

PRIVACY POLICY

effective 12.01.2024

This is the Privacy Policy of Trust Fractal (“**We**”, “**Us**”, or “**Fractal**”). It governs your personal data which is processed in the context of an agreement entered into between you and us on the use of the services of Fractal, including the use of our website and software (“**Services**”). Our Transparency Document with all Privacy Rights and Information, for example to comply with Art. 13 and 14 GDPR and CCPA/CPRA, is available [here](#). In terms of this policy, 'processing' means any operation or set of operations which is performed on your personal data. This personal data may include personal details, details about the way you access our website and software, and details about which Fractal partners you access, among others and is described below in more detail.

This remainder of the policy shall provide information on the processing, the legal basis upon which the Personal data is processed by us and how you may exercise your rights over your Personal Data. If the privacy policy of idOS applies to you, it applies in addition to this policy. Where this Policy refers to provisions contained in the General Data Protection Regulation (GDPR), these provisions shall apply. In case of any conflict between the GDPR and the terms of the Privacy Policy, the provisions of the GDPR shall prevail.

1. Controller and Processor

Your personal data will be processed and controlled by us. Fractal is your data controller in the context of our own software and services and the account you maintain with us.

In case you provide your consent and/or instruct us to process your personal data with Fractal in order to participate in third party services who have legal obligations to collect and process your personal data to be eligible to participate in those third party services, then Fractal is a data processor on behalf of those third parties, who are the controllers, regarding the personal data processing required for that eligibility. Information on such third parties is provided in our software or, alternatively, you can contact us via the email address provided below.

2. Purpose and Legal basis for the processing

In order to use our Services you must register with us. Your use of the Services requires submission of certain necessary information, particularly your e-mail address among other data. You may not use our Services without submitting the information stated as necessary at registration. Therefore, the processing of your personal data in this case, for which Fractal is the controller, is required to carry out our services to which the legal basis is Art. 6 (1) (b) of the GDPR.

After registration, you are able to voluntarily provide further personal data and store these with us so that you may use certain services or software. You may also provide this personal data and provide consent and/or instruct us to transfer such personal data to third parties for the purpose of registering and maintaining a business relationship with such third parties. The legal basis for the processing of personal data is your consent pursuant to Art. 6 (1) (a) of the GDPR and/or a contractual obligation pursuant to Art. 6 (1) (b) of the GDPR. In case your personal data is transferred to third parties for the purpose of

registering and maintaining a business relationship with such third parties, in such a case Fractal is the processor and the third party is the controller of such processing.

While providing personal data for the purposes of registering and maintaining a business relationship with third parties, you may also voluntarily verify yourself and your personal data through Fractal so that you may use your personal data in relation to third parties. The legal basis for the processing of such personal data, for which Fractal is the processor and the third party is the controller, is your consent pursuant to Art. 6 (1) (a) of the GDPR, or the legitimate interest of Fractal or the third party, namely providing and receiving services, pursuant to Art. 6 (1) (f) of the GDPR.

Similarly, your personal data and its verification may be collected, processed and stored for the purposes of satisfying a legal obligation that a third party must meet to enter into and maintain a business relationship with you. In such an event, the legal basis for the processing and storage of such personal data, for which Fractal is the processor and the third party is the controller, is compliance with a legal obligation pursuant to Art. 6(1) (c) of the GDPR.

During any verification process you decide to undergo, you may be asked to voluntarily provide biometric data for the purposes of uniquely identifying yourself as a natural person. In these cases, you give explicit consent for the processing for the purpose of identifying yourself as a natural person. The legal basis for the processing of such personal data, for which Fractal is the controller is your consent pursuant to Art. 9(2)(a) of the GDPR.

We also process your personal data in order to show you the third parties you have authorized and/or instructed us to send personal data to previously and also to make corresponding suggestions of other third parties who you may want to register with using our services. Without being able to process your personal data for this purpose, we would not be able to perform the services we have agreed to with you. Therefore, the processing of your personal data, for which Fractal is the controller is required to carry out our services to which the legal basis is Art. 6 (1) (b) of the GDPR or your consent pursuant to Art. 6 (1) (a) of the GDPR.

In order to notify you of the “Deals” (e.g., bonuses for registering with our partners, discounts in trading fees when using our partners’ services, etc.) we source for you and provide you with the information you need to participate in the Deals, as instructed by you under the terms of the User Agreement we entered into with you, we process your personal data in order to send you emails or SMSs (depending on the method you used to sign-up with Fractal). Without being able to process your personal data for this purpose, we would not be able to perform the services we have agreed to with you. Therefore, the processing of your personal data is required to carry out our services to which the legal basis is Art. 6 (1) (b) of the GDPR.

In case your email address or mobile phone number (depending on the registration method you selected), as well as social media accounts/handles and any other means of communication you provide us, are shared with our Partners as instructed by you under the terms of the User Agreement we entered into with you, we process your personal data in order to allow you to be directly contacted by such Partners about products and services. Without being able to process your personal data for this purpose, we would not be able to perform the services we have agreed to with you. Therefore, the processing of your personal data is required to carry out our services to which the legal basis is Art. 6 (1) (b) of the GDPR.

In case rewards are made available to you under the terms of the User Agreement you entered into with us or any other separate terms and conditions, we process your personal data in order to communicate with you results as well as to distribute rewards. Without being able to process your personal data for this purpose, we would not be able to perform the services we have agreed to with you. Therefore, the processing of your personal data, for which Fractal is the controller, is required to carry out our services to which the legal basis is Art. 6 (1) (b) of the GDPR.

We may use your personal data in order to send you marketing information or emails if you have agreed to receive such. If you have agreed to such, then we may also use the personal data that we collect in order to send you information on the products and services offered by Fractal or its third-party partners. The legal basis for the processing of such personal data, for which Fractal is the controller is your consent pursuant to Art. 6 (1) (a) of the GDPR.

If you voluntarily submit a customer support request via an email, chat or other correspondence system we will also process your personal data for the purpose of fulfilling such request. The legal basis for the processing of such personal data, for which Fractal is the controller is your consent pursuant to Art. 6 (1)(a) of the GDPR. Further, while providing information to us, we may need to contact you to be able to provide our services correctly. The legal basis for the processing of such personal data, for which Fractal is the controller is your consent pursuant to Art. 6 (1)(b) of the GDPR.

Finally, we also process your personal data for the purposes of the legitimate interests, in order to ensure the integrity, security and availability of our system, services, software and your personal data to you, us and the third parties you have authorized. The legal basis for the processing of such data, for which Fractal is the controller is Art. 6 (1) (f) of the GDPR.

3. Fractal Credentials Mechanism

In case you are issued a credential under the terms of the User Agreement you entered into with us, we also process your data for the purposes of issuing you a “Credential” on the blockchain, signed by Fractal, as defined in the aforementioned agreement. Therefore, the processing of your personal data is required to carry out our services to which the legal basis is Art. 6 (1) (b) of the GDPR.

Issuing you a Credential on the blockchain may entail the following processing activities:

- A. Deriving a cryptographic hash of the fields and values of the relevant Fractal ID Level (“hash”);
- B. Writing the hash on the blockchain;
- C. Signing the hash.

Your personal information is not directly written to the blockchain. Instead, to protect your privacy, we take a cryptographic hash of the values and fields of the relevant Fractal ID level and publish only that on-chain. **Please be aware that it is technically impossible to delete any elements written on-chain after being written, even if you retrieve your consent. Under Article 7, paragraph 3 of the GDPR, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.**

4. DID Registry

In case you are assigned a unique identifier - "Fractal ID Identifier" in connection with the DID Registry under the terms of the User Agreement you entered into with us, we also process your data for the purposes of maintaining, on public and/or private blockchains and/or off-chain, a "DID Registry", as defined in the aforementioned agreement. Therefore, the processing of your personal data is required to carry out our services to which the legal basis is Art. 6 (1) (b) of the GDPR.

Maintaining a DID Registry on the blockchain and/or off-chain, allows for the creation of "Arbitrary Membership Lists", such as "ID Level you are approved for", and may entail the following processing activities:

- A. On-chain and/or off-chain mapping of your Fractal ID Identifier to the set of wallet addresses you chose to verify with us;
- B. Addition or removal of your Fractal ID Identifier from those on-chain and/or off-chain Arbitrary Membership Lists, allowing third parties with whom you may register and/or maintain an account and/or business relationship with to enforce sanctions and/or conform with compliance obligations.

In case your information is issued in public and/or private blockchains and/or off-chain registries of other entities, as instructed by you under the terms of the User Agreement you entered into with us, we also process your data for the purposes of contributing to such registries, as defined in the aforementioned agreement. Therefore, the processing of your personal data is required to carry out our services to which the legal basis is Art. 6 (1) (b) of the GDPR.

Contributing to such registries may entail the following processing activities:

- A. Addition or removal of your provided wallet addresses, ID Levels, and any other information required or requested by the entity or the registry mechanisms, from those registries, allowing third parties with whom you may register and/or maintain an account and/or business relationship with to enforce sanctions and/or conform with compliance obligations.

Although the registries are maintained on public and/or private blockchains and/or off-chain, third parties cannot identify you with the information written on-chain and/or off-chain. **Please be aware that it is technically impossible to delete any elements written on-chain after being written, even if you retrieve your consent. Under Article 7, paragraph 3 of the GDPR, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.**

6. Polymath onboarding app

In case you provide your personal data for the purposes of registering and maintaining a business relationship with Polymath Inc., 1st Floor, One Welches, Welches, St. Thomas, BB22025, Barbados ("**Polymath**"), we also process your personal data for the purposes of onboarding you into Polymesh, a blockchain built specifically for security tokens operated

by Polymath (“**Polymesh**”). This is a legitimate interest, Art. 6 (1) (f) GDPR. For data transmission we rely on your consent (Art. 6 (1) (a) GDPR).

Onboarding you into Polymesh specifically may entail the following processing activities:

- A. Verifying with Polymesh whether you already have a [Polymesh “uID” \(unique ID\)](#);
- B. **In case you do not have a Polymesh uID:**
 - a. Requesting a new Polymesh uID from [Polymesh Unique Identity System \(PUIS\)](#);
 - b. Writing a new [Polymesh “distributed ID” \(DID\)](#) for you and publishing it on-chain (on the Polymesh blockchain);
 - c. Deriving a “Pedersen” (cryptographic hash) commitment of your uID and DID and writing it on-chain (on the Polymesh blockchain) on your behalf;
 - d. Revealing your uID to you;
 - e. Signing [Attestations](#) about you and writing a cryptographic hash of these attestations to your Polymesh DID on the Polymesh blockchain*;
- C. **In case you already own a Polymesh uID:**
 - a. Verifying that you own the Polymesh DID;
 - b. Signing [Attestations](#) about you and writing a cryptographic hash of these attestations to your Polymesh DID on the Polymesh blockchain*.

*Your uID is what represents you as a unique individual / entity in Polymesh. Your DID is your Polymesh account number - you can have several accounts associated with your uID. Attestations are descriptive properties of a Polymesh account (or DID) that confirm certain facts (e.g., that your name is Alice). Your uID is not directly written to Polymesh. Instead, to protect your privacy, we take a “Pedersen” (cryptographic hash) of your uID and DID and publish only that on-chain (see more about the linkage between uIDs and DIDs [here](#)). The same applies to Attestations: we do not write the Attestation’s content on-chain, but only a “Pedersen” (cryptographic hash) of the Attestation. These on-chain hashes reveal your personal information only if combined with your uID (which is known by you and Fractal). Your DID is also public and visible on chain, and is implemented as an obfuscated large number to protect your privacy. **Please be aware that it is technically impossible to delete any elements written on-chain after being written, even if you retrieve your consent. Under Article 7, paragraph 3 of the GDPR, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.**

Further information and the applicable data protection provisions of Polymath Inc. may be retrieved under <https://polymath.network/polymesh-testnet/privacy-policy>.

7. Transfer to third countries

We may use processors that process your data in countries outside of the EU. In case we transfer Personal Data outside the territorial scope of the GDPR, we ensure that there is either an adequacy decision by the European Commission or that a similar level of data

protection compared to the GDPR is guaranteed by the use of the contractual clauses at least as protective as those provided by the EU Commission. .

Our [general terms and conditions for data protection](#), which include, among other things, all five versions of the EU Standard Contractual Clauses, the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, a Data Processing Agreement governed by UK law, a CCPA-CPRA Contractor Agreement and a Data Protection and Confidentiality Agreement for suppliers, will automatically form part of all agreements entered into with us. By entering into any other agreement with us, you automatically agree to the respective terms. In detail:

A. EU Standard Contractual Clauses 2021/915 between Controller and Processor:

If you are an EU/EEA-based vendor of ours that processes personal data on our behalf, by conducting business for or with us, you automatically consent to the applicability of our published Standard Contractual Clauses 2021/915. If we are your processor, the Standard Contractual Clauses 2021/915 published by us will also automatically apply between you and us.

B. EU Standard Contractual Clauses 2021/914 MODULE ONE: Transfer Controller to Controller:

To the extent that you are a vendor of ours located in a third country and receive personal data (protected by the GDPR, Member State law or European Economic Area law) from us as a Controller and act as a Controller, by conducting business for or with us, you automatically consent to the applicability of the published Standard Contractual Clauses 2021/914 Module One. The same applies if you act as a Controller and transfer personal data to us as a Controller.

C. EU Standard Contractual Clauses 2021/914 MODULE TWO: Transfer Controller to Processor:

To the extent that you are a vendor of ours located in a third country and receive personal data (protected by the GDPR, Member State law or European Economic Area law) from us as a Controller and act as a Processor, by conducting business for or with us, you automatically consent to the applicability of the published Standard Contractual Clauses 2021/914 Module Two. The same applies if you act as a Controller and transfer personal data to us as a Processor.

D. EU Standard Contractual Clauses 2021/914 MODULE THREE: Transfer Processor to Processor:

To the extent that you are a vendor of ours and we are acting as a Processor (e.g., for a subsidiary or a third party), you are located in a third country and receive international data transfers of personal data (protected by the GDPR, Member State law or European Economic Area law), and you are therefore a (Sub)Processor, by conducting business for or with us, you automatically consent to the applicability of the published Standard Contractual Clauses 2021/914 Module Three. The same applies if you act as a Processor and transfer personal data to us as a (Sub)Processor.

E. EU Standard Contractual Clauses 2021/914 MODULE FOUR: Transfer Processor to Controller:

To the extent that you are a vendor of ours and we are acting as a Processor (e.g., for a subsidiary or a third party), you are located in a third country and receive international data transfers of personal data (protected by the GDPR, Member State law or European

Economic Area law), and you are a Controller, by conducting business for or with us, you automatically consent to the applicability of the published Standard Contractual Clauses 2021/914 Module Four. The same applies if you act as a Processor and transfer personal data to us as a Controller.

F. Confidentiality and Data Protection Agreement for Vendors:

If you are a vendor of ours that is not a processor, or if you receive other and non-personal data from us, by conducting business for or with us, you automatically consent to the applicability of the published Confidentiality and Data Protection Agreement for Vendors.

G. Confidentiality and Data Protection Agreement for Customers:

If you are a customer of ours and data is exchanged between us, we may separately agree to the published Confidentiality and Data Protection Agreement for Customers by a concurring statement. This Confidentiality Agreement shall only become effective upon a separately declaration of intent by the parties.

H. International Data Transfer Agreement (United Kingdom)

To the extent that you are a party to an agreement with us, and personal data transferred by us to you belongs to individuals who are from the United Kingdom or we are based in the United Kingdom, and you yourself are based outside the United Kingdom and receive personal data (protected by the UK GDPR or UK law) from us, by conducting or transacting business for or with us, you automatically consent to the applicability of the published "International Data Transfer Agreement".

I. International Data Transfer Addendum to the European Commission's Standard Contractual Clauses for International Data Transfers (United Kingdom)

To the extent that you are a party to an agreement with us, and personal data we transfer to you belongs to individuals who are based in the UK or where we are based in the UK and you yourself are based outside the UK and receive personal data (which is protected by the UK GDPR or UK law) from us, by carrying out or transacting business for or with us, you automatically consent to the applicability of the published " International Data Transfer Addendum to the European Commission's Standard Contractual Clauses for International Data Transfers".

J. Data Processing Agreement for the United Kingdom

To the extent that you are a party to an agreement with us, and both we and you have our registered office in the United Kingdom, and you process personal data (which is protected by the UK GDPR or UK law) on our behalf, you automatically agree to the applicability of the published "Data Processing Agreement for the United Kingdom" by executing or conducting business for or with us. The same applies if you act as a Controller and transfer personal data to us as a Processor.

K. CCPA-CPRA CONTRACTOR AGREEMENT for California

To the extent that you are a contractor of ours, and we or you have a place of business in California, or employ or engage employees, service providers, processors, or other persons from California, and if the Contractor processes consumer data protected by CCPA-CPRA or California law as part of the relationship, you automatically enter into the CCPA-CPRA CONTRACTOR AGREEMENT published by us with us by each execution or handling of business, either as a Business or as a Contractor.

7.1. Transfers to the United States via EU-U.S. Data Privacy Framework

The European Commission adopted the EU-U.S. Data Privacy Framework on July 10, 2023.

The EU-U.S. Data Privacy Framework is an adequacy decision that allows transfers of personal data from the European Economic Area (EEA), which includes the 27 EU member states and Norway, Iceland, and Liechtenstein, to any U.S. company that has undergone a specified self-certification process. U.S. companies certified through the EU-U.S. Data Privacy Framework are listed on the following website: <https://www.dataprivacyframework.gov/s/participant-search>

Until the EU-U.S. Data Privacy Framework is invalidated by the Court of Justice of the European Union (CJEU) or the European Commission, or superseded by a new adequacy decision, the Controller will transfer Personal Data from the EEA to all companies certified through the EU-U.S. Data Privacy Framework and identified in this Privacy Policy or in the List of Processors and Data Recipients based on the EU-U.S. Data Privacy Framework. These transfers are permitted under Article 45 GDPR.

The Controller points out that in the case of transfers based on the EU-U.S. Data Privacy Framework, neither an analysis of the legal situation in the recipient country (so-called Transfer Impact Assessment) nor supplementary measures, such as encryption to protect transferred personal data from access by U.S. authorities, are required or implemented.

The EU-U.S. Data Privacy Framework obligates certified companies from the U.S. to comply with defined data protection principles, which are based on the requirements of GDPR, and to fulfill data subject rights (e.g., right of access and deletion).

Data Subjects from the EEA who believe that the requirements of the EU-U.S. Data Privacy Framework are not being observed by a certified U.S. company may complain to the European Data Protection Authority responsible for them. This Data Protection Authority will forward the complaint to the European Data Protection Board, which subsequently transmits it to the U.S. authority responsible for handling the complaint.

EEA Data Subjects also have legal remedies before independent arbitration bodies in the United States.

If the Controller is based in the U.S. and certified under the EU-U.S. Data Privacy Framework, the Controller acts as a data importer and complies with the requirements of the EU-U.S. Data Privacy Framework.

If you have any questions about the EU-U.S. Data Privacy Framework, you may contact the Data Protection Officer of the Controller at any time.

A list of our sub-processors must be requested separately from us.

8. Recipients of Data

To conduct our Services, we use third party service providers to provide us with necessary services. We may transfer your personal data to these service providers for further processing based on the terms of this privacy policy and the [transparency document](#) or on the basis of your agreement to use our services. All transfer of data is undertaken by way of secure connections to these service providers. These service providers only receive your personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which your personal data are processed. These include the following categories of service providers: identification service providers, identity verification providers, monitoring services, server hosting providers, newsletter senders, customer relationship or support services, website hosting services, email sending services, web traffic analysis providers.

Additionally, through our services your data may be transferred to third parties so that you may register and/or maintain an account and/or business relationship with those services. The transfer and continual transfer of your personal data to those individual third-party services is based on your consent pursuant to Art. 6 (1) (a) of the GDPR and/or on a contractual obligation pursuant to Art. 6 (1) (b) of the GDPR. When the transfer and continual transfer is based on consent, you may revoke your consent to their access to your personal data on our servers at any time. We may however be required to store your personal data on their behalf and send personal data to them again if there is a legal obligation to do so.

We employ automated systems and software to monitor usage of our website, such as Cookie3 Analytics, which is utilized for both analytical and marketing purposes. Cookie3 Analytics is a resource employed to gather information on how users interact with our website, and it helps in constructing profiles of user activities. For detailed information about how Cookie3 Analytics processes data, please consult the Cookie3 Privacy Policy. Additionally, we might use other methods of analysis to assess our website. These tools aid us in enhancing the website's functionality and the experiences of our users. These entities might use cookies and tracking methods to provide their services. Your Personal Information is not disclosed by us to these third parties.

9. The categories of personal data we process

As described above, we require that you provide us with your email address to register for our services. In addition to collecting your email address, we may collect and process information about the device you use, location settings of the device, and your IP address.

During the use of our services we may require you to provide the following categories of personal data to access certain third parties or even our own services. Your provision of this personal data is always voluntary, but if certain personal data is not provided you may not be able to utilize all services:

name, nationality, country of residence, address, IP address, wallet address, phone number, place of birth, date of birth, identification document information, personal photo, biometric face scans, financial details, and company/workplace details.

Under the terms of the User Agreement we entered into with you, from time to time, while verifying you and your personal data, Fractal may correct information you entered or that we or the software which conducts automated screening of personal data captured from your submitted documentation in order to keep the data accurate, correcting any typos, and to rectify expiry dates of certain documents you uploaded which have a validity period, based on the documentation provided to us, while full traceability is maintained.

We may send you direct advertising about our own goods or services that are similar to those you have requested, ordered or purchased. You may object to direct advertising at any time (e.g. by e-mail). In doing so, you will not incur any costs other than the transmission costs according to the basic rates.

In case your e-mail address is shared with our Partners (as defined under the terms of User Agreement we entered into with you) as instructed by you under the terms of the

aforementioned User Agreement, in order to be directly contacted by such Partners about products and services, as part of our technical and organisational measures to comply with the security of data processing from art. 32 of GDPR and

the protection of your personal data, we will not give access to your originally provided e-mail address to such Partners, but rather make accessible to such Partners only masked e-mail addresses.

10. Your rights when your Personal Data are being processed

We guarantee you the applicable rights of the German data protection laws. Please note that we will require you to provide us with proof of identity before we respond to any requests for the exercise of your rights.

To exercise any of your rights, please contact us at:

Trust Fractal GmbH
Kochhannstraße 6,
10249 Berlin, Germany
Email: privacy@fractal.id

As soon as personal data is being processed, you have the following rights:

(a) Right of access

Pursuant to Art. 15 GDPR, you have the right to access the personal data concerning you. The right to access extends to all data processed by us. The right can be exercised easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing (Recital 63 GDPR). You may contact us to exercise the right to access.

(b) Right to rectification

In accordance with Art. 16 GDPR, you are entitled to demand that we rectify your personal data if they are inaccurate or erroneous. Moreover, you are entitled, taking into account the purposes of the processing, to have incomplete personal data completed, including by means of providing a supplementary statement. You may contact us to exercise the right of rectification.

(c) Right to restriction of processing

In accordance with Art. 18 GDPR, you have the right to demand a restriction of processing for your personal data if one of the conditions set out in Article 18(1) lit. a-d GDPR is fulfilled. This may result in us being no longer able to offer you services. However, if we stop processing the Personal Data, we may use it again if there are valid grounds under data protection law for us to do so (e.g. to comply with regulatory obligations, for the defence of legal claims or for the protection of

another natural or legal persons or for reasons of important public interest of the EU or a Member State). You may contact us to exercise the right to restrictions of processing.

(d) Right to erasure ('right to be forgotten')

In accordance with Art. 17 GDPR, you have the right to have your personal data erased without undue delay. This does not include your personal data that has to be stored due to statutory provisions or in order to assert, execute or defend legal claims. Please note that after deleting the Personal Data, we may not be able to provide the same level of servicing to you as we will not be aware of your preferences. You may contact us to exercise the right to erasure.

(e) Right to data portability

Pursuant to Art. 20 GDPR, you have the right to receive your personal data provided to us in a structured, commonly used and machine-readable format. You also have the right to transfer this data to a third party without hindrance from Fractal, if:

- The processing is based on consent pursuant to Article 6 (1)(a) GDPR or on a contract pursuant to Article 6 (1)(b) GDPR; and
- The processing is carried out by automated means.

The relevant subset of Personal Data is data that you provide us with your consent or for the purposes of performing our contract with you. You may contact us to exercise the right to data portability.

(f) Right to object

Pursuant to Art. 21 GDPR, you have the right to object at any time, on grounds relating to your particular situation, to processing of your personal data which is based on Article 6 (1) lit. e) or lit. f) GDPR, including profiling based on those provisions. However, your personal data might continue to be processed if compelling legitimate grounds for processing which override your interest, rights and freedoms can be demonstrated or if the processing is for the establishment, exercise or defence of legal claims. You may contact us to exercise the right to object.

(g) Right to withdraw your consent

You have the right to withdraw your consent under the data protection law at any time. Withdrawing your consent does not affect the lawfulness of processing based on consent before its withdrawal. The withdrawal of your consent regarding your personal data may lead us not be able to provide the same level of servicing to you as the whole contractual relationship between Fractal and You is dependent on personal data. You may contact us to exercise the right to withdraw your consent.

(h) Right to lodge a complaint with a supervisory authority

Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, place of work or place of the alleged infringement if you consider that the processing of your personal data infringes the GDPR. You have the right to address the supervisory authority for any questions or complaints.

The supervisory authority of Fractal is the data protection supervisory authority in Berlin (*Berliner Beauftragte für Datenschutz und Informationsfreiheit*) <https://datenschutz-berlin.de/>.

11. Automated individual decision-making

Our software conducts automated screening of personal data to issue a decision on your eligibility to participate in third party services. This decision may negatively impact your ability to participate in those third-party services. Pursuant to Art. 22 GDPR, you have the right not to be subject to a decision based solely on automated processing of your biometric data and which produces legal effects concerning you. You have the right to elect to have your data reviewed by a natural person assigned by Fractal. In case you do not agree with the automated decision, or its review, you may not be able to use our services.

12. Data Retention

We will not retain your personal data for longer than is necessary for the purpose it was collected. Thus, we store your data for as long as you have an account with Fractal. You may cancel your account with Fractal at any time, in which case we will delete your data once all outstanding transactions are settled and once we confirm there are no legal retention obligations to continue storing the data. Should we have a legal obligation to continue storing your personal data, either on our own behalf, or on behalf of a third party, we will delete the data as soon as that legal obligation ends.

13. Contact Details

Our full address is:

Trust Fractal GmbH
Kochhannstraße 6,
10249 Berlin, Germany
E-mail: privacy@fractal.id

You may also contact our data protection officer at the above e-mail address or:

Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E.
Franz-Joseph-Str. 11
80801 München (Germany)
Email: info@dg-datenschutz.de
Website: <https://dg-datenschutz.de/>

14. E-mail advertising to customers or prospective customers

We may send you advertising using electronic mail in corresponding application of Section 7 (3) of the German Unfair Competition Act (UWG) if the advertising is in connection with the sale of products or services from us, if we received the electronic mail address from you, and use this address for direct advertising for our own similar goods or services, and you have not objected to the use. You were clearly informed when the

address was collected and will be clearly informed each time it is used that you can object to the use at any time without incurring any costs other than the transmission costs according to the basic rates.

15. Webinars and Online-Meetings

We organize webinars and invite customers, prospective customers, service providers and suppliers, including their and our employees, to online meetings. We use different third-party providers (operators of online meeting applications, application providers). Which third-party provider we use for a specific webinar or online meeting is recognizable from the participation link. You can find the privacy policy and, if applicable, additional legally required information on the website of the respective third-party provider.

By registering, accepting, and/or participating in a webinar or online meeting, you explicitly consent to your personal data being processed for the purposes of registering, planning, organizing and conducting the webinar or online meeting, which includes transfers to third-party providers (which may be located in a third country), and to audio, film or photo recordings being transmitted and/or published, and/or published to other participants as part of the webinar or online meeting. By a single action, you give multiple consents. By registering, accepting, in and/or participating, you also voluntarily give your explicit consent pursuant to 49 (1) (1) (a) GDPR for data transfers to third countries for the purposes of registration, planning, organization and implementation of the webinar or online meeting, in particular for such transfers to third countries for which an adequacy decision of the EU/EEA is absent or does exist, and to companies or other entities that are not subject to an existing adequacy decision on the basis of self-certification or other accession criteria, and that involve significant risks and no appropriate safeguards for the protection of your personal data (e.g., because of Section 702 FISA, Executive Order EO12333 and the CloudAct in the USA). We hereby inform you in advance regarding your voluntary and explicit consent that in third countries there may not be an adequate level of data protection and that your data subject rights may not be enforceable, and that published personal data may not be deleted, may not be altered or may not be made anonymous at all, only conditionally and/or with a delay. You give your consent voluntarily. You are not obligated to give consent and may choose to stay away from or not participate in the webinar or online meeting, which we will consider a refusal of our request to give consent. You have the right to withdraw your data protection consent in whole or in part at any time with effect for the future, in particular by deactivating, switching off or not activating your sound, film or photo transmissions during the webinar or online meeting. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. By your action, you also confirm that you have read and acknowledged this Privacy Policy and the transparency document linked in it.

16. Changes to the privacy policy or the purpose of processing

This Policy was last updated on the effective date noted above. This Policy may be amended or updated from time to time to reflect changes in our privacy practices with respect to the processing of personal data or changes in the applicable law. We encourage you to save this Privacy Policy locally on your computer and to regularly check this page so that you may review any changes we might make. If we make a material change to the Privacy Policy, you will be provided with appropriate notice.