

# Privacy Policy

## I. Introduction

We are aware of the trust you are placing in us. Therefore, we would like to provide comprehensive information to you on how we handle your personal data at AQ Green TeC GmbH. In particular, we would like to inform you about what data we collect when you use our application (in the following “**App**”) and how we use this data. If we have received personal data from you via other communication channels (e.g., by email), the following Privacy Policy also applies.

Given that our App and the technologies on which it is based, as well as our business processes are subject to continuous development, the Privacy Policy may need to be changed too. All future changes will be published here.

## II. Use of the App and data protection

### 1. Name and contact data of the controller of the App

We, AQ Green TeC GmbH, represented by the managing directors David Grundlingh and Jost Rodewald with seat in Neuer Wall 63, 20354 Hamburg, Germany as the provider of this App, are the controller within the meaning of Art. 4 no. 7 GDPR.

### 2. Contact data of the data protection officer

AQ Green TeC GmbH is partner of Aquila Capital (meaning Aquila Capital Holding GmbH and its affiliated companies in the sense of §§ 15 et seq. German Stock Corporation Act (AktG)). The data protection officer of Aquila Capital can be reached as follows:

Aquila Capital Holding GmbH  
c/o the data protection officer  
Valentinskamp 70, 20355 Hamburg  
[DSGVO@aquila-capital.com](mailto:DSGVO@aquila-capital.com),

### 3. Automatic data processing during App use

#### a. Log files when using our App

If you download our App via an app store, the required information is transferred to the app store, i.e. in particular username, email address and customer number of your account, time of download, payment information and the individual device identification number. We have no influence on this data collection and are not responsible for it. We only process the data insofar as it is necessary for downloading the App to your mobile device.

If you wish to use our App, we collect the following data that is technically necessary for us to offer you the functions of our App and to ensure stability and security:

That data is:

1. Date and time of your request
2. Duration of your visit
3. Time zone difference compared to Greenwich Mean Time (GMT)
4. Content of the request (specific page)
5. Access status/HTTP status code
6. IP address used (if applicable: in anonymised form)
7. Device Operating Systems (Android or iOS)

#### **aa. Purpose and legal basis of data processing**

We process data related to the end device, in order to create use statistics, for example, or to identify and trace unauthorised attempts to access our web servers. We only create profiles regarding the use of our App in anonymised form and only to improve user navigation and optimise our services. Our legitimate interest in data processing pursuant to Art. 6 para. 1 sentence 1 lit. f GDPR also lies in these purposes. We do not create or process behaviour profiles relating to a specific person from the aforementioned information.

#### **bb. Duration of data storage**

The data will be deleted as soon as they are no longer necessary to achieve the purpose for which they were collected. In the case of the collection of data for the provision of the App, this is the case when the respective session has ended.

#### **b. Firebase by Google**

We use the Firebase service from Google LLC (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA) in order to derive application behavioural analytics. We use that information to see how users interact with our App. Firebase is part of the Google Cloud Platform and offers numerous services for developers. A list can be found here: <https://firebase.google.com/terms/>.

Currently, we use the following Firebase service:

#### **Google Analytics for Firebase**

The App uses a cookie-like token (Instance ID) to recognize the device at Firebase Analytics and to enable an analysis of your usage behaviour only with your prior consent to do so. The token is unique to the App and not retained on reinstalling the App or resetting the mobile device. We have disabled collection of Advertising IDs and Identifiers, so that persistent, a cross-app and cross-device recognition is not possible. **The information about app usage gathered by means of the Instance ID is sent to Google's servers in the USA.** The IP address used during use is shortened before leaving the EU or the EEA. Only in exceptional cases does this reduction take place in the USA. The IP address transmitted by the App is not linked to any other data at Google. Google will use this data to analyze app usage on behalf of AQ Green TeC GmbH, and compile reports for AQ Green TeC GmbH. These reports are anonymised. Therefore, they do not contain personal data and do not allow the identification of individual users. Instead, the data is aggregated over all users. These reports include, for example, the

frequency of use, the place of use and the content viewed. With the help of these reports, we can improve our product quality.

The legal basis for the use of Firebase Analytics is Art. 6 para. 1 sentence 1 lit a. GDPR. The collected data will be deleted after 2 months.

The analysis of your user data is only carried out if you have given your consent in advance to do so. You can also opt-out of the analysis of your user data at any time by deactivating the “Analytics” settings in the app. This prevents the future collection of your data and sending it to Google. You will need to disable this setting on all devices on which you use the App.

### **Firestore Crashlytics**

Only with your prior consent, we are using “Firestore Crashlytics” for crash reporting’s, which sends the aforementioned Instance ID when using the App. When a crash occurs, the App will also send crash reports to Google’s servers to help us improve the quality of the app by being able to in-depth analyze crashes of the app.

The legal basis for the use of Firestore Crashlytics is Art. 6 para.1 sentence 1 lit. a GDPR. The collected data will be deleted after 90 days. Further information and Google’s and Firestore’s current privacy policy can be found at <https://policies.google.com/privacy?gl=de>; <https://firebase.google.com/support/privacy>

The analysis of your crash report is only carried out if you have given your consent in advance to do so. You can also opt-out of the analysis of your crash report data at any time by deactivating the “Performance Tracking” settings in the app. This prevents the future submission of your crash report and sending it to Google. You will need to disable this setting on all devices on which you use the App.

### **c. Sentry**

We use Sentry to improve the technical stability of our service by monitoring system stability and identifying code errors. By using Sentry, information about your use of this service may be transmitted to a server of Sentry (Functional Software Inc., Sentry, 132 Hawthorne Street, San Francisco, California 94107, USA.). Processed data are usage data, metadata (device ID, device data, IP address and others if applicable). Sentry serves these purposes alone. The Sentry privacy policy can be found at <https://sentry.io/privacy/>. Our Use of Sentry is based on a legitimate interest pursuant to Art. 6 para. 1 sentence 1 lit. f GDPR, which is not opposed by any overriding interest or right of the user.

## **4. Processing of personal data during the use of our App features**

We process personal data when you use our App features. The following data processing activities are considered in this context:

### **a. Contact by e-mail**

Data transmitted by contacting us at support@aq-green.com will be stored in order to be able to process your request or to be available for follow-up questions (Art. 6 para. 1 sentence 1 lit. b GDPR). This data will not be passed on without your consent. The data will be stored until you request us to delete it or until there is no longer any need to store the data. Mandatory legal provisions - in particular retention periods - remain unaffected.

### **b. Registration in the App**

You can register in our App by providing personal data. The personal data processed for registration is specified in the input mask used for registration. Next to this we process sign-up/registration date, last login date & time, last logout date & time.

We use the so-called double-opt-in procedure for registration, i.e. your registration is only completed when you have previously confirmed your registration via a confirmation e-mail sent to you for this purpose by clicking on the link contained therein. The provision of the aforementioned data is mandatory.

### **c. Footprint Calculator**

In order for us to provide you with information on your carbon footprint, we ask a number of questions about your lifestyle. This data that you create within the App is transmitted securely on our cloud servers. We do not share the information with anybody outside of the Aquila Capital and you need to be logged into your account to access this data.

This data is stored by us for 365 days after the account has been inactive and is then irrevocably deleted. The data processing is carried out in accordance with Art. 6 para. 1 sentence 1 lit. a GDPR.

The calculator or parts of the calculator will also be available on the webpages of our corporate partners. All the data you enter in this context is processed by our corporate partners as controllers in the sense of Art. 4 no.7 GDPR.

### **d. Redemption or referral Code**

If you have received a redemption or referral code from one of our corporate partners which is valid for offsetting a pre-agreed amount of CO<sub>2</sub>e and you enter this code after registration in the App, we receive the personal data contained in the code. These are your calculated CO<sub>2</sub>e emissions and, if applicable, the data on which the calculation is based.

### **e. Data processing for the execution of contracts**

For the purpose of concluding contracts with you, we process the personal data provided by you that is required for the initiation of this contract and for its execution as well as, if applicable, for the provision of warranty services or for the reversal of the contract (Art. 6 para. 1 sentence 1 lit. b GDPR). The processed data include first name, last name, email address, your stripe subscription ID and the amount that will be paid for the subscription as well as the date of your subscription. Furthermore, we are also storing the portfolio that you as the user will offset against (all portfolios consist of projects). Furthermore, your technical connection data is collected during the electronic ordering process.

In order to process contracts concluded via the App, we work together with the service provider Stripe who support us in whole or in part in the performance of concluded contracts. Certain personal data is transmitted to Stripe in accordance with the following information.

### **Stripe**

If you choose a payment method from the payment service provider Stripe, the payment will be processed via the payment service provider Stripe Payments Europe Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Ireland, to whom we will pass on the information you provided during the payment process in accordance with Art. 6 para 1. sentence 1 lit. b GDPR. Your data will only be passed on for the purpose of payment processing with the payment service provider Stripe Payments Europe Ltd. and only insofar as it is necessary for this purpose. You can find more information about Stripe's data protection at the URL <https://stripe.com/privacy-center/legal>. You can find full and up-to-date information on Stripe's data retention policy here: <https://support.stripe.com/questions/data-retention-policy>

## **5. Transfer of your personal information to third parties**

To facilitate the purposes described we may transfer your personal data to commissioned service providers in Germany and abroad if this is necessary for economic or technical reasons.

For this purpose, we will carefully select the respective service provider, agree on a contract for data processing with them in accordance with Art. 28 GDPR and carefully monitor them. Disclosure of data may be considered in the following cases

### **aa. Payment service provider**

Please see under clause 4 e. the information about the payment service provider we are working with.

### **bb. Disclosure of data within Aquila Capital**

Due to the group structure of the Aquila Capital, it may be, or become, necessary to transfer your data to another entity within Aquila Capital. In these cases, the personal data will only be transferred if there is a legitimate interest of the concerned Aquila company and if the interests or fundamental rights and freedoms of the person concerned do not outweigh Aquila's interests, Art. 6 para. 1 sentence 1 lit. f GDPR.

### **cc. Disclosure of data to the corporate partners of the redemption and referral codes**

If you received a redemption or referral code (see clause 7 of the Terms of Service) from our corporate partners and redeem it in the App, our corporate partner will be informed that you have used the code. In case of the use of a referral code the partner will also be informed if you purchase the pre-set amount of carbon offsets via the App.

## **6. Data security, TLS encryption with https**

AQ Green TeC GmbH takes diligent precautions to protect your data managed by us against manipulations, loss, destruction and against access by unauthorised persons. We continuously

improve our security measures in accordance with the development of technology. Our employees are obligated to maintain data confidentiality in accordance with the provisions of the GDPR.

We use https to transmit data in a tap-proof manner on the Internet (data protection through technology design Art. 25 para 1 GDPR). Using TLS (Transport Layer Security), an encryption protocol for secure data transmission on the Internet, we can ensure the protection of confidential data. You can recognize the use of this data transmission security by the small lock symbol in the upper left corner of the browser and the use of the https scheme (instead of http) as part of our Internet address.

## 7. Your rights

You have the following rights with respect to your personal data:

- right of access  
You have the right to request information about your personal data processed by the controller. In particular, about the purposes of processing, the categories of personal data and about recipients or categories of recipients to whom the personal data have been disclosed. Furthermore, you have the right to obtain information about the planned duration of storage.
- right to rectification or erasure.  
You have the right to request the correction of incorrect data or the completion of your personal data stored by the controller without delay. You have the right to request the erasure of your data under the conditions specified in Art. 17 GDPR.
- right to restriction of processing.  
In specific cases set out in the GDPR, you have the right to request the restriction of the processing of your personal data.
- right to withdraw the consent  
Insofar as we process your data on the basis of your consent you have the right to revoke this consent at any time with effect for the future, without this affecting the lawfulness of the consent valid until then. The revocation is - like the granting of consent itself - possible orally or in text form.
- right to object to processing.  
**Insofar as personal data are processed based on legitimate interests pursuant to Art. 6 para. 1 sentence 1 lit. f GDPR, you have the right to object to the processing of your personal data, insofar as there are grounds for doing so that arise from your particular situation.**
- right to data portability  
In specific cases set out in the GDPR, you have the right to receive and transfer all personal data concerning you to another controller (right to data portability).

You can contact us or our data protection officer to assert your rights (for contact details see II. Clause 1 and 2).

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