PRIVACY POLICY
EVITBE AB

This Privacy Policy explains how we process (collect, use, share and otherwise process) your personal information. We will process any personal information about you in accordance with this Privacy Policy, as well as applicable law.

Purpose

The purpose of this policy is to describe how we, Evitbe AB, handle personal data, what we use them for and who can access it. The policy is based on current data protection legislation, such as the General Data Protection Regulation[1] and, where applicable, other laws and regulations describing the processing of personal data. The policy clarifies our actions to safeguard the rights and privacy of individuals when storing their personal data. For example, people who reported that they want information from us, applied for a job with us, suppliers, employees, partners, customers, or former employees.

Background

We primarily handle personal data to fulfill our obligations. Our starting point is to not collect or store any more personal information than is necessary for the purpose, to delete personal data that we no longer need, and we always strive to use no more sensitive data than necessary.

We also use personal data to run our business and provide good service. This may be e.g. in sales and marketing, follow-up, internal and external information or in conducting different types of surveys. We may also need personal data to comply with government laws and regulations or to comply with existing agreements.

When we collect information about a person for the first time, that person shall be informed of what the data will be used for and consent will be obtained if this is required. If the collection of data is based on consent the data subjects may object directly or later to the fact that we store the data, in which case their data is deleted or anonymized. They can also object to using the data for certain purposes, such as direct marketing. When processing personal data, we ensure not to create registries that we do not need, to send or distribute them safely and delete files when they are no longer used.

[1] (EU 2016/679), General Data Protection Regulation, GDPR

Guidelines

Legal processing of personal data

Personal data may only be collected for specific, explicitly stated and legitimate purposes. Basic principles of privacy protection are not collecting more information than needed, not storing information longer than necessary and not using data for any other purpose than intended when it was collected. If the data subject has consented to the processing of personal data, processing is usually allowed. A consent must be specific, individual, freely given and unambiguous. The data subject must prior to the consent be informed of the intended processing of the personal data provided. The data subjects may at any time withdraw consent, after which processing is no longer permitted.

In some cases, no consent is required under Article 6 of the General Data Protection Regulation. This applies to processing in the following cases:

- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child.

Sensitive personal data

Specific rules apply to sensitive personal data. Article 9 of the GDPR prohibits the processing of sensitive personal data. There are exceptions described in Article 9. An exception can be made if the processing is necessary and the data subject has given explicit consent for the processing.

What personal data do we process?

We process only personal data when we have legal right to do so. Here are examples of personal data we process:

- Name, username, e-mail address, phone number, address, date of birth, bank account number, social security number, photos, etc.
- Information that employees, clients or others have given freely and voluntarily registered
- Information that data subject themselves have published, so-called user-generated content

When do we collect personal information?

We collect personal data when required, see the section Legal Processing of Personal Data. When collecting personal data, we shall obtain consent when required. The consent may be revoked at any time, after which the data is deleted or anonymized, provided that the information is not required to fulfill our obligations under law, agreement or other legitimate interest.

We may also access personal information, for example when:

- People seek employment with us, visit us or otherwise contact us
- Individuals sign up for our courses, seminars, newsletters and other mailings
- Individuals respond to polls and surveys
- Our employees receive personal data in customer assignments
- We receive information from authorities and public records

Is personal information processed in a safe way?
We have developed routines and an IT security policy that describes how we process personal data safely. The ground rule is that only persons in our organization who need the personal data to perform their duties shall have access to them. For access to sensitive personal data special authorization is required. We have appropriate physical and electronic protection for personal data storage and we do not transfer personal data from one place to another for purposes other than those specified in this policy. We have procedures for detecting and reporting personal data breach in accordance with applicable data protection legislation.

When do we disclose personal information?
The ground rule is to disclose personal data to third parties, eg. authorities, only if it is necessary to fulfill our obligations under law or agreement or if consent has been given beforehand. In cases not relating to disclosure by law, we implement non-disclosure agreements with third parties and ensure that personal data is handled and processed in a safe manner.
If the third party is outside the EU, we will follow EU's standard agreement clauses [2]. The purpose of the EU's standard agreement clauses is to provide adequate guarantees that individuals' rights are protected in the transfer of personal data to countries that do not have an adequate level of protection.

The rights of the data subjects
The main rights of the data subjects include the right to:

- Access their personal data by a registry extract (right of access by the data subject)
- Get incorrect personal information corrected (right to rectification)
- Get their personal data deleted (right to erasure)
- Oppose the use of personal data for automated decision making and profiling (right to object and automated individual decision-making)
- Move the personal data that the data subject himself has provided to us (right to data portability)

The GDPR contains an obligation to provide, on request, information to the data subject on what personal data relating to the data subject is processed by the data processor. This means that a registry extract is submitted, see appendix. When such a request is handled, additional information such as how long the personal data will be stored and the right to have incorrect information corrected shall be shared with the data subject. If such a request is made electronically, the data subject must also be able to request to receive the information electronically.

Changes to the policy
Evitbe reserves the right, at any time and for any reason, to make additions to and amend this policy. Changes may be called upon in particular as a result of changes in laws and regulations.

This policy has been set by Evitbe CEO and Management, 2018-04-27, and should be evaluated annually and, if necessary, amended.

[2] http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

Appendix

FREQUENTLY USED DEFINITIONS

Personal Data: Any information relating to an identified or identifiable natural person (hereinafter "data subjects"), an identifiable physical person being a person identified directly or indirectly with reference to an identifier such as a name, an identification number, a location or online identifiers or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the physical person.

Sensitive personal data: Sensitive personal data are data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, sexuality and health information, and genetic and biometric data.

Processing: an action or combination of actions on personal data or sets of personal data, whether performed automated or not, such as collection, registration, organization, structuring, storage, processing or modification, production, reading, use, transfer by transmission, dissemination or displacement, adjustment or assembly, restriction, erasure or destruction.

Weighing of interests: means that there must be a legitimate interest for the data controller with a higher weight than the data subject's interest in protection against personal privacy violations. For example, it may concern collecting personal data through cookies to improve the user's experience of the site or simplify log-in, or sending marketing information to an existing client's email address. Use of this category of personal data (cookies and e-mail address) is considered to be a low risk of violation of personal privacy if the purpose is relatively harmless.

Profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Anonymization: processing of personal data in such a way that personal data can no longer be attributed to a specific data subject without using additional information, provided that this additional information is kept separately and subject to technical and organizational measures that ensure that personal data are not attributed to an identified or identifiable physical person.

Register: A structured collection of personal data that is available according to specific criteria, whether the collection is centralized, decentralized or spread based on functional or geographical basis.

Record list: Includes records such as the personal data being processed, for what purpose, how long they are stored, and to whom they were issued. A registry extract does not include personal data in itself.

Controller: A physical or legal person, public authority, institution or other body that alone or together with others determines the purposes and means of processing personal data; if the purposes and means of processing are determined by Union law or the national law of the Member States, the controller or the specific criteria for its appointment may be provided for by Union law or in the national law of the Member States.

Processor: A natural or legal person, public authority, institution or other body handling personal data for the personal data controller.

Consent of the data subject: any kind of voluntary, specific, informed and unambiguous statement of intent through which the registered person, either by statement or by unambiguous confirmatory act, accepts processing of personal data relating to him or her.

Personal Data breach: A security incident that leads to accidental or illegal destruction, loss or change or to unauthorized disclosure or unauthorized access to the personal data transferred, stored or otherwise processed. Other examples of personal data breaches may, for example, be:

- A visitor has used the printer and left printouts in the printer containing customer lists with contact information
- An employee deletes information in a database containing personal data
- An email containing personal data sent to the wrong recipient outside the organization