Privacy Policy

We are very pleased that you are interested in our organization. The protection of your personal data is particularly important to our management. You can generally use our websites without disclosing personal data to us. However, if you wish to use more specific services via our websites, other online presences, applications, and social media pages operated by us, we may need to process your personal data. If we wish to process data about you and cannot rely on any other legal basis, we will always first ask for your consent (for example, via a cookie banner).

We always comply with applicable data protection laws when handling your personal data (such as name, address, e-mail address, or telephone number). With this privacy policy, we inform you about which data we process. In addition, this privacy policy explains which rights you have as a data subject.

We have taken various technical and organizational measures to protect your data on our websites as best as possible. Nevertheless, there are always risks on the Internet, and complete protection cannot be guaranteed. Therefore, if you prefer, you can also provide us with your personal data by other means, for example, by telephone.

This privacy policy serves not only to fulfill the obligations of the GDPR and to comply with the laws of the member states of the European Union (EU) and the European Economic Area (EEA). This privacy policy is also intended to comply with the legal provisions of countries such as the United Kingdom (UK-GDPR), the Swiss Federal Data Protection Act and the Swiss Data Protection Ordinance (DSG, DSV), the California Consumer Privacy Act (CCPA/CPRA), China’s Personal Information Protection Law (PIPL), the Delaware Personal Data Privacy Act (DPDPA), the Tennessee Information Protection Act (TIPA), the Minnesota Consumer Data Privacy Act (MCDPA), the Iowa Act Relating to Consumer Data Protection (ICDPA), the Maryland Online Data Privacy Act (MODPA), the Nebraska Data Privacy Act (NDPA), the New Hampshire Consumer Data Privacy Law (SB255), the New Jersey Data Privacy Law (SB332), the South Carolina Consumer Privacy Bill (House Bill 4696) and other global data protection regulations, and should be interpreted accordingly. The following privacy policy shall be interpreted for each country, state, or province in such a way that the terminology and legal bases used correspond to those applicable in the respective jurisdiction.

For reasons of better readability, we refrain from using gendered language (male, female, diverse, and other gender identities (m/f/d/other)) simultaneously on our websites, in publications, in communication, and in this privacy policy. All terms used apply equally to all genders.

For suggestions for improvement regarding the texts in this privacy policy, or if you need an external data protection officer, please contact the author of the texts: Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E.

Definitions

In our privacy policy, we use specific terms from various data protection laws. We want our statement to be easy to understand and therefore explain these terms in advance.

The following definitions may, where applicable, be interpreted or extended based on the jurisprudence of the Court of Justice of the European Union (CJEU), the General Court (GC), the Swiss Federal Supreme Court (BGE), the Supreme Court of the United Kingdom (UKSC), or on the basis of national data protection laws or national case law of a country or state, including but not limited to California, including judge-made law, also under Common Law, if this is necessary for the application of the law in a particular case.

We use, among others, the following terms in this privacy policy:

a) Personal data

Personal data means any information relating to an identified or identifiable natural person (hereinafter referred to as the "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person, or who must be regarded as such based on national data protection laws or national case law of a state or province, including judge-made law, also under Common Law.

b) Data subject

A data subject is any identified or identifiable natural person whose personal data is processed by the controller, a processor, an international organization, or another data recipient, and persons who must be regarded as such on the basis of national

data protection laws or national case law of a state or province, including judge-made law, also under Common Law.

c) Processing

Processing means any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

d) Restriction of processing

Restriction of processing means the marking of stored personal data with the aim of limiting its future processing.

e) Profiling

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

f) Pseudonymization

Pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

g) Controller

Controller means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

h) Processor

Processor means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

i) Recipient

Recipient means a natural or legal person, public authority, agency, or another body to which personal data is disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients.

j) Third party

Third party means any natural or legal person, public authority, agency, or body other than the data subject, the controller, the processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

k) Consent

Consent means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

Name and address of the controller

Controller within the meaning of the General Data Protection Regulation, other data protection laws applicable in the Member States of the European Union and the European Economic Area, the British data protection laws, the Swiss data protection laws (DSG, DSV), the California data protection laws (CCPA/CPRA), the Chinese data protection law (PIPL), as well as international laws and other provisions of a data protection nature, is:

Digital Tribe GmbH

Alte Landstraße 237

22391 Hamburg

E-mail: support@digitaltri.be

Website: https://www.digitaltri.be/

Name and contact details of the data protection officer

Prof. Dr. h.c. Heiko Jonny Maniero

Franz-Joseph-Str. 11

80801 Munich

Germany

Tel.: +49 (0)178 - 6264376

E-mail: info@dg-datenschutz.de

Collection of general data and information

Our websites collect a series of general data and information with each access of the websites by a data subject or an automated system. This general data and information are stored in the log files of the respective server. Collected may be, among other things, (1) the types and versions of browsers used, (2) the operating system used by the accessing system, (3) the website from which an accessing system reaches our websites (so-called referrer), (4) the sub-websites accessed by an accessing system on our websites, (5) the date and time of access to the website, (6) an Internet protocol address (IP address), (7) the Internet service provider of the accessing system, and (8) other similar data and information used for security purposes in the event of attacks on our information technology systems.

When using this general data and information, we generally do not draw any conclusions about the data subject. This information is needed to (1) deliver the contents of our websites correctly, (2) optimize the content of our websites and the advertising for them, (3) ensure the long-term functionality of our information technology systems and the technology of our websites, and (4) provide law enforcement authorities with the information necessary for prosecution in the event of a cyberattack. Therefore, this anonymously collected data and information are evaluated statistically and also with the aim of increasing data protection and data security in our company, ultimately ensuring an optimal level of protection for the

personal data we process. The data of the server log files are stored separately from all personal data provided by a data subject.

Purpose of processing is hazard prevention and ensuring IT security, as well as the purposes mentioned above. Legal basis is Art. 6 (1) (f) GDPR. Our legitimate interest is, in particular, the protection of our information technology systems. The log files are deleted after the purposes mentioned have been achieved.

Contact possibility via the website and other data transmissions and your consent

Our websites contain information that enables quick electronic contact with our company as well as direct communication with us, which also includes a general address of the so-called electronic mail (e-mail address) and, where applicable, a telephone number. If a data subject contacts us by e-mail, via a contact form, via an input form, or otherwise, the personal data transmitted by the data subject is stored automatically. Such personal data transmitted voluntarily by a data subject to us is processed for the purpose of handling or contacting the data subject.

For the transmission, storage, and processing of your contact data and inquiries and for establishing contact, we obtain your consent according to Art. 6 (1) (a) GDPR and Art. 49 (1) (1) (a) GDPR as follows:

By transmitting your personal data, you voluntarily consent to the processing of the personal data you have entered or transmitted for the purpose of handling your inquiry and for establishing contact. By transmitting your data to us, you also voluntarily give express consent according to Art. 49 (1) (1) (a) GDPR to data transfers to third countries to and by the companies named in this privacy policy and for the stated purposes, in particular for such transfers to third countries for which there is or is not an adequacy decision of the EU/EEA, as well as to companies or other entities not covered by an adequacy decision due to self-certification or other adherence mechanisms, and in which or for which there are significant risks and no adequate safeguards for the protection of your personal data (e.g., due to §702 FISA, Executive Order EO12333, and the Cloud Act in the USA). When giving your voluntary and express consent, you were aware that in third countries there may not be an adequate level of data protection and that your data subject rights may not be enforceable. You can revoke your data protection consent at any time with effect for the future. The lawfulness of the processing carried out on the basis of the consent until revocation shall not be affected by the revocation of the consent. With a single action (the input and transmission), you grant several consents. These include consents under EU/EEA data protection law

as well as under the CCPA/CPRA, ePrivacy and telecommunications law, and other international legal provisions that serve, among other things, as a legal basis for the intended further processing of your personal data. By your action, you also confirm that you have read and acknowledged this privacy policy.

Routine erasure and restriction of personal data

We process and store personal data only for the period necessary to achieve the purpose of processing or insofar as this is provided for by the European legislator or another legislator in laws or regulations to which we are subject, or as long as a legal basis for the processing exists.

If the purpose of processing ceases to apply, or if a storage period prescribed by the European legislator or another competent legislator expires, or if the legal basis for processing ceases to apply, the personal data will be routinely and in accordance with the statutory provisions restricted or deleted.

Rights of the data subject under the GDPR

a) Right of confirmation

Every data subject has the right to obtain confirmation from the controller as to whether or not personal data concerning them are being processed.

If a data subject wishes to exercise this right, they may contact us at any time.

b) Right of access

Every data subject has the right to obtain from the controller, at any time and free of charge, information about the personal data stored about them and a copy of such data. Furthermore, the European legislator has granted the data subject access to the following information:

• the purposes of processing,

• the categories of personal data that are processed,

• the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations,

• where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period,

• the existence of the right to request rectification or erasure of personal data or restriction of processing concerning the data subject or to object to such processing,

• the existence of the right to lodge a complaint with a supervisory authority,

• where the personal data are not collected from the data subject: any available information as to their source,

• the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Furthermore, the data subject has the right to know whether personal data have been transferred to a third country or an international organization. Where this is the case, the data subject also has the right to be informed of the appropriate safeguards relating to the transfer.

If a data subject wishes to exercise this right, they may contact us at any time.

c) Right to rectification

Every data subject has the right to obtain the rectification of inaccurate personal data concerning them without undue delay. Furthermore, the data subject has the right to have incomplete personal data completed, including by means of a supplementary statement, taking into account the purposes of the processing.

If a data subject wishes to exercise this right, they may contact us at any time.

d) Right to erasure (“right to be forgotten”)

Every data subject has the right to obtain from the controller the erasure of personal data concerning them without undue delay where one of the following grounds applies and insofar as the processing is not necessary:

• The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

• The data subject withdraws consent on which the processing is based according to Article 6 (1) (a) GDPR or Article 9 (2) (a) GDPR, and there is no other legal ground for the processing.

• The data subject objects to the processing pursuant to Article 21 (1) GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21 (2) GDPR.

• The personal data have been unlawfully processed.

• The erasure of the personal data is required for compliance with a legal obligation in Union or Member State law to which the controller is subject.

• The personal data have been collected in relation to the offer of information society services referred to in Article 8 (1) GDPR.

If one of the above reasons applies and a data subject wishes to request the deletion of personal data stored by us, they may contact us at any time.

Where we have made the personal data public and our organization as controller is obliged pursuant to Article 17 (1) GDPR to erase the personal data, we, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other controllers processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data, insofar as processing is not required.

e) Right to restriction of processing

Every data subject has the right to obtain from the controller restriction of processing where one of the following applies:

• The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.

• The processing is unlawful, the data subject opposes the erasure of the personal data and requests the restriction of their use instead.

• The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims.

• The data subject has objected to processing pursuant to Article 21 (1) GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

If one of the above conditions is met and a data subject wishes to request the restriction of personal data stored by us, they may contact us at any time.

f) Right to data portability

Every data subject has the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used, and machine-readable format. They also have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on consent pursuant to Article 6 (1) (a) GDPR or Article 9 (2) (a) GDPR, or on a contract pursuant to Article 6 (1) (b) GDPR, and the processing is carried out by automated means, unless the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

In exercising their right to data portability pursuant to Article 20 (1) GDPR, the data subject has the right to have the personal data transmitted directly from one controller to another, where technically feasible and provided that this does not adversely affect the rights and freedoms of others.

If a data subject wishes to exercise this right, they may contact us at any time.

g) Right to object

Every data subject has the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them which is based on Article 6 (1) (e) or (f) GDPR, including profiling based on those provisions.

We shall no longer process the personal data in the event of the objection, unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject, or the processing serves the establishment, exercise, or defense of legal claims.

Where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to processing of personal data concerning them

for such marketing, which includes profiling to the extent that it is related to such direct marketing. If the data subject objects to processing for direct marketing purposes, we will no longer process the personal data for such purposes.

Furthermore, the data subject has the right, on grounds relating to their particular situation, to object to processing of personal data concerning them for scientific or historical research purposes or statistical purposes pursuant to Article 89 (1) GDPR, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

If a data subject wishes to exercise this right, they may contact us at any time. The data subject is also free, in the context of the use of information society services, notwithstanding Directive 2002/58/EC, to exercise their right to object by automated means using technical specifications.

h) Automated individual decision-making, including profiling

Every data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, unless the decision (1) is necessary for entering into, or the performance of, a contract between the data subject and the controller, or (2) is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or (3) is based on the data subject's explicit consent.

If the decision (1) is necessary for entering into, or the performance of, a contract between the data subject and the controller, or (2) is based on the data subject's explicit consent, we shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express their point of view, and to contest the decision.

If a data subject wishes to exercise this right, they may contact us at any time.

i) Right to withdraw data protection consent

Every data subject has the right to withdraw consent to the processing of personal data at any time.

If a data subject wishes to exercise this right, they may contact us at any time.

General purpose of processing, categories of data processed, and categories of recipients

The general purpose of processing personal data is the execution of all operations that concern the controller, customers, prospects, business partners, or other contractual or pre-contractual relationships between these groups (in the broadest sense) or legal obligations of the controller. This general purpose applies where no more specific purposes are stated for a particular processing activity.

The categories of personal data we process include customer data, prospect data, employee data (including applicant data), and supplier data. The categories of recipients of personal data are public authorities, external entities, internal processors, intra-group processors, and other entities.

A list of our processors and data recipients in third countries, as well as any international organizations, is either published on our website or can be requested from us free of charge.

Legal bases for processing

Article 6 (1) (a) GDPR serves as the legal basis for processing operations for which we obtain consent for a specific processing purpose. If the processing of personal data is necessary for the performance of a contract to which the data subject is party, such as processing operations required for the supply of goods or the provision of any other service or consideration, the processing is based on Article 6 (1) (b) GDPR. The same applies to such processing operations that are necessary for carrying out pre-contractual measures, for example in the case of inquiries concerning our products or services.

If our company is subject to a legal obligation by which processing of personal data is required, such as for the fulfillment of tax obligations, the processing is based on Article 6 (1) (c) GDPR.

In rare cases, processing of personal data may be necessary in order to protect the vital interests of the data subject or of another natural person. This would be the case, for example, if a visitor were injured in our company and their name, age, health insurance data, or other vital information had to be passed on to a doctor, hospital, or other third party. In this case, the processing would be based on Article 6 (1) (d) GDPR.

If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, the legal basis is Article 6 (1) (e) GDPR.

Ultimately, processing operations could be based on Article 6 (1) (f) GDPR. This legal basis applies to processing operations that are not covered by any of the aforementioned legal grounds, if processing is necessary for the purposes of the legitimate interests pursued by our company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. Such processing operations are particularly permitted because they have been specifically mentioned by the European legislator, who considered that a legitimate interest could be assumed, for example, where the data subject is a client of the controller (Recital 47, sentence 2 GDPR).

Legitimate interests pursued by the controller or by a third party and direct marketing

If the processing of personal data is based on Article 6 (1) (f) GDPR and no more specific legitimate interests are specified, our legitimate interest is the conduct of our business for the benefit of the well-being of our employees and our shareholders.

We may send you direct marketing communications regarding our own goods or services that are similar to those you have requested, ordered, or purchased. You may object to direct marketing at any time (for example, by email). You will incur no costs other than the transmission costs according to basic rates. The processing of personal data for direct marketing purposes is based on Article 6 (1) (f) GDPR. The legitimate interest is direct marketing.

Duration for which the personal data are stored

The criterion for the duration of storage of personal data is the respective statutory retention period. If no statutory retention period exists, the criterion is the contractual or internal retention period. After the period has expired, the corresponding data will be routinely deleted, provided they are no longer necessary for the fulfillment of a contract or the initiation of a contract. This applies in particular to all processing operations for which no more specific criteria have been defined.

Statutory or contractual requirements to provide personal data; necessity for contract conclusion; obligation of the data subject to provide personal data; possible consequences of failure to provide

We inform you that the provision of personal data may in part be required by law (for example, tax regulations) or may also result from contractual provisions (for example, information about the contracting party). In some cases, it may be necessary for a data subject to provide us with personal data that must subsequently be processed by us in order to conclude a contract. The data subject is, for example, obliged to provide us with personal data if our organization enters into a contract with them. Failure to provide personal data would mean that the contract with the data subject could not be concluded.

Before providing personal data, the data subject must contact us. We will inform the data subject on a case-by-case basis whether the provision of personal data is required by law or contract or necessary for the conclusion of a contract, whether there is an obligation to provide the personal data, and what the consequences of failing to provide the personal data would be.

Existence of automated decision-making

As a responsible company, we normally refrain from automatic decision-making or profiling. If, in exceptional cases, we carry out automated decision-making or profiling, we will inform the data subject separately or in a subsection of this privacy policy (here on our website). In this case, the following applies:

Automated decision-making, including profiling, may occur if this (1) is necessary for entering into, or the performance of, a contract between the data subject and us, or (2) is authorized by Union or Member State law to which we are subject and that law provides for appropriate measures to safeguard the rights and freedoms and legitimate interests of the data subject, or (3) takes place with the explicit consent of the data subject.

In the cases referred to in Article 22 (2) (a) and (c) GDPR, we shall take appropriate measures to safeguard the rights and freedoms and legitimate interests of the data subject. In such cases, you have the right to obtain human intervention on the part of the controller, to express your own point of view, and to contest the decision.

Meaningful information about the logic involved, as well as the significance and intended consequences of such processing for the data subject, will be provided in this privacy policy where applicable.

Recipients in a third country and appropriate or suitable safeguards and the possibility of obtaining a copy thereof or where they are available

According to Article 46 (1) GDPR, the controller or a processor may only transfer personal data to a third country if the controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Appropriate safeguards may, without requiring specific authorization from a supervisory authority, be provided through standard data protection clauses under Article 46 (2) (c) GDPR.

With all recipients in third countries, before the first transfer of personal data, EU Standard Contractual Clauses or other suitable safeguards are agreed, or the transfers are based on adequacy decisions. Consequently, it is ensured that for all personal data processing, appropriate safeguards, enforceable rights, and effective remedies are guaranteed. Every data subject may obtain a copy of the Standard Contractual Clauses or adequacy decisions from us. In addition, the Standard Contractual Clauses and adequacy decisions are available in the Official Journal of the European Union.

Article 45 (3) GDPR empowers the European Commission to decide, by means of an implementing act, that a non-EU country ensures an adequate level of protection. This means a level of protection for personal data that is essentially equivalent to that guaranteed within the EU. Adequacy decisions result in personal data flowing freely from the EU (as well as from Norway, Liechtenstein, and Iceland) to a third country without any further barriers. Similar provisions apply for the United Kingdom, Switzerland, and several other states.

In all cases where the European Commission, or a government or competent authority of another state, has decided that a third country ensures an adequate level of protection and/or a valid framework exists (e.g. EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework, UK Extension to the EU-U.S. Data Privacy Framework), all transfers from us to members of such frameworks (e.g. self-certified entities) are based solely on the entity’s membership in the respective framework or on the relevant adequacy decisions. If we or one of our group companies are members of such a framework, all transfers to us or our group companies are based solely on the membership of the respective company in this

framework. If we or one of our group companies are located in a third country with an adequate level of protection, all transfers to us or our group companies are based solely on the respective adequacy decisions.

Every data subject may obtain a copy of the frameworks from us. In addition, the frameworks are available in the Official Journal of the European Union or in the published legislative materials or on the websites of data protection authorities or other government agencies or institutions.

Right to lodge a complaint with a supervisory authority

As a controller, we are obliged to inform the data subject of the existence of the right to lodge a complaint with a supervisory authority. The right to lodge a complaint is governed by Article 77 (1) GDPR. According to this provision, every data subject has the right, without prejudice to any other administrative or judicial remedy, to lodge a complaint with a supervisory authority, in particular in the Member State of their habitual residence, place of work, or place of the alleged infringement, if the data subject considers that the processing of personal data relating to them infringes the General Data Protection Regulation.

The right to lodge a complaint has been restricted by the Union legislator only to the extent that it may be exercised with only one supervisory authority (Recital 141, sentence 1 GDPR). This rule is intended to avoid duplicate complaints about the same matter by the same data subject. Therefore, if a data subject wishes to lodge a complaint about us, they are kindly requested to contact only one supervisory authority.

Data protection in applications and in the application procedure

During the application process, we collect and process the personal data of applicants. The processing may also take place by electronic means. This is particularly the case if an applicant submits the relevant application documents to us electronically, for example by e-mail or via a web form on our or third-party websites.

For applicant data, the purpose of data processing is to conduct an evaluation of the application within the recruitment process. For this purpose, we process all data provided by you. Based on the information transmitted within the scope of the application, we check whether you will be invited to an interview (as part of the selection process). Furthermore, in the case of generally suitable applicants, we

process certain additional personal data provided by you during the interview that are essential to our selection decision.

The legal bases for data processing are Article 6 (1) (b) GDPR, Article 9 (2) (b) and (h) GDPR, Article 88 (1) GDPR, as well as national legal provisions.

If no employment contract is concluded with the applicant, the application documents will be deleted no later than six months after notification of the rejection decision, unless the deletion conflicts with other legitimate interests of the controller. A legitimate interest in this sense could, for example, be the need to present evidence in a legal proceeding.

Data protection provisions for the use and application of Hetzner

Hetzner Online GmbH is a provider of hosting services and data center infrastructure, offering a wide range of products from web hosting and managed hosting to dedicated servers and cloud solutions. With powerful and reliable technology, Hetzner supports companies and individuals in building and scaling their online presence. Customers benefit from state-of-the-art data centers, comprehensive security and data protection, and dedicated customer service.

When using Hetzner services, personal data such as names, addresses, contact details, payment information, and usage data of the provided services are processed. This information is necessary to manage user accounts, provide services, offer support, and ensure system security.

The operating company of the service and thus the recipient of the personal data is Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany. The representative under national law in the United Kingdom is Hetzner Ltd, 7 Coronation Road, Dephna House, Launchese #105, London, NW10 7PQ, United Kingdom.

Purposes for which personal data are to be processed, and the legal basis for processing: The purpose of processing lies in the use and optimization of hosting services and data center infrastructure. Processing is based on Article 6 (1) (b) GDPR for the performance of a contract to which the data subject is a party, as well as Article 6 (1) (f) GDPR, with the legitimate interest being the provision and use of secure, reliable, and efficient hosting solutions.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and the operator of the service or statutory

or contractual retention periods. The provision of personal data is generally neither legally nor contractually required nor necessary for the conclusion of a contract. You are generally not obliged to provide personal data to us or the operator of the service. However, if you do not provide personal data, our services or those of the operator may not be usable.

Further information and the applicable data protection provisions of Hetzner can be found at https://www.hetzner.com

Data protection provisions for the use and application of STRATO

STRATO is a provider of web hosting services, domain registration, cloud storage, online stores, and other Internet-based services. With a comprehensive portfolio of products, STRATO supports both individuals and businesses in effectively creating and managing their online presence. STRATO's services are designed to offer users reliable, secure, and user-friendly solutions for their web projects.

When using STRATO services, personal data such as names, addresses, e-mail addresses, telephone numbers, payment information, and usage data of the offered services are processed. This information is necessary to provide the services, manage user accounts, handle support requests, and ensure the security of user data.

The operating company of the service and thus the recipient of the personal data is STRATO GmbH, Otto-Ostrowski-Straße 7, 10249 Berlin, Germany.

Purposes for which personal data are to be processed, and the legal basis for processing: The purpose of data processing lies in the use of web hosting services and other products offered. Processing is based on the performance of a contract pursuant to Article 6 (1) (b) GDPR, to which the data subject is a party, as well as on legitimate interests pursuant to Article 6 (1) (f) GDPR, such as improving our services, ensuring network and information security, and using external hosting.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and the operator of the service or statutory or contractual retention periods. The provision of personal data is generally neither legally nor contractually required nor necessary for the conclusion of a contract. You are generally not obliged to provide personal data to us or the operator of the service. However, if you do not provide personal data, our services or those of the operator may not be usable.

Further information and the applicable data protection provisions of STRATO can be found at https://www.strato.de

Data protection provisions for the use and application of Cloudflare

Cloudflare provides a wide range of services to enhance the security, performance, and reliability of websites and web applications. The core features include DDoS protection, web application firewall, content delivery network services, secure DNS services, and more. By using Cloudflare, we can protect our online presence from cyberattacks, improve the loading speed of our website, and ensure the overall availability of our services.

When using Cloudflare services, data such as IP addresses, system configurations, and network traffic information are processed. This information is necessary to prevent threats, optimize data traffic, and provide insights into website usage.

The operating company of the service and thus the recipient of the personal data is Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, United States of America. For data subjects in the EU and EEA, Cloudflare Netherlands B.V., Keizersgracht 62, 1015CS Amsterdam, Netherlands, acts as the contact and representative under Article 27 GDPR. The representative under national law in the United Kingdom is Cloudflare, Ltd., County Hall/The Riverside Building, Belvedere Road, London, SE1 7PB, United Kingdom.

Purposes for which personal data are to be processed, and the legal basis for processing: The purpose of processing lies in the use of services to secure and optimize websites and web applications. Processing is based on Article 6 (1) (f) GDPR, with the legitimate interest being to ensure the security, performance, and reliability of our online presence.

The operator of the service is based in a third country, namely the United States. Transfers to third countries may be based on the conclusion of standard contractual clauses or other appropriate or suitable safeguards referred to in Article 46 (2) GDPR. Cloudflare, Inc. may have concluded one of the EU standard contracts with us. You can request a copy of the appropriate or suitable safeguards from us.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and the operator of the service or statutory or contractual retention periods. The provision of personal data is generally neither legally nor contractually required nor necessary for the conclusion of a contract. You are generally not obliged to provide personal data to us or the operator of the

service. However, if you do not provide personal data, our services or those of the operator may not be usable.

Further information and the applicable data protection provisions of Cloudflare, Inc. can be found at https://www.cloudflare.com

Data protection provisions for the use and application of Google Cloud Platform (GCP)

The Google Cloud Platform (GCP) is a suite of cloud computing services provided by Google that enables companies to build, deploy, and scale applications, websites, and services on Google's infrastructure. The services include computing power, data storage, databases, networking, big data, machine learning, and developer tools. The use of GCP allows us to operate our applications and store data securely and efficiently in the cloud.

When using GCP services, personal data such as user identification, IP addresses, metadata, and content data (such as files or database entries) may be processed. This data is required to provide, secure, and optimize the services.

The operating company of the Google Cloud Platform and thus the recipient of the personal data is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. For data subjects in the EU and EEA, Google Ireland Limited acts as the controller. The parent company is Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States of America.

Purposes for which personal data are to be processed and the legal basis for processing: The purpose of data processing is the use of cloud computing services to host, manage, and process data as part of our business activities. The processing is based on Article 6 (1) (b) GDPR for the performance of a contract, as well as Article 6 (1) (f) GDPR, with our legitimate interest being the secure and efficient operation of our digital infrastructure.

Transfers to third countries (in particular the USA) are based on the EU Standard Contractual Clauses pursuant to Article 46 (2) (c) GDPR or adequacy decisions such as the EU-U.S. Data Privacy Framework.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and Google or statutory or contractual retention periods. The provision of personal data is generally neither legally nor contractually required nor necessary for the conclusion of a contract. However, if no

personal data are provided, the services or applications based on GCP may not function correctly.

Further information and the applicable data protection provisions of Google can be found at https://cloud.google.com/privacy and https://policies.google.com/privacy

Data protection provisions for the use and application of Twilio

Twilio provides cloud-based communication solutions that enable companies to integrate communication services such as voice, SMS, video, and messaging into their applications via APIs. Using Twilio allows us to send messages, make calls, and offer interactive communication functionalities within our services.

When using Twilio, data such as telephone numbers, message contents, call recordings, and metadata (such as time, duration, and IP addresses) are processed. This information is necessary to deliver and manage the communication services.

The operating company of the service and thus the recipient of the personal data is Twilio Ireland Limited, 25-28 North Wall Quay, Dublin 1, Ireland. The parent company is Twilio Inc., 101 Spear Street, 5th Floor, San Francisco, CA 94105, United States of America.

Purposes for which personal data are to be processed and the legal basis for processing: The purpose of processing is the provision of communication services within our products and services. Processing is based on Article 6 (1) (b) GDPR for the performance of a contract, as well as Article 6 (1) (f) GDPR, with the legitimate interest being the provision of efficient and reliable communication options.

The operator of the service is based in a third country (USA). Transfers to the USA are based on the EU Standard Contractual Clauses pursuant to Article 46 (2) (c) GDPR or the EU-U.S. Data Privacy Framework.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and Twilio or statutory or contractual retention periods. The provision of personal data is generally neither legally nor contractually required nor necessary for the conclusion of a contract. However, if personal data are not provided, communication functionalities may be restricted or unavailable.

Further information and the applicable data protection provisions of Twilio can be found at https://www.twilio.com/legal/privacy

Data protection provisions for the use and application of Firebase

Firebase is a platform provided by Google that offers a variety of services for developing mobile and web applications. These include real-time databases, authentication, analytics, cloud storage, hosting, and more. We use Firebase to develop and manage our applications efficiently and to analyze their use.

When using Firebase services, data such as user IDs, IP addresses, usage behavior, device information, and app interaction data may be processed. This data helps improve app performance and security and provide a better user experience.

The operating company of the service and thus the recipient of the personal data is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. The parent company is Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States of America.

Purposes for which personal data are to be processed and the legal basis for processing: The purpose of data processing is the operation, improvement, and security of mobile and web applications. Processing is based on Article 6 (1) (f) GDPR, with the legitimate interest being the efficient and secure operation of our digital services. If consent is required for specific features (e.g., analytics), processing is based on Article 6 (1) (a) GDPR.

Transfers to third countries (in particular the USA) are based on EU Standard Contractual Clauses pursuant to Article 46 (2) (c) GDPR or the EU-U.S. Data Privacy Framework.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and Google or statutory or contractual retention periods. The provision of personal data is generally not legally or contractually required. However, without certain data, the functionality of our applications may be limited.

Further information and the applicable data protection provisions of Firebase can be found at https://firebase.google.com/support/privacy and https://policies.google.com/privacy

Data protection provisions for the use and application of Stripe

Stripe is a payment service provider that enables online payments via credit card, direct debit, and other payment methods. The use of Stripe allows us to process transactions securely and efficiently.

When using Stripe, personal data such as name, e-mail address, billing address, payment data (e.g., card numbers), and transaction information are processed.

The operating company of the service and thus the recipient of the personal data is Stripe Payments Europe, Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Ireland. The parent company is Stripe, Inc., 354 Oyster Point Boulevard, South San Francisco, CA 94080, United States of America.

Purposes for which personal data are to be processed and the legal basis for processing: The purpose of processing is the handling of payment transactions. The processing is based on Article 6 (1) (b) GDPR (performance of a contract) and Article 6 (1) (f) GDPR (legitimate interest in secure payment processing).

Transfers to third countries (in particular the USA) are based on EU Standard Contractual Clauses pursuant to Article 46 (2) (c) GDPR or the EU-U.S. Data Privacy Framework.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and Stripe or statutory retention periods (e.g., under tax law).

The provision of personal data is contractually required for payment processing. Without this data, payments cannot be processed.

Further information and the applicable data protection provisions of Stripe can be found at https://stripe.com/privacy

Data protection provisions for the use and application of OpenAI

OpenAI provides artificial intelligence models and APIs that enable text generation, natural language understanding, and other AI-powered functionalities. We use OpenAI technologies to enhance our products and services, such as chatbots, text analysis, and automation tools.

When using OpenAI services, data such as user inputs, context information, and usage data may be transmitted to and processed by OpenAI’s servers to generate responses and improve the model.

The operating company of the service and thus the recipient of the personal data is OpenAI Ireland Limited, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland. The parent company is OpenAI, L.L.C., 3180 18th Street, San Francisco, CA 94110, United States of America.

Purposes for which personal data are to be processed and the legal basis for processing: The purpose of processing lies in the use of AI models to enable automated responses, analysis, or optimization within our services. Processing is based on Article 6 (1) (f) GDPR, with our legitimate interest being the improvement and automation of our services. If processing involves user consent, the legal basis is Article 6 (1) (a) GDPR.

The operator of the service is based in a third country (USA). Transfers to the USA are based on EU Standard Contractual Clauses pursuant to Article 46 (2) (c) GDPR or the EU-U.S. Data Privacy Framework.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and OpenAI or applicable statutory retention periods. The provision of personal data is generally neither legally nor contractually required. However, if personal data are not provided, certain AI-driven functions may not be available.

Further information and the applicable data protection provisions of OpenAI can be found at https://openai.com/privacy

Data protection provisions for the use and application of WhatsApp Business

WhatsApp Business is a messaging service provided by Meta Platforms, Inc. that enables businesses to communicate efficiently with customers via WhatsApp. We use WhatsApp Business to provide support, notifications, and customer communication.

When using WhatsApp Business, personal data such as names, telephone numbers, messages, attachments, and usage data are processed.

The operating company of the service and thus the recipient of the personal data is WhatsApp Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland. The parent company is Meta Platforms, Inc., 1601 Willow Road, Menlo Park, CA 94025, United States of America.

Purposes for which personal data are to be processed and the legal basis for processing: The purpose of data processing lies in customer communication. The processing is based on Article 6 (1) (b) GDPR (performance of a contract) or Article 6 (1) (f) GDPR (legitimate interest in effective communication).

Transfers to third countries (in particular the USA) are based on EU Standard Contractual Clauses pursuant to Article 46 (2) (c) GDPR or the EU-U.S. Data Privacy Framework.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and WhatsApp or applicable statutory retention periods. The provision of personal data is voluntary, but communication via WhatsApp cannot occur without it.

Further information and the applicable data protection provisions of WhatsApp can be found at https://www.whatsapp.com/legal/business-policy

Data protection provisions for the use and application of Meta Platforms (Facebook & Instagram)

Meta Platforms provides social media and communication services through platforms such as Facebook and Instagram. We maintain company profiles on these platforms to communicate with users, present our services, and perform marketing activities.

When using Meta’s services, data such as profile information, communication content, interactions, device data, and usage behavior are processed.

The operating company of the services and thus the recipient of the personal data is Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland. The parent company is Meta Platforms, Inc., 1601 Willow Road, Menlo Park, CA 94025, United States of America.

Purposes for which personal data are to be processed and the legal basis for processing: The purpose of data processing lies in public relations, marketing, and communication with interested parties. The processing is based on Article 6 (1) (f) GDPR, with our legitimate interest being direct communication and brand presence. If a contractual relationship exists, the legal basis is Article 6 (1) (b) GDPR.

Transfers to third countries (in particular the USA) are based on EU Standard Contractual Clauses pursuant to Article 46 (2) (c) GDPR or the EU-U.S. Data Privacy Framework.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and Meta or statutory or contractual retention periods. The provision of personal data is voluntary, but interaction via social media is not possible without it.

Further information and the applicable data protection provisions of Meta can be found at https://www.facebook.com/about/privacy and https://privacycenter.instagram.com

Data protection provisions for the use and application of Slack

Slack is a collaboration platform that allows team communication via messages, channels, and integrations with other tools. We use Slack for internal communication and project coordination.

When using Slack, personal data such as names, messages, contact information, and usage data are processed.

The operating company of the service and thus the recipient of the personal data is Slack Technologies Limited, One Park Place, Upper Hatch Street, Dublin 2, Ireland. The parent company is Salesforce, Inc., 415 Mission Street, 3rd Floor, San Francisco, CA 94105, United States of America.

Purposes for which personal data are to be processed and the legal basis for processing: The purpose of data processing lies in internal communication and collaboration. The processing is based on Article 6 (1) (f) GDPR (legitimate interest in efficient communication) or Article 6 (1) (b) GDPR if it concerns contractual coordination.

Transfers to third countries (in particular the USA) are based on EU Standard Contractual Clauses pursuant to Article 46 (2) (c) GDPR or the EU-U.S. Data Privacy Framework.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and Slack or statutory retention periods. The provision of personal data is generally not legally or contractually required. However, without personal data, Slack communication cannot take place.

Further information and the applicable data protection provisions of Slack can be found at https://slack.com/trust/privacy/privacy-policy

Data protection provisions for the use and application of Zoom

Zoom Video Communications, Inc. provides a platform for online meetings, video conferencing, webinars, and instant messaging. We use Zoom to conduct virtual meetings, training sessions, and communication with customers and partners.

When using Zoom, personal data such as name, e-mail address, meeting ID, device and connection data, recordings (if applicable), and communication content (such as chat messages or video/audio data) are processed.

The operating company of the service and thus the recipient of the personal data is Zoom Video Communications, Inc., 55 Almaden Boulevard, 6th Floor, San Jose, CA 95113, United States of America. For users in the EU/EEA, Zoom Video Communications Germany GmbH, Platz der Einheit 2, 60327 Frankfurt am Main, Germany, acts as the responsible contact.

Purposes for which personal data are to be processed and the legal basis for processing: The purpose of processing is the facilitation of digital communication. Processing is based on Article 6 (1) (b) GDPR (performance of a contract) or Article 6 (1) (f) GDPR (legitimate interest in efficient communication).

Transfers to third countries (in particular the USA) are based on EU Standard Contractual Clauses pursuant to Article 46 (2) (c) GDPR or the EU-U.S. Data Privacy Framework.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and Zoom or statutory or contractual retention periods. The provision of personal data is generally voluntary, but participation in Zoom meetings is not possible without it.

Further information and the applicable data protection provisions of Zoom can be found at https://explore.zoom.us/en/privacy

Data protection provisions for the use and application of Microsoft 365

Microsoft 365 is a cloud-based productivity suite that includes services such as Outlook, Word, Excel, PowerPoint, Teams, and OneDrive. We use Microsoft 365 for communication, document management, and collaboration.

When using Microsoft 365, personal data such as names, e-mail addresses, login information, usage data, and document contents may be processed.

The operating company of the service and thus the recipient of the personal data is Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland. The parent company is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, United States of America.

Purposes for which personal data are to be processed and the legal basis for processing: The purpose of processing lies in the use of productivity and collaboration tools. Processing is based on Article 6 (1) (b) GDPR (performance of a contract) and Article 6 (1) (f) GDPR (legitimate interest in efficient business operations).

Transfers to third countries (in particular the USA) are based on EU Standard Contractual Clauses pursuant to Article 46 (2) (c) GDPR or the EU-U.S. Data Privacy Framework.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and Microsoft or statutory or contractual retention periods. The provision of personal data is generally voluntary, but without it, access to Microsoft 365 services is not possible.

Further information and the applicable data protection provisions of Microsoft can be found at https://privacy.microsoft.com/en-us/privacystatement

Data protection provisions for the use and application of Google Workspace

Google Workspace is a suite of cloud-based collaboration and productivity tools including Gmail, Google Drive, Google Docs, Google Meet, and Google Calendar. We use Google Workspace for internal communication, document management, and data storage.

When using Google Workspace, personal data such as names, e-mail addresses, messages, files, and usage data are processed.

The operating company of the service and thus the recipient of the personal data is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. The parent company is Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States of America.

Purposes for which personal data are to be processed and the legal basis for processing: The purpose of processing is the use of cloud-based office tools and collaboration functions. Processing is based on Article 6 (1) (b) GDPR (performance of a contract) and Article 6 (1) (f) GDPR (legitimate interest in efficient business communication).

Transfers to third countries (in particular the USA) are based on EU Standard Contractual Clauses pursuant to Article 46 (2) (c) GDPR or the EU-U.S. Data Privacy Framework.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and Google or statutory or contractual retention periods. The provision of personal data is voluntary, but without it, the use of Google Workspace is not possible.

Further information and the applicable data protection provisions of Google can be found at https://workspace.google.com/terms/privacy.html and https://policies.google.com/privacy

Data protection provisions for the use and application of GitHub

GitHub is a development and collaboration platform that enables version control and code management for software projects. We use GitHub to host, manage, and collaborate on software development projects.

When using GitHub, personal data such as usernames, contact details, profile information, commits, and usage data may be processed.

The operating company of the service and thus the recipient of the personal data is GitHub B.V., Vijzelstraat 68-72, 1017 HL Amsterdam, Netherlands. The parent company is GitHub, Inc., 88 Colin P. Kelly Jr. Street, San Francisco, CA 94107, United States of America.

Purposes for which personal data are to be processed and the legal basis for processing: The purpose of processing lies in code management and developer collaboration. Processing is based on Article 6 (1) (b) GDPR (performance of a contract) and Article 6 (1) (f) GDPR (legitimate interest in software development and project management).

Transfers to third countries (in particular the USA) are based on EU Standard Contractual Clauses pursuant to Article 46 (2) (c) GDPR or the EU-U.S. Data Privacy Framework.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and GitHub or statutory retention periods. The provision of personal data is generally not legally or contractually required. However, participation in GitHub-hosted projects requires the processing of personal data.

Further information and the applicable data protection provisions of GitHub can be found at
https://docs.github.com/en/site-policy/privacy-policies/github-privacy-statement

Data protection provisions for the use and application of Notion

Notion is a cloud-based productivity and collaboration platform that provides tools for project management, documentation, and team organization. We use Notion for internal documentation, planning, and coordination of projects.

When using Notion, personal data such as names, e-mail addresses, profile pictures, notes, content entered by users, and metadata (e.g., usage data, time stamps, IP addresses) are processed.

The operating company of the service and thus the recipient of the personal data is Notion Labs, Inc., 2300 Harrison Street, San Francisco, CA 94110, United States of America.

Purposes for which personal data are to be processed and the legal basis for processing: The purpose of data processing lies in the use of a productivity platform to manage workflows and collaborate internally. The processing is based on Article 6 (1) (f) GDPR, with our legitimate interest being the efficient management and organization of information.

The operator of the service is based in a third country (USA). Transfers to the USA are based on EU Standard Contractual Clauses pursuant to Article 46 (2) (c) GDPR or the EU-U.S. Data Privacy Framework.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and Notion or statutory or contractual

retention periods. The provision of personal data is voluntary, but the use of the platform is not possible without it.

Further information and the applicable data protection provisions of Notion can be found at https://www.notion.so/privacy

Data protection provisions for the use and application of Figma

Figma is a collaborative interface design tool that allows real-time design and prototyping of digital products. We use Figma for UI/UX design, wireframing, and prototyping of applications and websites.

When using Figma, personal data such as names, e-mail addresses, usage data, design files, and communication content within projects may be processed.

The operating company of the service and thus the recipient of the personal data is Figma, Inc., 760 Market Street, Floor 10, San Francisco, CA 94102, United States of America.

Purposes for which personal data are to be processed and the legal basis for processing: The purpose of processing lies in the use of design collaboration tools. Processing is based on Article 6 (1) (f) GDPR, with the legitimate interest being the efficient and secure design and management of digital design projects.

The operator of the service is based in a third country (USA). Transfers to the USA are based on EU Standard Contractual Clauses pursuant to Article 46 (2) (c) GDPR or the EU-U.S. Data Privacy Framework.

The criteria for determining the duration for which personal data are processed are the contractual relationship between us and Figma or statutory or contractual retention periods. The provision of personal data is voluntary but required for collaboration within Figma projects.

Further information and the applicable data protection provisions of Figma can be found at https://www.figma.com/privacy

Final provisions

We reserve the right to adapt this privacy policy to ensure that it always complies with current legal requirements or to reflect changes in our services, for example,

when introducing new services or technologies. The new privacy policy will then apply to your next visit.

If you have any questions about data protection or would like to exercise your data subject rights, you can contact us at any time via the contact details provided in this privacy policy.

Digital Tribe GmbH

Alte Landstraße 237

22391 Hamburg

E-mail: support@digitaltri.be

Website: https://www.digitaltri.be/