Datenschutzerklärung

gemäß Artikel 13 EU-Datenschutz-Grundverordnung (DSGVO)

Die nachfolgende Datenschutzerklärung gilt für die Nutzung des Cloud-Service ekey bionyx (in weiterer Folge „**bionyx**"), der dazugehörigen App „ekey bionyx App" (in weiterer Folge die „**App**") und der zugehörigen Geräte (in weiterer Folge „**Geräte**") sowie bei Supportanfragen im Zusammenhang mit der Nutzung von bionyx (in weiterer Folge „**Support**").

Verantwortlicher gemäß Artikel 4 Abs. 7 EU-Datenschutz-Grundverordnung (in weiterer Folge „**DSGVO**") ist ekey biometric systems GmbH, Lunzerstraße 89, A-4030 Linz.

Der Schutz Ihrer personenbezogenen Daten ist der ekey biometric systems GmbH (in weiterer Folge „**ekey**") ein besonderes Anliegen. Wir verarbeiten Ihre Daten ausschließlich auf Grundlage der gesetzlichen Bestimmungen gemäß der EU-Datenschutz-Grundverordnung (in weiterer Folge „**DSGVO**") und des Bundesgesetzes zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (in weiterer Folge „**DSG**"). In dieser Datenschutzinformation informieren wir Sie über die wichtigsten Aspekte der Datenverarbeitung im Rahmen unseres Unternehmens sowie bei der Verwendung unserer Produkte.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

1. Rechtsgrundlage und Zwecke der Verarbeitung

Die Verarbeitung Ihrer personenbezogenen Daten durch ekey kann auf folgende Rechtsgrundlagen gestützt werden:

- Personenbezogene Daten werden auf Grundlage Ihrer Einwilligung gemäß Artikel 6 Abs 1 lit a DSGVO verarbeitet. Daneben kann die Verarbeitung personenbezogener Daten im Rahmen der Vertragsanbahnung bzw. zur Vertragserfüllung gemäß Artikel 6 Abs 1 lit b DSGVO erforderlich sein. Außerdem kann es im Einzelfall zur Verarbeitung personenbezogener Daten zur Wahrung unserer berechtigten Interessen an der Sicherstellung der Sicherheit unserer informationstechnischen Systeme und der Aufdeckung und Verhinderung krimineller kommen (Artikel 6 Abs 1 lit f DSGVO)
- Biometrische Daten (Fingerabdruck) als besondere Kategorie personenbezogener Daten werden ausschließlich auf Grund Ihrer ausdrücklichen Einwilligung gemäß Artikel 9 Abs 2 lit a DSGVO verarbeitet.

Sämtliche Einwilligungen in eine Datenverarbeitung können unabhängig voneinander und jederzeit widerrufen werden. Ein Widerruf hat zur Folge, dass wir Ihre Daten ab diesem Zeitpunkt zu oben genannten Zwecken nicht mehr verarbeiten und somit die entsprechenden Rechte, Vorteile etc. nicht mehr in Anspruch genommen werden können. Für einen Widerruf wenden Sie sich bitte an folgende E-Mail-Adresse: datenschutz@ekey.net. Durch einen Widerruf wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

2. Kategorien von Datenverarbeitungen

2.1. Datenverarbeitung bei Nutzung des ekey bionyx Systems

Das System bietet mit Hilfe von biometrischen Daten durch den Fingerabdruck (sogenannte Templates) Öffnungs- und Schließfunktionen an. Im Folgenden informieren wir über die Erhebung und Verarbeitung personenbezogener Daten bei Nutzung unseres Systems.

Im Rahmen der produktspezifischen und -vorgesehenen Anwendung werden personenbezogene Daten benötigt und verarbeitet. Um eine komfortable und nachvollziehbare Nutzung des Systems zu gewährleisten, ist die Verarbeitung der folgenden personenbezogenen Daten notwendig:

Profildaten der Endnutzer:

- ID
- Biometrische Daten (Fingerabdruck)

Nutzungsdaten:

- Zutrittsprotokolle & Logdaten (Person, Ort, Zeit, Funktion) – verschlüsselt (Zweck: Nachvollziehbarkeit und Informationsweiterleitung an andere Nutzer über die dazugehörige App)

Die Speicherung der Daten erfolgt im Speicher des Systems direkt, sowie in einem durch einen Auftragsverarbeiter bereitgestellten Cloud-Service (ekey bionyx Cloud). Alle Daten im Cloud-Service sind verschlüsselt und können von ekey nur mit dem kundenspezifischen Systemschlüssel, welcher rein dem Nutzer des Systems bekannt ist, eingesehen werden.

2.2. Datenverarbeitung bei Nutzung der ekey bionyx App

Die nachfolgenden Informationen und Erklärungen sind zusätzlich für das Produkt „ekey bionyx App" gültig.

Wir stellen Ihnen eine mobile App zur Verfügung, die Sie auf Ihr mobiles Endgerät herunterladen können. Im Folgenden informieren wir über die Erhebung und Verarbeitung personenbezogener Daten bei Nutzung unserer mobilen App.

Bei Herunterladen der mobilen App werden die erforderlichen Informationen an den App Store bzw. Google Play übertragen, also insbesondere Nutzername, E-Mail-Adresse und Kundennummer Ihres Accounts, Zeitpunkt des Downloads, Zahlungsinformationen und die individuelle Gerätekennziffer. Auf diese Datenerhebung haben wir keinen Einfluss und sind nicht dafür verantwortlich. Wir verarbeiten die Daten nur, soweit es für das Herunterladen der mobilen App auf Ihr mobiles Endgerät notwendig ist.

Bei Nutzung der mobilen App verarbeiten wir die nachfolgend beschriebenen personenbezogenen Daten, um die komfortable Nutzung der Funktionen zu ermöglichen. Wenn Sie unsere mobile App nutzen möchten, erheben wir die folgenden Daten, welche für uns technisch erforderlich sind, um Ihnen die Funktionen unserer mobilen App anzubieten und die Stabilität und Sicherheit zu gewährleisten:

Gerätedaten der Endnutzer

- Gerätenummer/ID
- Gerätename
- Browser Agent
- Browsereinstellungen und - Betriebssystem

Profildaten der Endnutzer

- Name
- E-Mail-Adresse
- Passwort (verschlüsselt)
- Profilbild (optionale Profilerweiterung)
- Registrierungsdaten der Endnutzer
- Username
- Registrierungsdatum

Hostingdaten

- IP-Adresse
- Browsertyp und -einstellungen
- Standort auf IP-Basis
- Zeitpunkt des Downloads der App
- Zeitpunkt und Ausmaß von Serveranfragen

2.3. Optionale Anbindung Ihres Alexa-Kontos von Amazon

Sofern Sie ein „Alexa"-Konto von Amazon.com Inc. (im Folgenden: „Amazon") haben, können Sie dieses Konto mit Ihrem ekey-bionyx-Konto verbinden. Auf diese Weise haben Sie insbesondere die Möglichkeit, mittels Sprachbefehl eine Türöffnung zu veranlassen oder über eine Türöffnung durch Sprachausgabe eines Alexa Gerätes informiert zu werden.

Zur Anbindung des Alexa-Kontos ist es erforderlich, dass Sie in der Alexa-App die Funktion „ekey bionyx" aktivieren und anschließend die Informationen Ihres ekey-bionyx-Kontos (E-Mail-Adresse und Passwort) in unserer Anmeldestrecke eingeben. Wenn Sie dabei auf „Anmelden" klicken, erteilen Sie uns Ihre Einwilligung zur Datenübermittlung an Amazon. Der genaue Ablauf zur Anbindung des Alexa-Kontos ist unter folgendem Link erläutert: https://www.ekey.net/faq-bionyx/wie-fuehre-ich-die-anbindung-meines-ekey-systems-mit-alexa-durch/.

Bei der Anbindung des Alexa-Kontos kommt es – neben den vorstehend angeführten Datenverarbeitungen – zusätzlich zur Datenübermittlung an Amazon, die folgende Kategorien von personenbezogenen Daten umfasst: Gerätedaten der Endnutzer (Gerätenummer/ID) und Profildaten der Endnutzer (User-ID, Name und E-Mail-Adresse). Außerdem ist für Amazon stets der Onlinestatus Ihres bionyx-Geräts erkennbar.

Amazon tritt in diesem Zusammenhang teilweise als unser Auftragsverarbeiter und teilweise als selbständiger Verantwortlicher auf:

- Einerseits betreiben wir einen Server auf der AWS Cloud, was für die automatisierte Datenübermittlung an das Alexa-System erforderlich ist. Diesbezüglich tritt Amazon als unser Cloud-Dienstleister und Auftragsverarbeiter auf (zur Datenverarbeitung durch Auftragsverarbeiter siehe auch Punkt 5.).

- Andererseits ist Amazon selbstständiger Verantwortlicher für die Datenverarbeitungen im Rahmen Ihres Alexa-Kontos (wir haben auf die Datenverarbeitungen in Ihrem Alexa-Konto keinen Einfluss und übernehmen dafür auch keine Verantwortung). Die Datenschutz-Informationen von Amazon Alexa sind unter folgendem Link abrufbar: https://www.amazon.de/Datenschutzportal-f%C3%BCr-Alexa/b?ie=UTF8&node=17084415031.

Die Datenübermittlung an Amazon kann dazu führen, dass Ihre Daten in die USA übermittelt werden. Amazon ist nach dem EU-U.S. Data Privacy Framework zertifiziert. Deshalb kann die Datenübermittlung auf einen Angemessenheitsbeschluss der Europäischen Kommission nach Artikel 45 DSGVO gestützt werden. Folglich entspricht diese Datenübermittlung an Amazon den Anforderungen der DSGVO für Datenübermittlungen in Drittstaaten.

Sie können die Anbindung des Alexa-Kontos jederzeit deaktivieren. Zu Ihrer Sicherheit müssen Sie die Alexa-Anbindung nach 3 Monaten in der ekey bionyx App erneut durchführen. Sie erhalten einige Tage davor einen Hinweis in der App und auch eine Push-Nachricht, um früh genug darüber informiert zu sein.

2.4. Datenverarbeitung im Rahmen des Supports

Betreiber von Zutrittskontrollanlagen (in weiterer Folge „**Betreiber**") können sich bei technischen Schwierigkeiten über die App an unsere Supportabteilung wenden. Bei der Bearbeitung von Supportanfragen verarbeiten wir (im Folgenden näher konkretisierte) personenbezogene Daten, soweit dies zur Kontaktaufnahme, Fehlersuche und Problembehebung erforderlich ist. Für die Datenverarbeitung im Rahmen des Supports gilt Folgendes:

- Der Betreiber muss den Datenzugriff durch unsere Supportmitarbeiter vorab über die App freigeben, andernfalls haben die Supportmitarbeiter keinen Zugriff auf diese Daten. Eine solche Freigabe erfolgt lediglich aus Sicherheitsgründen und stellt insbesondere keine datenschutzrechtliche Einwilligung nach Artikel 6 Abs 1 lit a DSGVO dar.
- Daten, die im Rahmen von Supportanfragen anfallen, sind ausschließlich für unsere Support-Mitarbeiter zugänglich und werden über eine verschlüsselte Verbindung (HTTPS) an einen ekey-Server in Linz/Österreich übertragen.
- Von ekey abgerufene Daten im Rahmen dieses Datenverarbeitungsprozess werden ausschließlich für Analysezwecke und zur Problembehebung genutzt. Sie werden weder intern weiterführend verwendet noch an Dritte weitergegeben.
- Nach Abschluss des Supportprozesses werden sämtliche in diesem Zusammenhang verarbeitete Daten gelöscht. Gleichzeitig wird auch der Datenzugriff durch unsere Supportmitarbeiter gesperrt.
- Je nach Art der Störung kann es sein, dass wir bei der Bearbeitung von Supportanfragen auch Daten benötigen, die beim Normalbetrieb der Anlage nicht anfallen und die daher gesondert aufgezeichnet werden müssen.

Je nachdem, ob eine solche Datenaufzeichnung erforderlich ist, können zwei Supportfälle unterschieden werden.

2.4.1. Supportfall A

Bei der Bearbeitung von Supportfall "A" können folgende Daten verarbeitet werden:

- Kontaktdaten des Betreibers (Name, E-Mail-Adresse, sowie optional Adresse und/oder Telefonnummer)
- Biometrische Daten (Fingerbilder der Nutzer)
- Applogdaten (Telemetriedaten zur Nutzung der App durch den Nutzer)

Dabei wird – abgesehen von der Kontaktdaten des Betreibers – stets nur eine der Datenkategorien verarbeitet.

Die hierfür erforderlichen Daten (insbesondere die biometrischen Daten und die Applogdaten) werden im Normalbetrieb der Anlage nicht verarbeitet. Wir ersuchen den Betreiber die Aufzeichnung und Analyse dieser Daten daher in einem zweistufigen Prozess vorab freizugeben. Nach entsprechender Freigabe durch den Betreiber, starten wir mit der

Aufzeichnung der in der Anfrage unserer Supportabteilung genannten Daten (Aufzeichnung der Fingerbilder und/oder Applogdaten). Diese Datenaufzeichnung erfolgt in der Regel über einen Zeitraum von bis zu zwei Wochen, wobei wir diese Daten zunächst nur verschlüsselt erhalten.

Um die Daten auswerten und analysieren zu können, müssen sie entschlüsselt werden. Nach Ablauf dieses Aufzeichnungszeitraums ersuchen wir daher den Betreiber, die Entschlüsselung dieser Daten freizugeben. Nach erfolgter Freigabe werden wir diese Daten zur Analyse und Problembehebung verwenden.

2.4.2. Supportfall B

Im Rahmen von Supportfall "B" können folgende Daten verarbeitet werden:

- Kontaktdaten des Betreibers (Name, E-Mail-Adresse, sowie optional Adresse und/oder Telefonnummer)
- Personalisierte Biometrielogdaten (Daten zur Feststellung der Funktion und Qualität des biometrischen Identifikationsprozesses)
- Zutrittsprotokolldaten (Telemetriedaten, die zeigen, wann und wie das Zutrittskontrollsystem genutzt wird)
- Referenz-Templates (Datensätze, die die Identifikationsmerkmale von Fingerabdrücken enthalten)
- Änderungen im bionyx-System (Systemeinstellungen, die für Analysezwecke verändert bzw geprüft werden und fehlerhafte Einstellungen der Zutrittskontrollanlage, die durch unseren Support korrigiert werden)

Dabei wird – abgesehen von der Kontaktdaten des Betreibers – stets nur eine der Datenkategorien verarbeitet.

Diese Daten werden bereits im Normalbetrieb eines Zutrittskontrollsystems verarbeitet. Ohne Freigabe können wir allerdings nicht darauf zugreifen. Wir ersuchen den Betreiber daher vorab, die Verarbeitung der in der Anfrage genannten Daten durch unser Support-Team freizugeben. Nach erfolgter Freigabe werden wir diese Daten von den Geräten, der App und dem Betreiberkonto abrufen und diese zur Analyse und Problembehebung verwenden.

3. Verwendung von Cookies

Cookies sind kleine Textbausteine, die von einer Website auf dem Gerät des Nutzers abgelegt werden. Viele Cookies enthalten eine sogenannte Cookie- ID. Eine Cookie-ID ist eine eindeutige Kennung des Cookies. Sie besteht aus einer Zeichenfolge, durch welche Websites und Server dem konkreten Internetbrowser zugeordnet werden können, in dem das Cookie gespeichert wurde. Dies ermöglicht es den besuchten Websites und Servern, den individuellen Browser der betroffenen Person von anderen Internetbrowsern, die andere Cookies enthalten, zu unterscheiden. Ein bestimmter Internetbrowser kann über die eindeutige Cookie-ID wiedererkannt und identifiziert werden.

Die mobile App nutzt folgende Arten von Cookies, deren Umfang und Funktionsweise im Folgenden erläutert werden:

- Technisch notwendige Cookies: Diese sind zwingend erforderlich, grundlegende Funktionen zu nutzen und die Sicherheit der App und der Daten zu gewährleisten; sie sammeln weder Informationen über Sie zu Marketingzwecken noch speichern sie diese.

4. Datenverarbeitung außerhalb der EU/des EWR

Eine Datenverarbeitung erfolgt in einem Rechenzentrum mit einem Standort in Europa. Eine Datenverarbeitung außerhalb der EU/des EWR findet nicht satt.

Sofern eine Anbindung des Alexa-Kontos von Amazon erfolgt (siehe Punkt 2.3) kann die Datenübermittlung an Amazon dazu führen, dass Ihre Daten in die USA übermittelt werden. Amazon ist nach dem EU-U.S. Data Privacy Framework zertifiziert, weshalb die Datenübermittlung an Amazon den Anforderungen nach Artikel 44 ff DSGVO für Datenübermittlungen in Drittstaaten entspricht.

5. Übermittlung der Daten an Auftragsverarbeiter

Bei der Verarbeitung personenbezogener Daten bedient sich ekey Hilfspersonen, insbesondere im Bereich IT. Diese verarbeiten die Daten als sogenannte Auftragsverarbeiter, d.h. auf Grundlage eines schriftlichen Vertrags gemäß Artikel 28 DSGVO, in dem die Einzelheiten der Datenverarbeitung im Auftrag von ekey geregelt sind und in dem sich der Auftragsverarbeiter zum sorgfältigen Umgang mit den Daten verpflichtet. Eine solche Auftragsverarbeitung liegt beispielsweise vor, wenn ekey Daten in einem externen Rechenzentrum speichert. ekey setzt solche Auftragsverarbeiter beispielsweise in den folgenden Bereichen ein:

- IT Services
- Telekommunikation
- Cloud-Dienstleister

Die Auftragsverarbeiter werden von ekey unter besonderer Berücksichtigung der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt und auf deren Einhaltung überprüft. Unsere Auftragsverarbeiter verarbeiten die Daten grundsätzlich nur in der Europäischen Union (zur Datenübermittlung an Amazon siehe Punkt 2.3).

6. Datenweitergabe an Dritte

Wir geben – abgesehen von unseren Auftragsverarbeitern – keine personenbezogenen Daten an Dritte weiter, es sei denn, dies ist für unsere legitimen beruflichen und geschäftlichen Bedürfnisse erforderlich, und/oder wenn dies gesetzlich oder durch berufliche Standards vorgeschrieben oder erlaubt ist.

7. Höchstdauer der zulässigen Datenaufbewahrung

Die Daten unserer Kunden werden nur so lange gespeichert, wie diese zur Vertragsverfüllung erforderlich sind. Danach werden die Daten gelöscht. Es können darüber hinaus gesetzliche Aufbewahrungspflichten bestehen z. B. nach dem Unternehmensgesetzbuch (UGB) und der Bundesabgabenordnung (BAO). Nach Ablauf der gesetzlichen Aufbewahrungsfristen werden wir Ihre personenbezogenen Daten unverzüglich aus unseren Datenbanken (sowohl digital als auch physisch) löschen.

Personenbezogene Daten unserer Kunden werden bei Löschung des Kontos oder bei einer Inaktivität von 5 Jahren (keine Nutzeraktivitäten in der App) inklusive Logdaten gelöscht.

Während die App aktiv ist, werden die Profildaten, exklusive des Passworts, des Benutzers im RAM-Cache des mobilen Endgeräts gespeichert. Aufgrund der Speichereigenschaften können diese Daten auch nach dem Beenden der App im Speicher für eine unbestimmte Dauer verweilen.

Daten, die im Zusammenhang mit einer Supportanfrage erhoben und verarbeitet werden, werden nur für die Dauer der Problembehebung gespeichert. Nach Behebung des technischen Problems werden wir die Daten umgehend löschen.

8. Sicherheit der Datenverarbeitung

Zur Gewährleistung der Datensicherheit wurden bei ekey die erforderlichen technischen und organisatorischen Maßnahmen unter Berücksichtigung des Stands der Technik implementiert. Diese Vorkehrungen betreffen insbesondere den Schutz vor unerlaubtem, rechtswidrigem oder auch zufälligem Zugriff, Verarbeitung, Verlust, Verwendung und Manipulation.

Außerdem besteht ein Verfahren zur regelmäßigen Überprüfung und Bewertung der Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen.

Bitte beachten Sie, dass wir keine wie immer geartete Haftung für die Offenlegung von Informationen aufgrund nicht von uns verursachter Fehler bei der Datenübertragung und/oder unautorisiertem Zugriff durch Dritte übernehmen (z. B. Hackerangriff).

9. Automatisierte Entscheidungsfindung

Als verantwortungsbewusstes Unternehmen weisen wir ausdrücklich darauf hin, dass keine automatisierte Entscheidungsfindung auf Basis der erhobenen personenbezogenen Daten stattfindet.

10. Ihre Rechte

Sie haben gegenüber uns folgende Rechte hinsichtlich der Sie betreffenden personenbezogenen Daten:

- Recht auf Auskunft,
- Recht auf Berichtigung oder Löschung,
- Recht auf Einschränkung der Verarbeitung,
- Recht auf Widerspruch gegen die Verarbeitung,
- Recht auf Datenübertragbarkeit.

Des Weiteren haben Sie auch das Recht, Beschwerde bei der zuständigen Aufsichtsbehörde (in Österreich die Datenschutzbehörde mit Sitz in Wien) zu erheben. Die Datenschutzbehörde ist unter folgender Adresse erreichbar:

Österreichische Datenschutzbehörde
Barichgasse 40-42, A-1030 Wien
Telefon: +43 1 52 152 - 0

Bei Fragen hinsichtlich der Verarbeitung Ihrer personenbezogenen Daten sowie Ihrer Rechte erreichen Sie uns unter: datenschutz@ekey.at

11. Aktualisierung der Datenschutzerklärung

Wir behalten uns das Recht vor, jederzeit Änderungen an dieser Datenschutzerklärung vorzunehmen. Die Datenschutzerklärung wird regelmäßig aktualisiert und alle Änderungen auf www.ekey.net automatisch veröffentlicht.