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"**) as well as the app "ekey bionyx app" (hereafter **"app"**) and associated devices (hereafter **"devices"**).

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.

Legal basis and purposes of processes

The processing of your personal data by ekey for contract initiation or fulfillment is justified by Article 6 paragraph 1 letter b GDPR, and is necessary to fulfill the contract. We also process your personal data on the basis of our justified interest in ensuring the security of our IT systems and, if applicable, to uncover and prevent criminal threats and actions (Article 6 paragraph 1 letter f GDPR). We solely process your biometric data (fingerprints) on the basis of your explicit consent as per Article 9 paragraph 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 e-mail address if you wish to revoke your consent: datenschutz@ekey.net.

Revocation does not affect the legality of the processing conducted before revocation.

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.

Processing of personal data while using the ekey bionyx 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 order 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.

In the event of a support case, the necessary data can only be processed together with the user, as the user must provide their explicit consent and the required data (such as log data).

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.

Processing of personal data while using our mobile app

When downloading the mobile app, the necessary information is sent to the App Store or Google Play, namely the username, e-mail 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
- Browser agent
- Browser settings and operating system

Profile data of end users

- Name
- E-mail address
- Password (encrypted)
- Profile picture (optional profile addition)
- Registration data of end users
- Username
- Date of registration

Hosting data

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

Diagnostics data

You can send data from the **app** to ekey support for analysis after granting your explicit consent as per Article 6 paragraph 1 letter a GDPR. In this case, diagnostic data relating to your ekey system are sent to ekey biometric systems GmbH along with contact details such as your name and email address and, optionally, your address and/or telephone number so that ekey can contact you. The user must actively perform this transfer. In the event that support should be required, contact and analysis data can only be accessed by our support team; this information is then only saved until the support case is closed. Diagnostic data are transferred to an ekey server in Linz, Austria via an encrypted connection (HTTPS). The data sent are used solely to make contact with the user and for analysis and troubleshooting; they are not shared with third parties.

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 your for marketing purposes.

Data processing outside of the EU/EEA

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

Forwarding of data to contracted data processors

ekey relies on assistants, in particular in the field of IT, to process personal data. These parties process the data as contracted 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 contracted 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 contracted processors in the following areas, among others:

- IT services
- Telecommunications
- Cloud service providers

The contracted 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. ekey only processes the data in Austria and within the European Union.

Forwarding of data to third parties

We do not disclose any personal data to third parties, 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.

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.

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).

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.

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

The data processor as per Article 4 paragraph 7 EU General Data Protection Regulation (GDPR) is

ekey biometric systems GmbH
Lunzerstraße 89
A-4030 Linz, Austria

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

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.