

Privacy Policy

I. Privacy Policy for the Use of the JIFU Website

§ 1 Information on the Collection of Personal Data

(1) Below, we provide information about the processing of personal data when using our website <https://jifu.com/>. Personal data is any data that can be related to you personally, e.g., name, address, email addresses, user behavior. In doing so, we would like to inform you about our processing operations and at the same time comply with legal obligations, in particular those arising from the EU General Data Protection Regulation (GDPR).

(2) The controller pursuant to Art. 4 (7) GDPR is JIFU USA LLC 30 N. Gould St. Ste R, Sheridan, Wyoming 82801 United States, email: memberservices@jifu.com (see our legal notice).

If you have any questions about data protection, please contact the above address.

(3) When you contact us by email, we will store the data you provide (your email address, your name and telephone number, if applicable) in order to answer your questions. We delete the data collected in this context—if the inquiry is assigned to a contract—after the contract term has expired.

Otherwise, we delete the data after it is no longer necessary to store it, at the latest three years after the data was created at the end of the general limitation period or restrict its processing if there are legal retention obligations.

(4) If we use contracted service providers for individual functions of our offer or wish to use your data for advertising purposes, we will always select and monitor these service providers carefully and inform you in detail about the respective processes below. We will also specify the criteria for the storage period.

§ 2 Processing of personal data when visiting our website

When using the website for informational purposes, i.e., simply viewing it without registering and without otherwise providing us with information, we process the personal data that your browser transmits to our server. The data described below is technically necessary for us to display our website to you and to ensure stability and security and must therefore be processed by us. The legal basis is Art. 6 (1) (f) GDPR:

- IP address
- Date and time of the request
- Time zone difference to Greenwich Mean Time (GMT)
- Content of the request (page visited)
- Access status/HTTP status code
- Amount of data transferred
- Previously visited page
- Browser

- Operating system
- Language and version of the browser software.

§ 3 Conditions of use of the JIFU website, registration

(1) If you wish to use our portal, you must register by providing your email address, a password of your choice, and a username of your choice. The provision of the aforementioned data is mandatory. For this service, we use the so-called double opt-in procedure, i.e., you will receive an email in which you must confirm that you are the owner of the email address provided and that you wish to receive notifications. You can unsubscribe from the notifications at any time, e.g. by clicking on the link in the email or using the contact details provided. We store the data you provide, the time of your registration for the service, and your IP address until you unsubscribe from the notification service.

(2) When you use our portal, we store the data required to fulfill the contract until you permanently delete your account. We also store the voluntary data you provide for the duration of your use of the portal, unless you delete it beforehand. You can manage and change all your details in the secure customer area. The legal basis for this is Art. 6 (1) (b) GDPR.

(3) To prevent unauthorized access by third parties to your personal data, in particular financial data, the connection is encrypted using TLS technology.

§ 4 Newsletter

(1) You can subscribe to our newsletter, which we use to inform you about our current interesting offers, by giving your consent. The advertised goods and services are named in the declaration of consent.

(2) We use the double opt-in procedure for registration for our newsletter. This means that after you register, we will send an email to the email address you provided, asking you to confirm that you are the owner of the email address provided and that you wish to receive the notifications. If you do not confirm your registration within 48 hours, your information will be blocked and automatically deleted after one month. In addition, we store your IP addresses and the times of registration and confirmation. The purpose of this procedure is to verify your registration and, if necessary, to investigate any possible misuse of your personal data.

(3) The only mandatory information required for sending the newsletter is your email address. After your confirmation, we will store your email address for the purpose of sending you the newsletter. The legal basis for this is Art. 6 (1) (a) GDPR.

(4) You can revoke your consent to receive the newsletter at any time and unsubscribe from the newsletter. You can revoke your consent by clicking on the link provided in every newsletter email.

§ 5 Transfer of data / use of service providers

(1) If we use contracted service providers for individual functions of our offer or wish to use your data for advertising purposes, we will always select and monitor these service providers carefully and inform you in detail about the respective processes below. We will also specify the criteria for the

storage period. If our service providers or partners are based in a country outside the European Economic Area (EEA), we will inform you of the consequences in the description of the offer.

(2) In order to provide our contractual services and within the scope of the technical provision of our online offer, we use external service providers (processors) within the meaning of Art. 28 GDPR. Specifically, we currently use:

- Google Cloud Platform (including Google Firestore), operated by Google Ireland Limited and, for certain services, by Google LLC, USA. The latter is certified under the EU-U.S. Data Privacy Framework (DPF), meaning that an adequacy decision pursuant to Art. 45 GDPR exists for these transfers. .

- Exigo, headquartered in Dallas, Texas, USA. Personal data is transferred on the basis of appropriate safeguards in accordance with Art. 46 GDPR, in particular through the conclusion of the current EU Standard Contractual Clauses (SCCs).

- Tyga LLC, based in Provo, UT, USA. Personal data is transferred on the basis of appropriate safeguards in accordance with Art. 46 GDPR, in particular through the conclusion of the current EU Standard Contractual Clauses (SCCs).

(3) The data processed by the aforementioned external providers will be deleted as soon as it is no longer required for the respective purpose, unless statutory retention obligations or contractual agreements prevent this. Further information on the storage period can be found in the privacy policies of the respective service providers.

(4) When transferring data outside the EEA, we take appropriate technical and organizational measures to ensure an adequate level of protection within the meaning of the GDPR, such as encryption and access restrictions.

§ 6 Your rights

(1) You have the following rights vis-à-vis a controller with regard to personal data concerning you:

- Right to information
- Right to rectification or erasure
- Right to restriction of processing
- Right to object to processing
- Right to data portability
- Right to object to advertising and withdraw consent.

(2) You also have the right to complain to a data protection supervisory authority about our processing of your personal data.

II. Privacy policy for the use of the JIFU 360 app

§ 1 Information about the processing of personal data

(1) In addition to our online offering, we provide you with a mobile app that you can download to your mobile device. Below, we provide information about the processing of personal data when using our mobile app. Personal data is any data that can be related to you personally, e.g. name, address, email addresses, user behavior. In doing so, we would like to inform you about our processing operations and at the same time comply with legal obligations, in particular those arising from the EU General Data Protection Regulation (GDPR).

(3) The controller pursuant to Art. 4 (7) GDPR is JIFU USA LLC 30 N. Gould St. Ste R, Sheridan, Wyoming 82801, e-mail: memberservices@jifu.com (see our imprint).

If you have any questions about data protection, please contact the above-mentioned contact.

(4) When you contact us by email or via a contact form, the data you provide (your email address, your name and telephone number, if applicable) will be stored by us in order to answer your questions. We will delete the data collected in this context if the request is assigned to a contract upon request or after the contract period has expired or if the account has been inactive for three years. Otherwise, we will delete the data after it is no longer necessary for storage, at the latest three years after the data was created at the end of the general limitation period or restrict processing if there are legal storage obligations.

§ 2 Transfer of data / use of service providers

(1) If we use commissioned service providers for individual functions of our offer or wish to use your data for advertising purposes, we will always select and monitor these service providers carefully and inform you in detail about the respective processes below. We will also specify the criteria for the storage period. If our service providers or partners are based in a country outside the European Economic Area (EEA), we will inform you of the consequences in the description of the offer.

(2) Use of external service providers and transfers to third countries In order to provide our contractual services and within the scope of the technical provision of our online offering, we use external service providers (processors) within the meaning of Art. 28 GDPR. Specifically, we currently use:

- Google Cloud Platform (including Google Firestore), operated by Google Ireland Limited and, for certain services, by Google LLC, USA. The latter is certified under the EU-U.S. Data Privacy Framework (DPF), meaning that an adequacy decision pursuant to Art. 45 GDPR exists for these transfers.
- Exigo, headquartered in Dallas, Texas, USA. Personal data is transferred on the basis of appropriate safeguards in accordance with Art. 46 GDPR, in particular by concluding the current EU Standard Contractual Clauses (SCCs).
- Tyga LLC, based in Provo, UT, USA. Personal data is transferred on the basis of appropriate safeguards in accordance with Art. 46 GDPR, in particular through the conclusion of the current EU Standard

Contractual Clauses (SCCs).

- (3) The data processed by the aforementioned external providers will be deleted as soon as it is no longer necessary for the purpose for which it was collected, unless statutory retention obligations or contractual agreements prevent this. Further information on the storage period can be found in the privacy policies of the respective service providers.
- (4) When transferring data outside the EEA, we take appropriate technical and organizational measures to ensure an adequate level of protection in accordance with the GDPR, such as encryption and access restrictions.

§ 3 Your rights

(1) You have the following rights with regard to a controller in relation to your personal data:

- Right to information
- Right to rectification or erasure
- Right to restriction of processing
- Right to object to processing
- Right to data portability
- Right to object to advertising and withdraw consent

(2) You also have the right to complain to a data protection supervisory authority about our processing of your personal data.

§ 4 Processing of personal data when using our mobile app

- (1) When you download the mobile app, the necessary information is transferred to the app store, in particular your user name, email address and customer number for your account, the time of download, payment information and the individual device ID. In addition, the app store independently collects various data and provides you with analysis results. We have no influence on this data processing and are not responsible for it. We only process the data to the extent necessary for downloading the mobile app to your mobile device.
- (2) When you use the mobile app, we process the personal data described below to enable you to use the functions conveniently. If you wish to use our mobile app, we process the following data, which is technically necessary for us to offer you the functions of our mobile app and to ensure stability and security, so that it must be processed by us. The legal basis is Art. 6 para. 1 sentence 1 lit. f GDPR:

- IP address
- Date and time of the request
- Time zone difference to Greenwich Mean Time (GMT)
- Content of the request (page visited)

- Access status/HTTP status code
- Amount of data transferred
- Previously visited page
- Browser
- Operating system
- Language and version of the browser software.

(3) In order to provide app notification and related services, we may collect one or more of the following information: your device identifier, unique number of the end device (IMEI = International Mobile Equipment Identity), unique number of the network subscriber (IMSI = International Mobile Subscriber Identity), mobile phone number (MSISDN), MAC address for Wi-Fi use, name of your mobile device, email address.

§ 5 Processing of data from your end devices (so-called “cookie policy”)

(1) In addition to the aforementioned data, technical tools for various functions are used when you use our mobile app, which may be stored on your device. We mainly use so-called authentication tokens, which are only stored for the duration of your login. In addition, other technical tools such as the Advertising ID or authentication cache may be used. When you open our mobile app and at any time thereafter, you can choose whether you wish to generally allow the use of individual or all voluntary additional functions. You can make changes in the settings of the mobile app or via our consent manager. Below, we first describe the technical functions (2) before going into more detail about your individual options by describing technically necessary functions (3) and functions that you can voluntarily select or deselect (4). The functions we use, which you can select and revoke individually via the consent manager, are described below.

(2) We use technical functions that provide you with additional services. Our app does not use cookies, but so-called authentication tokens. These tokens are only stored for the duration of your login in the app and are automatically deleted as soon as you log out or close the app. Tokens are used to identify you during app usage and to enable access to certain functions.

(3) Technically necessary functions: The app requires certain tokens for correct functionality. These are stored exclusively for the duration of use and are automatically deleted. Deactivation is not possible if you wish to use the app. The legal basis for this processing is Art. 6 (1) sentence 1 lit. f GDPR.

(4) Optional functions: Additional technologies (e.g., analytics, advertising) are only used if you give your consent. The legal basis for this processing is Art. 6 (1) lit. a GDPR. You can withdraw your consent at any time.

(5) In iOS, you have various options for restricting advertising and tracking to a large extent. Tracking is generally carried out via the so-called “Advertising Identifier” (IDFA). This is a unique, but non-personalized and non-permanent identification number for a specific device, which is provided by iOS.

The data collected via the IDFA is not linked to other device related information. We use the IDFA to provide you with personalized advertising and to evaluate your use.

If you go to "Privacy & Security" in the iOS settings, you can largely disable advertising analysis under "Tracking." If you enable the "Allow Apps to Request Tracking" feature, our app will ask you whether you agree to advertising measures when you first use it, and you can enable or disable advertising. In addition, you can select the "Apple Advertising" option in the "Privacy & Security" option and disable "personalized advertising." In the "Analysis & Improvements" option, you can also disable the "Share iPhone Analysis" and "Improve Siri & Dictation" functions, which will prevent statistical information about your use of iOS from being transmitted to Apple.

§ 6 Objection or revocation of the processing of your data

(1) If you have given your consent to the processing of your data, you can revoke this consent at any time. Such revocation affects the permissibility of the processing of your personal data after you have notified us of your revocation. The permissibility of the processing of your data until the time of your revocation remains unaffected.

(2) Insofar as we base the processing of your personal data on the balancing of interests, you may object to the processing. This is the case if the processing is not necessary for the fulfillment of a contract with you, which is explained by us in the following description of the functions. When exercising such an objection, we ask you to explain the reasons why we should not process your personal data as we have done. We will then review the situation and either adjust the data processing, discontinue it, or inform you of our compelling legitimate grounds for continuing the processing.

(3) You can, of course, object to the processing of your personal data for advertising and data analysis purposes at any time. The best way to object to advertising is to contact us using the contact details provided above.

Status of the privacy policy: June 17, 2026