KNAPP

knapp.com

Information nach Art 13 DSGVO **und zur Einwilligung** in die Verwendung des Health Token für Externe

Zu welchem Zweck führt KNAPP den Health Token ein?

Zum Zweck der Gesundheitsvorsorge und Prävention von Infektionen sowie Eindämmung der Verbreitung des Sars-CoV-2 Virus (im Folgenden auch „Coronavirus" oder „COVID-19") führt KNAPP ein System („contact tracing") zur Ermittlung von Personen ein, die sich mit dem Coronavirus infiziert haben (COVID-19 Infektion) oder haben könnten (Verdachtsfall): der **KNAPP Health Token**. KNAPP tut dies um ihrer Sorgfaltspflicht als Arbeitgeber[1] gewissenhaft nachzukommen und so eine für alle MitarbeiterInnen sichere Umgebung zu schaffen.

Auf welcher Rechtsgrundlage wird der Health Token eingeführt?

Für die Verarbeitung dieser Daten in der Form des HealthToken holen wir hiermit Ihre **Einwilligung** ein (Art 9 Abs 2 lit a DSGVO). Wir hoffen, alle tragen gerne dazu bei, sich und ihre Familien zu schützen – schau auf mich, schau auf dich **#weareknapp**

Die Pflicht zur Erhebung und Durchführung dieser Maßnahmen hat KNAPP auf gesetzlicher Grundlage, etwa der oben beschriebenen Sorgfaltspflicht oder Erfassung- und Meldepflichten aus dem Pandemiegesetz und Art 9 (2) i DSGVO (Verarbeitung aus Gründen der öffentlichen Gesundheit, etwa Pandemien)

Eine automatisierte Entscheidungsfindung einschließlich Profiling erfolgt nicht.

Welche Daten werden vom HealthToken gesammelt?

Folgende personenbezogene Daten werden von Ihnen verarbeitet:

Daten auf dem Token: Der Token ist in der Lage, mit anderen Token in der unmittelbaren Umgebung Kontakt aufzunehmen und Zeitpunkt (Datum des Kalendertags) und die ID des anderen Token zu speichern (pseudonymisierte Daten).

Daten die für eine Meldung an covid19@knapp.com im Verdachtsfall übermittelt werden: Name, Firma/Abteilung, Symptome und Datum Eintritt, Status Test, Quarantänebescheid

Allgemeine Daten: Zuordnung der Person (Name, Personalnummer) zu Token-ID

Information die betroffenen Verdachts- oder Kontaktpersonen durch den Krisenstab mitgeteilt werden als Resultat des „contact tracing": Bestehen eines Kontaktes (**nicht aber** wer es ist, wann, wo oder wie lange der Kontakt war)

1 Fürsorgepflicht iSd. §1157 ABGB iVm. § 3 ANSchG zum Ausschluss von Gesundheitsrisiken am Arbeitsplatz (Prävention von Infektionen und Eindämmung einer Virusverbreitung am Arbeitsplatz);

Wie erfolgt der Prozess zur Einsichtnahme in die Daten?

Ausschließlich in den folgenden Fällen[2] dürfen die relevanten „kritischen" Kontakte erhoben werden:

1. Im Falle einer positiven Testung auf eine COVID-19 Infektion eines Mitarbeiters/externer Person mit KNAPP Health Token
2. Bei Auftreten des Verdachts einer COVID-19 Infektion eines Mitarbeiters/ externer Person mit KNAPP Health Token
3. Bei Kontakt eines Mitarbeiters/externer Person mit KNAPP Health Token mit einer positiv getesteten Person
4. Bei Kontakt eines Mitarbeiters/ externer Person mit KNAPP Health Token mit einem Verdachtsfall

Wie wird eine unrechtmäßige oder missbräuchliche Verwendung der Daten am Token verhindert?

Durch den beschriebenen protokollierten und technisch eingeschränkten Prozess wird sichergestellt, dass eine missbräuchliche Verwendung von Daten von Seiten des Unternehmen nicht möglich ist.

Wir treffen gewissenhaft Vorkehrungen, um Ihre Daten vor Verlust, Manipulation und unberechtigtem Zugriff zu schützen. Die Vorkehrungen entsprechen dem technologischen Entwicklungsstand und den gesetzlichen Vorgaben.

Wie lang werden die Daten gespeichert?

Die am Token gespeicherten Daten werden entsprechend der gesetzliche Vorgaben, zurzeit für die Dauer von **14 Tagen,** bei der KNAPP AG gespeichert und dann automatisch gelöscht.

Im Falle einer Auswertung der Daten anhand des definierten Prozesses wird die relevante Auswertung sowie zugehörige Dokumentation für die Dauer von 3 Jahren gespeichert. Der Zweck dieser Aufbewahrung ist der Nachweis der Einhaltung unserer Sorgfaltspflichten.

Werden die Daten an Dritte weitergegeben?

Eine Weitergabe an Dritte erfolgt ausschließlich in folgenden Fällen:

- Weitergabe an Behörden, etwa auf Verlangen an die Bezirksverwaltungsbehörden nach Art 9 Abs. 2 lit i DSGVO iVm. § 5 Abs. 3 Epidemiegesetz 1950
- Bereitsteller der IT Infrastruktur: Dienstleister für den Server

Die weitergegebenen Daten dürfen von dem Dritten ausschließlich zu den genannten Zwecken verwendet werden.

2 KNAPP definiert die Fälle entsprechend den behördlichen Vorgaben, insbesondere wenn eine Person durch die Gesundheitsberatung 1450 als solcher Fall eingestuft wurde

Was muss ich bei der Verwendung des Health Token beachten?

Der Health Token ist Eigentum der KNAPP AG. Wenn Sie den Health Token nutzen, dann stimmen Sie auch zu, dass sie die entsprechende Funktion und Handhabung wie vorgegeben anwenden (z.B. nicht ablegen, Akku aufladen, etc.). Ein Verlust des Health Token ist umgehend beim Empfang zu melden. Der Health Token darf ausschließlich von der zugeordneten Person verwendet werden. Eine Weitergabe ist nicht gestattet. Bei Verlust wähend ich den Helath Token in Verwendung habe oder mutwilliger Beschädigung des Health Token ist für den Ersatz eine Kostenbeteiligung von € 25.- zu leisten.

App für die Nutzung des Health Token

Der Hersteller des Health Token stellt auch eine App zur Verfügung, über die die Daten auf dem Token in den Server übertragen werden können. Die Nutzung dieser App ist eine freiwillige Alternative. Hierfür gelten die in der App für die Nutzung zu Grunde gelegten Nutzungsbedingungen. KNAPP stellt weder die App zur Verfügung, noch ist KNAPP Verantwortlicher im Datenschutzrechtlichen Sinn.

Über die App können auch Push-Benachrichtigungen erhalten werden. Bitte nehmen Sie zur Kenntnis, dass ausschließlich die in der offiziellen Benachrichtigung durch KNAPP AG genannten relevanten Maßnahmen zu befolgen sind.

Was sind meine Rechte als Betroffener?

Bezüglich meiner personenbezogenen Daten habe ich das Recht auf Auskunft, Berichtigung, Löschung, und Einschränkung der Datenverarbeitung, Widerruf der Einverständniserklärung sowie das Recht der Datenübertragbarkeit.

Ein Widerruf der Einverständniserklärung ist jederzeit mittels Mail an datenschutz@knapp.com möglich, wobei die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung meiner personenbezogenen Daten unberührt bleibt.

Sie haben außerdem das Recht, sich über die Verarbeitung personenbezogener Daten durch uns bei einer Aufsichtsbehörde für den Datenschutz zu beschweren. Zuständig ist in Österreich die Datenschutzbehörde. Die Anschrift lautet: Österreichische Datenschutzbehörde, Barichgasse 40-42, 1030 Wien, Telefon: +43 1 52 152-0, E-Mail: dsb@dsb.gv.at

Mehr Informationen

zum Datenschutz finde ich unter https://www.knapp.com/home/datenschutzerklaerung/.

Für Fragen steht mir das KNAPP-Datenschutz-Team unter datenschutz@knapp.com zur Verfügung.