knapp.com

Information according to Article 13 GDPR and Consent for the use of the Health Token for external persons

Why is KNAPP implementing the Health Token?

KNAPP is implementing a system for contact tracing to be able to track the contacts of anyone who has become infected with the coronavirus (COVID-19) or may be infected (suspected case) with the aim of promoting health, preventing infection and curbing the spread of the Sars-CoV-2 virus (termed "corona-virus" or "COVID-19" in the following): the **KNAPP Health Token**. KNAPP is acting to conscientiously fulfil its duty of care as an employer[1] and to create a safe environment for all employees.

What is the legal basis for the introduction of the Health Token?

We hereby obtain your **consent** to process the data gained through/collected by the Health Token, (Article 9 (2) (a) GDPR). We hope that everybody will gladly participate in protecting their own and their family's health – we look out for one another **#weareknapp**

KNAPP has a legal duty to collect this data and implement these measures, which fall under the above described due diligence obligation or for collecting and reporting under the Epidemics Act and Article 9 (2) i GDPR (processing is necessary for reasons of public interest in the area of public health)

There is no automated decision-making or profiling.

Which data does the Health Token collect?

The following types of personal data are collected:

Data on the Token: The Token is able to establish contact with another token in the immediate vicinity and to save the time (calendar day) and the ID of the other Token (pseudonymized data).

Data that is transmitted for notification to COVID19@knapp.com in a suspected case: Name, company/department, symptoms and date they began, test status, quarantine notice

General data: Allocation of the person to the Token ID (name, personnel number)

Information shared by the crisis committee with the affected suspected case or contacts as result of contact tracing: Existence of a contact (**not, however,** who it is, when the contact took place or the duration of the contact)

1 Duty of care according to § 1157 ABGB Austrian General Civil Code in conjunction with § 3 ANSchG Employee Protection Law (Prevention of infections and controlling the spread of virus at the workplace);

How is the data access process carried out?

Only in the following cases[2] may the relevant "critical" contacts be compiled:

1. When an employee/external person using the KNAPP Health Token tests positive for a COVID-19 infection
2. When an employee/ external person using the KNAPP Health Token is a suspected case for a COVID-19 infection
3. When an employee/ external person using the KNAPP Health Token has had contact with a person who tested positive
4. When an employee/ external person using the KNAPP Health Token has had contact with a person who is a suspected case.

How will the unlawful or improper use of the token data be prevented?

The described process, which includes protocols and technical limitations, ensures that misuse of the data by the company is not possible.

We take careful precautions to protect your data from loss, manipulation and unauthorized access. The precautions are in accordance with the latest state-of-the-art technology and legal requirements.

How long will the data be saved?

The data on the token is saved in accordance with the legal requirements, currently for **14 days** and is then automatically deleted.

When data is evaluated according to the defined processes, the relevant evaluation and the associated documentation is saved for a period of 3 years. The purpose of keeping these records is to be able to demonstrate compliance with our duty of care.

Will the data be passed on to third parties?

The data is only passed on to third parties in the following situations:

- Disclosing the data to the authorities, e.g., when the district administrative authorities request it according Article 9(2)(i) GDPR in connection with paragraph 5(3) of the Epidemics Act 1950.
- Service provider for the server

Third parties may only use the provided data for the above-mentioned purposes.

2 KNAPP defines the cases only as stipulated by the authorities, especially if a person has been determined as such a case by the 1450 health hotline

What should I be aware of when using the Health Token?

The Health Token is the property of KNAPP AG. When you use the Health Token, you agree to use it according to its function and to handle it as specified (e.g. not taking it off, charging the battery, etc.).Loss of the Health Token must be immediately reported to the reception desk. The Health Token may only be used by the person to whom it was assigned. Passing the token to another person is not permitted. If the Health Token is lost or wilfully damaged during use, you must pay € 25.00 for its replacement.

Is there an app used with the Health Token?

The maker of the Health Token also provides an app, which can be used to transmit the data on the token to the server. Using the app is a voluntary alternative. The app has a terms of use, which apply when you use the app. KNAPP is not providing the app, nor is KNAPP responsible under data protection law for this.

Push notifications are possible through the app. Please not that only the measures given in the official notification by the KNAPP crisis committee are to be followed.

What are my rights as an affected person?

With respect to my personal data, I have the right of information and access, rectification and erasure, to restrict processing, to revoke my declaration of consent and a right to data portability.

I may revoke my declaration of consent at any time by writing to datenschutz@knapp.com, whereby the legality of processing the personal data collected so far remains intact.

You furthermore have the right to complain to the data protection supervisory authority regarding our processing of personal data. The Austrian Data Protection Authority is the responsible party. They can be contacted at: Österreichische Datenschutzbehörde, Barichgasse 40-42, 1030 Vienna, telephone: +43 1 52 152-0, E-Mail: dsb@dsb.gv.at

More information

On data protection is available at https://www.knapp.com/en/home/privacy-policy/

The KNAPP data protection team can answer any questions at datenschutz@knapp.com.