

Privacy Notice for the Trade Republic App

Last updated on: 2024-01-09

Our Privacy Notice informs you about the collection and processing of your data by Trade Republic. It applies to the Trade Republic Application and Web Application (hereinafter "**Trade Republic App**" or "**App**") and to the services offered by us and our social media pages (together referred to "**Services**"). It also includes how we collect data in our App from your device; you can find more information about this in the section on App Tracking below. Information on the data processing taking place when you visit www.traderepublic.com is available directly on the website.

The data controller and service provider is:

Trade Republic Bank GmbH ("**Trade Republic**" or "**we**"), Brunnenstr. 19-21, 10119 Berlin, Germany.

In some cases, we may also act as joint controllers or third parties may process your data on their own behalf as data controllers. We will inform you in this Privacy Notice when this is the case so far this is legally necessary.

In general, and independent of your location or residency, we process your data in a similar way. However, there are also exceptions in which your data will be processed or stored differently due to your residency and you will find more information below.

1. Purpose and Legal Basis of our Data Processing

We rely on the following purposes and legal bases when processing your personal data.

Additionally, we provide further information on the purpose and legal basis of the respective processing activity when we explain it below in this document. We will explicitly mention whether a processing activity is based on your consent, is performed to fulfill our contractual obligation, is performed to fulfill our legal obligations or based on our legitimate interest.

1.1 Consent – Art. 6 (1) lit. a GDPR

We process your personal data based on Art. 6 (1) lit. a GDPR, if you have consented to the specific processing activity. Your consent is **voluntary and may be revoked by you at any time**. You will always receive further details on the processing activity based on your consent. Please note that revoking your consent has no retroactive effect; processing that took place before is not affected.

1.2 Performance of a Contract – Art. 6 (1) lit. b GDPR

We process your personal data based on Art. 6 (1) lit. b GDPR, if the processing is done in order to provide our Services based on the contract we concluded with you. This includes processing in the banking, trading or crypto context.

For example the processing is carried out for the opening or provision of your bank account or banking transaction, or processing of trading orders, the receipt and execution of instruction for corporate actions or the provision of our App for these purposes, trading of crypto assets including the transfer of personal data to crypto custodians.

Further information on the scope of the Services provided by us, can be found in the respective contract documents and their terms and conditions.

1.3 Legal obligation – Art. 6 (1) lit. c GDPR

We process your personal data based on Art. 6 (1) lit. c GDPR due to our legal obligations as a bank. We are subject to various legal obligations, such as statutory requirements (e.g., German Banking Act, German Money Laundering Act, German Securities Trading Act, German tax laws) and banking supervisory 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, the obligation to conduct identity and age checks, to prevent fraud and money laundering, specific customer complaints procedures or the fulfillment of control and reporting obligations under tax law.

1.4 Legitimate interest – Art. 6 (1) lit. f GDPR

We process your personal data based on Art. 6 (1) lit. f GDPR, if we have a legitimate interest to do so. This means that our interest in processing your data is not overridden by your interests or your fundamental rights and freedoms. Whether this is the case will be determined by us on a generic basis and prior to the initiation of a processing activity. We will consider the purposes below and assess the particular circumstances in the individual situation while taking into consideration the reasonable expectations you may have based on your relation to us. We carry out this analysis in order to verify that these processing activities do not harm your data protection rights.

This includes the following purposes:

- assertion of legal claims and defense in legal disputes;
- ensuring our IT security and the overall IT operation;
- prevention and investigation of criminal acts;
- non-marketing related email correspondence;
- testing and optimisation of demand analysis procedures including customer segmentation;
- direct marketing or market research regarding functionality and performance of our Services;
- measures for the further development of the performance of our Services (for example our App).

If you want more information about the aforementioned considerations or would like to opt out from specific processing activities which are based on our legitimate interest due to your specific circumstances, please contact us and we can further evaluate your situation and the processing taking place.

2. Which Data does Trade Republic Process

Most of the personal data we process is provided by you (for example your name or email address or your transactions). We also process data from your device that we collect during your use of our app or website and, in so far permissible, data we may collect from third parties or public sources.

2.1 Data processing performed in our role as bank

2.1.1 Anti Money Laundering, Fraud Prevention, Tax Law and Risk assessments

As a regulated financial institute various legal obligations and diligence obligations apply to us. This means, we process and share personal data in order to follow banking-related regulations or tax laws, perform risk assessments, prevent anti money laundering, counter terrorism financing and to protect you, us and others from financial crimes.

Therefore, we might request further documents or information from you to prevent misuse or illegal behavior; this includes documents such as income statements, tax reports, bank statements from other banks, birth certificates, proof of (real estate) ownership, etc to prove your identity or that the funds you want to transfer to your Trade Republic Account are rightfully owned by you. Additionally, we also process and store information from publicly available sources such as trade registries, land registries, registries of associations, media, internet, etc when there is a specific reason to do so. Depending on the Services you use, we might also process personal data that we permissibly receive from third parties such as solvency score providers or background check service providers.

To prevent financial crimes, we additionally process data relating to your use of our Services and data that we collect while you use our App or Website.

These processing activities are done to adhere to our legal obligations or, with regard to decreasing risks and preventing harm from you, us or third parties, in order to preserve our legitimate interest.

2.1.2 Preparing, processing and sharing anonymised reports

We process your personal data (for example, how you use our Services, the value of your assets or financial transactions) to compile aggregated and/or anonymised statistics or reports about our customers, held assets, spending behaviors or usage patterns for improving our Services, forecasts and to adhere to our legal reporting obligations regarding risk assessments or deposit protection schemes. As far as possible, we do not share your personal data but only aggregated anonymised statistical information under this clause with other data controllers.

This processing is done to adhere to our legal obligations or, with regard to Service improvements (including forecasts), in line with our legitimate interest.

2.1.3 Capital Gains Tax and similar taxes, regular reports and account statements

We process your personal data including your tax identification number when calculating your capital gains tax.

Depending on your country of residence, we may settle your capital gains tax directly with local authorities or inform them about outstanding payments. We may also provide you with a summary of transactions and tax implications in line with our customer agreement. This information may be used by you when declaring your taxes.

If you do not reside in Germany, we use the services provided by KPMG AG, Raefelstrasse 28, CH-8045 Zurich, Switzerland, for providing you with a summary of transactions and tax implications.

For this purpose, solely the identifiers that we use internally to identify you, as well as the trades and transactions you have performed as our customer of Trade Republic are transferred; not your name or email address.

Depending on your country of residence, this processing is done to adhere to our legal obligations or to fulfill our contractual obligations towards you.

We also process your personal data, especially your account information, assets held by you, incoming and outgoing payments, when providing you with account statements and regular reports on your activities.

This processing is done to adhere to our legal obligations and to fulfill our contractual obligations towards you.

2.2 Registration and first steps

We collect and process your personal data when you open an account. If you do not provide the following data, you cannot open an account with us:

- country of residence,
- phone number,
- first name,
- last name,
- date of birth,
- email address,
- referral code (if provided by you),
- PIN,
- registered address,
- place of birth,
- nationality,
- tax residencies,
- previous trading experience,
- identification information (including a copy of your ID or passport),
- reference account,

- tax identification number,
- occupancies (only in some jurisdiction like Spain).

During your registration, we also collect your device location (which you will need to permit through your device settings) and we might also ask for further information or documents due to our legal obligations as a financial institution.

We collect and process this data in order to fulfill our legal obligations and to fulfill our contractual obligations.

2.2.1 Onboarding Profile

As long as you have not finished your registration you have a so-called onboarding profile with us. You finish your registration when you have successfully performed an identification process and accepted the Online Brokerage Framework Agreement ("Customer Agreement") and the associated annexes and opened a bank account or an escrow bank account. Your onboarding profile allows you to a limited extent to browse our app, it does however not enable you to trade financial instruments, deposit funds or use similar financial services (including trading of crypto assets or similar products).

This processing is done to fulfill our contractual obligations.

2.2.2 Customer Profile

Once you have a full customer profile, you can use the different functionalities of our Services (this also depends on your location and whether you have accepted the applicable terms). As such, you are in general able to further personalize the Service by following specific financial instruments, setting price alarms and/or checking the different documents available to you in your profile. You are also able to change your contact information and other personal data.

This processing is done to fulfill our contractual obligations.

2.2.3 Online Verification

We use an online identification procedure for the required identification of our customers in accordance with applicable anti money laundering laws. You can use different identification documents for the verification, such as your passport, identification card or residence permit.

We use the following service providers for identification:

- WebID Solutions GmbH, Friedrichstraße 88, 10117 Berlin, Germany ("**WebID**"), or
- SafeNed-Fourthline B.V., Tesselschadestraat 12, 1054 ET Amsterdam, Netherlands ("**Fourthline**") together with Namirial S. p. A., Via Caduti sul Lavoro n.4, Senigallia (AN), IT-60019, Italy ("**Namirial**").

You can see during your registration which service provider processes your data. Both service providers process the data for our purposes and on our behalf.

This processing is done to adhere to our legal obligations.

2.2.3.1 WebID

We transmit the information you provide about yourself, meaning your full name, your date and place of birth, your email address, your telephone number, citizenship and your selected language to WebID. WebID verifies this information and provides us with further information contained on your identification document. For this purpose, video recordings and photos are taken of you and your identification document. The bank account details you provide will be processed as part of the account identification. WebID stores this data as our data processor for 30 days. Afterwards, the data which was processed for us will be automatically deleted.

You can find further information about WebID and a possible subsequent use of your data by WebID based on your consent granted to WebID [here](#).

2.2.3.2 Fourthline

We transmit the information you provide about yourself, meaning your full name, your date and place of birth, your email address, your telephone number, citizenship and your selected language, to Fourthline. Fourthline verifies this information and provides us with further information contained on your identification document. For this purpose, Fourthline requires photos of your identification document. After confirming the information on the photos, you take a so-called video selfie of yourself. The photos of you and your identification document, along with your device location, will then be used to verify your identity and shared by Fourthline with us. Fourthline offers further information [here](#).

Since we use the method of video selfie identification, we are obliged to create a so-called qualified electronic signature. You must separately agree to the creation of the qualified electronic signature. We use Namirial to create this signature. You will receive a six-digit code from us and you must enter the code in the App to complete the verification. Namirial stores your data as data controller and in accordance with legal regulations for a period of 20 years. Namirial offers further information [here](#).

2.3 App Tracking and App permissions

2.3.1 App Permissions

When using our App, we may ask you to access certain functions of your device (so called app permissions). Depending on your operating system, you must either explicitly grant permission or you can revoke it for each permission in your operating system app settings.

During the onboarding we require access to your microphone and camera and to your device location. We need this access and process the data collected through this app permission based on our legal obligations as a bank regarding the online identification of our customers. You may revoke these permissions in your operating system settings any time after the onboarding.

Additionally, we may also request permission to send you Push Notifications or use information on your device to secure your login (for example, Face-ID or Fingerprint Unlock).

You are free to consent to this processing or not and we will process your data based on your consent.

2.3.2 App Tracking, SDKs and Service Providers

We use app tracking to ensure the functionality and safety of our Services, to analyze our App usage and improve our Services and to market our Services. Whether tracking takes place and for which purposes, depends on the purpose of the tracking, your profile settings and/or whether you consented to it. We use Software Development Kits ("SDKs") for this; an SDK is a piece of code that is provided by a third party. The SDK can enable specific app features or be used for data transfers.

We use the following third party providers in our app for tracking and other purposes Google Firebase, Adjust, mParticle, Braze, Adyen and Zendesk.

2.3.2.1 Firebase

Firebase is a service offered by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland ("Google"). We use Firebase for monitoring and ensuring our app performance (so called Performance Monitoring) and for pre-loading and subsequently enabling specific features or functionalities into our App without forcing users to update their apps for every change (so called Remote Config).

Our use of Firebase is technically necessary to provide our Services and ensure their safety and the data collection does not require your consent.

We process your data in order to fulfill our contractual obligations and provide our Services to you.

2.3.2.2 Braze

Braze is a service offered by Braze Inc., 318 West 39th Street, 5th Floor, New York 10018, United States ("Braze"). We use Braze as a communication tool to send you emails, Push Notifications or in-app messages and banners. While technically possible, we do not use Braze to directly collect information on your app usage. This data is collected through other tools about which we inform you in this Privacy Notice and which will only collect your data in accordance with your settings. Braze only receives personal data after it has been initially collected by other tools.

This means that our use of Braze is technically necessary to communicate with you and does not require your consent.

In so far, we process data for marketing purposes with Braze, this is based on our legitimate interest (for more information see below). You can opt out of receiving marketing emails and/or push notification from us at any time.

In so far we process data in order to provide you with legally necessary information, we fulfill our contractual obligations.

2.3.2.3 Adjust

Adjust is a service offered by adjust GmbH, Saarbrücker Str. 37A, 10405 Berlin, Germany ("Adjust"). We use Adjust for marketing purposes; namely in order to track how our campaigns perform and improve them, display (or not display) personalized ads to you, to prevent marketing fraud and to attribute sign ups or other customers behavior to specific campaigns, affiliate marketing partners or influencers. This means that we forward data collected through Adjust to our advertising partners and you will find more

information on our marketing activities below. Adjust does not collect or forward clear data like your name, email address, phone number and it does also not collect specific information regarding the value of your account, financial instruments you traded, etc.

Additionally, Adjust allows us to prepopulate the referral code field for you. You do not have to reenter this code if you clicked on a referral link provided by a friend of yours or a third party.

We will only collect data through Adjust in line with your profile settings which you can change any time. You are free to consent to this processing or not and we will process your data based on your consent.

2.3.2.4 mParticle

mParticle is a service offered by mParticle, Inc., 257 Park Avenue South, Floor 9, New York, NY 10010, United States ("**mParticle**"). We use mParticle for marketing purposes as well as for analytical purposes and product improvements. This means that we collect specific events through mParticle which will then be stored in Braze in order to send you personalized marketing communication or which will be stored in other internal systems to ensure that our app runs smoothly and to analyze how our app is being used.

We will only collect data through mParticle in line with your profile settings which you can change any time. You are free to consent to this processing or not and we will process your data based on your consent.

2.3.2.5 Adyen

Adyen is a service offered by Adyen B.V., Simon Carmiggeltstraat 5-60, 1011 DJ Amsterdam, Netherlands ("**Adyen**"). We use Adyen as payment service provider when you transfer money to and from your account via credit card payment in our App.

This means you provide your card details directly to Adyen which operates a secure server to process payment details, encrypting your credit/debit card information and authorizing payment. Adyen processes your data in accordance with its one privacy policy which can be found here: <https://www.adyen.com/policies-and-disclaimer/privacy-policy>

We process your data in order to fulfill our contractual obligations and provide our Services to you.

2.3.2.6 Zendesk

Zendesk is a customer service management tool with different functionalities, provided by Zendesk, Inc., 1019 Market Street, San Francisco, CA 94103 USA ("**Zendesk**").

We use Zendesk to provide you with our customer service and to enable you to chat with us in our App. For this purpose Zendesk collects and processes data on our behalf which is further described below.

We process your data in order to fulfill our contractual obligations and provide our Services to you.

2.4 App Personalization, Referral Program, Waiting List, Cash Tab

2.4.1 App Personalization

We use information you provided us with to personalize our Service to a limited extent and as described

below.

You can personalize our Services by for example choosing different display modes, colors, whether or for which purposes we may collect and use your in-app data.

You can also follow specific financial instruments, set price alarms for financial instruments or display your portfolio growth in percentages or absolute numbers with different reference times.

Based on the information regarding your trading experience, provided to us during your onboarding or at a later stage, we might also show you warning notices in accordance with applicable law.

Additionally, we will also process your personal data such as referrals, transactions you made, when you deposit money and other events initiated by you, to show you updates in our app regarding your contract, new functionalities or new services, or advice on how you can use our Services.

We process the data to fulfill our contractual obligations based on the choices you made, in so far applicable based on the consent you provided us with and with regard to warning notices based on our legal obligations.

2.4.2 Refer-a-Friend

Our customers can refer new customers and receive a bonus in exchange; more details can be found in the applicable terms for customer referrals.

When you receive a referral code from a friend and you enter this code during your registration, we may provide your friend with limited information regarding your registration and activities (for example, your registration status, whether you paid in money, concluded a trade or a saving plan as well as your first name). This is done to provide your friend an overview over sent referrals, their status and earned rewards and to subsequently provide you and your friend with your reward in accordance with our terms. We also make you aware of this, when you enter the referral code.

You are free to use referral codes when you register. We process information relating to referrals in accordance with our contractual obligations in order to provide the inviter and invitee with the referral bonus. Additionally, providing updates on the referral status is done in line with our legitimate interest in a transparent and efficient referral program.

2.4.3 Waiting List

While we try to offer all of our different Services in all countries in which we operate, there might still be services or features which are not available in your location or to which access is currently limited. If you are interested in these services, want to become one of its early customers, and remain up to date with our latest news prior to the launch, you have the choice of signing up to our waiting list.

For this, we will need further data from you to identify and contact you. You can unsubscribe from this list at any time.

This processing is done to fulfill our contractual obligations.

2.4.4 Cash Tab

The "Cash Tab" available in our App provides you with an overview of your transactions and also visualizes and sorts them.

We process your transaction data which includes name of financial instruments bought, data relating to recipients of transaction like retailers, transaction amount, or subject of the transaction to provide you with this feature.

This processing is done to fulfill our contractual obligations.

2.5 Crypto

When trading crypto assets, you need to conclude a custody agreement with a crypto custodian who is a separate company.

Depending on your location, this agreement is concluded either with Trade Republic Custody GmbH, Kärtner Ring 5-7, 1010 Vienna, Austria ("**Trade Republic Custody**") or with BitGo Europe GmbH, Neue Rothofstr. 13-19, c/o WeWork, 60313 Frankfurt a. Main, Germany ("**BitGo**"). You can see your respective crypto custodian when you conclude the custody agreement. This agreement is also available in your customer profile.

We transfer your personal data collected by us during your onboarding process (or if applicable updated data) with the respective crypto custodian. Since the crypto custodians have to adhere to anti money laundering laws which includes identifying you as their customer, they need access to this information and might upon request receive further information from us.

2.5.1 BitGo

BitGo processes your data as a data controller and you can find more information in your custody agreement with BitGo.

We transfer your data to BitGo based on our contractual obligation with you to enable you to trade crypto assets.

2.5.2 Trade Republic Custody

Trade Republic and Trade Republic Custody have concluded a joint controllership agreement regarding the processing of your personal data (Art. 26 GDPR). Both entities pursue the fulfillment of their legal obligations and enable through their joint controllership a structured and secure storage of the personal data of crypto asset holders. According to the joint controllership agreement, Trade Republic will ensure and answer to your data subject rights. These rights are explained at the end of this Privacy Notice. You are however free to exercise your rights against each of the two entities.

We and Trade Republic Custody process information relating to the trading of crypto assets in order to fulfill our contractual obligations and provide our Services to you.

Additionally, and as described for other financial instruments in this Privacy Notice, your data will also be processed to ensure adherence to legal obligations relating to the trading of crypto assets such as tax law obligations or anti money laundering; this includes the possible transfer of your personal data to third parties such as regulators, authorities or tax advisors.

2.6 Trading of financial instruments and Savings Plans

To enable you to trade financial instruments, we process your personal data and may share it, to a limited extent, with third parties. This includes, for example, the processing of trading orders or similar transactions, the receipt and execution of instructions for corporate actions, as well as the associated communication and subsequent storage and attribution of your respective financial instruments.

Additionally, you can also set up Savings Plans. We process your personal data and account information when executing your Savings Plans and will provide you with updates on it.

We process your data in order to fulfill our contractual obligations and provide our Services to you.

2.7 Escrow Accounts

We use escrow service providers for the safekeeping of customer balances and the settlement of securities orders and instructions and card transactions. We maintain collective escrow accounts with the following **"Escrow Service Providers"**:

- solarisBank (solaris Bank AG, Anna-Louisa-Karsch-Straße 2, 10178 Berlin, Germany),
- Citi (Citi Europe plc, 1 North Wall Quay, Dublin, Ireland),
- J.P. Morgan (J.P. Morgan SE, Taunustor 1, 60310 Frankfurt am Main, Germany),
- Deutsche Bank (Deutsche Bank AG, Taunusanlage 12, 60325 Frankfurt am Main, Germany).

You can see with which Escrow Service Provider your funds are held in your customer profile. During your onboarding we also provide you with information on the respective Escrow Service Provider.

When opening your account, we transfer your data to the respective Escrow Service Provider in order to fulfill your request and to enable them to adhere to their legal obligations (including anti money laundering). Your Escrow Service Provider also receives information from us on an ongoing basis, for example, when your personal data is being updated, your account is closed or when money is transferred from or to your account.

We process your data in order to fulfill our contractual obligations and adhere to our legal obligations.

The Escrow Service Providers process your data in order to fulfill their contractual obligation and to adhere to their legal obligations.

2.8 Trade Republic Debit Card

We process your personal data when you use your Trade Republic Debit Card. We do so to provide you with our Debit Card and its features and to fulfill our contractual obligations. Additionally, we also process your data in accordance with our legal obligations as a bank and based on our legitimate interest to secure our services and prevent harm from you, third parties and us.

When you order your Debit Card, you need to provide us with your delivery address which we will process to fulfill our contractual obligation process in order to deliver your Debit Card.

2.8.1 Withdraw money and payments

We share your account details and transaction data with the respective ATM Partner in case you want to withdraw cash.

We will also share this information in case you use your Trade Republic Debit Card for online payments and point of sale terminals.

2.8.2 Google Pay and Apple Pay

If you use Google Pay or Apple Pay, we will need to transfer data relating to your transactions to Google or Apple Distribution International Limited, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland ("**Apple**"), as data controllers.

When transferring your data, we use tokens instead of your clear data in order to protect your privacy.

2.8.3 Trade Republic Debit Card features

When using your Trade Republic Debit Card we may offer you the features Round Up and Saveback which you can choose to use in line with the applicable terms.

In order to provide you with these features we process your personal data which includes especially the kind of the transaction, the value of the transactions and the investment choices you have made in connection with these features.

2.9 Data of non-customers

We process personal data of non-customers when they transfer money to or receive money from our customers. This includes displaying their information in customer account statements as well as processing their data for fraud prevention purposes, to prevent misuse and similar purposes.

Since we do not have a direct contractual relationship with these persons, we process their data based on our legitimate interest to provide our services to our customers and to adhere to our legal obligations.

3. Account Closure, Data Retention and Deletion

We will only keep your data only as long as we need it to provide you with our Services or to adhere to our legal obligations.

As a bank, there are different statutory data retention rules that apply to us and that determine for how long we are legally obliged to store data. These laws also apply, even if you explicitly request us to delete your data.

Our retention periods stem from our regulatory and tax reporting obligations which can differ between 2 to 10 years and in some exceptions up to 15 years (usually beginning at the end of the respective calendar year). Since we are a German company, the German statutory retention periods apply, unless laws within your country of jurisdiction explicitly state otherwise.

The main German laws (which usually come from EU Directives and Regulations) in this regard are the

Abgabenordnung ("AO"), Geldwäschegesetz ("GwG"), Wertpapierhandelsgesetz ("WpHG"), Verordnung zur Konkretisierung der Verhaltensregeln und Organisationsanforderungen für Wertpapierdienstleistungsunternehmen ("WpDVerOV"), Abgabenordnung ("AO"), and Handelsgesetzbuch ("HGB").

Additionally, the retention period also depends on the statutory limitation periods, which depend on the respective jurisdiction and run between 2 years to up to 30 years.

In general, the following data retention timelines apply for the following pieces of personal data:

3.1 Retention periods based on banking regulations

First name, last name, citizenship, date and place of birth, address, other personal data that was collected during the (video-)identification process (including pictures, videos, identification document, email address and phone number):

We have to retain this data for 5 years after the end of the customer relationship with you according to §§ 8 (4), 10 (3) GwG. The retention period applies usually once you have finished the onboarding and only starts at the end of the calendar year in which the customer relationship was terminated. Additionally, we also have to retain this information for 5 years according to § 9 WpDVerOV together with §§ 77 (3), 83 (8) and (11) WpHG.

First name, last name, tax identification number, and address also need to be retained for 6 years beginning at the of the calendar year in which the customer relationship was terminated according to the so-called obligation of authenticity of accounts in line with § 154 AO and § 147 AO.

In case you have traded with financial instruments and generated revenue for us, we will need to retain this information together with your account number, first name, last name and contact information for 10 years beginning at the end of the calendar of the respective actions according to § 147 AO together with § 257 HGB.

Personal data relating to your bank account with us, trading of financial instruments or money transfers need to be retained for 5 years according to § 83 (8) and § 8 (4) GwG and 10 years according to § 147 AO together with § 257 HGB; both beginning at the end of the respective calendar year.

Communication with our customer care and our Complaints Team (includes name, banking information and contact information) is retained for a maximum of 5 years after closing the respective complaint according to § 9 (4) WpDVerOV; beginning on the date of the end of the complaints proceeding.

The customer's confirmation of the respective current customer agreement is retained for 5 years at the end of the calendar year in which the customer agreement was terminated according to § 9 WpDVerOV together with §§ 77 (3), 83 (11) WpHG.

We process and retain your data in line with these statutory retention periods in order to fulfill our legal obligations.

In so far we retain your data in line with statutory limitation periods to ensure our own claims, we process your data with our legitimate interest.

3.2 Retention Periods based on consent

Personal data that we process based on your consent will be retained until you do revoke consent or until you close your account and once we do not have a legitimate interest to retain this data anymore. For example, if you consent to receiving marketing emails, we will need to retain your consent for a certain period of time, to prove that marketing emails you received from us were based on your validly given consent.

3.3 Retention Periods based on crypto regulation

Specific data retention obligations can apply to the purchase and sale of Crypto assets. These retention obligations can depend on the country in which the crypto custodian is being as well as on the country in which the person trading crypto assets resides.

If you are trading crypto assets and are a customer of Trade Republic Custody, data collected on you during your onboarding needs to be retained for 10 years beginning at the of the calendar year in which the customer relationship was terminated according to Section 21 (1) Austrian Finanzmarkt-Geldwäschegesetz. Data relating to the purchase and sale of crypto assets as well as data collected on you during your onboarding needs to be retained for 10 years after the date of the relevant transaction or longer if other retention obligations like § 147 AO together with § 257 HGB apply.

You can find more information on BitGo's retention periods as independent data controller in BitGo's privacy policy.

4. Marketing Activities and Social Media

We process personal data for our marketing activities and in connection with our use of social media.

We also process personal data to display or send personalized advertising. For this purpose, we use the information provided to us as well as data collected during the use of our app or confirmations of receipt and information that messages have been read.

You can object to this processing at any time by contacting us or closing your account.

The processing of your data for advertising purposes, unless consent is required, is based on our legitimate interest in direct advertising and marketing.

We only use tracking data based on your consent for marketing purposes and you are free to withdraw your consent in your profile settings at any time.

4.1 Company Profile on Social Media Pages

We have company pages or company profiles ("**Company Profiles**") on the following networks: TikTok, X, LinkedIn, Facebook, Youtube, Snapchat and Instagram (together "**Social Network**").

When you interact with our Company Profiles or with our content shared through the Company Profiles, the respective Social Network collects your personal data. Additionally, if you directly interact with us, for example messaging us, posting under our content, etc, we also collect your personal data which includes the content you shared with us, your profile picture, profile handle and other publicly visible profile

information.

As a general rule, no Social Network provides us with personal data which allows us to identify specific visitors of our Company Profiles or users who have seen our advertisements. Any statistics we receive from Social Networks cannot be linked to individual users by us.

With regard to personal data being processed by the respective Social Network in order to provide Company Profile statistics, we are joint controllers together with the respective Social Network in line with Art. 26 GDPR.

Company Profiles and processing personal data in connection to our Company Profiles serves our legitimate interest in marketing, communicating with the public and improving and personalizing the user experience for Company Profile visitors.

4.1.1 TikTok

The Social Network TikTok is operated by TikTok Technology Limited, 10 Earlsfort Terrace, Dublin, Ireland ("TikTok"), and provides us with usage statistics regarding our Company Profile and marketing activities, including impressions, spend and costs per event. To provide us with this information, TikTok processes personal data of its users and our Company Profile visitors.

You can find the joint controller agreement concluded with TikTok here:

<https://www.tiktok.com/legal/page/global/tiktok-analytics-joint-controller-addendum/en>

4.1.2 X

The Social Network X is operated by Twitter International Unlimited Company, One Cumberland Place, Fenian Street, Dublin 2, Ireland ("Twitter"), and provides us with usage statistics regarding our Company Profile and marketing activities. To provide us with this information, Twitter processes personal data of its users and our Company Profile visitors.

You can find more information on Twitter's privacy practices here: <https://twitter.com/de/privacy>

4.1.3 LinkedIn

The Social Network LinkedIn is operated by LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland ("LinkedIn"), and provides us with usage statistics regarding our Company Profile and marketing activities. To provide us with this information, LinkedIn processes personal data of its users and our Company Profile visitors.

You can find the joint controller agreement concluded with LinkedIn here:

<https://legal.linkedin.com/pages-joint-controller-addendum>

4.1.4 Instagram

The Social Network Instagram is operated by Meta Platforms Ireland Limited, 4 Grand Canal Square, Dublin 2, Ireland ("Meta"), and provides us with usage statistics regarding our Company Profile and marketing

activities. To provide us with this information, Meta processes personal data of its users and our Company Profile visitors.

You can find the joint controller agreement concluded with Meta here:

https://www.facebook.com/legal/terms/page_controller_addendum

4.1.5 Facebook

The Social Network Facebook is operated by Meta, and provides us with usage statistics regarding our Company Profile and marketing activities. To provide us with this information, Meta processes personal data of its users and our Company Profile visitors.

You can find the joint controller agreement concluded with Meta here:

https://www.facebook.com/legal/terms/page_controller_addendum

4.1.6 Snapchat

The Social Network Snapchat is operated by Snap Group Limited, 50 Cowcross Street, Floor 2, London, United Kingdom ("Snapchat"), and provides us with usage statistics regarding our Company Profile and marketing activities. To provide us with this information, Snapchat processes personal data of its users and our Company Profile visitors.

You can find more information on Snapchat's privacy practices here:
<https://values.snap.com/privacy/privacy-policy>

4.1.7 Youtube

The Social Network and video hosting service Youtube is operated by Google and provides us with usage statistics regarding our Company Profile and marketing activities. To provide us with this information, Google processes personal data of its users and our Company Profile visitors.

You can find more information on Google's privacy practices with regard to Youtube here:
<https://policies.google.com/privacy>

4.2 Marketing Activities

4.2.1 Raffles and comparable promotions

If you decide to participate in a raffle or a comparable promotion, we will process your data to the extent necessary to run the raffle and determine the winners. You will receive more detailed information in the respective raffle terms and we collect your consent if necessary.

Your participation in a raffle is voluntary and we process your data based on our contractual obligations with regard to running the raffle and, if collected, based on your consent.

4.2.2 Online Display Advertising and Social Network Advertising

4.2.2.1 Online Display Advertising

We use different display ad networks, including Google Display Network offered by Google, and affiliate networks when showing you ads online outside of Social Networks. Based on the ad network features, we might segment viewers based on data and characteristics provided by the respective ad network.

Additionally and in line with your in app profile settings or based on your consent with regard to cookies and similar technologies, we might also use usage data collected through Adjust to show you personalized ads online. In case you reject such personalization based on our data, this will not necessarily have an effect on the amount of advertisements you see from us and this will also not have an effect on ads which are personalized based on data controlled by the respective ad network.

4.2.2.2 Social Network Advertising

When advertising on Social Networks (for example, YouTube, Facebook, Instagram), advertisers have the option to target specific user groups based on data collected by the respective Social Network or the option to forward encrypted information regarding the advertisers' customers like email addresses or advertising IDs. The Social Network will then - either on the advertiser's behalf as a data processor or as data controller with the consent of the relevant user - match the encrypted data with its own data and enable the advertiser to display or also not display ads to the matched Social Network users. Non-matched data will be deleted after a short period of time. We use such features provided by Social Networks to market our Services.

We also use other features provided by Social Network to analyze our campaign efficiency or ad attribution. This is done by sharing limited user information with the respective Social Network which usually includes identifiers provided by the Social Network and relating to its specific users.

In so far your app usage data is used for these purposes, it will be collected through Adjust and our use of Adjust will adhere to your profile settings. This means that if you did not consent to tracking for marketing purposes or opted out of it, we will not transfer or use your data for the abovementioned purposes.

Additionally, you can contact us at any time to opt out of personalized advertising on Social Networks based on data we collected on you.

In case you do reject such personalization based on our data, this will not necessarily have an effect on the amount of advertisements you see from us and this will also not have an effect on ads which are personalized based on data controlled by the respective Social Network.

We currently use the following Social Networks for showing you advertisements and to collect information on our campaign performances. To clarify, your data may not necessarily have been processed in connection with even one or all of the following Social Network; this depends on your own use of the respective Social Network as well as on our own different campaigns.

- TikTok
- Facebook
- Instagram

- Youtube
- Snapchat
- LinkedIn
- Reddit, Inc., 1455 Market Street, Suite 160, San Francisco, CA 94103, United States

4.2.3 Influencer / Affiliate Advertising

We collaborate with Influencers and other affiliate partners. This means that you may see paid for content about our Services on their social media pages or on other sites or apps. These partners do receive aggregated information from us regarding the performance of their respective content or campaigns. Depending on our agreement with these partners, their remuneration might also be calculated based on this aggregated information. We do not share your personal data with these partners.

More information regarding the data processing taking place when creating these aggregated reports can be found below.

4.2.4 Conversion Tracking

We process your data (in-app usage data and account information) to better understand the performance of our marketing activities and to provide aggregated statistics and reports to our advertising partners (including Influencers). Additionally, Social Networks also process your data to provide us with information regarding our marketing activities on their platforms.

We process your in-app usage data to create conversion tracking reports based on your consent and you are free to withdraw your consent in your profile settings at any time.

We process your account information to create conversion tracking reports based on our legitimate interest in efficient and cost-saving advertising.

4.2.5 Marketing Communication

We also process your data to send you marketing communication. For this purpose, we use the information provided by you during your registration, your transaction history and to which of our services and products you have signed up to and how you use them as well as data collected during your use of our app (in so far you consented to our use of in-app usage data). In particular, we also process your location for this purpose, as some of our products and services are only available in certain jurisdictions. You can object to this processing at any time by contacting us or closing your account.

Additionally, we may also show you personalized commercial in-app notifications based on the personal data mentioned above.

If you use our Services, we may send you product recommendations, surveys or product review requests via email based on the fact that you are an existing customer. If you no longer wish to receive these emails from us, you may opt-out at any time, free of charge, by clicking on the unsubscribe link available in each email, by changing your settings or by reaching out to us.

With regard to push notifications, you can change your preferences any time in your device settings.

The processing of your data for marketing communications, is based on our legitimate interest in direct advertising (especially to existing customers), unless consent is legally required which will then be our legal basis.

4.3 Market Research and Surveys

If you decide to participate in a survey, we will process the data and answers you provide to the extent necessary to conduct the survey and analyze the results. In case any additional processing takes place, we will inform you about it in our survey terms and collect your consent if necessary.

Your participation in our surveys is voluntary and we process your data based on our legitimate interest to conduct surveys and improve our Services and, in so far granted, based on your consent.

5. Communication, SMS and Customer Service

5.1 Communication

Besides sending you marketing messages (including emails), we also send informational communication such as In-App messages, Push notifications, emails, Whatsapp, SMS and sometimes even regular mail. These messages may include information about your transactions, incoming payments, withdrawals or other important information regarding our Services (for example service or trading restrictions). We will also send you communication, if you request us to do so (for example, Price Alarms).

This processing is done to provide you with our Services requested by you and, in so far legally necessary, to adhere to our legal obligations. With regard to providing you with information about transactions, withdrawals or other important information, process your data based on our legitimate interest of informing you and improving and securing our Services.

5.2 SMS and SMS verification

To pair your device with your account and to increase your account security and prevent fraud, we send SMS messages. We send these messages based on the phone number provided by you in the onboarding process.

It can happen that sometimes users accidentally or fraudulently enter a wrong number. In such cases, we may send SMS to persons who have not requested this. This does not have an effect on the account security of existing accounts and it does also not mean that an account in the name of the phone number owner has been opened.

We may also use these SMS services to send you reminders regarding important communications you receive from us. We send such reminders only if our original request has the purpose of fulfilling legal obligations we are required to follow as a financial services provider.

This processing is done to adhere to our legal obligations or, with regard to decreasing risks and prevent harm from you, us or third parties, in order to preserve our legitimate interest.

5.3 Customer Care

You can contact our customer care team via email, webform, and chat. We process the personal data that you share with us when you reach out; this includes the content of our communication, your name and email address. Additionally, when you use our chat, we also store additional information such as your login status, your preferred language and your app version together with the content of your communication. This is done via the Zendesk SDK.

This information helps us to provide better support to you.

We also analyze our communication in order to better understand why customers reach out to us, what issues our customers face and what are the reasons for their complaints. This helps us to improve our customer services and our Services in general.

We process your data in order to fulfill our contractual obligations. When we process your data in order to improve our Services (including our customer service), we process your data for our legitimate interest.

6. Recipients or categories of recipients

We only transfers your data to third parties (data processors as well as other data controllers) if this is in line with applicable law. Data controllers process your data within their own responsibility and you can exercise your data subject rights directly against them. Data processors process your data based on our instruction and under our responsibility.

We usually use data processors when we outsource individual sub-parts of our services, such as IT services, handling of some customer care requests, logistics or printing services.

When we transfer data to other financial institutions or public bodies, these entities will usually be data controllers, since they do not process your data based on our instructions and also with regard to their own legal obligations such as anti money laundering, etc.

Depending on how you use our Services, we may transfer your personal data to the following categories of recipients:

- public bodies and institutions (e.g. Deutsche Bundesbank, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), European Banking Authority, European Central Bank, financial authorities or other public authorities of the European states from where Trade Republic operates) for purposes of fulfilling legal (reporting) obligations, fraud and crime prevention, enforcement of claims or legal defense of claims;
- External advisors or lawyers for purposes of fulfilling legal (reporting) obligations, fraud and crime prevention, enforcement of claims or legal defense of claims;
- other credit and financial services institutions or comparable institutions to which Trade Republic transfers personal data in order to carry out the business relationship with you; e.g. escrow banks, payment service providers, stock exchanges or credit agencies, tax reporting service providers;
- service providers that, for example, provide technical services, such as sending SMS messages or performing video identifications, customer service support services or text analysis service (including artificial intelligence services) in order to render our Services to you;

- service providers for risk screenings, background checks, diligence reports or solvency scores;
- service providers regarding crypto assets custody in order to render our Services to you;
- service providers which host and provide the IT infrastructure for us or ensure our IT security in order to render our Services to you;
- Payment cards service providers and document management service providers (like printing services or data destruction services) in order to render our Services to you;
- Marketing services like Social Networks, email service providers, customer data platforms, technical service providers for marketing campaigns or raffles and advertising networks in order to promote our Services to you and others.

You can reach out to us, if you want to receive further information on the respective recipients of personal data.

7. Transfer of personal data to third countries

We only transfer personal data to third parties outside of the European Economic Area, when at least one of the following transfer mechanisms is given to ensure an appropriate level of data protection.

- If the third country has been confirmed by the EU Commission to have an adequate level of data protection pursuant to Art. 45 (1) GDPR;
- Binding Corporate Rules have been established by the recipient;
- The EU Standard Data Protection Clauses as adopted by the European Commission have been agreed upon between us and the third party; or
- You have consented to the transfer.

You can reach out to us, if you want to receive further information on the respective transfer mechanism (possibly including copies of the respective mechanism) and the service providers we use.

8. Automated decision making

We make automated decisions in the meaning of Art. 22 GDPR, when profiling customers in order to fulfill our legal obligation as a bank. These are, for example, requirements to combat money laundering, terrorist financing and crimes that endanger assets. For this purpose, we process your personal data and especially information relating to your transactions, the transaction value, recent changes in your personal data, etc. You can request a review of the automated decision at any time.

Additionally, insofar not prohibited by law, we will inform you of an automated decision in the meaning of Art. 22 GDPR and provide you with further information.

This processing is done to adhere to our legal obligations.

9. Your Privacy Rights and Contact

You have the following privacy rights:

- the right to access your personal data (Art. 15 GDPR);
- the right to rectification (Art. 16 GDPR);
- the right to deletion (Art. 17 GDPR);
- the right to restriction of processing (Art. 18 GDPR);
- a right to object to processing (Art. 21 GDPR); and
- the right to data portability (Art. 20 GDPR) within the framework of the legal requirements.

With regard to the right to access your data and the right to erasure, the restrictions pursuant to Art. 17 (3) GDPR and pursuant to local law Act must be taken into account. You have the right to revoke your consent at any time with effect for the future (Art. 7 (3) sentence 1 GDPR). However, the lawfulness of the processing carried out until the revocation is not affected by this.

In addition, there is the right to complain to the data protection supervisory authority pursuant to Art. 77 GDPR in conjunction with Section 19 German Federal Data Protection Act.

In case of general questions or if you want to exercise your privacy rights, you can reach out to our data protection team under dataprotection@traderepublic.com at any time.

For a direct contact to our data protection officer, please send a letter to Trade Republic Bank GmbH, Data Protection Officer, Brunnenstr. 19-21, 10119 Berlin, Germany or reach out via email asking for a direct contact.

10. Changes to this Privacy Notice

This Privacy Notice may be occasionally updated due to further development of our Services, new features or the implementation of new technologies to secure our Services.

We recommend that you re-read this Privacy Notice from time to time.