Policy regarding Personal Data management at beebyte AB

Table of Contents

Roles and responsibilities

Role	Name	Contact details
Chief Executive Officer, CEO	Niclas Alvebratt	+46 54 20 33 331
Chief Technology Officer, CTO	Simon Ekstrand	+46 54 20 33 331
Supervising authority	Datainspektionen	+46 8 657 61 00

Responsible part of the organisation for processing all personal data i beebytes headquarter in Karlstad, Sweden:

Beebyte AB
Sommargatan 101A
656 37 Karlstad
Sweden

Beebytes collecting of personal data information

Beebyte AB (here after beebyte) aims to never collect more data than necessary to be able to deliver its services within hosting and cloud services. The collection of personal data information is necessary to be able to bill and invoice customers and in case of incidents notify the affected subscribers.

No personal data is allowed to be collected for other purposes without the consent from users of beebytes services.

Regarding sales to individuals (not registered companies) collecting and processing of such information may be necessary to be able to setup a valid agreement.

Regarding sales to organizations and companies collecting and processing of personal data information is a must to be able to deliver the ordered services to the registered end users.

Beebyte also collects and process personal data information to be able to inform customers and users about services and offers.

Data is mainly collected from the registered user it self, in special cases data might be collected from credit institutes or tax authorities.

What is considered to be personal data information?

All data or information that might be used to identify a human being is considered as personal data and should be protected as such. This includes but are not limited to:

- Address
- E-mail
- Phone number
- Social security number
- IP addresses

Limited responsibility

Beebyte is responsible for the security while processing and storing personal data within its systems and platforms. Beebyte is not responsible, and cant be held responsible, for systems, applications, code or similar that users, customers, resellers or partners installs or runs on beebytes services.

Beebyte cant be held responsible for systems, code, applications or similar delivered by a third party.

Processing of personal data

Transferring

All types of sensitive data, including personal data, is only allowed to be sent over an encrypted link. If possible data should be password protected and/or encrypted during transfer.

Storage

All personal data must be stored in a safe way that ensures that only authorized persons, resellers, the customer himself, or persons that the customer has granted permission to, has access to it.

Authorized persons from beebyte is appointed by CEO or CTO. During the process of authorization it is CEO or CTOs responsibility to make sure that the appointed persons has read, understood and signed this policy.

Automatically discarding data

In the case of no user activity on a account and no active subscriptions during a period of 6 months the user account and its personal data will be removed automatically.

Personal data in third party systems will also be erased at the same time.

Destruction of components

Beebyte does not resell any hardware where data from users and customers has been stored. In cases where hardware with storage capabilities is to be discarded, this is done via environmental friendly methods and with destruction certificates.

Use of third party systems

Beebyte uses the following third party systems and might store personal data information in them

Function	Stored details	Part
Support / Tickets	E-mail, phone number, name	Zendesk Inc.
Invoicing/economy	E-mail, phone number, address, name, social security number	Fortnox AB and Noxfinans AB
Project management	E-mail, phone number, name	Asana Inc.
E-mail marketing	E-mail	Mailchimp / The Rocket Science Group, LLC
E-mail	E-mail: general correspondence	Google Ireland Ltd.
Phone	Phonen umber, name	Telavox AB
Banking	Name	Swedbank AB
Domain registration	Name, phone number, social security number and E-mail	Tucows Inc. and IIS (Internet Stiftelsen)
Integrations	Name, phone number, social security number, E-mail	Zapier Inc.
CRM	Name, phone number, social security number, E-mail	Copper CRM Inc.
Chat	Name, E-mail, phone number	Tawk.to Inc.

Details are only stored in the above systems in the cases that they are considered a necessity to deliver the services.

’Security by design’

All components that beebyte uses or construct shall only collect the necessary data to fulfill its tasks. Also the following criteria must be met:

- Data shall transfer, process and stored according to this policy
- The use of security technologies such as encrypted tunnels and firewalls is enforced
- Security patches must be installed on systems storing and processing personal data at every service windows

Users and customers rights

Except the following rights, registered users and customers also have the right to:

- withdraw their consent for marketing and commercial information
- request and have verified that storing of personal data only is done within the time that beebyte verifies its correctness
- opt-out from personal data processing if beebyte is unable to show how it is necessary to be able to deliver the ordered services
- receive information about how personal data information is stored and processed

Data portability

All users and customers can request a copy of all personal data information stored about them. Data will be delivered in a transferable open file format (i.e. CSV).

The right to be forgotten

A user or customer can always waiver the right to be forgotten from beebyte and third party systems. This can be done through an email to support@beebyte.se or through forms in beebytes user portal.

For it to be executed it is necessary that the user has no active subscriptions and no debts to settle. If an inquiry is made about to be forgotten, it will normally be executed within 7 days.

The right to change and correct data

A user or customer can whenever they desire, change their data within beebytes customer portal.

Personal data assistant agreement

Customers and users have the option to sign Data Processing Agreements with beebyte AB. This is only valid for registered companies.

Incident management

Routine at suspected or confirmed incident

If there is a suspicion that personal data information has leaked or is being suspected that it has been stolen the personal data responsible person must be notified, if absent beebytes CEO must be notified.

If beebyte suspect that there is an ongoing attack, every person within beebyte has the right to turn of the system or do what is necessary to protect the data from leaking.

The personal data responsible person or CEO will then immediately inform the supervising authority and file a police report about it.

If the incident can be assumed to cause risk for the registered persons rights or freedoms the personal data responsible person or CEO shall notify the registered person.

POST Analyzes

After an incident it is very important to commit a post analyzes to assess future risks of the incident to be repeated. Therefore each post analyzes must contain and answer to the following questions:

Did we follow our routines and did we reach the intended effect of them?

How can we adjust our routines to get a more efficient incident management?

What was the root cause to the incident?

Have we managed to stop this from happen again and if so – how?