

VAIB Privacy Notice

Effective as of 8th of November 2022

Introduction

This Privacy Notice explains in a comprehensive manner how we collect, use, and store your personal information. The information about you can be categorized as personally identifiable and non-personally identifiable information depending on whether information can make you identifiable. Personally identifiable information shall be referred to as "personal data."

Who we are

We are VAIB and we are responsible for compliance with the applicable legislation regarding the processing of your personal data. If you have any questions or concerns regarding your privacy, do not hesitate to contact us at contact@vaib.me.

Terminology explained

In addition to the definitions provided for in the Terms and Conditions ("T&Cs"), the following words and abbreviations shall have the meaning provided herein:

"personal data" means any information relating to an identified or identifiable natural person ("Customer"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"processor" means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of VAIB.

"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Types of personal data processed

During your interaction with VAIB's services or with us directly, we may process the following personal data:

- Identity data (your gender)
- Contact data (email address and telephone number(s))
- Transaction data (such as details of payments and services purchased)
- Profile data (such as password, preferences, feedback, and survey responses)
- Usage data (such as information about how our services are used)
- Marketing data (such as marketing and communication preferences)
- Photos (such as content uploaded as a data source for avatar generation, including face data)
- Technical data (such as internet protocol (IP) address, login data, browser, time zone setting and location, and operating system used for access)
- Other information you choose to provide.

We may collect personal data when you interact with the services, when you register and customise an account, or when you contact us.

For what purpose(s) do we process personal data

We process your personal data for the following purposes:

- to provide you with access to our services,
- to provide you with the services you requested,
- to create and manage your account,
- to provide you with customer support,
- to send you information about the services,
- to analyse and develop technical improvements to the services,
- to process payment for the paid services,
- to send you advertising messages,
- to comply with our legal obligations.

Legal grounds for processing personal data

Having regard to the type of personal data and the purpose(s) for which it is processed, we process the personal data on the following legal grounds:

- You have given us consent for data processing for a specific purpose,
- Processing is necessary for the performance of our obligations under the T&Cs,
- Processing is necessary for compliance with legal obligations,
- Processing is necessary for the purpose of our legitimate interest.

We may process information about how you use the services through third-party analytics tools. We process this data under our legitimate interest in analysing the performance of the services and updating our services. We aim to minimise the amount of personal data included in such information and to anonymise the data wherever possible.

We may process your IP address and other technical data automatically when you access the services. This is because we have a legitimate interest in ensuring the safety and integrity of our services, and by collecting technical data, we can monitor it and prevent malicious behavior such as extraordinary password failures, seeking exploits, and so forth.

We may process the content you provided to generate an avatar through services for our internal research or to improve our services or other VAIB technologies. We rely on our legitimate interest of improving the services and developing new technologies. Such processing of your content is typically expected with services that depend on constant research and development through the use.

Disclosure and sharing

In order to deliver the service to our users we are using our private third-party storage not publicly accessible. This is where we store all users' personal data, including face data. In accordance with our contractual relationship with the third-party we have control over such data so we can comply with our obligations regarding users' personal data in a reasonable manner.

Security

While there is an inherent risk in any data being shared over the Internet, we have put in place appropriate security measures to prevent your personal data from being accidentally lost, used, damaged, or accessed in an unauthorized or unlawful way, altered, or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a legitimate business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

Depending on the nature of the risks presented by the processing of personal data, we will have in place the following appropriate security measures:

- organisational measures (including but not limited to staff training and policy development);
- technical measures (including but not limited to physical protection of data, pseudonymization and encryption); and

- securing ongoing availability, integrity, and accessibility (including but not limited to ensuring appropriate back-ups of personal data are held).

We have put in place procedures to deal with any suspected personal data breach and will notify you and any relevant regulator of a breach where we are legally required to do so.

International transfers

Personal data will be stored on secure servers controlled and maintained in accordance with sufficient privacy safeguards. We may store or transfer information on Customers to processors located outside of the United Kingdom and European Economic Area, provided that such processors implement appropriate and suitable safeguards regarding the security of personal information.

Retention period

To determine the appropriate retention period for personal data, including face data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

Here are some exemplary circumstances which we usually consider when determining how long we need to retain your personal data:

- in the event of a complaint;
- if we reasonably believe there is a prospect of litigation in respect to our relationship with you or if we consider that we need to keep information to defend possible future legal claims
- to comply with any applicable legal and/or regulatory requirements with respect to certain types of personal data
- if information is needed for audit purposes and so forth;
- in accordance with relevant industry standards or guidelines;
- in accordance with our legitimate business need to prevent abuse of the promotions that we launch. We will retain a customer's personal data for the time of the promotion and for a certain period after its end to prevent the appearance of abusive behavior.

Customer's Rights

You have rights we need to make you aware of. The rights available to you depend on our reason for processing your personal data. If you need more detailed information or wish to exercise any of the rights set out below, please contact us at contact@vaib.me:

You may:

- request access to your personal data, which enables you to obtain confirmation of whether we are processing your personal data, to receive a copy of the personal data we hold about you and information regarding how your personal data is being used by us;
- request rectification of your personal data by asking us to rectify information you think is inaccurate and to complete information you think is incomplete, though we may need to verify the accuracy of the new data you provide to us;
- request erasure of your personal data by asking us to delete or remove personal data we hold about you; note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you;
- object to the processing of your personal data, where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms; in some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms; you also have the right to object where we are processing your personal data for direct marketing purposes;
- require that decisions be reconsidered if they are made solely by automated means, without human involvement; we use automated tools to make sure that content which you may generate is not abusive taking into account our interests and legal obligations; if these automated tools indicate that such a content does not meet our acceptance criteria, we will not process it;
- request restriction of processing your personal data, which enables you to ask us to suspend the processing of your personal data, if you want us to establish the data accuracy; where our use of the data is unlawful, but you do not want us to erase it; where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims, or if you have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it;
- request the transfer of your personal data to you or to a third party, and we will provide to you, or a third party you have chosen (where technically feasible), your personal data in a structured, commonly used, machine-readable format; note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you;
- withdraw consent at any time where we are relying on consent to process your personal data; however, this will not affect the lawfulness of any processing carried out before you withdraw your consent; if you withdraw your consent, we may not be able to provide certain products or services to you, but we will advise you if this is the case at the time you withdraw your consent;
- complain to any relevant authority about any perceived violation and to seek compensation for damages in the courts.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is manifestly unfounded or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

Period for replying to a legitimate request

The period throughout which we will usually reply to a legitimate request is one month. That period may be extended by two further months where necessary, considering the complexity and number of the requests.

Please note that we may request that you provide some details necessary to verify your identity when you request to exercise a legal right regarding your personal data.