Trade Republic Privacy Notice - Website

Current version: 22.03.2024

1. Privacy Notice

We, Trade Republic Bank GmbH and all its affiliated companies (hereinafter "**Trade Republic**", or "**we**"), as the operator of the website under https://www.traderepublic.com as well as other subdomains to this domain (also "**website**") are **responsible data controllers** for the processing of the personal data of the user ("**you**") undertaken within the context of this website, within the scope of applicable data protection law, in particular the General Data Protection Regulation ("GDPR") and the (German) Federal Data Protection Act (*Bundesdatenschutzgesetz*).

This privacy notice describes the processing activities of personal data we perform in the context of your visit to our website, within the scope of our information obligations (Art. 13 et seq. GDPR) ("**Privacy Notice**").

In addition, we provide information on the types of Personal Data we collect, how we use the information, with whom we may share it and the choices available to you regarding our use of the information. We also describe the measures we take to protect the security of the information and how you can contact us about our privacy practices.

This Privacy Notice may be updated periodically and without prior notice to you to reflect changes in our Personal Data practices. We will post the updated version on the Website and indicate at the top of the Privacy Notice when it was most recently updated. We encourage you to review this privacy notice from time to time to gain information about the latest updates.

2. Information about the data controller

Trade Republic Bank GmbH
Brunnenstr. 19-21
10119 Berlin
Germany

E-Mail: service-it@traderepublic.com

3. Data Protection Officer

We have appointed a Data Protection Officer. They can be reached via the following contact details:

Trade Republic Bank GmbH
– Datenschutz –
Brunnenstr. 19-21
10119 Berlin
Germany

E-Mail: dataprotection@traderepublic.com

4. Processing of your personal data

We want to be transparent with our visitors and users: we would like to point out that we may use service providers with whom we have concluded order processing contracts when processing your personal data. If processors carry out data processing in a third country (not within the EU), we ensure that the level of protection of your data guaranteed by the GDPR is not undermined (Ch. 5 GDPR).

In this Privacy Notice, we describe the individual processing operations systematically and individually. This means that the website is first described, followed by the individual processing activities which might take place in the context of your use of our website. In each section, we describe the processing activity and scope of the processing, describe the purpose of the processing and the legal basis, and finally share how long we store this data. If we are not able to specify an exact retention period - because it depends on a variety of factors – then we will at least inform you about how the applied retention period is assessed. It may happen that processing is mandatory for a legal requirement or for the opening of a deposit ("conclusion of contract"). Should this be the case, we expressly point this out within this Privacy Notice.

Without the processing activities performed under the grounds of a contractual obligation or entry into a contractual obligation (art. 6 (1) lit. b GDPR) or fulfilment of a legal requirement (art. 6 (1) lit. c GDPR), you will not be able to become our customer, unfortunately.

Insofar as we use service providers who carry out this processing for us and on our instructions (so-called order processing), we represent this within the processing activity, so that you know exactly for which process which service provider is used. These are usually technical service providers who, for example, organise the e-mail dispatch or host our website.

a. Data Hosting

Publishing a website involves a great deal of data production and collection. The data can range from sole connection data and log files, to event-triggered data, to even the data necessary for fulfilling your requests while you make use of our web trading application. Some of this data can be classified as personal data, in accordance with the definition provided in art. 4 (1) GDPR.

We store all information, not restricted to sole personal information, which is necessary for providing the website, as well as fulfilling all your requests and orders which you provide through our website. All stored information reaches the hosting servers not before being first pseudonymised by us by means of hashing methods. Moreover, the collected data is then "structurised", which means that it is saved in a manner which makes it available for us to fulfil our processes and obligations towards you and the law.

The applicable retention periods, purposes, scopes and legal basis for each processing activity are detailed in the following sections of this Privacy Notice.

The data hosting and structuring activities themselves are based on our legitimate interest, art. 6 (1) lit. f GDPR, of being able to provide our services while maintaining the highest level of security available for us. Without such processing activity, neither our products and services, nor the website itself, can be provided.

Service providers, appropriate safeguards for third country transfer

All data mentioned above is hosted in data centres built with state-of-the-art security standards and measures applied. The data hosting is provided by Amazon Web Services ("**AWS**"), a service of Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855

Luxembourg, Luxembourg, an affiliated company of Amazon Web Services, Inc., P. O. Box 81226, Seattle, WA 98108-1226, USA.

The data centre provided by AWS which we solely use is located in Germany (Frankfurt/Main) and is certified according to ISO 27001, 27017 and 27018 as well as PCI DSS Level 1, therefore meeting the highest security standards.

For structuring the collected information in a legible manner we use the services provided by Snowflake Computing Netherlands B.V., FOZ Building, Gustav Mahlerlaan 300-314, 1082 ME Amsterdam ("**Snowflake**"). Snowflake receives all the data received beforehand by AWS, still pseudonymised.

Both AWS and Snowflake potentially transfer personal data to a third country in the context of providing their services. For more information about such transfers, scroll down to section **5.** of this Privacy Notice.

b. Informational use of our website

aa. Log files

When you visit our website, so-called **log files** are collected by our system **automatically**. This is done directly by the web server that provides the website.

The following personal data are processed automatically in the log files:

- IP address of the requesting computer
- Type of Internet browser used
- Language of the Internet browser used
- Version of the Internet browser used
- Operating system and its version
- Date and time of visit
- Time zone difference to Greenwich Mean Time (GMT)
- Access status / http status code
- Amount of data transferred
- Accessed website
- Referrer
- Websites accessed by the visitor's system through our website
- User's Internet service Provider

The log files therefore contain the personal data mentioned above, but may not necessarily contain all of them. However, we only store your data temporarily and in particular not together

with other personal data, such as your customer data, should you already be a customer with us.

For the provision of our website, the processing of the above-mentioned data is technically necessary. We also store the data for the purpose of the security of our information technology systems and to prevent attacks. For these purposes, the **legal basis** for the processing of personal data regarding you is our legitimate interest, pursuant to Art. 6 (1) lit. f GDPR. The log files will be deleted or anonymized immediately when they are no longer necessary to achieve the aforementioned purposes, at the latest after 14 months The retention period is set to this time in order to be able to conduct forensics investigations and generally improve the security and stability of our website.

Service provider, appropriate safeguards for third country transfer

We use AWS services for storing this information.

bb. Website content

We perform a few activities within our website in order to determine the content shown to each visitor.

Your country settings are saved via session based cookies, which means that they are deleted immediately, once your browsing session is over. Meanwhile, your language settings are saved in the same way for an entire year, after which it is deleted (unless you delete all cookies from your browser, of course).

The lawful basis of processing for these cookies is legitimate interest, Art. 6 (1) lit. f GDPR. It is our legitimate interest to provide you with a service which is as relevant as possible to you by showing you the correct website content.

cc. Contentful

We work with a content management platform, to manage the content on our website (including text, images, videos, etc.). This content is made available on our website via CDN-Content Delivery Network.

In order to provide content on our Website, we use the service Contentful from Contentful GmbH, Max-Urich-Straße 3, 13355 Berlin, Germany (“**Contentful**”).

The legal basis for data processing through Contentful is Art. 6 (1) lit. f GDPR (legitimate interest). It is our legitimate interest to offer you a website with appealing features, content and flow, as well as to make the information contained in our website easy to read and access.

dd. DataDog

We use the analysis technology of Datadog from DataDog, Inc., 620 8th Avenue, 45th Floor, New York, NY 10018, USA ("**Datadog**").

This tool sets up a cookie to the browser session and collects geolocation, user's device and operating system data. DataDog collects information about the performance of our own website and reports any arising technical issues, so that we may swiftly act accordingly. This impacts the confidentiality in our product, as such monitoring is crucial for enabling you to securely perform and order transactions in our app without threat of wrongfully repeated or cancelled requests, for example.

The security of our platforms are extremely important for the secure provision of our services, without which there would be a higher risk of damages for our customers. It is our legitimate interest to maintain such security to the highest standard. Our lawful basis for processing resides in Art. 6 (1) lit. f GDPR.

The data collected through the cookie set up in your browser session is saved for a period of 15 minutes, after which it is automatically deleted.

We also use Datadog as our main security monitoring dashboard, through which we retain and are able to monitor all event logs throughout our website. The purpose of the log retention in Datadog is to enable constant monitoring of the security and performance of the website, in order to quickly recognise possible cyberattacks and swiftly act accordingly, all in the interest of maintaining a safe and stable visiting experience for our website visitors and customers. The collected data logs are retained for a maximum of 90 days, after which they are sent to our servers (AWS see the "Data hosting" section above), and deleted from the Datadog monitoring platform.

The data collected by this tracking activity may be sent to the DataDog servers located in the EU and United States. For more information about transfers of personal data to a third country, such as the United States, and how these transfers are regulated under GDPR, scroll down to section 5. of this Privacy Notice.

ee. Myra Security - DDoS monitoring

We use the services provided by Myra Security GmbH, Landsberger Str. 187, 80687 Munich, Germany ("**Myra**"), for monitoring the website and other access points to our servers against distributed denial of service (DDoS) attack attempts. Myra offers its services by analysing web traffic in real time, filtering out harmful data streams automatically. In doing so, Myra collects logs which include a website visitor's IP address and metadata related to the visit (such as date and time of web request, action requested etc.).

A DDoS is potentially hazardous for our website and our entire IT infrastructure, which would, in turn, potentially damage our own customers. For this reason, the continuous monitoring against DDoS attacks is one of the fundamental aspects of security within Trade Republic. It is our legitimate interest to maintain such security to the highest standard. Our lawful basis for processing resides in Art. 6 (1) lit. f GDPR.

The security logs collected by Myra are stored for one year since collection, after which they are automatically and permanently deleted.

More information regarding Myra's privacy policy can be found on their website, here.

ff. Customer referral program

We offer referral programs to our existing customers consisting in the referral of our services to 3rd individuals (e.g. friends, family etc.) who are not customers. If those individuals successfully set up an account at Trade Republic through a referral program, we offer a specific service to the referring customer.

In order to successfully run the program, we use the analysis technology "Adjust" of adjust GmbH, Saarbrücker Str. 37A, 10405 Berlin ("**Adjust**").

As already in our mobile app, Adjust is also used on our website in a similar way. It is not a conventional cookie, but rather a so-called "Software Development Kit" - or "SDK" in short - in this case designed for web use, which are essentially program kits built in our very own interface.

We use Adjust to track whether a new customer has created an account at Trade Republic due to our referral program.

The legal basis for data processing performed through Adjust is Art. 6 (1) lit. b GDPR (performance of the contractual obligations in the context of the customer referral program). Without this processing activity, we would not be able to track the individuals that would benefit from the customer referral program.

c. Contacting us

Description, scope, purpose, legal basis and retention period

You can contact us electronically, e.g. by sending an email to one of the e-mail addresses we have provided or by filling one of the contact forms we make available on the Website. In these cases, we process the personal data contained in your communication to us, such as the e-mail address or your name. **We highly recommend you to not include any personal data which is unnecessary for the purpose of the request!** Never forget that an email is a postcard on the Internet and could theoretically be read by third parties, as an e-mail is generally not encrypted.

If you are already our customer or are undergoing the procedure necessary for becoming our customer, and you contact us for support, the legal basis of this processing activity shall be the act of fulfilling or performance of an act leading to the entry of a contractual obligation, in accordance with Art. 6 (1) lit. b GDPR. Due to legal obligation, the personal data processed under this legal basis is retained for 5 years after the termination of your account in Trade Republic (and we would be saddened to see you go as a customer!). Without this processing activity we would not be able to provide you with support for your inquiries.

If you contact us in any scenario other than the one mentioned just above, the legal basis for this processing activity shall be Art. 6 (1) lit. f GDPR (legitimate interest). We have a legitimate interest in processing this data in order to be able to respond to you at all or to address you correctly and to prevent abuse. For this legal basis, we delete the personal data received through your contact as soon as they are no longer necessary for the achievement of the purpose. This is usually the case when the respective conversation has ended. We assume the conversation ends, when it can be inferred from the circumstances that the matter in question has been conclusively clarified. Of course, we limit the processing of personal data to what is necessary.

There may be longer retention periods applicable to the responses we provide, insofar as these responses have commercial or tax-related content. Here, the legal retention period may go up to 10 years.

Service providers, appropriate safeguards for third country transfer, if applicable

aa. TRS

We use the services provided to us by our subsidiary company, the Trade Republic Service GmbH, Brunnenstr. 19-21, 10119 Berlin, Germany ("**TRS**"). TRS takes care of all matters relating to customer services for Trade Republic: in doing so, TRS has access to all information relevant to satisfy your request, limited to the extent necessary.

Further information regarding the data processing activities we perform for processing support requests can be found in the privacy notice for customer support, which we present the moment a support request is initiated.

bb. Zendesk

We use the ticket system Zendesk, a customer service platform of Zendesk Inc, 989 Market Street #300, San Francisco, CA 94102, United States, ("**Zendesk**") to process customer requests. We have entered into a processing agreement with Zendesk that governs the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects, and our obligations and rights. Zendesk will only process your personal data on our instructions. Zendesk guarantees all necessary technical and organizational measures to ensure security of your personal data appropriate to the risk.

Zendesk potentially transfers personal data to a third country in the context of providing its services. For more information about such transfers, scroll down to section 5. of this Privacy Notice.Further information can be found under: https://www.zendesk.com/company/agreements-and-terms/privacy-policy/ at the service provider directly (last retrieved on: 11.10.2021).

d. Communicating with you

aa. Customer data platform

We have set up a customer data platform ("**CDP**"), with which we are able to automise all our communications and the initiation of workflows, depending on the events users trigger with the

use of our web trading application (for further details on the web trading application available through our website, please scroll down to "**g. Web Trading**" in this Privacy Notice). These events include, not only the sheer events triggered within the app, such as going from one screen to another, but also, if you are our customer, your trading activity and related information, as well as the personal data associated with your Trade Republic account.

All personal data that enters our CDP is pseudonymised beforehand with hashing techniques. This enables us to initiate the necessary event-dependent workflows with the sole strictly necessary information.

The legal basis of processing for this activity is art. 6 (1) lit. f GDPR (legitimate interest), on the basis of our interest of not only being able to reliably provide communications in a timely manner to each customer, but also provide potentially interesting information to our customers and onboarding prospects. An example would be automatically providing valuable information for requesting support, in case a prospective customer encounters difficulties during the onboarding procedure. An additional benefit, which also is one of our legitimate interests, is to enable a much more efficient and error-prone procedure for customers and prospective customers alike to see their data subject requests fulfilled in a timely and complete manner.

You may object to this processing at any time for reasons arising from your particular situation, as is further detailed below in this notice (scroll down to Section 6. of this Privacy Notice).

We retain personal data in our customer data platform for the sole duration of our customer relationship with you. After termination, personal data associated with you is automatically and permanently deleted from the CDP. If you are not a customer of Trade Republic, the personal data linkable to you is automatically and permanently deleted after a period of time between three (3) and six (6) months since its collection, unless retention periods determined by law apply.

Service provider, appropriate safeguards for third country transfer, if applicable

Our CDP is provided by mParticle, Inc., 257 Park Avenue South, Floor 9, New York, NY 10010, United States ("**mParticle**"). For the processing of personal information, mParticle has agreed a data processing agreement: in such agreement, mParticle has agreed to solely store and otherwise process personal data on our behalf through servers located within the EU.

It is still possible that, in the context of the processing activities performed on our behalf, mParticle transfers data to or accesses data from a third country which does not guarantee the same standard of protection for personal information as in the EU. More information about our contractual setup and further measures implemented with mParticle for the safe processing of personal data can be found below, on Section **5.** of this Notice.

bb. Email delivery

Description, scope, purpose, legal basis and retention period

For sending emails, we use the SendGrid service (**"SendGrid**") provided by Twilio Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105, United States, and the services provided by Braze Inc., 318 West 39th Street, 5th Floor, New York 10018, USA ("Braze").

The sending of e-mails is organised and analysed by these service providers. This makes it possible to determine whether an email has been opened or not.

For this purpose, SendGrid and Braze use so-called "webbeacons". This is a reference to a small graphic that is embedded in the text of the e-mail, but is so small that it is not seen. Most of the time it is simply transparent. When you open the email, your email program calls up this graphic from SendGrid and Braze's web servers. Just like when you visit a website, the web servers now store from where the graphic was accessed and can therefore determine that you have viewed and read this email. SendGrid collects the following data:

- IP address;
- date of last profile update;
- geolocation and time zone;
- language information of the browser.

The data processing of the mere sending of emails takes place for the purpose of communicating with you. Data processing for analysis is carried out to ensure effective communication: in such a way, we are able to guarantee that emails reach you and do not end up in data nirvana. This is useful, for example, to ensure that transactional emails, such as registrations, are delivered. We also use this to determine which emails are really of interest to you as a customer. A simple example: If we determine that some information is not being read, then we try to improve and adapt our information so that it really interests you as a customer.

We base this data processing of the email analysis on our legitimate interest, which also results from the purpose. The legal basis is Art. 6 (1) lit. f GDPR. If the email we send you has content of contractual nature, the legal basis of processing shall be the performance of the contract, pursuant to Art. 6 (1) lit. b GDPR. Without the possibility of providing you with this information we would not be able to fulfil our contractual obligations towards you as a customer.

You can find information on the retention period under the heading "**Contacting us**".

Service provider on behalf, appropriate safeguards for third country transfer

We have entered into processing agreements with SendGrid and Braze, that govern the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects, and our obligations and rights. SendGrid and Braze process your personal data only on our instructions. SendGrid and Braze guarantee all necessary technical and organisational measures to ensure security of your personal data appropriate to the risk.

SendGrid potentially transfers personal data to a third country in the context of providing its services. For more information about such transfers, scroll down to section **5.** of this Privacy Notice.

More information on this service provider's data processing can be found at SendGrid's (last verified on 13.06.2022) and Braze's (last verified on 13.06.2022) privacy notices.

Right to Object

You can easily prevent the analysis of the email by disabling the reloading of external sources in your email program - see the instructions of your email program. You can stop receiving emails which are not necessary for your contractual relationship with us by clicking the "**unsubscribe**" link at the bottom of each email and thus exercising your right to object. You can also send us an email at dataprotection@traderepublic.com to unsubscribe from the mailing list.

You will not receive any further emails from us after you unsubscribe, which we understand, even though it is very unfortunate. Please note: **necessary** emails that we need to send to you as part of the contractual relationship will continue to be sent to you despite unsubscribing. We call these emails "transactional" emails.

e. Customer surveys

Description, scope, purpose, legal basis and retention period

In order to align and improve our offering to the needs of our customers, we send out surveys from time to time to collect feedback on different topics by using the services offered by zenloop GmbH, Pappelallee 78/79, 10437 Berlin ("**Zenloop**").

Legal basis for sending you the surveys is our legitimate interest, pursuant to Art. 6 (1) lit. f GDPR, in conducting customer surveys, in order to improve our offer.

Of course, you don't have to take part in a survey. If you choose to take part in the survey, the data below will be processed.

When you use the feedback tool Zenloop collects public IP addresses, device and browser data, and the website from which you use the feedback platform. Zenloop also uses cookies and similar technologies to collect aggregate data about users. In addition, Zenloop collects your survey responses.

Since the choice for taking part of the survey remains to you, the legal basis of processing of the conducted survey is your consent, Art. 6 (1) lit. a GDPR.

We delete this data after the processing purpose has been fulfilled. This will usually be at the end of the survey and after we have drawn our necessary conclusions from the survey.

Appropriate safeguards for third country transfer

We have entered into an order processing agreement with zenloop in accordance with Art. 28 (3) GDPR. You can find more information about this in the privacy policy at https://www.zenloop.com/en/legal/privacy.

Zenloop does not send data to third countries in the context of the processing activities performed on our behalf. If a transfer to third countries were to take place through subcontractors of Zenloop, this would only take place on the basis of appropriate safeguards within the meaning of Art. 44 et seq. GDPR.

Right to Object

You may object to this processing at any time for reasons arising from your particular situation. You can find more details under "**Your rights**" in the last section.

f. Opening a customer account with Trade Republic

We appreciate your interest in becoming a customer with us. In the following paragraphs, we describe the process for opening an account via our website and the data processing that takes place, in a transparent manner. As indicated by the lock symbol at the top of your browser bar, the data connection is always encrypted (TLS procedure). There, you should be able to view further technical details, such as the exchanged security keys.

aa. Securities account opening on our website

Description, scope, purpose, legal basis and retention period

You can open a securities account with us on our website by clicking on the “Open a securities account now” button and following the next steps. We will ask you for the following data and process it to open a securities account with us:

- verification code and personal identification number (PIN);
- mobile phone number;
- name (first and last name);
- e-mail address;
- date and place of birth;
- country of origin and address (registration address);
- citizenship(s) and tax liability;
- payment account;
- experience and knowledge of financial instruments;
- your agreement to sole private use of the account, contract documents, escrow account, in-app notifications, and confirmation regarding receipt of information.

The purpose of data processing is the initiation of a customer relationship as well as compliance with legal requirements.

As a regulated entity, we are subject to legal obligations, i.e., statutory requirements (e.g., German Banking Act, German Money Laundering Act, German Securities Trading Act, tax laws) as well as banking supervisory and financial intermediaries requirements (e.g., of the European Central Bank, the European Banking Authority, the Deutsche Bundesbank, and the German Federal Financial Supervisory Authority -BaFin-). These include, in particular, identity and age

checks, fraud and money laundering prevention, and the fulfilment of control and reporting obligations under tax law.

The data processing of this personal data at the opening of the securities account is based on the legal basis Art. 6 (1) lit. b GDPR (initiation of a contractual relationship) and Art. 6 (1) lit. c GDPR (legal obligation to which the controller is subject). Without this processing activity we would not be able to open your account in Trade Republic and, thus, you would not be able to use our products and services.

We only store this data as long as necessary. Once you become our customer, your data remains stored during the term of the customer relationship. In addition, due to legal obligations, it may be necessary for us to store your data beyond the contractual relationship, i.e. beyond the date of termination of the customer relationship.

If, for whichever reason, you don't become a customer, we will store the data collected so far for a period between three (3) and six (6) months after the opening process begins. We may contact you within this period to offer assistance in opening the securities account.

bb. SMS sending

Description, scope, purpose, legal basis and retention period

We use the sending of security codes via SMS to your mobile number as an additional and necessary security feature. Through this additional feature, we secure your access to your depot and pair your terminal device and mobile number with your customer account. When opening the depot, we also make sure that you are not already a customer with us and therefore check whether the mobile number you have specified is not already present in our database – this is by means of a pseudonymised and secure hash algorithm. This also corresponds to the state of the art.

This step only provides for the processing of your mobile number. Depending on the described purpose of the processing, the legal basis of the data processing is either to initiate a contractual relationship or to be able to fulfill our contractual relationship with you pursuant to Art. 6 (1) lit. b GDPR. Without this processing activity we would not be able to open your account in Trade Republic.

If you become our customer, your mobile number will be transferred to the customer database – otherwise you would have to transmit your mobile number to us a second time.

Please see also the previous section for more details. We only store this data as long as we need it. Once you become our customer, your data will remain stored during the term of the customer relationship. In addition, due to legal obligations, it may be necessary for us to store your data beyond the contractual relationship, i.e. beyond the date of termination of the customer relationship.

If, for whichever reason, you don't become a customer, we will store the data collected so far for a period of time between three (3) and six (6) months after the opening process begins, unless retention periods determined by law apply. We may contact you within this period to offer assistance in opening the deposit.

We point out that without entering the mobile number it is not possible to open an account with us. Also, no mobile numbers can be used together for multiple Accounts.

Service providers, appropriate safeguards for third country transfer

For sending the SMS, we use service providers on our behalf, who automatically send the SMS based on our instructions and your input of the mobile number. These are the following service providers:

aaa. Twilio

Twilio Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105 ("**Twilio**") is a company incorporated in the United States. There is therefore a transfer of third party countries. For this purpose, we have concluded a Data Processing Agreement with Twilio.

Twilio potentially transfers personal data to a third country in the context of providing its services. For more information about such transfers, scroll down to section 5. of this Privacy Notice.

bbb. MessageBird

MessageBird B. V., Trompenburgstraat 2C, (1079 TX) Amsterdam ("**MessageBird**"). There is no third-country transfer between Messagebird and us in the context of MessageBird's processing activities done on our behalf. If, on the other hand, a third-country transfer occurs through

subcontractors employed by MessageBird, this will only take place on the basis of suitable guarantees within the meaning of Art. 44 et seq. GDPR. This data transfer obligation is also mandatorily applied by MessageBird in relation to data transfers to its own subprocessors, which might be located in third countries. These obligations are part of the data processing agreement stipulated between us and MessageBird.

The privacy statement, and other details of MessageBird, you can find here: https://www.messagebird.com/en/legal/privacy.

cc. Identification

Description, scope, purpose, legal basis and storage period

In order to facilitate the opening of the account, we offer an possible online identification procedure required in accordance with the Law on the Detection of Profits from Serious Criminal Offences - Money Laundering Act ("GwG") and the interpretative and application information on the Money Laundering Act of the Federal Financial Supervisory Authority ("BaFin").

For the purpose of identification, the personal data you provide (name, date of birth, address, e-mail address, telephone number and desired language) for verification is processed. For the identification procedure, photos of you and your ID document (passport, ID card) are taken via the camera of the customer's device. Finally, the bank account details you provide are processed for verification purposes. The photos of the identification document are then stored to fulfill the identification, enable the account opening and fulfill our retention obligations.

The legal basis for data processing is Art. 6 (1) lit. b and c GDPR (pre-contractual performance and legal obligation) in accordance with the Law on the Detection of profits from Serious Criminal Offences (Money Laundering Act – GwG for short) and laws from other competent authorities.

We would like to point out that it is not possible to become a customer with us without this video identification procedure. Personal identification on site is not possible, nor is sending a copy of an identity document sufficient. The reason for this are the statutory provisions.

Service provider on behalf **–** The online identification procedure is carried out on our behalf by SafeNed-Fourthline B.V., Tesselschadestraat 12 1054 ET, Amsterdam ("**Fourthline**"), a company specialising in this field and an obligated party in accordance with Art. 2, paragraph 1 of the

Directive (EU) 2015/849. Fourthline shall process data on our behalf, thus acting as data processor, mandatorily complying with all applicable data protection regulations.

Fourthline does not save any personal data they process for the purpose of this identification process. On the other hand, we are obliged to and only store this data for as long as necessary in accordance with legal obligations. From the moment you become our customer, your data will remain stored during the term of the customer relationship. The retention period for identification data goes beyond the end of your contractual relationship with us: according to §§ 8, 10 GwG, we are obliged to store the identification data for at least **five years**. This retention obligation only begins with the end of the calendar year in which our customer relationship with you is terminated – therefore, the entire retention period may be longer than five years after the end of the contract.

Fourthline's privacy policy can be found at this link.

g. Web Trading

Within our website, customers have the possibility to log in to their Trade Republic account and carry out certain actions within their Trade Republic account via their computers or other supported devices ("**Web Trading**").

For being able to provide this service, Trade Republic processes information relating to:

- your login information for your Trade Republic account
- your mobile phone number
- securities business, such as your level of knowledge and/or experience with securities, your tax information (e.g. information on church tax liability), and documentation data (e.g. declarations of appropriateness and instructions on corporate actions). All this information is provided by you during your use of Web Trading
- metadata, including your IP address, session data, approx. geographical location.

The purpose of this processing activity is to be able to provide you with the requested services. The legal basis of processing is Art. 6 (1) lit. b GDPR (fulfillment of contractual obligations). Without such information, we would not be able to fulfill your requests. Without this processing activity you would not be able to use our products and services by utilising our web trading application.

We deploy a first-party cookie in order to determine whether Web Trading has been made available in your country. For more information about our implemented cookies please consult this information sheet here.

For logging in onto your Trade Republic account we have set up a two-factor authentication. This security measure involves the processing by us of your login information, as well as your mobile phone number. After you have entered your login information successfully, you will receive an SMS message with a verification code.

Service provider, appropriate safeguards for third country transfer

For sending the SMS, we use **Twilio** and **MessageBird** as service providers on our behalf.

The data is stored in our hosting databases, provided as a service by **AWS**.

We retain the information processed in the context of Web Trading according to the retention periods determined by legal obligations, such as the German Commercial Code (HGB), the German Fiscal Code (AO), the German Banking Act (KWG), the German Money Laundering Act (GwG) and the German Securities Trading Act (WpHG), to which Trade Republic, as a regulated entity, must abide by. The retention periods may vary from a minimum of 2 to a maximum of 10 years. The legal basis of the retention of the personal data for these purposes is Art. 6 (1) lit. c GDPR (legal obligations). Without retaining this data in such a way we would not be able to fulfil our legal obligations and, in turn, we would not be able to provide our products and services to you.

For the same legal purposes, we disclose the personal information processed in the context of your use of Web Trading to public bodies and institutions (e.g. Deutsche Bundesbank, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), European Banking Authority, European Central Bank, financial authorities).

h. Marketing and Tracking

In this section, we inform you about the marketing and analysis processes we intend to use, especially on our website. We perform these tracking activities only after your explicit consent - which you can give in the cookie consent banner, displayed on every first visit of our website. In the default settings, marketing and analytics processing are disabled, you must enable these either individually or together for your consent to be effective. You have the option to give us

consent for **all cookies** by clicking "*Accept all cookies*". You have the option to reject all not "Necessary" cookies, or accept just selected ones by you, by clicking "*Accept Selected Only*". You can find more information about cookies, including their lifespans, by clicking on the Information about our use of cookies link.

You may revoke your consent at any time in the same simple way by accessing our cookie banner again and toggling the settings accordingly in the footer of the webpage.

We encourage you to read all details about the cookies we use and their purpose before you agree. We have put at your disposal a cookie information sheet where we detail all information, including information about the duration of processing, of each tracking tool. Meanwhile, in the following section we describe the individual providers of these services.

In order to maintain an overview, we have divided the individual service providers into "**Marketing**" and "**Analytics**". The marketing tools focus on our own advertising campaigns, while with analytics we have the goal of learning more about our visitors and customers, in order to improve our products or to make advertising more interesting. You can find the exact details at the respective service provider.

Lawfulness of processing

The lawfulness of processing marketing and analytical tracking tools is always based on your consent, thus aligning with Art. 6 (1) lit. a GDPR.

aa. Marketing

aaa. Google Ads

We use the offer of Google Ads Conversion to refer us on other websites with the help of so-called Google Ads, a service provided by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland ("**Google**"). We can determine how successful the individual advertising measures are in relation to the data of the advertising campaigns.

Google delivers this advertising through your own device. For this purpose, we use ad server cookies, through which certain details for measuring success, such as display of the ads or clicks by you and other users, can be measured. If you have reached our website via a Google ad, Google Ads (and not us) will store a cookie on your terminal device. These cookies usually expire after 30 days and are not intended to identify you personally. The unique cookie ID,

number of ad impressions per placement (frequency), last impression (relevant for post-view conversions) and opt-out information (marking that the user no longer wishes to be addressed) are usually stored as analysis values for this cookie.

These cookies enable Google to recognize your internet browser. If a user visits certain pages of the website of an Ads customer and the cookie stored on his computer has not yet expired, Google and the customer can recognize that the user clicked on the ad and was redirected to this page. A different cookie is assigned to each Ads customer. Cookies can therefore not be tracked across Ads customers' websites. Please note that Google may have obtained consent from you for the merging of data, we have no control over this.
We do not collect or process any personal data in the aforementioned advertising measures. We only receive statistical evaluations from Google. Based on these evaluations, we can see which of the advertising measures used are particularly effective.

We do not receive any further data from the use of the advertising media; in particular, we cannot identify users on the basis of this information.

Due to the marketing tools used, your browser automatically establishes a direct connection with the Google server. We have no influence on the scope and further use of the data collected by Google through the use of this tool. Please find below the information we have gathered regarding further uses of the data collected by Google.

Through the integration of Ads Conversion, Google receives the information that you have called up the relevant part of our website or clicked on an ad from us. If you are registered with a Google service, Google can also assign the visit to your account and thus to you personally. Even if you are not registered with Google or are not logged in, it is possible that Google learns your IP address and stores it.

We are aiming to display advertising that is really interesting for you, to make our website more interesting and to determine the costs of advertising in a fairer way.

Google Ads Remarketing

We use the remarketing function within the Google Ads service.

Thanks to the remarketing function, we can present users of our website with advertisements based on their interests on other websites within the Google advertising network (in Google

Search or on YouTube, so-called "Google Ads" or on other websites). For this purpose, the interaction of the users on our website is analyzed, e.g. which offers the user was interested in, in order to be able to display targeted advertising to the users on other sites even after they have visited our website. For this purpose, Google stores a number in the browsers of users who visit certain Google services or websites in the Google display network. This number, known as a "cookie", is used to record the visits of these users. This number is used to uniquely identify a web browser on a specific end device and not to identify a person; personal data is not stored.

Google potentially transfers personal data to a third country in the context of providing its services. For more information about such transfers, scroll down to section 5. of this Privacy Notice.

Conversion API's by Google and Facebook

In order to improve the measurement of successful creations of new Trade Republic accounts as a direct result of Google and Facebook Ads marketing campaigns (so-called "conversions"), we use Conversion API services by Google and Meta Ireland Ltd, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland ("Facebook").

The Conversion API's use server-side tracking to track when a click on an ad does or doesn't result in the creation of a new Trade Republic account. To enhance measurement accuracy, we transfer offline conversion information to both providers. We furthermore utilise the Conversion API's to enable more efficient audience targeting, including the inclusion of users within campaigns as well as ensuring that successfully onboarded customers can be excluded from receiving our ads. Additional personal data such as name, email address, telephone number and home address, may be transmitted to Google and Facebook via a corresponding integration, after their pseudonymisation through a secure hash algorithm.

bbb. Facebook Pixel

We use the re-marketing function "Custom Audiences" of Facebook on our website. Here, a so-called "tracking pixel" and cookies are used.

This allows us to display behavioral advertising ("Facebook Ads") to you via the Facebook social network or other websites. We also use the Facebook service for campaign optimization.

Your browser automatically establishes a connection to the Facebook servers. We have no influence on the data processing at Facebook. According to our knowledge, the following happens at Facebook: Facebook receives the information that you have called up a website from our offer, or clicked on one of our advertisements. If you are a user of the Facebook service, Facebook can also assign this visit to your account. If you do not have a Facebook account or are not logged in, it is still possible that Facebook identifies and assigns you based on your IP address. The information collected via the Pixel can therefore be compiled by Facebook and the information collected in this way can be used by Facebook for its own advertising purposes as well as for advertising purposes of third parties. Thus, Facebook can infer certain interests from your surfing behavior on this website and also use this information to advertise third-party offers. Facebook may also combine the information collected via the Pixel with other information that Facebook has collected about you via other websites and / or in connection with the use of the social network "Facebook", so that a profile about you can be stored at Facebook. This profile can be used for advertising purposes.

Through this data processing, we want to ensure that we only show you advertising that is appropriate to your interests. This also allows us to make our offer more appealing.

Facebook potentially transfers personal data to a third country in the context of providing its services. For more information about such transfers, scroll down to section 5. of this Privacy Notice.You may find more information on how to disable the setting in your Facebook account here: https://www.facebook.com/help/568137493302217.

For more information about Facebook''s data processing, please visit: https://www.facebook.com/about/privacy.

ccc. Linkedin Insight Tag

We use functions of the LinkedIn network. The provider for this is the LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA (“**LinkedIn**”). When a website is called up, a connection to the LinkedIn servers is established. This tells LinkedIn that you have visited this website with your IP address. We have no influence on the further data processing at LinkedIn. If you have a user account with LinkedIn, LinkedIn can also assign your visit to us to this account. If you are not logged in or do not have an account with LinkedIn, LinkedIn can identify and assign you based on your IP address. It also stores whether a customer relationship was successfully established or not and passes this information on to LinkedIn.

LinkedIn potentially transfers personal data to a third country in the context of providing its services. For more information about such transfers, scroll down to section 5. of this Privacy Notice.We use the cookie for the purpose of optimizing our marketing to be able to determine whether users reach us via LinkedIn or not.

Further information about LinkedIn's data privacy policy can be found under: https://www.linkedin.com/legal/privacy-policy.

ddd. Universal Event Tracking (UET) - Microsoft Advertising

Our website uses Microsoft Advertising technologies to collect and store data from which user profiles are created using pseudonyms. This is a service of Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA ("**Microsoft**"). This service allows us to track the activities of users on our website when they have reached our website via ads from Microsoft Advertising. So if you clicked on an advertisement and came to our website, a cookie is set here on your computer. A corresponding UET tag is stored on our website. This is a code used in connection with the cookie to store some data about the use of the website. This includes, among other things, the length of time spent on the website, which areas of the website have been accessed and via which advertisement the users have reached the website. Through tracking, Microsoft Advertising recognizes which campaigns and ads have been successful and applies this information to optimize campaigns, i.e. adjust bids or distribute budgets. In addition, user groups can also be created with the UET Tag, e.g. a group of all users who have been to the website before. This means that advertising is targeted at individual user groups.

The purpose of data processing lies in the effective design of our marketing strategies and advertising campaigns. We use the service to optimize individual campaigns.

These cookies are stored for up to 1 year and 25 days.

You can object here: https://choice.microsoft.com/de-de/opt-out.

More information about Microsoft Advertising's analysis services can be found here: (https://about.ads.microsoft.com/en-us/solutions/audience-targeting/universal-event-tracking)
.

Further information on data protection at Microsoft can be accessed here (https://privacy.microsoft.com/en-GB/privacystatement).

eee. FinanceAds

We work together with "**FinanceAds**", the financeAds GmbH & co. KG Karlstraße 9, 90403 Nürnberg, Germany, to reach via advertising partners, new customers. In this case, the advertising partner receives a commission from us, should you come to us from this advertising partner and become a customer. The industry speaks of Sales and/or Leads. Tracking technologies are used so that the advertising partner can prove to us how many customers they have placed.

These FinanceAds tracking technologies store an identification of the mediating advertising partner as well as the order number of the advertising material clicked by the website visitor. This information is required for payment processing between the website operator and the advertiser. When a transaction is concluded, the partner identification number serves to assign the commission to be paid to the intermediary partner.

Further information on data usage by FinanceAds can be found here: https://www.financeads.net/aboutus/datenschutz/.

fff. Twitter

On our website, we use "**Twitter Analytics**", a service of Twitter International Company, One Cumberland Place, Fenian Street, Dublin 2, D02 AX07 Ireland (hereinafter referred to as: "**Twitter**"). Twitter Analytics stores and processes information about your user behavior on our website. The following data can be processed:

- browser Cookie ID;
- mobile Device ID;
- demographic or interest data;
- viewed content or actions performed on a Website or App.

This allows us to collect behavioral data about you to optimize our campaigns.

Twitter potentially transfers personal data to a third country in the context of providing its services. For more information about such transfers, scroll down to section 5. of this Privacy Notice.Further information can be found under: https://twitter.com/en/privacy,

https://help.twitter.com/en/safety-and-security/data-through-partnerships and https://gdpr.twitter.com/nl.html.

ggg. Adisfaction

We use the services provided by adisfaction GmbH, Haus Meer 2, 40067 Meerbusch, Germany ("**Adisfaction**") for tracking the success of marketing campaigns promoted on our website.

Adisfaction places a tracking pixel, which records the following personal data of the visitor:

- session data (visited web pages, no. of clicks on links involved with the marketing campaign);
- metadata (IP addresses, approximate geolocation, device IDs).

Adisfaction retains this information for 28 days, after which time they are automatically permanently deleted.

This data processing is performed within servers located in the EU.

Further information can be found here: https://www.adisfaction.de/datenschutzerklaerung/.

hhh. Snap

We make use of the "Audience Match" and "Conversion" technologies provided by Snap, Inc., 3000 31st Street, Santa Monica, CA, 90405 USA ("**Snap**") on our website as a remarketing function. This allows us to optimize our advertisements on the Snapchat social network, to display only relevant advertisements there and to measure the success of our advertising campaigns on the Snap social network. Based on your consent, we use corresponding cookies from Snap, which are stored on your device. You can find more details about these cookies in our Cookie Information Sheet.

Through this activity we are able to recognize which visitor was on our website at what time and how they interacted with the website. In addition, Snap may use the collected information for its own advertising purposes as well as for advertising purposes of third parties. Snap may infer certain interests about visitors' browsing behavior and combine it with other information.

We retain the information collected for 13 months.

Snap potentially transfers personal data to a third country in the context of providing its services. For more information about such transfers, scroll down to section 5. of this Privacy Notice.You may find more information on how to disable the setting in your Snap account here: https://support.snapchat.com/en-GB/a/advertising-preferences .

For more information about Snap's data processing for all its activities, please visit: https://snap.com/en-GB/privacy/privacy-policy .

bb. Analytics

aaa. Google Analytics

For the needs-based design of our websites, we create pseudonymous usage profiles with the help of **Google Analytics**, a service provided by **Google**. Google Analytics uses targeting cookies that can be stored on your device and read out by us. In this way, we are able to recognize and count recurring visitors as such and to learn how often our websites have been accessed by different users.

If individual pages of our website are accessed, the following data is stored:

- three bytes of the IP address of the calling system ("anonymizeIP“);
- the website accessed;
- the website from which you accessed the page of our website (referrer);
- the subpages accessed from the page accessed;
- the length of stay on the website;
- the frequency of access to the website.

As shown above, the software is also set so that the IP addresses are not stored completely, but the last part of the address is masked (e.g. 192.168.1.***). In this way, it is no longer possible for you to assign the shortened IP address to the calling computer or terminal device. This website also uses Google Analytics for cross-device analysis of visitor flows, which is carried out via a user ID. If you become a new customer with us and have agreed to the tracking analysis here, then we can also determine from which channel and/or campaign you have found your way to us.

bbb. Google Analytics for Firebase

In the context of processing data in Web Trading, we have implemented the services of Google Analytics for Firebase, a service provided by Google. Google Analytics for Firebase deploys a

software development kit for web ("web SDK") which enables the analysis of the use of the Web Trading web application. This means that information about the use of Web Trading is collected, transmitted to Google and stored in servers managed by Google. For this purpose, end-user device information, IP address, data about the browser used, the operating system used and information on individual requests (events) within Web Trading are processed. The data is used to analyze user behavior and make decisions regarding product and marketing optimization based on the results.

i. Social Media

We do not use social media plugins on our website. If our website contains symbols of social media providers (e.g. Facebook), we only use these for passive linking to the pages of the respective providers.

We maintain publicly accessible profiles on various social networks. Your visit to these profiles sets a variety of data processing operations in motion. Below we give you an overview of which of your personal data is collected, used and stored by us when you visit our profiles.

When you visit our profiles, your personal data is not only collected, used and stored by us, but also by the operators of the respective social network. This also happens if you do not have a profile in the respective social network. The individual data processing operations and their scope differ depending on the operator of the respective social network and they are not necessarily applicable to the processing activities performed by Trade Republic.

Details about the collection and retention of your personal data as well as the type, scope and purpose of their processing by the operator of the respective social network can be found in the data protection declarations of the respective operator:

- the privacy policy for the **Facebook** social network operated by Facebook Ireland Limited, 4 Grand Canal Square, Dublin 2, Ireland, can be viewed here https://www.facebook.com/about/privacy;
- the privacy policy for the social network **Instagram**, which is operated by Instagram LLC, 1601 Willow Road, Menlo Park, CA 94025, USA, can be found at https://help.instagram.com/155833707900388;
- the privacy policy for the social network **YouTube**, which is operated by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, can be found at https://www.gstatic.com/policies/privacy/pdf/20190122/f3294e95/google_privacy_policy_en_eu.pdf;

- the privacy policy for the social network **Twitter**, Twitter Inc., 1355 Market Street, Suite 900, San Francisco, CA 94103, United States, can be found at https://twitter.com/en/privacy.

As the operator of a Facebook fan page (and also a Facebook group), we can only view the information stored in your public Facebook profile, and this only if you have such a profile and are logged into it while you visit our fan page. In addition, Facebook provides us with anonymous usage statistics that we use to improve the user experience when visiting our fan page. We do not have access to the usage data that Facebook collects to compile these statistics. Facebook has committed itself to us to assume the primary responsibility under the GDPR for the processing of this data, to fulfill all obligations under the GDPR with regard to this data and to provide the affected parties with the essentials of this obligation.

This data processing serves our legitimate interest to improve the user experience when visiting our fan page in a targeted manner. The legal basis for data processing is therefore Art. 6 (1) lit. f GDPR. In addition, Facebook uses so-called cookies, which are stored on your device when you visit our fan page even if you do not have your own Facebook profile or are not logged into it during your visit to our fan page. These cookies allow Facebook to create user profiles based on your preferences and interests and to display ads tailored to you (inside and outside Facebook). Cookies remain on your device until you remove them. Details can be found in the privacy policy of Facebook.

If you use our Profiles in social networks to contact us (eg. by creating your own contributions, responding to one of our contributions or sending us private messages), the data you provide us with will be processed by us exclusively for the purpose of being able to contact you. The legal basis is Art. 6 (1) lit. b GDPR. See also the sub-item **Contact** in this notice.

aa. Customer reviews

We are a company that strives to continuously improve our product and services, to match our customer's needs. Your opinion is of great value to us, which is why we are keen to know what your opinion is in regards to the use of our product and the services we provide. Sometimes we ask our customers direct questions through our surveys (see 4. (d.) above), but, sometimes, this is not enough.

Description, scope, purpose, legal basis

With this intent, we use the information you provide in the product reviews you leave in product review platforms (e.g. TrustPilot) and your social media posts in which you mention us directly (e.g. on Facebook or Twitter) for gathering information about how our customers view and interact with our product and services.

The information obtained from your comments or posts is then centrally gathered in our product management board, in order to give us the best view of what the most current and pressing customers demands are and what we can do to give them, and you, what you desire.

The legal basis of the processing activity is our legitimate interest, art. 6 (1) lit. f GDPR: it is our legitimate interest to use publicly available information about our products and services, in order to keep improving them.

Service providers

We have entered into a data processing agreement with TrustPilot A/S, Pilestraede 58, 5. Floor, DK-1112 Copenhagen K, Denmark ("**TrustPilot**"), in order to obtain from them information contained in the reviews that users of their platform publish about our product and services, as well as the overall net promoter score assigned to us based on such reviews. The information we obtain from TrustPilot refers to the sole information you have provided in your reviews. More information on TrustPilot's own data processing can be found in their privacy policy.

We use the services provided by Zapier Inc., 548 Market St. #62411; San Francisco, CA 94104-5401, United States ("**Zapier**"), for collecting information from social media posts or product reviews published in consumer review platforms other than TrustPilot, about our product or services and which mention Trade Republic directly. The information gathered by Zapier is publicly available and is, therefore, controlled by the author or publisher directly. Zapier obtains and sends us only the content of the post or the review: no other personal data is processed by Zapier in the context of these processing activities. More information about Zapier's privacy practices can be found in their privacy policy.

Our product management board is provided by ProductBoard, Inc., 612 Howard Street, 4th floor, San Francisco, CA 94105, United States ("**ProductBoard**"). ProductBoard receives information directly from Zapier by means of an API: therefore, ProductBoard obtains solely the information that Zapier has gathered. If the consumer review or social media post were, in fact, containing no personal information, then ProductBoard would not receive any personal

information either. On the contrary, ProductBoard might receive personal information contained in the consumer review or social media post pulled by Zapier. More information about ProductBoard's privacy practices can be found in their privacy policy.

Zapier and ProductBoard potentially transfer personal data to a third country in the context of providing their services. For more information about such transfers, scroll down to section 5. of this Privacy Notice.

j. Careers

aa. Applying through our website

Description, scope, purpose, legal basis and retention period

Through our website, it is possible for applicants to apply for job openings from time to time. In order to do this, you have to submit certain information through our Website (e.g. your CV, reference letter) which contains personal data.

The applications will be considered ONLY if they have been sent through the appropriate channels! Any application received through any other means (e.g. post, personal addresses, email addresses of Trade Republic employees without their permission) will not be considered and discarded immediately.

The legal basis for the processing of this personal data is Art. 6 (1) lit. b GDPR in conjunction with § 26 (1) BDSG. The purpose of the processing is to make hiring decisions. Without this processing activity, we would not be able to process your application for hiring.

We delete applications after six months from the moment a hiring decision regarding your application is made.

Service provider, appropriate safeguards for third country transfer

In order to process job applications, we use the services of Greenhouse Software, Inc. (18 West 18th Street, 11th Fl., New York City, NY 11232, United States) ("**Greenhouse**").

We have entered into a processing agreement with Greenhouse that governs the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects, and our obligations and rights. Greenhouse will process your personal data only on our instructions. Greenhouse guarantees all necessary

technical and organizational measures to ensure security of your personal data appropriate to the risk.

The legal basis of the transfer of personal data to Greenhouse is Art. 6 (1) lit. a GDPR (consent).

Greenhouse potentially transfers personal data to a third country in the context of providing its services. For more information about such transfers, scroll down to section 5. of this Privacy Notice.

bb. Applying through a platform other than our website

You may also choose to apply to one (or more) of our open positions from LinkedIn or any other job portals in which we post. In this case, the processing activity is initiated by you from said job portal. We do not control the processing activities performed by the job portal in this context.

However, once you decide to apply from the job portal to one of our open positions, you may be redirected to a web page from which you may insert all the necessary information for your application.

Depending on which open position you are applying for, said entered information may be collected by our service provider JOIN Solutions AG, Landsgemeindeplatz 6, 9043 Trogen, Switzerland ("**Join**").

We engage this service provider for the purpose of publishing job postings in multiple job portals, as well as gathering all applications for our open job positions from said job portals.

Join processes the sole personal information you provide in the context of your application. This would imply processing of your name, personal details, educational and professional history, resumé, and any other information you include in your application.

Legal basis for this processing activity is our legitimate interest, art. 6 (1) lit. f GDPR: it is in our legitimate interest to utilize the aforementioned providers' services in order to have improved outreach of our job postings and receive as many job applications as possible, as well as potentially improve the quality of candidates.

Join deletes all the information the moment the application information is forwarded to us. Join does not retain any of the collected personal data beyond their transfer to us.

In the context of this processing activity, neither service provider mentioned herein transfers personal data to a third country which does not benefit from an adequacy decision from the EU Commission, in accordance with Art. 45 GDPR. Join transfers collected personal information to Switzerland, in order to provide us their services: Switzerland benefits from such an adequacy decision, which implies that the level of protection of privacy rights and freedoms found in Switzerland is adequate in comparison to the rights and freedoms set under GDPR.

More information regarding the privacy practices established by Join can be found here.

5. Transfers of personal data to third countries

As stated at times throughout this Privacy Notice, some of Trade Republic's service providers potentially transfer personal data outside of the European Economic Area ("EEA") to so-called "third countries", in the context of providing their services to us and to you. These third countries are, for example, the United States of America or the United Kingdom, but, in essence, can be defined as any country that is not part of the EEA.

It is our responsibility to ensure that any possible transfer of your personal data to a third country does not undermine your rights and freedoms as a data subject, established under GDPR. There are many ways at our disposal with which we are able to guarantee the adequate safeguards to the transfers of personal data to third countries: the most prominent one is the use of standard data protection clauses (also known as "**standard contractual clauses**" - pursuant to Art. 46 (2) lit. c GDPR), published recently by the EU Commission implementing decision 2021/914/EU. The use of standard contractual clauses, though, is not the sole transfer mechanism available: some companies elect to establish their own set of rules governing the data processing practices throughout their entire company or group of companies, which need to be approved by a competent supervisory authority in order to be valid ("**binding corporate rules**" - pursuant to Art. 47 GDPR).

Some third countries or international organisations benefit from an "adequacy decision" from the EU Commission - pursuant to Art. 45 GDPR - which certifies that they "ensure an adequate level of protection" of your rights and freedoms as a data subject, under GDPR. The latest example of an adequacy decision has come in favour of South Korea, but many more third

countries have obtained such a decision, such as the United Kingdom. You may find the entire list of said third countries here.

The United States and the 'Schrems II' case

In its ruling of July 16, 2020, the European Court of Justice (ECJ) declared the EU-U.S. Privacy Shield invalid (Case C-311/18; so-called Schrems II). The ruling has raised the necessity for data controllers to evaluate on a 'case-by-case' basis whether the implemented transfer mechanisms are enough to ensure an adequate level of protection. In response to this ruling, we apply additional measures whenever necessary, in order to guarantee that EU data protection requirements are also met when processing data in the United States.

Below we provide an overview of which service providers potentially transfer personal data to a third country in the context of providing their services, and the type of transfer mechanisms that govern such potential transfers. All further details on the processing activities performed by each of these service providers can be found within the previous sections.

Service providers which base transfers of personal data to third countries on Standard Contractual Clauses, in pursuit of Art. 46 (2) lit. c GDPR:

Service Provider	**Purpose of Processing**	**(Potential) Recipient Third Country**
AWS	Data hosting (HaaS)	United States
Snowflake	Data structuring	United States
Datadog	Security monitoring, analysis	United States
mParticle	Customer data platform	United States
SendGrid	Email sending service	United States
Braze	Email sending service	United States
Google Ads, Youtube	Marketing performance analytics, remarketing, communication via social media	United States
Facebook, Instagram	Marketing performance analytics, advertising, communication via social media	United States
LinkedIn	Marketing performance analytics, advertising	United States

Microsoft Advertising	Marketing performance analytics, advertising	United States
Twitter	Marketing performance analytics, advertising, communication via social media	United States
Snap	Marketing performance analytics, advertising, communication via social media	United States
Google Analytics	Website-usage, performance analytics	United States
Google Analytics for Firebase	"Web Trading" web application usage and performance analytics	United States
Zapier	Product reviews, net promoter score analysis	United States
ProductBoard	Product reviews, net promoter score analysis	United States
Greenhouse	Application, hiring tracking, management system	United States

Service providers which base transfers of personal data to third countries upon their own Binding Corporate Rules, in pursuit of Art. 46 (2) lit. b and Art. 47 GDPR:

Service Provider	Purpose of Processing	(Potential) Recipient Third Country	Link to Service Provider's BCRs
Zendesk	Support ticket management system	United States	https://www.zendesk.co.uk/company/privacy-and-data-protection/#corporate-rules
Twilio	SMS sending provider	United States	https://www.twilio.com/legal/bcr/processor

6. Your rights

You have the following rights: right of **access** , right to **rectification**, right to **restriction** of processing, right to **Erasure**, right to **information** and right to **data portability**. In addition, you have a right of **objection** and a right of **withdrawal of your consent**, as well as the right to **appeal to the supervisory authority**.

a. Right to Information

You have the right to obtain confirmation from us as to whether we are processing your personal data. If we process your personal data, you have the right to obtain information about the following information:

- the processing purposes;
- the categories of personal data being processed;
- the recipients or categories of recipients to whom your personal data has been or will be disclosed, in particular recipients in third countries or international organisations;
- if possible, the planned duration for which your personal data will be stored, or, if this is not possible, the criteria for determining this duration;
- the existence of a right to rectification or erasure of personal data concerning you or to restriction of processing by us or a right to object to such processing;
- the existence of a right of appeal to a supervisory authority;
- if the personal data has not been collected directly from you, all available information about the origin of the data;
- the existence of automated decision-making including profiling in accordance with Art. 22 (1) and (4) GDPR and – at least in these cases – meaningful information about the logic involved and the scope and intended effects of such processing for you.

If we transfer your data to an international organization or to a third country, you have the right to request information on whether appropriate guarantees pursuant to Art. 46 GDPR in connection with the transmission.

b. Right to Rectification

You have the right to correct and/or complete the data we have stored about you if this data is incorrect or incomplete. Of course, we report this data immediately.

c. Right to Restriction of Processing

Under certain conditions, you have the right to obtain that we restrict the processing of your personal data. At least one of the following conditions must be fulfilled:

- you contest the accuracy of the personal data for a period that allows us to verify the accuracy of the personal data;
- the processing is unlawful and you refuse to delete the personal data and instead you want to restrict the use of the personal data;
- we no longer need the personal data for the purposes of processing, but you need it for the establishment, exercise or defence of legal claims; or

- you have objected to the processing in accordance with Art. 21 (1) GDPR, as long as it is not yet clear whether our legitimate reasons outweigh your interests.

d. Right to Erasure

You have the right to obtain that we delete your personal data immediately, if **we are obliged to do so**. This is the case if one of the following conditions are met:

- the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
- you revoke your consent, on which the processing is based according to Art. 6 (1) lit. a or Art. 9 (2) lit. a GDPR, and there is no other legal basis for the processing;
- you object to the processing pursuant to Art. 21 (1) GDPR and there are no overriding legitimate reasons for the processing, or you object to the processing pursuant to Art. 21 (2) GDPR;
- your personal data has been processed unlawfully;
- the deletion of personal data is necessary to fulfil a legal obligation under Union law or the law of the Member States to which we are subject;
- your personal data has been collected in relation to information society services offered in accordance with Art. 8 (1) GDPR.

If we have made your personal data **public** and we are obliged to delete it in accordance with the aforementioned conditions, we shall take reasonable steps, including technical measures, taking into account the technologies and implementation costs available to us, to inform other data controllers who process the personal data that you have requested us to delete all links to such personal data or copies or replications of such personal data.

There are some instances in which we are **required to** or have a **legitimate grounds in processing** your personal data, **which would supersede your right to object** to the data processing. These instances are:

- the exercise of the right to freedom of expression and information;
- the fulfillment of a legal obligation that requires processing in accordance to the law of the Union or the Member States to which we are subject, or to perform a task that is in the public interest or in the exercise of official authority vested in us;
- reasons of public interest in the field of public health pursuant to Art. 9 (2) lit. h and i as well as Art. 9 (3) GDPR;
- archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes in accordance with Art. 89 (1) GDPR, insofar as the law referred to in (1) is likely to render impossible or seriously impair the achievement of the objectives of such processing; or
- assertion, exercise or defence of legal claims.

e. Right to Information

If you have exercised your right of rectification, erasure or restriction against us, we are obliged to notify all recipients to whom we have disclosed your personal data of the rectification, erasure or restriction of the processing of your data, **unless this proves impossible or involves a disproportionate effort**.

f. Right to Data Portability

Under the following condition, you have the right to receive the personal data that **you have provided to us** in a structured, commonly used and machine-readable format and the right to have these data transmitted to another controller. Such processing is based on consent in accordance with Art. 6 (1) lit. a) or Art. 9 (2) lit. a) GDPR or on a contract pursuant to Art. 6 (1) lit. b GDPR and processing is carried out using automated procedures.

You have the right that we transmit your personal data directly to another controller, insofar as this is **technically feasible** and does not affect the freedoms and rights of other persons.

This right to data portability does not apply if the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority conferred on us.

g. Right to Object

You have the right, for reasons arising from your particular situation, to object at any time to the processing of your personal data, which is based on Art. 6 (1) lit. e (public interest) or lit. f (legitimate interest) GDPR. This also applies to profiling referred to in these provisions.

After an objection, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing that outweigh your interests, rights and freedoms, or the processing serves to assert, exercise or defend legal claims.

h. Right of objection to direct advertising

From time to time, we may send marketing material to you which we think may be of interest to you. We will only do so after obtaining your explicit consent allowing us to use your personal data for such purposes, unless you are an existing customer of ours. In that case we will only send you marketing material which relates to or is similar to the goods or services we have provided to you in the past. We will ensure that in each communication with you which contains

such digital marketing material we will include a link to unsubscribe from receiving such material in the future.

i. Right of withdrawal of consent

In accordance with Art. 7 (3) GDPR, you have the right to revoke your consent at any time. The withdrawal of consent does not retroactively invalidate the lawfulness of the processing activities performed until the time of such withdrawal.

j. Right of lodge complaints to a supervisory authority

You have the right to lodge a complaint with a supervisory authority, without prejudice to any other administrative or judicial remedy. In particular, you can exercise your right of appeal in the Member State of your place of residence, your place of work or the place of the alleged infringement if you believe that the processing of your personal data violates the GDPR. An overview of the respective country data protection officers of the countries and their contact details can be found here:
https://edpb.europa.eu/about-edpb/about-edpb/members_en.

The data protection supervisory authority responsible for us may be reached through the following addresses:

Berliner Beauftragte für Datenschutz und Informationsfreiheit

Alt-Moabit 59-61

10555 Berlin

Phone: +49 30 13889-0

E-Mail: mailbox@datenschutz-berlin.de

Homepage: https://www.datenschutz-berlin.de