Privacy Statement

“Dräger RAM Link ” Applikation („App“)

§ 1 Information on the processing of personal data

(1) In the following, we inform you about the processing of personal data when using our mobile app. Personal data is all data that can be related to you personally, e.g. name, address, email addresses, user behavior.

(2) The controller pursuant to Art. 4 (7) of the EU General Data Protection Regulation (GDPR) for the basic functions for the provision of the app and data processing in its own interest is Dräger Safety AG & Co. KGaA, Revalstraße 1, D-23560 (see our Provider Identification). You can reach our Group Data Protection Officer at dataprivacy@draeger.com.

(3) When you contact us by e-mail or via a contact form, the data you provide (your e-mail address, name and telephone number, if applicable) will be stored by us in order to answer your questions. We delete the data accruing in this context, if the inquiry is assigned to a contract, after the time limits for the term of the contract, otherwise after the storage is no longer necessary or restrict the processing if there are legal obligations to retain data.

(4) If we use service providers for individual functions or use your data for advertising purposes, we will always carefully select and monitor these service providers and inform you in detail about the respective processes below. In doing so, we will also state the defined criteria for the storage period.

(5) Insofar as we provide the app to support a product or service and the client, as the controller, determines the data processing, we shall only act as a processor within the meaning of Art. 28 GDPR. In this respect, the client is responsible for the (further) provision of information on data processing within the meaning of Art. 13 and 14 GDPR.

§ 2 Your rights

(1) Depending on the applicable data protection law, you may have the following rights with regard to the personal data concerning you:

- Right of access / information

- Right to rectification or erasure

- Right to restriction of processing (blocking)

- Right of object

- Right to data portability

- Right to complain to a data protection supervisory

authority about our processing of your personal data.

§ 3 Processing of personal data when using our mobile app

(1) When you download the mobile app, the required information is transferred to the app store, i.e. in particular username, email address and customer number of your account, time of download, payment information and the individual device identification number. In addition, the app store still independently collects various data and provides you with analysis results. We have no influence on this data processing and are not responsible for it. We process the data only insofar as it is necessary for downloading the mobile app to your mobile device.

(2) When you use the mobile app, we process the personal data described below to enable you to use the functions conveniently. If you want to use our mobile app, we process the following data, which are technically necessary for us to offer you the functions of our mobile app and to ensure stability and security, so that they must be processed by us. For users from the European Union: The legal basis is Art. 6 (1) (f) GDPR:

-IP address

-Date and time of the request

-time zone difference from Greenwich Mean Time (GMT)

-content of the request (page visited)

-Access status/HTTP status code

-amount of data transferred in each case

-previously visited page

-Browser

-Operating system
-language and version of the browser software.

(3) Dräger only stores your personal data for as long as is necessary to provide the service or as required by law. The legal basis for the stated data processing is Art. 6 (1) (b) GDPR

(4) Furthermore, in order to provide the services of the app, we require your
Device identification, unique number of the end device (IMEI = International Mobile Equipment Identity), unique number of the network subscriber (IMSI = International Mobile Subscriber Identity), mobile phone number (MSISDN), MAC address for WLAN use, name of your mobile end device, e-mail address.

(5) In iOS, you have various options for largely restricting advertising and tracking. Tracking is generally carried out via the so-called "Advertising Identifier" (IDFA). This is a unique, but non-personalized and non-permanent identification number for a specific end device, which is provided by iOS. The data collected via the IDFA is not linked to other device-related information. We use the IDFA to provide you with personalized advertising and to evaluate your usage. If you go to the "Privacy" option in the iOS settings, you can largely deactivate advertising analysis under "Tracking". If you activate the "Allow apps to request tracking" function, our app will ask you the first time you use it whether you agree to advertising measures and you can activate or deactivate advertising. In addition, you can select the "Apple advertising" option in the "Privacy" option and deactivate "personalized advertising". In the "Analysis & Improvements" option, you can also deactivate the "Share iPhone analysis" and "Improve Siri & Dictation"

function, which means that no static information about your use of iOS is transmitted to Apple. We would like to point out that you may not be able to use all the functions of our app if you restrict the use of IDFA.

(6) The services and functionalities in detail:

(a) This app uses the Firebase Crashlytics tool from Google Ireland Limited, at Gordon House, Barrow Street, Dublin 4 DUBLIN, D04 E5W5, Ireland ("Crashlytics"). Crashlytics helps us to collect analyses and details about crashes and errors that may occur in our app.

This is done in various ways:

- Logs: Events in the app that are sent along with the crash report to provide context when your app crashes.
- Crash reports: Every crash is automatically converted into a crash report and sent the next time the app is opened.
- Stack Traces: Even if an error has occurred and your application is working again, the Dart stack trace can be sent to track the error.

Crashlytics installation UUIDs, crash traces and breakpad minidump-formatted data are temporarily stored and automatically deleted after 90 days.
The data collected as part of Crashlytics is processed in order to detect and rectify errors and crashes at an early stage. Storing the data on the user's device is technically necessary in this context. The legal basis is our legitimate interest in maintaining the stability and security of the application, Art. 6 (1) (f) GDPR.

You can read more about this in the information on data protection and security in Firebase: https://firebase.google.com/support/privacy.

§ 4 Transfer of personal data
In principle, the processing of personal data by us takes place exclusively within the European Union (EU) or the European Economic Area (EEA). In certain cases, however, it may be necessary for us to transfer information to recipients in so-called "third countries".

"Third countries" are countries outside the EU or the EEA Agreement in which it cannot be readily assumed that the level of data protection is comparable to that in the EU. If the transferred information also includes personal data, we ensure before such a transfer that the required adequate level of data protection is guaranteed in the respective third country or at the recipient in the third country. This may result in particular from a so-called "adequacy decision" of the European Commission. Alternatively, we can also base the data transfer on the so-called EU standard contractual clauses agreed with a recipient. We will be happy to provide you with further information on the suitable and appropriate guarantees for compliance with an appropriate level of data protection on request

§ 5 Sub-processors for the provision of services
As part of the provision of services, the following subcontractors are used depending on the controller named in § 1 (2). We have taken (contractual and technical) security precautions to comply with the relevant data protection regulations.
- The entities of the Dräger Group that are used to provide services for operation and support include, in particular, Drägerwerk AG & Co. KGaA based in Lübeck, Germany, and Dräger Tehnika d.o.o., based in Belgrade, Serbia.

§ 6 Data permission in our mobile app
If you want to connect our mobile app in conjunction with our device, we need permission / Bluetooth to communicate with the device. If you want to receive push notifications even when you are not in our app, you must allow us to do so. We will ask you when you install (Android) or use (iOS) the app for the first time. Additional push notifications for other services are optional.If you wish to interact with us via the app (competitions, uploads, etc.), you must grant the app access to certain functions of your smartphone. We will inform you in detail about the services offered by our app under the menu item "Help". All notifications and access options can be subsequently switched on or off in the settings menu. For push notifications, we use the services Firebase Cloud Messaging from Google (Android) and Apple Push Notifications (iOS). Firebase and Apple generate a calculated key that is made up of the app identifier and the device identifier. This key is stored on our push platform together with the settings you have selected in order to deliver the content according to your preferences. The Firebase or Apple servers cannot draw any conclusions about users' requests or determine any other data about a person. Firebase and Apple only serve as intermediaries.

Status: January 2024