other SAFEDI devices, which were near your SAFEDI, are stored. It also records the number of contacts between two SAFEDI devices and the date of contact.

Data processed during activation the contact log

Without activating the contact log, only the distance maintenance function can be used. The contact log can be activated in two ways:

1. About the SAFEDI app

If you download the SAFEDI app from the App Store (Google Play Store or Apple App Store), data must be entered there. This data is transmitted to the respective App Store together with other information such as the customer number of your account, the time of the download and the individual device identification and processed there. This data processing is carried out exclusively by the respective App Store. It cannot be influenced by us. We are not the data controller for this processing. The respective data protection information can be found at Google and Apple.

It is not necessary for you to enter any personal data when installing the SAFEDI app.

Your SAFEDI is activated once by entering the ID or by scanning the QR code, which is on the package of your SAFEDI, in the SAFEDI app. The following steps are performed:

- It automatically checks which company the ID belongs to. This is done by comparison with a database stored on a server of SAFEDI Distance Control GmbH. This database contains a list of MAC addresses of SAFEDI devices assigned to specific companies. This list does not allow a SAFEDI to be assigned to a specific person, but only to a company.
- The transmission of the contact log via the SAFEDI app is activated. The cloud server is saved in the app as the addressee for the transmission of the contact log.
- Furthermore, an asymmetric key pair (token) is created in your app. This is used to receive push messages. The public key is transmitted to a push message service, the private key remains on your end device in the app.

This data is processed on the basis of your express consent (Art. 6 para. 1 lit. a and Art. 9 para. 2 lit. a GDPR). If you do not give your consent, you will not be able to use the contact log. Nor can push messages be sent to you. You can also revoke this consent at any time by uninstalling the SAFEDI app.

2. Via a Synchro Hub

The company may also operate a synchro hub. In this case it is not necessary to install the SAFEDI app on a mobile end device. The contact diary is activated once by entering the ID or by scanning the QR code on the synchro hub.

The transmission of the contact log via the synchro hub is activated. In this case no asymmetric key pair is created for sending push messages. This function is not available.

This data is processed on the basis of your express consent (Art. 6 para. 1 lit. a and Art. 9 para. 2 lit. a GDPR). If you do not give your consent, you will not be able to use the contact log. You can also revoke this consent at any time by switching off or no longer using your SAFEDI.

Data processed during the contact

In your SAFEDI, the MAC addresses of other SAFEDIs are stored, which were located at a sufficient distance from your SAFEDI for a sufficiently long time. The MAC addresses are exchanged via Bluetooth. Besides the MAC address, the date and time of the contact are stored. No data is stored concerning which person is wearing the respective SAFEDI device.

The legal basis for this processing is the legitimate interests of the respective wearer of a SAFEDI (Art. 6 para. 1 lit. f GDPR), as the storage of MAC addresses is indispensable for the functioning of the device. Furthermore, MAC addresses arepseudonymised data that is deleted from the device during download.

Data processed during transmission of the contact log

If your SAFEDI is located near a sync hub or the mobile end device (smart phone) with which the SAFEDI was activated, the contact log is downloaded from the SAFEDI device and transferred to the cloud server. This will delete all the contacts stored in the SAFEDI.

A list is transferred to the server containing the MAC addresses of two SAFEDI devices that were in contact and the number, date and time of contact. A retransmission of this data from the server to the SAFEDI app or to the SAFEDI device is not possible.

The data is encrypted during transmission between synchro hub/SAFEDI App and server with a transport encryption corresponding to the current security standard. The storage of the data on the server is also encrypted.

The legal basis for this processing is your consent (Art. 6 para. 1 lit. a and Art. 9 para. 2 lit. a GDPR). This consent can be revoked at any time, whereby a revocation does not affect the legality of the processing that has taken place in the meantime.

Data processed when an infection is reported

An infection is reported by a person of trust (e.g. the company doctor or an authority). This ensures that only confirmed illness reports are carried out. The reporting of an infection is specially protected health data.

In order to carry out the illness notification it is necessary that you pass on the ID of your SAFEDI (MAC address and signature) to the named trusted person. This ID is located on the box of your SAFEDI and is only known to you.

You are not obliged to pass on the ID of your SAFEDI to the respective person of trust. The disclosure of an infection is voluntary. The processing of this data is therefore based on your express consent (Art. 9 para. 2 lit. a GDPR). This consent can be revoked at any time, whereby a revocation does not affect the legality of the processing that has taken place in the meantime. However, please note that you may be obliged to inform your employer about a corona infection under labour law regulations. In this case, the processing is carried out because it is necessary for the exercising of rights or the fulfilment of obligations arising from employment rights (Article 9 para. 2 lit. b GDPR).

Data processed in the event of a warning

If an infection is reported, the SAFEDIs whose MAC addresses are stored in the contact log for the reporting SAFEDI are notified. A notification can also be made across companies.

If the SAFEDI was set up via the SAFEDI app, a push message is generated for notification purposes and sent to the app. The asymmetrical key pair generated when the SAFEDI is activated is used for this purpose. The recipient of the message does not know which SAFEDI initiated the infection report. Neither does the person who has initiated an illness report know which SAFEDIs will be notified.

If the SAFEDI has been activated via a synchro hub, the manager of the synchro hub receives a list of MAC addresses of those SAFEDIs that are available as an option in the contact log of the SAFEDI that reported the infection. If MAC addresses of SAFEDIs assigned to synchro hubs of another administrator or company are stored in the contact log, this administrator also receives a list of the SAFEDIs registered for this synchro hub. This list contains exclusively MAC addresses and therefore does not allow any conclusion to be drawn about the respective users to whose SAFEDI the MAC address is assigned. This list can be made available to all employees of a company so that they themselves can check whether the MAC address of their SAFEDI appears on the list.

The legal basis for such processing is consent (Art. 6 para. 1 lit. a as well as Art. 9 para. 2 lit. a GDPR). This consent can be revoked at any time, whereby a revocation does not affect the legality of the processing that has taken place in the meantime.

Data processed when the all-clear is given

If it subsequently turns out that you did not contract COVID-19 after all, for example because a later test showed that there was no infection, your trusted person should be informed. By entering the ID of your SAFEDI you can issue an all-clear signal. The legal basis for this processing is the consent (Art. 6 para. 1 lit. a and Art. 9 para. 2 lit. a GDPR), which is given to send the all-clear. This consent can be revoked at any time, whereby a revocation does not affect the legality of the processing that has taken place in the meantime.

The all-clear to the respective SAFEDI users is given in the same way as the warning.

Technical provision of services

Every communication via the Internet or other networks requires certain data to enable the flow of information. This data includes the IP address of the respective devices, the date and time of transmission and configuration data of the respective end device.

The processing of this data is based on a legitimate interest (Art. 6 para. 1 lit. f GDPR), as the temporary processing of the listed data by the system is necessary to enable communication between the terminal and the server. This data is not stored or merged with other personal data. The data is deleted as soon as it is no longer required, which is when the transmission in question has ended.

Will data be passed on?

Personal data will only be passed on for the purposes explicitly specified in this data protection information. In addition, however, legal obligations may exist, for example in the interest of criminal prosecution to pursue abuse or due to the Austrian Epidemics Act, which oblige us to pass on data to authorities. In this context, however, we would like to point out that we only store pseudonymous data, which does not allow us to draw conclusions about the respective user.

Processors and external services

For the provision of parts of the service we are dependent on external service providers (contract processors). We have carefully selected our external service providers as processors, check them regularly and have contractually obliged them to process all personal data exclusively in accordance with our instructions and to comply with the provisions of the GDPR (Art. 28 GDPR).

We use the following external service providers:

1. Firebase Cloud Messaging

Push notifications are sent via the "Firebase Cloud Messaging" service

To enable the sending of push notifications, a "Firebase Cloud Messaging Registration Token" is created when the SAFEDI app is started for the first time, which clearly identifies the app installation on your device. The token is used to identify the message destination. The messages are sent via the Google Firebase Cloud Messaging service, which is provided by Google, Inc, Mountain View, USA. More information about Google Firebase Cloud Messaging can be found at https://firebase.google.com/products/cloud-messaging/ and in Google's privacy policy at http://www.google.de/intl/de/policies/privacy.

For Apple devices running iOS, Firebase Cloud Messaging forwards the push notifications to the Apple

Push Notification Service.

2. Heroku, MongoDB und Microsoft Azure

To process and store the contact log, we use the services of Heroku, Inc, a subsidiary of salesforce.com, inc., with headquarters at Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, California, 94105, USA; MongoDB, Inc, with headquarters at 1633 Broadway, 38th Floor, New York, NY 10019, USA, und der Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA. Further information can be found at https://devcenter.he- roku.com/articles/security-privacy-compliance, https://docs.atlas.mongodb.com/refe- rence/faq/security/ and https://azure.microsoft.com/de-de/overview/trusted-cloud/privacy/.

The external service providers we use are based outside the European Economic Area, namely in the USA. The European Commission has authorised the use of standard contractual clauses as a means to ensure adequate protection when transferring data to the US. We have therefore concluded agreements with these service providers on the processing of commissioned data using the standard contractual clauses.

Deletion of data

All personal data is deleted as soon as it is no longer necessary for the purposes for which it was collected and used.

If data is stored locally on your end device (token of the Firebase Cloud Messaging service), it will be deleted by uninstalling the SAFEDI app.

Data in your contact log is automatically deleted after 14 days. Where national legislators specify longer periods, this period may also be extended.

Furthermore, all personal data will be deleted even after the end of the Corona epidemic. At present it is not possible to foresee when this will be the case.

Your rights

We only process anonymous and pseudonymous data. We can therefore not identify you on the basis of this data. In order to meet your requirements, it is therefore necessary for you to cooperate, in particular by sending the ID of your SAFEDI (MAC address and signature).

To assert your rights, you can contact us at the following address SAFEDI Distance Control GmbH
Dr. Walter Zumtobel Straße 2 A-
6850 Dornbirn
Telephone: +43 / 5572 / 22000 600
E-Mail: info@safedi.com

You have the following rights in particular:

1. Right of information

You have the right to obtain from us, at any time and upon request, information on the personal data processed by us and concerning you (Art. 15 GDPR).

2. Rectification of incorrect data

You have the right to demand that we immediately rectify any personal data concerning you if it is incorrect (Art. 16 GDPR).

3. Right to deletion

You have the right, under the legal prerequisites, to demand that we delete the personal data concerning you. In accordance with Art. 17 of the GDPR, such a right of deletion exists in particular if the personal data are no longer necessary for the purposes for which they were collected or otherwise processed, and in cases of unlawful processing, even if you withdraw your consent and there is no other legal basis for the processing.

4. Right to restriction of processing

You have the right to ask us to restrict processing (Art. 18 GDPR). This right shall apply in particular if the accuracy of the personal data is disputed between you and us, for the period of time required to verify its accuracy. There is also the case of an existing right of deletion where you request limited processing. Processing may also be restricted if the data is no longer required for the purposes pursued by us, but you need this data to assert, exercise or defend legal claims.

5. Right to data portability

You have the right to receive from us the personal data concerning you which you have made available to us in a structured, common, machine-readable format (Art. 20 GDPR).

6. Right to object

Insofar as processing is carried out on the basis of Art. 6 para. 1 lit. f GDPR, you have a right of objection (Art. 21 para. 1 GDPR). This means that you can object to data processing at any time for reasons arising from your particular situation. However, an objection only leads to the omission of processing if the objection is justified by special reasons. In this case, we no longer process the personal data, unless we can provide compelling reasons for processing worthy of protection which outweigh your interests, rights and freedoms, or the processing serves to assert, exercise or defend legal claims.

7. Right to appeal

You have the right to complain to the competent supervisory authority: Austrian Data Protection Authority
Barichgasse 40-42
A-1030 Vienna
Telephone: +43 1 52 152-
0 E-Mail: dsb@dsb.gv.at
Internet: www.dsb.gv.at

Version: 29.10.2020