

Philip Heymans Allé 7
DK-2900 Hellerup
Phone: +45 3334 4000

Ref. 170512

October 2020

DATA PROTECTION POLICY

For clients, users and others whose address is connected to key systems in private households or who have contacted Bekey directly via the website or otherwise.

1. PERSONAL DATA PROTECTION

Bekey A/S (hereinafter named Bekey) has a responsible approach to your personal data. We ensure that data processing is fair and transparent in accordance with the applicable regulations regarding personal data processing.

We process personal data and have adopted this data protection policy to inform you how we process data concerning you, when e.g. you use www.bekey.dk and our SaaS (Software as a Service) solution – whether you access these via mobile applications or a desktop browser.

Our data protection policy covers three groups:

- Customers (usually private individuals) who use Netkey Lite
- Users who have received a key via Netkey Lite as part of a Bekey solution
- Potential customers and clients who have contacted us via our website or otherwise.

Bekey is the Data Controller for all three groups. We ensure that your personal data are processed in accordance with data legislation.

We offer key systems to private customers and business clients. This data protection policy explains how we process personal data concerning private customers whose address is connected to the key system, users who, by dint of connection to our

customer's key system, have a digital key, and all potential and former customers whose data is recorded in our customer registry.

Bekey is also the Data Controller for commercial clients. See section 6.2.

2. DATA RESPONSIBILITY AND CONTACT DETAILS

Bekey is the Data Controller responsible for processing the personal data we receive concerning you. Our contact details are as follows:

Bekey A/S
VAT No. DK27507980
Gladsaxe Møllevvej 28
DK-2860 Søborg
E-mail: drift@bekey.dk
Website: www.bekey.dk
Phone: +45 43 43 99 90

If you have questions about how we process your personal data, please do not hesitate to contact us.

3. OBJECTIVES AND LEGAL BASIS FOR DATA PROCESSING

3.1. Objectives

We process your personal data for the following purposes:

- To facilitate effective and successful use of our system as part of an active customer relationship
- To facilitate effective and successful use of our system for the user
- To facilitate communication in response to your enquiry
- To offer relevant services associated with the above
- To provide advice and guidance regarding the Bekey solution

3.2. Legal basis

We are obliged to inform you of the legal basis for how we process your personal data. This is as follows:

- Article 6(1)(a) of the EU General Data Protection Regulation (GDPR) regarding consent
- Article 6(1)(b) of the GDPR regarding data processing necessary for the performance of a contract an agreement or in order to take steps towards entering into a contract

4. WE PROCESS THE FOLLOWING INFORMATION CONCERNING YOU

We process data concerning you in order to optimise our services and ensure that we provide good quality products and services and communicate effectively with you.

The personal data we process concerning our private customers who are connected to the key system:

- Ordinary customer contact details
- Information about purchase(s)
- Customer enquiries

- Address
- Names of door units
- Reading access to the customer's contact book

The personal data we process concerning users who, because they are connected to our customer's key system, have a digital key:

- Username
- Person's name
- Phone no.
- IP address
- Address and times, at which the digital key is used
- User-related correspondence
- Location

We must record the above data in order to fulfil our contractual obligations with regard to the customer regarding the supply of a key system at the address including an option to connect multiple users. We receive user data from the customer.

Netkey Lite:

Netkey Lite requires an additional permission from the user to allow the app reading contacts. It is needed to:

- list users (from contacts) to whom the person wants to give access
- show the list of issued keys (not by phone numbers, but by names as in the contact book)
- show the text of push messages with names of contacts as in the contact book, not just the phone numbers.

*in case if the user is not found in the contact book - then the phone number is shown instead of a name.

Android app permissions disclosure:

We require the location-data because it is necessary to discover and communicate with our Bluetooth-based hardware devices. In addition, your location might be transmitted to and stored on our servers (via a secure connection) for troubleshooting purposes.

The personal data we process concerning potential customers who, via our website or otherwise, have contacted Bekey:

- Person's name
- Phone no.
- E-mail address
- Correspondence in connection to the enquiry

We collect, process and store only the data we need

We collect, process and store only the personal data we need i.e. relevant and adequate data in order to resolve our objectives. Furthermore, we may be obliged to meet legal requirements regarding data collection and storage in connection with our business operations. The type and scope of the personal data we process may also be necessary in order to meet contractual or other legal obligations.

Access to check and update your personal data

To ensure that data recorded is neither incorrect nor misleading, it is important that you can ensure that the data you have entered are correct. As a private customer and user, you have access to edit/rectify the personal data you entered – with exception of your phone number. If you wish to edit incorrect telephone data, you must contact Bekey.

As our services rely on the user having provided correct and updated personal data, we request that you regularly check and, if necessary, update personal data entries.

We collect anonymised data based on recorded personal data

Bekey consistently collects data in an anonymised or pseudonymised (i.e. rendered non-identifiable) format – i.e. data based on the personal data recorded and data collected by the system. For example, we might record that a customer has seen an advertisement within a given period. It is not possible to identify the customer in question as the data is anonymous. This means that there is no sensitive personal data associated with this record.

We ask for your consent before we process your personal data

We ask for your consent before we process your personal data for the purposes listed above, unless we have a legal basis for collecting them. We will inform you *if* we have a legal basis and *why* we have a legitimate interest in processing your personal data.

You give us your consent voluntarily and can withdraw your consent at any time. You can withdraw your consent online via the contact form at www.bekey.dk.

If we wish to use your personal data for purposes other than those foreseen, we will inform you of the new purpose and request your consent before we begin to process the data. If we have a new legal basis for the new process, we will inform you of it.

The Bekey solution does not allow Bekey to identify the age of a user. As our products and services require users to have a telephone and user profile and to have received a key from an administrator who has a Bekey door unit fitted, it is reasonable to assume that a child's guardian has consented to the use of our solution. We do not therefore believe that we are obliged to obtain parental consent.

We will not disclose your personal data without your consent

If we wish to disclose your personal data to partners and other players, e.g. for marketing purposes, we will request your consent and inform you how your data will be used. You may at any time object to this type of disclosure. You can withdraw your consent online.

We will obtain your consent before we disclose your personal data to a partner in a third country. If we disclose your personal data to a partner in a third country, we will ensure that the level of personal data protection offered by that partner meets the applicable legal requirements stipulated by this policy. Our requirements include data processing, data security and securing your rights, e.g. to object to profiling and to complain to Datatilsynet (The Danish Data Protection Authority).

We do not request your consent if we are legally obliged to disclose personal data, e.g. as part of a mandatory report to a public authority.

Consent – and associated functions

In effect, you give consent to a series of measures that are adapted to individual services provided by Bekey.

When you consent to our terms and conditions, you essentially accept the terms of Bekey's data protection policy and concomitantly agree to allow Bekey to send so-called "transactional e-mails" to your email address. These are:

- Mails confirming the agreement

- Mails confirming payments in accordance with the agreement
- Mails regarding a change of password
- Other mails that are necessary for the contract to continue.

You cannot unsubscribe to these mails – unless the agreement is terminated.

When you use Bekey's services, you can choose which functions to use, e.g. "Freshdesk" and "contact form". These choices will also result in mails to the e-mail address you gave us. If you do not wish to receive mails associated with these functions, you should desist from using the functions in question. Service functions presuppose that it is possible to communicate by e-mail.

Bekey also allows you to opt to receive e-mail newsletters, in which Bekey provides information about new products, events, tips, etc. that may be useful to you as our customer and user. As newsletters are not specifically linked to the service for which you have opted to enter an agreement with Bekey, we must allow customers an option to unsubscribe. They are deactivated by default.

Cookies, objectives and relevance

If we set cookies, you will be informed of their use and the purpose of collecting data via cookies.

We request your consent to use cookies

Before we set cookies on your device, we will request your consent to do so. However, we are permitted to set cookies without consent if they are necessary for functionality and settings purposes.

For further information on how we use cookies or to learn how to delete or block them, visit our website.

5. DATA SECURITY

We protect your personal data and have our own data security policy

Our data security policy contains instructions and measures to protect your personal data from destruction, loss or alteration, unauthorised disclosure, and unauthorised access or knowledge of them.

We have established procedures for assigning access rights to those of our employees who process sensitive personal data and data that discloses information about personal interests and habits. To prevent loss of data, we take consistent back-ups of our data sets. We also safeguard the privacy and authenticity of your data by means of data encryption.

In the event of a personal data breach that results in a serious risk of discrimination against you, theft of your identity, financial loss, damage to your reputation or causes any other significant inconvenience to you, we will inform you of the data breach without undue delay, as indeed we are obliged to do in accordance with Article 34 of the GDPR.

In order to protect unauthorised access to your personal data, we deploy technical measures that automatically ensure that the data are accessible only to relevant employees.

6. PARTNERS

Disclosure

We will disclose your data to partners only if we have your consent to do so or if the partners are necessary in order to meet our contractual obligations with you.

Please find a list of necessary partners here:

- We do not currently disclose data to any partners at all.

6.1. Data Processors

In order to provide the best possible service, Bekey uses the following Data Processors:

Suppliers of hosting/back-up services:

- Amazon Web Services EMEA SARL
- Hetzner Online GmbH
- OVH Hosting Ltd.

IT development and support:

- FK Distribution A/S
- Technology Staffing Corporation (Go Interactive)
- Cekura A/S
- Freshdesk (Freshworks) Inc.
- Google Ireland Ltd.

Administration:

- Twilio Inc.

6.2. Data Processing Agreement with Bekey

Any company including a public enterprise that uses the Bekey solution must enter a specific Data Processing Agreement (DPA) with Bekey. The DPA is required under the terms of the GDPR and seeks to ensure that the customer meets requirements with regard to the processing of personal data made necessary by dint of the contract.

7. DATA TRANSFERS TO A THIRD COUNTRY

We will transfer your personal data to recipients outside the EU/EEA.

We will transfer to the USA and Ukraine. Neither country is considered to provide an adequate level of personal data protection.

Data transfer to the USA will be achieved via Data Processor, FreshWorks Inc. and Twilio inc. The basis for these transfers is a Standard Contract Clause. To receive a copy, contact us. See also section 2 above.

Data transfer to the Ukraine takes place via a Data Processor, Technology Staffing Corporation (Go Interactive). Here the basis for data transfer is a Standard Contract Clause. To receive a copy, contact us. See also section 2 above.

8. ERASURE

We store your data for as long as we need to in order to meet our obligations vis-à-vis the customer and for a period of up to five years after expiry of the contract and/or to ensure compliance with the applicable legal obligations, including in particular the provisions of the Danish Bookkeeping Act regarding the storage of accounting records for a period of five years after the end of the financial year.

We delete personal data when we no longer need the data for the objectives for which your data were originally collected, processed or stored. The following general regulations apply to erasure:

- The one-year rule: If a user ceases to use the Netkey Lite solution and no longer manages a door unit, we will erase his/her personal data within 12 months.

- If you are an administrator who manages a door unit, Bekey will not erase your profile, as this would constitute a data breach because it would then be possible to link the door unit to another user without your consent. To avoid this situation, you can dismount the unit. This means that you will no longer be registered as the administrator and we will be able to erase your data in accordance with item 1 above.

- Your right to be forgotten: This function allows you to initiate an erasure process in which Bekey erases any personal data that are not covered by the aforementioned rules. If you have reached no agreements with Bekey (i.e. you have never used the Bekey solution), the erasure process allows us to delete all the data we have recorded concerning you.

- The erasure process itself can take up to 30 days.

- Bekey does not erase personal data that is in an anonymised or pseudonymised (non-identifiable) format.

9. YOUR RIGHTS

9.1. Contact details in the event that you wish to exercise your rights

If you wish to exercise any of the following rights, you must contact us. See contact details listed at the top of the data protection policy.

We will process and respond to your request as soon as possible and within one month of receipt unless the scope and complexity of your request make it impossible for us to respond with a month. In this case, we are obliged to respond within three months in all (see Article 12 of the GDPR).

9.2. You have a right to know which personal data we process concerning you

You are entitled at any time to be informed which data we process concerning you, the origin of the data and to what purpose we use them. You have a right to know for how long we store your personal data, who receives data concerning you and to what extent

we disclose the data to third parties in Denmark and abroad. This is described in our data protection policy.

9.3. You have a right to have inaccurate personal data rectified or erased

If you believe that the personal data, we process concerning you are inaccurate, you have a right to have them rectified. See Articles 16 and 17 of the GDPR.

If you believe that your data are no longer required for the purpose for which we recorded them, you may ask to have them erased. You can do this online. You may also contact us if you believe that your personal data are not processed in compliance with the legislation and other legal obligations.

However, Bekey will not erase or rectify data if Bekey is legally obliged to store all or some of your personal data or if the data are necessary in order to establish or defend legal claims. In this case, Bekey will store only the data that Bekey is legally obliged or entitled to store – and erase any other personal data concerning you.

9.4. You have a right to object to how we process your personal data

Under the following circumstances, you have a right to restrict to how Bekey processes your personal data (see Article 18 of the GDPR):

- While Bekey investigates in response to your having contested the accuracy of the personal data. Restrictions will not be lifted until Bekey has completed processing your objection.
- If Bekey's processing is unlawful and you oppose erasure of your personal data and request restrictions to their use instead.

You may activate this measure at your discretion. You can request either deactivation or erasure.

9.5. Right to data portability

As our processing of your personal data is based on your consent or a contractual agreement and our data processes are automatic, you have a right to data portability.

The right to data portability means that you are entitled to have the personal data you submitted to us sent to you in a structured, commonly used and machine-readable format and have the right to transmit those data to another Data Controller. See Article 20 of the GDPR.

If you wish to exercise the right to data portability, visit www.bekeyBekey.dk. You can ask us to send you your personal data records in a commonly used format.

9.6. Right to object

You have a right to object to how Bekey processes your personal data if processing is made in accordance with Articles 6(1)(e) and (f) of the GDPR.

Upon receipt of an objection, Bekey may no longer process personal data unless Bekey can prove that our processes are necessary on compelling legitimate grounds, which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims. See Article 21 of the GDPR.

You also have a right to object to how Bekey processes your personal data if we process them for direct marketing purposes, including profiling. See Article 21 of the GDPR. Upon receipt of an objection, Bekey is no longer entitled to process your personal data for these purposes.

9.7. Right to withdraw consent

As our data processing depends on your consent, you have a right at any time wholly or in part to withdraw your consent to process your personal data. See Article 7 of the GDPR.

If you withdraw consent, Bekey will cease to process any personal data, for the processing of which you have withdrawn consent, unless Bekey is legally obliged or entitled to store all or part of that personal data. In this case, Bekey will store only the data that Bekey is legally obliged to retain and erase all other personal data concerning you. Withdrawal of your consent has no legal bearing on data processing undertaken by Bekey until we received notice of withdrawal.

10. RIGHT TO COMPLAIN

If you wish to complain about how Bekey processes your personal data, you have a right to lodge a complaint at Datatilsynet (The Danish Data Protection Authority). Contact details as follows:

Datatilsynet (The Danish Data Protection Authority)

Address: Carl Jacobsens Vej 35, 2500 Valby

Email: dt@datatilsynet.dk

Phone: + 45 33 19 32

Website: www.datatilsynet.dk

October 2020