Data privacy statement

as per Article 13 EU General Data Protection Regulation (GDPR)

The following data privacy statement applies to the usage of the cloud service ekey bionyx (hereafter "**bionyx**") the app "ekey bionyx app" (hereafter "**app**") and associated devices (hereafter "**devices**"), as well as to support requests in connection with the usage of bionyx (hereafter "**support**").

Controller in accordance with Article 4(7) of the EU General Data Protection Regulation (hereinafter "**GDPR**") is ekey biometric systems GmbH, Lunzerstraße 89, A-4030 Linz.

ekey biometric systems GmbH (hereafter **"ekey"**) takes the protection of your personal data very seriously. We solely process your data on the basis of the legal provisions within the EU General Data Protection Regulation (hereafter **"GDPR"**) and the Austrian Law to Protect Natural Persons during the Processing of Personal Data (hereafter **"DSG"**). In this data protection statement, we would like to inform you of the key aspects of the data processing carried out at our company and during the usage of our products.

Personal data are all information that pertains to an identified or identifiable natural person. A natural person is considered identifiable if they can be identified directly or indirectly through association with a characteristic such as a name, identifier number, location data, online identifier or one or more special characteristics indicating the physical, physiological, genetic, mental, financial, cultural or social identity of this natural person.

1. Legal basis and purposes of processes

ekey can process your personal data on the following legal bases:

- Personal data is processed based on your consent in accordance with Article 6(1)(a) GDPR. In addition, the processing of personal data can be required as part of the contract initiation or to fulfill the contract in accordance with Article 6(1)(b) GDPR. In addition, personal data may be processed in individual cases to preserve our legitimate interests in ensuring the security of our information technology systems and the detection and prevention of criminal activity (Article 6(1)(f) GDPR).
- Biometric data (fingerprint) as a special category of personal data are processed on the exclusive basis of your express consent in accordance with Article 9(2)(a) GDPR. Every instance of consent to data processing can be revoked at any time, independently of one another. Revocation results in us no longer being able to process your data upon the moment of revocation, meaning that the respective rights, benefits, etc., can no longer be claimed. Please contact the following email address if you wish to revoke your consent: datenschutz@ekey.net. Revocation does not affect the legality of the processing conducted before revocation.

2. Categories of data processing

2.1. Data processing when using the ekey bionyx system

The system uses biometric data obtained from fingerprints (referred to as templates) to offer opening and closing functions. Below we inform you of the retrieval and processing of personal data during your use of our system.

Personal data are required and processed when using the specific product as intended. The processing of the following personal data is required in order to ensure comfortable, comprehensible use of the system:

Profile data of end users:

- ID
- Biometric data (fingerprint)

Usage data:

- Access logs and log data (person, place, time, function) – encrypted (purpose: comprehensibility and forwarding of information to other users via the respective app)

The data are stored directly in the system's memory storage, as well as in a cloud service (ekey bionyx cloud) provided by the processor. All data in the cloud service are encrypted and can only be viewed by ekey with the customer-specific system key that is only known to the user of the system.

2.2. Data processing when using the ekey bionyx app

The following information and declarations also apply to the product "ekey bionyx app".

We provide you with a mobile app that you can download onto your mobile device. Below we inform you of the retrieval and processing of personal data during your use of our mobile app.

When downloading the mobile app, the necessary information is sent to the App Store or Google Play, namely the username, email address and customer number of your account, time of the download, payment information and individual device identifier. We have no influence over this retrieval of data and are not responsible for it. We only process the data to the extent required for you to download the mobile app on your mobile device.

While you use the mobile app we process the following personal data in order to facilitate convenient use of the functions. If you would like to use our mobile app, we retrieve the following, technically required data so that we can offer you the functions of our mobile app and to ensure stability and security:

Device data of end users

- Device number/ID
- Device name
- Browser agent
- Browser settings and operating system

Profile data of end users

- Name
- Email address
- Password (encrypted)
- Profile picture (optional profile addition)
- Registration data of end users
- User name
- Date of registration

Hosting data

- IP address
- Browser type and settings
- IP location
- Time of app download
- Time and scope of server requests

2.3. Optional connection of your Amazon Alexa account

If you have an "Alexa" account from Amazon.com Inc. (hereinafter: "Amazon"), you can connect this account with your ekey bionyx account. In this way, you can initiate the opening of a door using a voice command or be informed about a door opening by the voice output of an Alexa device.

To connect the Alexa account, you must activate the "ekey bionyx" function in the Alexa app and then enter the information for your ekey bionyx account (email address and password) in our registration form. If you click on "Register," you give us your consent to transfer data to Amazon. The exact process for connecting the Alexa account is explained at the following link: https://www.ekey.net/en/ekeybionyx_faq/how-do-i-connect-my-ekey-system-to-alexa/.

When connecting the Alexa account, in addition to the data processing listed above, data is also transferred to Amazon, which includes the following categories of personal data: end user device data (device number/ID) and end user profile data (user ID, name, and email address). In addition, Amazon can always see the online status of your bionyx device.

In this context, Amazon acts partly as our processor and partly as an independent controller:

- On the one hand, we operate a server on the AWS Cloud, which is necessary for automated data transmission to the Alexa system. In this regard, Amazon acts as our cloud service provider and processor (see also point 5 for data processing by processors).

  On the other hand, Amazon is the independent controller for the data processing in the context of your Alexa account (we have no influence on the data processing in your Alexa account and assume no responsibility for it). Amazon Alexa's data protection information is available at the following link: https://www.amazon.co.uk/b/?node=17084411031.

Data transfer to Amazon may result in your data being transferred to the USA. Amazon is certified according to the EU-US Data Privacy Framework. Therefore, the data transfer can be based on an adequacy decision by the European Commission in accordance with Article 45 GDPR. Consequently, this data transfer to Amazon complies with the requirements of the GDPR for data transfers to third countries.

You can deactivate the Alexa account connection at any time. For your security, you must connect Alexa again after three (3) months in the ekey bionyx app. You will receive a notification in the app a few days beforehand, as well as a push notification to ensure that you are promptly informed.

2.4. Optional use of the Notification API

We hereby inform you that by optionally activating the notification function, you consent to the processing of your personal data in accordance with Article 6(1)(a) GDPR. According to Article 7(1) GDPR, we are obliged to provide proof of and store this consent.

Purpose of the processing

By entering a destination address (URL) and activating the notification function, the operator of the ekey device has the option of transmitting personal data to third-party devices and services (usually building automation components) of their choice. The purpose of the processing of the data by the third-party provider is not known to ekey.

The following data is made available to the third-party provider in accordance with the principle of "data minimisation" (Article 5(1)(c) GDPR):

a) System mapping export (required to configure the third-party system):
   - System name
   - All user IDs in the system as a hash
   - All user names in the system
   - All devices in the system (serial number and name)
b) Each notification contains the following data for the respective processing:
   - Hash of the user ID
   - Finger index
   - Input number
   - Serial numbers of the devices involved
   - Timestamp
   - Result of data processing on the devices

Right of the data subject

As a data subject, you are granted the following rights:

- Right of access (Article 15 GDPR)
- Right to rectification (Article 16 GDPR)
- Right to erasure (Article 17 GDPR)
- Right to restriction (Article 18 GDPR)
- Right to data portability (Article 20 GDPR)
- Right to object (Article 21 GDPR)

By entering a destination address (URL) and activating the notification function on your device, you give your express consent for the third-party provider linked to the destination address (URL) to process your personal data. The aforementioned rights must therefore be claimed from the respective provider. ekey does not store any personal data in connection with this function.

2.5. Data processing in the context of support

Operators of access control systems (hereinafter "**operator**") can contact our support department if technical difficulties arise when using the app. When handling support requests, we process personal data (specified in more detail below) to the extent that this is necessary for contacting us, troubleshooting, and problem solving. The following applies to data processing as part of support:

- The operator must authorize data access by our support staff in advance via the app; otherwise, the support staff will not have access to this data. Such authorization is only for security reasons and, in particular, does not constitute data protection consent under Article 6(1)(a) GDPR.
- Data arising from support requests is only accessible to our support employees and is transmitted via an encrypted connection (HTTPS) to an ekey server in Linz/Austria.
- Data retrieved by ekey as part of this data processing process is used exclusively for analysis purposes and to resolve issues. This data will neither be used internally nor passed on to third parties.
- Once the support process has been completed, all data processed in this context will be deleted. At the same time, data access by our support staff is also blocked.
- Depending on the type of malfunction, when processing support requests, we may also need data that is not generated during normal operation of the system and which therefore must be recorded separately.

Depending on whether such data recording is required, two support cases can be distinguished.

2.5.1. Support case A

When handling support case "A", the following data can be processed:

- Contact details of the operator (name, email address, and optionally address and/or telephone number)
- Biometric data (user fingerprints)
- Application log data (telemetry data about the user's app use)

Apart from the operator's contact details, only one of the data categories is ever processed.

The data required for this (in particular the biometric data and the application log data) are not processed during normal operation of the system. We therefore ask the operator to approve the recording and analysis of this data, in a two-stage process in advance. After appropriate approval from the operator, we start recording the data mentioned in the request from our support department (logging the fingerprints and/or application log data). This recording of data usually takes place over a period of up to two weeks, although we initially only receive this data in encrypted form.

In order to evaluate and analyze the data, it must be decrypted. After this recording period has expired, we therefore ask the operator to approve the decryption of this data. Once approved, we will use this data to analyze and troubleshoot problems.

2.5.2. Support case B

The following data can be processed as part of support case "B":

- Contact details of the operator (name, email address, and optionally address and/or telephone number)
- Personalized biometric log data (data to determine the function and quality of the biometric identification process)
- Access log data (telemetry data that shows when and how the access control system is used)
- Reference templates (data sets that contain the identification features of fingerprints)
- Changes in the bionyx system (system settings that are changed or checked for analysis purposes and incorrect settings of the access control system that are corrected by our support)

Apart from the operator's contact details, only one of the data categories is ever processed.

This data is already processed during normal operation of an access control system. However, we cannot access it without permission. We therefore ask the operator in advance to allow our support team to process the data mentioned in the request. Once approved, we will retrieve this data from the devices, the app, and the operator account and use it to analyze and troubleshoot problems.

3. Use of cookies

Cookies are small text components saved on the user's device by a website. Many cookies contain a cookie ID. A cookie ID is a unique identifier of the cookie. It consists of a sequence of characters that allow websites and servers to identify the browser in which the cookie has been saved. This allows the websites and servers that the user visits to differentiate the respective browser from other browsers that contain other cookies. A specific browser can be recognized and identified with the unique cookie ID.

The mobile app uses the following types of cookies, the scope and function of which are explained below:

- Technically required cookies: These are required to use basic functions and to ensure the security of the app and data; they neither collect nor store information on you for marketing purposes.

4. Data processing outside of the EU/EEA

Data are processed in a server center located in Europe. There is no processing of data outside of the EU/EEA.

If a connection is made to an Amazon Alexa account (see point 2.3), the data transfer to Amazon can result in your data being transferred to the USA. Amazon is certified according to the EU-US Data Privacy Framework, which is why data transfer to Amazon meets the requirements of Article 44 et seq. GDPR for data transfers to third countries.

5. Forwarding of data to processors

ekey relies on assistants, in particular in the field of IT, to process personal data. These parties process the data as processors, i.e., on the basis of a written contract as per Article 28 GDPR in which the details of the data processing ordered by ekey are regulated and in which the processor is obligated to process the data with care. For example, this type of processing occurs when ekey stores data in an external server center. ekey commissions processors in the following areas, among others:

- IT services
- Telecommunications
- Cloud service providers

The processors are carefully selected by ekey, with special consideration of the suitability of their technical and organizational measures, and inspected for their abidance to them. Our processors process the data basically only in the European Union (for data transfer to Amazon see point 2.3).

6. Forwarding of data to third parties

We do not disclose any personal data to third parties apart from our processors, unless this is required for our organizational and company purposes, and/or if this is allowed or required on the basis of law or occupational standards.

7. Maximum duration of permissible data storage

We only store our customers' data as long as is required to fulfill the contract. Then the data are deleted. Legal retention obligations are in place, e.g., according to the Austrian Commercial Code (UGB) and Austrian Federal Tax Code (BAO). After the legal retention periods have ended, we will immediately delete your personal data from our databases (both digitally and physically).

Our customers' personal data, including log data, are deleted when their respective account is deleted or if it is inactive for 5 years (no user activities in the app).

When the app is active, the user's profile data, excluding the password, are stored in the RAM cache of the mobile end device. Based on the storage characteristics, these data may remain in the device memory for an indefinite period after the app has closed.

Data collected and processed in connection with a support request is only stored for the time required to resolve the problem. Once the technical problem has been resolved, we will delete the data immediately.

8. Security of data processing

To ensure data security, ekey has taken the necessary technical and organizational measures, under consideration of the state of technology. These precautions chiefly serve to prevent unauthorized, illegal or accidental access, processing, loss, use and manipulation. A process is also in place to regularly assess and evaluate the effectiveness of the technical and organizational measures.

Please note that we do not accept any liability whatsoever for the disclosure of information on the basis of errors during the data processing not committed by us, and/or unauthorized access by third parties (e.g., hacker attacks).

9. Automated decision-making

As a responsible company, we hereby inform you that there is no automated decision-making on the basis of your personal data that we obtain.

10. Your rights

You have the following rights concerning your personal data:

- Right to disclosure,
- Right to correction or deletion,
- Right to limitation of processing,
- Right to object to processing,
- Right to data portability.

You also have the right to file a complaint with the responsible supervisory authority (in Austria this is the data protection authority in Vienna). The data protection authority can be reached at the following address:

Österreichische Datenschutzbehörde
Barichgasse 40-42, A-1030 Vienna, Austria
Telephone: +43 1 52 152 - 0

If you have any questions concerning the processing of your personal data as well as your rights, please contact us at: datenschutz@ekey.at.

11. Updates to the data privacy statement

We reserve the right to update this data privacy statement at any time. The data privacy statement is regularly updated, and all changes are automatically published on www.ekey.net.