FAQ – Datenschutz beim Türkommunikationssystem Hager intercom

Was ist eine Türsprechanlage mit Videokamera?

Eine Türsprechanlage mit Videokamera ist ein System, das es ermöglicht, Besucher per Kamera zu sehen und per Mikrofon mit ihnen zu sprechen, bevor der Bewohner die Haustür öffnet. Optional kann die Türsprechanlage mit einer Gesichtserkennungsfunktion ausgestattet werden.

Welche personenbezogenen Daten werden verarbeitet?

Es werden Standbild und Liveaufnahmen der klingelnden Personen sowie die Stimme des Besuchers und Bewohners verarbeitet.
Das Standbild wird im Moment des Klingelns mit einem Zeitstempel und dem definierten Standort der Türsprechanlage versehen.

Was sind die Zwecke und Rechtsgrundlagen der Verarbeitung i. S. d. DSGVO?

Der datenschutzrechtlich Verantwortliche (nicht der Hersteller) muss Zweck und Rechtsgrundlage selber festlegen, die folgenden Ausführungen sind beispielhaft anhand des für die Klingelkamera gedachten Einsatzszenarios gewählt.
Grundsätzlich ist der Zweck der Verarbeitung die Identifikation des Besuchers ähnlich wie durch einen Türspion sowie die Kommunikation zwischen Besucher und Bewohner. Die Bilder werden mit Zeitstempel und Standort gespeichert, um zu einem späteren Zeitpunkt nachvollziehen zu können, wer wann die Ruftaste betätigt hat bzw. den Bewohner per App zu informieren, wer die Ruftaste betätigt (hat).
Die Verarbeitung stützt sich primär auf die Einwilligung der betroffenen Person (Art. 6 Abs. 1 a DSGVO). Durch das Betätigen der Klingel geben Besucher ausdrücklich ihre Zustimmung zur Bildübertragung, wenn sie im Einzugsgebiet der Kamera stehen.
Der Einwilligende muss ausreichend informiert werden. Hierzu muss ein deutliches Hinweisschild an der Haustür angebracht werden, das gem. Art. 13 DSGVO erklärt, wer der Verantwortliche ist, welche Daten erhoben werden, sobald die Ruftaste betätigt wird, und zu welchem Zweck, auf welcher Rechtsgrundlage und wie lange sie gespeichert werden.

Wie lassen sich die Privatsphäre von Besuchern und Nachbarn und öffentliche Bereiche schützen?

Sensible Bildbereiche (z. B. Bürgersteig, Nachbargrundstücke) können bei der Bilderfassung ausgeblendet werden. Im Konfigurationstool oder lokal am Gerät Hager intercom motion können pro Außenstation bis zu vier Maskierungen definiert werden. Während der Einstellung im Konfigurationstool wird ein Live-Bild (kein Videostream) angezeigt.
Vor der Haustür sollte der Bereich optisch markiert werden, der von der Kamera erfasst wird.

Welche Geräte werden bei einem Rufvorgang aktiviert?
Es werden mindestens die Außenstation und die Wechselsprechanlage des gerufenen Mieters aktiviert. Hat ein Bewohner mehrere Innenstationen (z. B. in einer großen Wohnung), werden alle Innenstationen gleichzeitig aktiviert.
Nutzt der Bewohner zusätzlich die App, wird außerdem die App aktiviert.

Wann und wohin wird Bild- und Tonmaterial übertragen?
Die Übertragung des Bild- und Tonmaterials erfolgt ausschließlich anlassbezogen, nämlich bei Betätigung der Ruftaste am Hauseingang.
Die Übertragung erfolgt von der Außenstation zu der Innenstation bzw. den Innenstationen des Bewohners und gegebenenfalls auf die App des Bewohners.
Es wird ein Live-Videostream übertragen, bis der Ruf beendet wird.

Wird das Bild- und Tonmaterial gespeichert?
Es wird ein Einzelbild des klingelnden Besuchers auf der Innenstation des Bewohners gespeichert. Bilder können jederzeit manuell gelöscht werden und werden nach 100 Einträgen im lokalen Speicher automatisch überschrieben.
Bei Nutzung der App wird das Bild in der sicheren Cloud gespeichert und kann manuell gelöscht werden. Spätestens nach 90 Tagen wird es automatisch gelöscht.
Es wird kein Tonmaterial gespeichert.

Wie lange dauert die Übertragung/das Gespräch?
Zeigt der Angerufene keine Reaktion, endet die Bildübertragung automatisch nach 90 Sekunden. Wird parallel die Ruftaste bei einem anderen Bewohner betätigt, wird der aktuelle Ruf sofort abgebrochen. Beendet der Angerufene die Verbindung nicht aktiv, wird die bestehende Verbindung nach 120 Sekunden automatisch beendet.

Kann ein Bewohner Kamera oder Mikrofon ohne Klingelruf aktivieren?
Nein.
Das Mikrofon und/oder die Kamera können nicht außerhalb eines aktiven Rufes aktiviert werden.

Verlassen Metadaten und Kommunikationsdaten das Hausnetzwerk?
Im Standardbetrieb bleiben Meta- und Kommunikationsdaten vollständig innerhalb des geschlossenen Haussystems. Bei Nutzung der optionalen App werden Metadaten (Zeitstempel, Geräte-ID, App-Nutzerkonto) in die Cloud übertragen. Der Bewohner entscheidet selbst, ob er die App nutzt, und verbindet die Innenstation dafür mit seinem privaten Netzwerk.

Wer hat Zugriff auf die Daten?
Grundsätzlich hat der Geräte- bzw. Installationsinhaber Zugriff auf die Daten im Hausnetzwerk. Der Bewohner allein hat Zugriff auf die Daten, die in der Innenstation gespeichert werden.
Dienstleister, die Cloud-Speicherung oder Analyse anbieten, haben ggf. Zugriff gemäß der vertraglichen Vereinbarung und nur nach schriftlichem Auftragsverarbeitungsvertrag (AVV).
Drittparteien (z. B. Strafverfolgungsbehörden) dürfen nur mit gültiger gerichtlicher Anordnung oder gesetzlicher Grundlage Zugriff erhalten.

FAQ – optionale Gesichtserkennung (nur verfügbar bei RTQ541X)

Was ist Gesichtserkennung und wie funktioniert sie?

Die Gesichtserkennung ist eine Technologie, die anhand von Gesichtsmerkmalen eine Person identifiziert. Hierbei wird das von der Kamera erfasste Gesichtsprofil mit den gespeicherten biometrischen Daten verglichen. Bei Übereinstimmung wird der Zutritt gewährt.

Welche personenbezogenen Daten werden verarbeitet?

Die Außenstation speichert ausschließlich biometrische Merkmale des Gesichts. Es werden keine Fotos oder Videos gespeichert. Diese Daten dienen nur dem Abgleich und können nicht zurückgerechnet werden, um ein Bild zu erzeugen.

Was sind die Zwecke und Rechtsgrundlagen der Verarbeitung i. S. d. DSGVO?

Der datenschutzrechtlich Verantwortliche (nicht der Hersteller) muss Zweck und Rechtsgrundlage selber festlegen, die folgenden Ausführungen sind beispielhaft anhand des für die Gesichtserkennung gedachten Einsatzszenarios gewählt.
Der Zweck der Verarbeitung ist es, Personen, deren biometrische Daten im System erfasst sind, vereinfacht Zutritt zum Gebäude zu ermöglichen.
Die Erfassung der Gesichtsdaten ist nur mit der ausdrücklichen Einwilligung der Person möglich, deren Gesicht erfasst wird. Hierzu muss der jeweiligen Person eine Datenschutzinformation vorgelegt werden, die den Anforderungen des Art. 13 DSGVO genügt (u. a. Information, wer der Verantwortliche ist, welche Daten erhoben werden, zu welchem Zweck, auf welcher Rechtsgrundlage und wie lange sie gespeichert werden).
Das Einlernen des Gesichts kann ausschließlich lokal an der Außenstation erfolgen. Dazu muss die jeweilige Person aktiv auf „Zustimmen“ klicken, damit die Erfassung gestartet werden kann. Ohne diese Zustimmung findet keine Datenerfassung statt.

Ist die Gesichtserkennung automatisch aktiviert?

Nein.
Gemäß den Vorgaben der DSGVO (*Privacy by Default*) ist die Gesichtserkennung in den Werkseinstellungen deaktiviert. Die Funktion muss manuell vom Betreiber aktiviert werden. Auch die Standardeinstellungen für den Scan-Modus und die Scan-Genauigkeit sind bewusst datenschutzfreundlich voreingestellt. Diese Werte können später individuell angepasst werden (*Privacy by Design*).

Werden die Daten an Dritte weitergegeben?

Nein.
Die gespeicherten Daten verlassen die Außenstation nicht und werden nicht in einer Cloud oder auf externen Servern gespeichert. Eine Weitergabe an Dritte erfolgt nicht.

Wer hat Zugriff auf meine Daten?

Nur autorisierte Personen vor Ort, z. B. der Betreiber oder Hausverwalter, können erkennen, ob für eine Person biometrische Daten gespeichert sind. Es gibt keine Möglichkeit, die biometrischen Daten auszulesen oder zu exportieren. Der Hersteller hat keinen Zugriff auf Ihre Daten.

Können die Daten jederzeit gelöscht werden?

Ja.
Die Daten können jederzeit über den Betreiber direkt am Gerät gelöscht werden.

Wie lange werden die Daten gespeichert?

Die biometrischen Daten bleiben so lange gespeichert, bis der Betreiber sie löscht. Es gibt keine automatische Löschung nach einer bestimmten Zeit. Die erfasste Person hat jederzeit das Recht auf Löschung.

Was passiert, wenn das Gerät ausgetauscht oder zurückgesetzt wird?

Wenn die Außenstation ersetzt oder auf Werkseinstellungen zurückgesetzt wird, werden alle lokal gespeicherten Daten automatisch gelöscht. Für die Gesichtserkennung muss dann ein neuer Einlernprozess durchgeführt werden.

Kann jemand die Daten missbrauchen, um unbefugt Zugang zu erhalten?

Nein.
Es wird kein Foto gespeichert, sondern nur berechnete Gesichtsmerkmale. Diese Daten können nicht rekonstruiert oder für andere Systeme verwendet werden.