

Datenschutz

Version 1.1 | 2026-09-24T05:25:45.944Z

1. Controller and contact

The controller responsible for operating the Vebelio platform is Matthias Stein-Schilling, Hal-lig-Hooge-Stieg 12, 22846 Norderstedt, Germany. Contact for data-protection matters: vebelio-daten-schutz@daytradermasterminds.com.

This notice covers processing carried out by the platform. Companies and experts may be independently responsible for their own offers, customer relationships and content. Please also read their privacy notices. Where Vebelio processes data exclusively on a company's documented instructions, this is governed by a data-processing agreement pursuant to Article 28 GDPR.

2. Purposes, data and legal bases

- Platform access and operation: IP address, time, requested address, device and browser data, and technical error data for delivery and security. The legal basis is Article 6(1)(f) GDPR; our legitimate interest is a secure and reliable service.
- Registration and use: contact and profile data, login information, memberships, access rights, booked services and content you provide, to perform the user contract under Article 6(1)(b) GDPR.
- Communication: messages, support requests and related contact data to handle your request, under Article 6(1)(b) or (f) GDPR.
- Payments, invoices and legal records: order, billing and transaction data and recorded consents to perform contracts and meet legal obligations, under Article 6(1)(b) and (c) GDPR. Article 6(1)(f) GDPR may also apply to asserting or defending claims.
- Optional analytics and personalisation: usage data for enabled features after your separate choice, under Article 6(1)(a) GDPR. Cookie consent and account-level product settings are controlled separately.

Providing required account and contract data is necessary for the relevant function. Without it, login, booking or support may be limited. Optional consent is voluntary.

3. Hosting and technical operation

The platform is operated on an own Windows server; STRATO is used for hosting and/or communication services. A future use of Hetzner is planned and is not stated here as already active. We review the service-provider information when this changes.

Technical providers receive data only to the extent required for their service. Where they act as processors, an Article 28 GDPR agreement is required.

4. Payments and external offer processing

Depending on the offer and enabled payment method, PayPal, Revolut or external offer processing through Ablefy may be available. The provider shown in the specific checkout is decisive. Listing these providers does not mean that every provider is active for every offer.

Contact, order, invoice and payment data may be transferred to the selected provider as required for processing. Payment providers process data under their own responsibility, including for statutory checks and fraud prevention. Their privacy notices supplement this notice:

- PayPal: <https://www.paypal.com/de/legalhub/paypal/privacy-full>
- Revolut: <https://www.revolut.com/de-DE/legal/privacy/>
- Ablefy: <https://ablefy.io/privacy-policy/>

5. Google Analytics and cookies

If enabled for this installation, Google Analytics is loaded only after explicit statistics consent. Pseudo-anonymous usage identifiers, device and connection data, and page views of selected public pages may be processed. Google may receive your IP address. This platform integration is not used for page-view measurement in private member areas. The provider is Google Ireland Limited; processing by affiliated companies in the United States may occur.

Further information about consent, browser storage and withdrawal is provided in the cookie notice and privacy settings. Required storage access is based on Section 25(2) of the German Telecommunications and Telemedia Data Protection Act (TDDDG); optional access is based on Section 25(1) TDDDG and the related processing on Article 6(1)(a) GDPR.

6. Vebelio AI / OpenAI

When you use AI features, your input, selected attachments and the access-authorized context required for the feature may be sent to OpenAI. Do not enter unnecessary sensitive data or data about third parties obtained without authorisation. The implementation uses the OpenAI API; disabling storage of an API response does not promise that the provider retains no security or operational data.

Conversations may also be stored in your platform account. Processing for the requested feature is based on Article 6(1)(b) GDPR; separate optional personalisation follows your choice. AI results may be incorrect and do not replace professional or legal review.

OpenAI processing may take place outside the European Economic Area. Provider information: <https://openai.com/policies/privacy-policy/>

7. Videos, live calls and recordings

Loading YouTube embeds may transmit data to Google Ireland Limited and affiliated companies, including IP address, device information and the page visited. Follow the consent and loading notices shown by the player. Privacy information: <https://policies.google.com/privacy>

Vebelio Meet uses Jitsi technology at meet.vebelio.com. Participation involves processing technically necessary connection data and any audio, video, chat or screen content you choose to share, which is transmitted to participating users. The use of Jitsi software alone does not mean that an external public Jitsi service receives your data.

Live calls may be recorded. The relevant organiser must inform participants before the call about the recording, purpose, recipients and retention period and obtain any required consent. Participation alone is not blanket consent to recording or publication. The identified organiser is responsible for their own recordings and sharing. Further publication requires an appropriate legal basis.

8. Recipients and international transfers

Data may be disclosed to authorised companies and participants, technical processors, payment providers and public authorities where legally required. Public content is visible to the audience selected by you or the provider. Consider this before posting content.

Transfers outside the European Economic Area must meet Articles 44 et seq. GDPR. Possible safeguards include an adequacy decision or appropriate safeguards such as EU standard contractual clauses with supplementary measures where necessary. Naming a provider does not confirm a specific certification. You may request information about the safeguards used in your case from our data-protection contact.

9. Retention and deletion

We retain personal data only as long as required for the relevant purpose, statutory duties or the protection of specific claims. Once the purpose ends, data is deleted or anonymised unless an exception applies.

Account data is processed while you use the service. When you request deletion, related contracts and retention obligations are reviewed. Booking and legal records therefore cannot always be removed together with the profile. In Germany, invoices and booking records are generally subject to eight-year retention periods, certain tax records to ten-year periods and commercial correspondence to six-year periods, subject to the applicable legal requirements. Necessary legal evidence remains for the relevant evidentiary and limitation periods.

The platform is configured to clean up optional activity data after 90 days by default. Files logically deleted from storage are physically removed by the existing cleanup process no earlier than 30 days later. Availability may end earlier. Backups and legally retained data are handled separately.

Recordings and AI histories are not deleted solely because cookie consent expires. The period stated for the specific offer applies to recordings; retention must end when there is no continuing purpose. For access or deletion requests concerning an offer, contact the offer controller or our data-protection contact.

10. Your rights

Subject to statutory requirements, you have rights of access, rectification, erasure, restriction of processing and data portability. You may withdraw consent at any time with effect for the future. You may object to

processing based on legitimate interests for reasons arising from your particular situation, and you may object to direct marketing at any time.

You may lodge a complaint with a data-protection supervisory authority, in particular in your place of residence, work or the alleged infringement. For the operator in Schleswig-Holstein, the Independent State Centre for Data Protection Schleswig-Holstein is a contact point: <https://www.datenschutzzentrum.de/>

11. Minors

The platform is not generally restricted to adults. Rules on legal capacity and parental consent still apply. Where an information-society service is directly offered to children and processing relies on consent, the required consent of a parent or guardian must be considered for persons under 16 in Germany. Individual offers may have additional objectively justified age requirements.

12. Versions and changes

The version, amendment date and, where applicable, effective date are shown on the document. Material changes are published as a new version. Required new consents are not inferred from earlier consents. Earlier versions of documented contract or consent records remain traceable.