VAIBE Privacy Policy

KENGAGE, LDA (Vaibe) takes the protection of your personal data very seriously. We treat your personal data confidentially and in accordance with the provisions of data protection law. The purpose of this Privacy Policy is to inform you how, to what extent and for what purposes we process personal data during use of the website of Vaibe.

1. Collection, processing and use of personal data on request

Our website can be used without providing personal data. You are not obliged to access this website or provide personal data. If you do not provide us with any personal data, you may not be able to use individual functions of this website. There will be no other consequences for you. If personal data (e.g. your name, address or e-mail addresses) are collected on our website, this takes place voluntarily except in the cases described below in more detail. We wish to point out that data transfers in the Internet (e.g. during communication by e-mail) may be subject to security breaches. It is not possible to protect personal data completely against access by third parties.

2. Contact form; Request for information material

When you contact us using the contact form, we will process your personal data (especially your name and salutation, your contact details, the name of your company, the country and your message) and process them in order to answer your inquiry. This also applies when you ask for information material. If you choose to give us your telephone number, we may contact you by phone to discuss your project or query and put you in touch with suitable contact partners.

If necessary to answer your inquiry or your inquiry is so intended, we may transmit your personal data to another company in the Körber Group (e.g. if your inquiry relates to a contract or a customer relationship with another company in the Körber Group or to its products). Depending on the purpose of your inquiry, related data processing is permitted to the extent necessary to handle your inquiry.

If you request to receive information by e-mail about the latest products and services of Vaibe, Vaibe may verify your identity (Double-Opt-In) and will send requested information by e-mail. Your personal data will for this purpose be processed in a distribution list. You may revoke your consent at any time with effect for the future. For this purpose, you may e.g. use the Unsubscribe link in every automated e-mail or send a letter to KENGAGE, LDA, Rua do Heroismo, 283, 4300-259 Porto, Portugal or an e-mail to unsubscribe@vaibe.com

3. Data processing enabling website use

When you visit our website, we will collect the personal and non-personal data necessary to facilitate your website use. This includes your IP address and information about the start,

end and purpose of your use of the website, as well as any identification data (e.g. your login data if you log into a secure area). These data will be used to provide and organize the service in accordance with users' needs. The data will normally be deleted as soon as they are no longer required and there are no retention obligations.

4. Consent for cookies and web analysis

We use so-called cookies or similar functions such as tracking pixels on our website to provide our website technically and to record the use of our website statistically and evaluate it for the purpose of optimization (see section 5). We base the processing of your data through the cookies and pixels used for the above-mentioned technically necessary purposes in accordance with Art. 6 para. 1 sentence 1 lit. f) GDPR on our legitimate interest, which is to be regarded as justified in the sense of the above-mentioned regulation.

In addition, we set cookies and process the data through the cookies used only on the basis of your consent in accordance with Art. 6 para. 1 sentence 1 lit. a) GDPR. You can revoke your consent at any time with effect for the future using our Consent Management Tool. You can access the Consent Management Tool at any time via the link at the end of the website.

Cookies

Cookies are small files that are automatically created by your browser and stored on your end device (laptop, tablet, smartphone or similar) when you visit our site. Cookies do not cause any damage on your terminal device, do not contain viruses, Trojans or other malware. Information is stored in the cookie that is related to the specific terminal device used. However, this does not mean that we obtain direct knowledge of your identity.

The use of cookies makes the use of our website more pleasant for you. For example, we use so-called session cookies to recognise that you have already visited individual pages of our website. These are automatically deleted when you leave our site. We also use cookies to record the use of our website statistically and to evaluate it for the purpose of optimising our offer for you (see section 5). These cookies enable us to automatically recognise that you have already been on our website when you visit it again. These cookies are automatically deleted after a defined period. Cookies are also used to provide our website techni.

2. Consent management tool

We use the Consent Management Tool of Usercentrics A/S Havnegade 39, 1058 Kopenhagen Denmark (hereinafter: cookiebot).[MK2] In this context, date and time of the

visit, browser information, information on consents, device information and the IP address of the requesting device are processed. The legal basis is Art. 6 para. 1 sentence 1. lit. f GDPR (legitimate interest). The obtaining and administration of legally required consents is to be regarded as a legitimate interest within the meaning of the aforementioned provision. cookiebot stores consents and revocations on our behalf and on our instructions. Further information on data protection at cookibot can be found here.

5. Processing of your data, if you contact us for business purposes

If you contact us as a interested party, supplier, service provider or other business partner, we process your personal data such as contact data or correspondence to the extent that this is necessary to process your enquiry (legitimate interest according to Art. 6 para. 1 letter f GDPR) or to initiate or process the respective transaction (Art. 6 para. 1 letter b GDPR) and, if necessary, store the data within the scope of statutory storage obligations (due to statutory obligations according to Art. 6 para. 1 letter c GDPR).

The same applies if you are an employee of an interested party, supplier, service provider or other business partner and we receive your personal data in this context; the legal basis in this case is our legitimate interest in establishing or carrying out the business relationship with your employer (Art. 6 para. 1 letter f GDPR).

6. Electronic communication

You are welcome to communicate with us by e-mail at any time. Please be advised that we use an E-mail Gateway of an external provider of security technologies to defend against SPAM e-mail, other threatening e-mail, threatening e-mail attachments and URLs. In doing so, this external provider may process your first and last name, e-mail address and IP address. The legal basis is our legitimate interest in preventing unauthorized access to communications networks, the spread of malicious code and damage to computers and electronic communications systems (Art. 6 para. 1 lit. f GDPR in conjunction with Recital 49).

7. Third country data transfers

A transfer of personal data to a third country or an international organisation will only take place if we inform you of this and if the conditions of Art. 44 et seqq. GDPR are given.

A third country is defined as a country outside the European Economic Area (EEA) in which the GDPR is not directly applicable. A third country is deemed to be unsafe if the EU Commission has not issued an adequacy decision for this country in accordance with Art. 45 (1) GDPR, confirming that adequate protection for personal data exists in the country.

The USA is a so-called unsafe third country. This means, that the US does not offer a level of data protection comparable to that in the EU. The risks involved in transferring personal data to the US are as follows: There is a risk that US authorities may gain access to personal data on the basis of the PRISM and UPSTREAM surveillance programmes based on Section 702 of the FISA (Foreign Intelligence Surveillance Act), and on the basis of Executive Order 12333 or Presidential Police Directive 28. EU citizens have no effective means of redress against such access in the US or the EU.

We will inform you in this privacy policy when and how we transfer personal data to the USA or other unsafe third countries. We will only transfer your personal data if

- the recipient provides appropriate safeguards in accordance with Art. 46 GDPR for the protection of personal data,

- you have explicitly agreed to the transmission, after we have informed you of the risks, in accordance with Art. 49 para. 1 lit. a) GDPR,

- the transmission is necessary for the fulfilment of contractual obligations between you and us

- or another exception from Art. 49 GDPR applies.

Safeguards under Art. 46 GDPR can be so-called standard contractual clauses. In these standard contractual clauses, the recipient assures to protect the data sufficiently and thus to ensure a level of protection comparable to that provided by the GDPR.

8. Deletion

We will delete your personal data when they are no longer required for collection and processing purposes and provided there are no statutory retention obligations preventing erasure of your personal data.

9. Data security

Vaibe has implemented technical and organizational measures to protect the personal data, in particular against loss, destruction, manipulation and unauthorized access. Our employees and everyone involved in data processing are obliged to comply with data protection laws and handle personal data confidentially. Our employees are trained accordingly. Both internal and external checks ensure that all data protection processes are observed at Vaibe.

In order to protect the personal data of our users, we utilize a secure online transmission method, i.e. so-called "Secure Socket Layer" (SSL) transmission. You can recognize this by the addition of an "s" to the address component http:// ("https://") or when you see a green locked lock symbol. By clicking on the symbol, you obtain information about the utilized SSL certificate. Display of the symbol depends on the browser version which you are using. SSL encryption ensures encrypted and complete transmission of your data.

10. Your data subject's rights

As a data subject, you have the right to confirmation as to whether personal data relating to you are processed, the right to access this personal data, the right to rectification of incorrect personal data, the right to erasure, the right to restrict processing of your data and the right to object to the processing and transmission of personal data. Whether and to what extent these rights are effective in individual cases and under what conditions they apply is stipulated by law. In particular including the German Data Protection Act and General Data Protection Regulation. You also have the right to submit a complaint to the responsible data protection supervisory authority. However, if you have any questions or complaints relating to data protection at Vaibe, we recommend that you first contact us (see below Section 12).

11. No automated individual decisions

We do not use your personal data for automated individual decisions in the meaning of Art. 22(1) GDPR.

12. How can you contact us?

If you want to exercise your data subjects' rights or have any questions relating to data protection in our company or this Data Protection Declaration, you can also contact us at dpo@vaibe.com

13. Changes to the Privacy Policy

New legal regulations, business decisions or technical development may require amendments to this Privacy Policy. You can always find the latest version on our website.