

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. As a rule, you can use our websites without disclosing any Personal Data to us. However, if you wish to use more specific services via our websites, including our other websites, applications and social media pages, we may have to process your Personal Data. If we wish to process data about you and we cannot rely on any other legal basis, we will always ask you for your Consent first (e.g. via a cookie banner).

We always comply with applicable data protection laws when handling your Personal Data (such as name, address, email or telephone number). With this Privacy Policy, we inform you about which data we process. This Privacy Policy also explains to you what rights you have as a Data Subject.

We have taken various technical and organizational measures to protect your data on our websites in the best possible way. Nevertheless, there are always risks on the internet and complete protection is not possible. For this reason, you can also transmit your Personal Data to us by other means, for example by telephone, if you prefer.

This Privacy Policy is not only intended to fulfill the obligations under GDPR and to comply with the law of the Member States of the European Union (EU) and the European Economic Area (EEA). This Privacy Policy is also intended to comply with legislation such as UK data protection laws (UK-GDPR), Swiss Federal Data Protection Act and Swiss Data Protection Ordinance (DSG, DSV), California Consumer Privacy Act (CCPA/CPRA), China's Personal Information Protection Law (PIPL), Delaware Personal Data Privacy Act (DPDPA), Tennessee Information Protection Act (TIPA), Minnesota Consumer Data Privacy Act (MCDPA), Iowa Act Relating to Consumer Data Protection (ICDPA), Maryland Online Data Privacy Act (MODPA), Nebraska Data Privacy Act (NDPA), New Hampshire Consumer Data Privacy Law (SB255), New Jersey Data Privacy Law (SB332), South Carolina Consumer Privacy Bill (House Bill 4696) and other global data protection regulations and shall be interpreted accordingly. The following Privacy Policy shall be interpreted for each country, state or federal state in such a way that the terms and legal bases used correspond to the terms and legal bases used in the respective state or federal state.

For reasons of better readability, the simultaneous use of the language forms male, female, diverse and other gender identities (m/f/d/other) is avoided on our websites, in publications, in communication and in our Privacy Policy. All formulations used apply equally to all genders.

If you have any suggestions for improving the texts in this Privacy Policy or if you want to hire an External Data Protection Officer, please contact the author of the text: [Prof. Dr. h.c. Heiko Jonny Maniero, LL.B., LL.M. mult., M.L.E.](#)

1. Definitions

In our Privacy Policy, we use special 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 shall be interpreted or expanded, as appropriate, based on the case law of the General Court of the European Union (EGC), the European Court of Justice (ECJ), the Swiss Federal Supreme Court (SFSC), the Supreme Court of the United Kingdom (UKSC) or on national data protection laws or national case law of a state or federal state, including but not limited to California, including case law, also under common law, if this is necessary for the application of the law in individual cases.

We use the following terms, among others, in this Privacy Policy:

a) Personal Data

Personal Data means any information relating to an identified or identifiable natural person. 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 under national data protection legislation or national jurisdiction of a state or federal state, including under common law.

b) Data Subject

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 under national data protection laws or national jurisdiction of a state or federal state, including case law, also under common law.

c) Processing

Processing is any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, 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 is the marking of stored Personal Data with the aim of limiting their Processing in the future.

e) Profiling

Profiling is 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 analyse or predict aspects concerning that natural person's performance at

work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

f) Pseudonymization

Pseudonymization is 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 are not attributed to an identified or identifiable natural person.

g) Controller

The Controller is 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

A Processor is a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

i) Recipient

A Recipient is a natural or legal person, public authority, agency or another body, to which the Personal Data are 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

A Third Party is a natural or legal person, public authority, agency or body other than the Data Subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to process Personal Data.

k) Consent

Consent is any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

2. Name and address of the Controller

The 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, British data protection laws, Swiss data protection laws (DSG, DSV), Californian data protection law (CCPA/CPRA), Chinese data protection law (PIPL), as well as international laws and provisions with a data protection nature is:

Pointofbrands GmbH

Borselstraße 20

22765 Hamburg

Phone.: +49 178 6264376

eMail: hi@pointofbrands.de

Website: <https://pointofbrands.de/>

3. Name and contact details of the data protection officer

Prof. Dr. h.c. Heiko Jonny Maniero

Franz-Joseph-Str. 11

80801 München

Deutschland

Phone.: +49 (0)178 - 6264376

eMail: info@dg-datenschutz.de

4. Collection of general data and information

Our websites collect a range of general data and information each time the websites are accessed by a Data Subject or an automated system. This general data and information are stored in the log files of the respective server. Among other things, the (1) browser types and versions used, (2) the operating system used by the accessing system, (3) the website from which an accessing system accesses our websites (so-called referrer), (4) the sub-websites which are accessed via 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 can be recorded.

When using this general data and information, we generally do not draw any conclusions about the Data Subject. Rather, this information is required to (1) correctly deliver the content of our websites, (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 criminal prosecution in the event of a cyber-attack. This anonymously collected data and information is therefore evaluated by us both statistically and with the aim of increasing data protection and data security in our organisation to ultimately ensure an optimal level of protection for the Personal Data processed by us. The data of the server log files are stored separately from all Personal Data provided by a Data Subject.

The purpose of processing is to avert danger and ensure IT security, as well as the aforementioned purposes. The legal basis is Art. 6 (1) (f) GDPR. Our legitimate interest is the protection of our information technology systems. The log files are deleted after the stated purposes have been achieved.

5. Contact possibility via the website and other data transfers and your Consent

Our website contains information that enables quick electronic contact with our organisation as well as direct communication with us, which also includes a general address of the so-called electronic mail (email address) and possibly a telephone number. If a Data Subject contacts us by email, via a contact form, via an input form or in any other way, the Personal Data transmitted by the Data Subject will be stored automatically. This Personal Data transmitted to us on a voluntary basis by a Data Subject is processed for the purposes of usage or contacting the Data Subject.

We obtain your Consent for the transmission, storage and Processing of your contact data and inquiries and for contacting you in accordance with 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 purposes of processing the inquiry and contacting you. By transmitting your data to us, you also voluntarily give your explicit Consent in accordance with 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 purposes stated, in particular for such transfers to third countries for which there is or is not an adequacy decision by the EU/EEA and to companies or other bodies that are not subject to an existing adequacy decision on the basis of self-certification or other accession criteria and in which or for which there are significant risks and no suitable guarantees for the protection of your Personal Data (e.g. due to Section 702 FISA, Executive Order EO12333 and the CloudAct in the USA). When you gave your voluntary and explicit Consent, you were aware that there may not be an adequate level of data protection in third countries and that your data subject rights may not be enforceable. You can withdraw your Consent under data protection law at any time with effect for the future. The withdrawal of Consent does not affect the lawfulness of Processing based on Consent before its withdrawal. With a single action (entry and transmission), you give several Consents. These are Consents under EU/EEA data protection law as well as those under the CCPA/CPRA, ePrivacy and telemedia law, and other international legislation, which are required, among other things, as a legal basis for any planned further Processing of your Personal Data. With your action, you also confirm that you have read and taken note of this Privacy Policy.

6. Routine deletion and restriction of Personal Data

We process and store Personal Data for the period required to achieve the purpose of processing or if this has been provided for by the European legislator or another legislator in laws or regulations to which we are subject, or if a legal basis for the Processing exists.

If the purpose of processing no longer applies or if a storage period prescribed by the European legislator or another competent legislator expires, or if the legal basis for the Processing no longer applies, the Personal Data will be routinely restricted or deleted in accordance with the statutory provisions.

7. Rights of the Data Subject according to GDPR

a) Right to confirmation

Each Data Subject has the right to obtain from the Controller confirmation as to whether or not Personal Data concerning him or her is being processed.

If a Data Subject wishes to exercise this right, he or she may contact us at any time.

b) Right to information

Each Data Subject has the right to obtain from the Controller free information about the Personal Data stored about him/her and a copy of this data at any time. 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 from the Controller rectification or erasure of Personal Data or Restriction of Processing of Personal Data concerning the Data Subject or to object to such Processing,
- the existence of a right to lodge a complaint with a supervisory authority,
- if the Personal Data is not collected from the Data Subject: All available information about the origin of the data,
- the existence of automated decision-making, including Profiling, referred to in Art. 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 a right to information as to whether Personal Data has been transferred to a third country or to an international organization. If this is the case, the Data Subject also has the right to obtain information about the appropriate safeguards in connection with the transfer.

If a Data Subject wishes to exercise this right, he or she may contact us at any time.

c) Right to rectification

Each Data Subject has the right to demand the immediate correction of incorrect Personal Data concerning them. Furthermore, the Data Subject has the right to request the completion of incomplete Personal Data, including by means of a supplementary declaration, taking into account the purposes of the Processing.

If a Data Subject wishes to exercise this right, he or she may contact us at any time.

d) Right to erasure (right to be forgotten)

Each Data Subject has the right, to obtain from the Controller the erasure of Personal Data concerning him or her without undue delay, and the Controller shall have the obligation to erase Personal Data without undue delay where one of the following grounds applies, as long as the Processing is not necessary:

- Personal Data was collected or otherwise processed for purposes for which it is no longer necessary.
- The Data Subject withdraws Consent on which the Processing is based according to Art. 6 (1) (a) GDPR, or Art. 9 (2) (a) GDPR, and where there is no other legal ground for the Processing.
- The Data Subject objects to the Processing pursuant to Art. 21 (1) GDPR and there are no overriding legitimate grounds for the Processing, or the Data Subject objects to the Processing pursuant to Art. 21 (2) GDPR.
- Personal Data was processed unlawfully.
- The deletion of Personal Data is necessary to fulfill a legal obligation under Union law or the law of the Member States to which the Controller is subject.
- The Personal Data was collected in relation to information society services offered in accordance with Art. 8 (1) GDPR.

If one of the aforementioned reasons applies, and a Data Subject wishes to request the erasure of Personal Data stored by us, he or she may contact us at any time.

If we have made the Personal Data public and if our organisation is obliged to delete the Personal Data in accordance with Art. 17 (1) GDPR, we shall take appropriate measures, including technical measures, taking into account the available technology and the implementation costs, to inform other data Controllers who process the published Personal Data that the Data Subject has requested the deletion of all links to this Personal Data or of copies or replications of this Personal Data from these other data Controllers, insofar as the Processing is not necessary.

e) Right to Restriction of Processing

Each 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, and 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 Art. 21 (1) GDPR pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.

If one of the aforementioned conditions is met, and a Data Subject wishes to request the restriction of the Processing of Personal Data stored by us, he or she may contact us at any time.

f) Right to data portability

Each Data Subject has the right to receive the Personal Data concerning him or her, which he or she has provided to a Controller, in a structured, commonly used and machine-readable format. He or she also has the right to transmit those data to another Controller without hindrance from the Controller to which the Personal Data have been provided, where Processing is based on Consent pursuant to Art. 6 (1) (a) GDPR or Art. 9 (2) (a) GDPR or on a contract pursuant to Art. 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.

Furthermore, in exercising their right to data portability pursuant to Art. 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, he or she may contact us at any time.

g) Right to object

Each Data Subject has the right to object, on grounds relating to his or her particular situation, at any time, to Processing of Personal Data concerning him or her, which is based on point (e) or (f) of Article 6(1) of the GDPR. This also applies to Profiling based on these provisions.

In the event of an objection, we will no longer process the Personal Data unless we can demonstrate compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defense of legal claims.

If we process Personal Data for direct marketing purposes, the Data Subject shall have the right to object at any time to Processing of Personal Data concerning him or her for such

marketing. This also applies to Profiling insofar as it is associated with such direct advertising. If the Data Subject objects to us to the Processing for direct marketing purposes, we will no longer process the Personal Data for these purposes.

In addition, the Data Subject has the right, on grounds relating to his or her particular situation, to object to Processing of Personal Data concerning him or her by us for scientific or historical research purposes, or for statistical purposes pursuant to Article 89(1) of the 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, he or she may contact us at any time. The Data Subject is also free, in the context of the use of information society services, and notwithstanding Directive 2002/58/EC, to exercise his or her right to object by automated means using technical specifications.

h) Automated decisions in individual cases including Profiling

Each Data Subject has the right not to be subject to a decision based solely on automated Processing, including Profiling, which produces legal effects concerning him or her, or similarly significantly affects him or her, provided that the decision (1) is not necessary for the conclusion or 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 a data Controller, or (2) it 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 his or her point of view and contest the decision.

If a Data Subject wishes to exercise this right, he or she may contact us at any time.

i) Right to withdraw Consent under data protection law

Each 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, he or she may contact us at any time.

8. General purpose of Processing, categories of processed data and categories of recipients

The general purpose of processing of Personal Data is the handling of all activities relating to the Controller, customers, interested parties, business partners or other contractual or pre-contractual relationships between the aforementioned groups (in the broadest sense) or legal obligations of the Controller. This general purpose applies if no more specific purposes for specific Processing are specified.

The categories of Personal Data that we process are customer data, prospective customer data, employee data (including applicant data) and supplier data. The categories of recipients of Personal Data are public bodies, external bodies, internal processing, intragroup processing and other bodies.

A list of our Processors and data recipients in third countries and, if applicable, international organizations is either published on our website or can be requested from us free of charge.

9. Legal basis for the Processing

Art. 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, as is the case, for example, when Processing operations are necessary for the supply of goods or to provide any other service or consideration, Processing is based on Art. 6 (1) (b) GDPR. The same applies to such Processing operations that are necessary to carry out pre-contractual measures, for example in cases of inquiries about our products or services. If we are subject to a legal obligation which requires the Processing of Personal Data, such as for the fulfillment of tax obligations, Processing is based on Art. 6 (1) (c) GDPR.

In rare cases, it may be necessary to process Personal Data to protect the vital interests of the Data Subject or another natural person. This would be the case, for example, if a visitor were injured in our organisation and their name, age, health insurance data or other vital information would have to be passed on to a doctor, hospital or other Third Party. The Processing would then be based on Art. 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 Art. 6 (1) (e) GDPR.

Ultimately, Processing operations could be based on Art. 6 (1) (f) GDPR. This legal basis is used for Processing operations which are not covered by any of the abovementioned legal grounds, if Processing is necessary for the purposes of the legitimate interests pursued by our organisation or by a Third Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data. We are permitted to carry out such Processing operations in particular because they have been specifically mentioned by the European legislator. In this respect, it took the view that a legitimate interest could be assumed, for example, if the Data Subject is a customer of the Controller (Recital 47 Sentence 2 GDPR).

10. Legitimate interests in Processing pursued by the Controller or a Third Party and direct marketing

If the Processing of Personal Data is based on Art. 6 (1) (f) GDPR and no more specific legitimate interests are stated, our legitimate interest is the performance of our business activities for the benefit of the well-being of our staff and our shareholders.

We may send you direct advertising about our own goods or services that are similar to the goods or services you have requested, commissioned or purchased. You may object to direct advertising at any time (e.g. by email). You will not incur any costs other than the transmission costs according to the basic rates. The Processing of Personal Data for direct marketing purposes is based on Art. 6 (1) (f) GDPR. The legitimate interest is direct marketing.

11. Duration for which the Personal Data is stored

The criterion for the duration of the storage of Personal Data is the respective statutory retention period. If there is no statutory retention period, the criterion is the contractual or internal retention period. After this period has expired, the corresponding data is routinely deleted if it is no longer required to fulfill or initiate a contract. This applies in particular to all Processing operations for which no more specific criteria have been defined.

12. Legal or contractual provisions for the provision of Personal Data; necessity for the conclusion of the contract; obligation of the Data Subject to provide the Personal Data; possible consequences of non-provision

We would like to inform you that the provision of Personal Data is partly required by law (e.g. tax regulations) or may also result from contractual obligations (e.g. information on the contractual partner). Sometimes it may be necessary for a contract to be concluded for a Data Subject to provide us with Personal Data that must subsequently be processed by us. For example, Data Subjects are obliged to provide us with Personal Data if our organisation concludes a contract with them. Failure to provide Personal Data would mean that the contract with the Data Subject could not be concluded. The Data Subject must contact us before providing Personal Data. We will inform the Data Subject on a case-by-case basis whether the provision of the Personal Data is required by law or contract or is necessary for the conclusion of the contract, whether there is an obligation to provide the Personal Data and what the consequences would be if the Personal Data were not provided.

13. Existence of automated decision-making

As a responsible company, we do not normally use automated decision-making or Profiling. If, in exceptional cases, we carry out automated decision-making or Profiling, we will inform the Data Subject either separately or via a sub-item in our Privacy Policy (here on our website). In this case, the following applies:

Automated decision-making, including Profiling, may take place if (1) this is necessary for the conclusion or performance of a contract between the Data Subject and us, or (2) this is permissible on the basis of Union or Member State legislation to which we are subject and this legislation contains appropriate measures to safeguard the rights and freedoms and legitimate interests of the Data Subject, or (3) this takes place with the explicit Consent of the Data Subject.

In the cases referred to in Art. 22 (2) (a) and (c) GDPR, we shall implement suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests. In

these cases, you have the right to obtain human intervention on the part of the Controller, to express your point of view and to contest the decision.

Meaningful information on the logic involved and the scope and intended effects of such Processing for the Data Subject will be provided in this Privacy Policy where applicable.

14. Recipients in a third country and appropriate or adequate safeguards and how to obtain a copy of them or where they are available.

According to Art. 46 (1) GDPR, the Controller or Processor may only transfer Personal Data to a third country if the Controller or Processor has provided appropriate safeguards and if enforceable rights and effective legal remedies are available to the Data Subjects.

Appropriate safeguards can be provided by standard contractual clauses without the need for special approval from a supervisory authority, Art. 46 (2) (c) GDPR.

The EU standard contractual clauses or other appropriate safeguards are agreed with all recipients from third countries prior to the first transfer of Personal Data, or the transfers are based on adequacy decisions. Consequently, it is ensured that appropriate safeguards, enforceable rights and effective legal remedies are guaranteed for all Processing of Personal Data. Any Data Subject can 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.

Art. 45 (3) GDPR authorizes the European Commission to decide by means of an implementing decision that a non-EU country ensures an adequate level of protection. This means a level of protection for Personal Data that essentially corresponds to the level of protection within the EU. Adequacy decisions mean that Personal Data can flow from the EU (as well as from Norway, Liechtenstein and Iceland) to a third country without further obstacles. Similar regulations apply to the United Kingdom, Switzerland and some other countries.

In all cases where the European Commission, or a government or competent authority of another country, 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 by us to the members of such frameworks (e.g. self-certified entities) are based solely on the membership of that entity in the respective framework or on the respective adequacy decisions. If we or one of our group companies is a member of such a framework, all transfers to us or our group company are based exclusively on the membership of the respective company in this framework. If we or one of our group companies is located in a third country with an adequate level of protection, all transfers to us or our group company are based solely on the respective adequacy decisions.

Any Data Subject can obtain a copy of the frameworks from us. In addition, the frameworks are also available in the Official Journal of the European Union or in the published legal materials or on the websites of data protection supervisory authorities or other authorities or institutions.

15. Right to lodge a complaint with a data protection supervisory authority

As the 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 regulated in Art. 77 (1) GDPR. According to this provision, without prejudice to any other administrative or judicial remedy, every Data Subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the Data Subject considers that the Processing of Personal Data relating to him or her infringes the General Data Protection Regulation. The right to lodge a complaint has been restricted by the EU legislator to the effect that it can only be exercised with a single supervisory authority (Recital 141 Sentence 1 GDPR). This provision is intended to avoid duplicate complaints in the same matter by the same Data Subject. If a Data Subject wishes to complain about us, it is therefore requested that only one supervisory authority is contacted.

16. Data protection for applications and in the application process

We collect and process Personal Data of applicants in the application process. Processing may also take place electronically. This is particularly the case if an applicant submits relevant application documents to us electronically, for example by email or via a web form on our or third-party websites.

For applicant data, the purpose of data processing is to carry out a review of the application in the application process. For this purpose, we process all data provided by you. Based on the data submitted as part of the application, we check whether you will be invited to an interview (part of the selection process). Then, in the case of generally suitable applicants, in particular during the interview, we process certain other Personal Data provided by you that is essential for our selection decision.

The legal basis for data Processing is Art. 6 (1) (b) GDPR, Art. 9 (2) (b) and (h) GDPR, Art. 88 (1) GDPR and national legislation.

If we do not conclude an employment contract with the applicant, the application documents will be deleted no later than six months after notification of the rejection decision, provided that no other legitimate interests of the Controller stand in the way of deletion. Another legitimate interest in this sense is, for example, the provision of evidence in legal proceedings.

17. Registration or filling in input masks on our website and your Consent

You have the option of registering on our websites by providing Personal Data and/or filling out input masks. Which Personal Data is transmitted to us in the process is determined by the respective input mask used for registration or input. The Personal Data you enter will be processed exclusively for internal use by us and for our own purposes. However, we may pass on your Personal Data to one or more Processors, for example to parcel service providers, who also use your Personal Data exclusively for purposes that are attributable to us as the Controller. Disclosure may also take place if you have commissioned the disclosure from us. The legal basis is then Art. 6 (1) (b) GDPR.

When you register or enter data on our website, the IP address assigned by your internet service provider (ISP), the date and time of registration or entry may also be stored. This data is stored against the background that this is the only way to prevent misuse of our services and, if necessary, to make it possible to investigate criminal offenses. In this respect, the storage of this data is necessary for our security. The purpose of processing is the prevention and detection of misuse and the investigation of criminal offenses, as well as the aforementioned purposes. The legal basis is Art. 6 (1) (f) GDPR. Our legitimate interest is in particular the protection of our information technology systems and the investigation of criminal offenses. This data is not disclosed to Third Parties unless there is a legal obligation to disclose it, or the disclosure serves the purpose of criminal prosecution.

The registration, entry and transmission of your Personal Data also enables us to offer you content or services which, due to the nature of the matter, can only be offered to registered persons or persons known to us. You are free to change the Personal Data provided during registration at any time or to have it completely deleted from our database. The purposes of processing are the receipt of data by us and the use of your data for further Processing, for communication with you and the illustration or implementation of the registration or input purposes. The legal basis is your Consent in accordance with Art. 6 (1) (a) GDPR and/or Art. 49 (1) (1) (a) GDPR.

By entering and transmitting your data, you voluntarily consent to the Processing of the Personal Data you have entered. By entering and transmitting your data to us, you also voluntarily give your explicit Consent in accordance with 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 purposes stated, in particular for such transfers to third countries for which there is or is not an adequacy decision by the EU/EEA and to companies or other bodies that are not subject to an existing adequacy decision on the basis of self-certification or other accession criteria and in which or for which there are significant risks and no suitable guarantees for the protection of your Personal Data (e.g. due to Section 702 FISA, Executive Order EO12333 and the CloudAct in the USA). When giving your voluntary and explicit Consent, you were aware that there may not be an adequate level of data protection in third countries and that your data subject rights may not be enforceable. You can withdraw your Consent under data protection law at any time with effect for the future. The withdrawal of Consent does not affect the lawfulness of Processing based on Consent before its withdrawal. With a single action (entry and transmission), you give several Consents. These are Consents under EU/EEA data protection law as well as those under the CCPA/CPRA, ePrivacy and telemedia law, and other international legislation, which are required, among other things, as a legal basis for any planned further Processing of your Personal Data. With your action, you also confirm that you have read and taken note of this Privacy Policy.

Upon request, we will provide any Data Subject at any time with information about which Personal Data about the Data Subject is stored. We will also correct or delete Personal Data at the request or notice of the Data Subject, provided that this does not conflict with any statutory retention obligations or other reasons justifying Processing. All our employees are available to you as contact persons in this context.

18. Data protection provisions about the application and use of Complianz - GDPR/CCPA Cookie Consent

Complianz - GDPR/CCPA Cookie Consent is a WordPress plugin that supports compliance with data protection regulations (GDPR and CCPA) by providing a user-friendly solution for managing cookie Consents. This plugin helps website operators to obtain and document legally required Consents for data Processing and cookie use from website visitors. It processes and stores information about users' Consent to cookies and their IP addresses.

The application is installed on our own IT infrastructure. We are the company operating the service.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of using Complianz - GDPR/CCPA Cookie Consent is to comply with data protection laws through the use of cookie Consent tools. Processing is based on Art. 6 (1) (c) GDPR, as the Processing is necessary for compliance with a legal obligation to which our organisation is subject.

The criteria for determining the duration for which the Personal Data is processed are the statutory or contractual retention periods. The use of Personal Data is required by law, as it is necessary to fulfill legal obligations in the area of data protection and Consent management. Users are required to indicate their cookie preferences or reject cookies, and this information must be stored to properly document the decision.

Further information about Complianz - GDPR/CCPA Cookie Consent can be found at <https://complianz.io/>.

19. Data protection provisions about the application and use of Apple Safari

We use Safari as a web browser to display and use web content on various endpoints, in particular Apple devices. When using Safari, technical data may be processed by the browser that is required to display content, execute scripts and communicate with servers. As part of processing, personal data may also be transmitted to Apple as the provider of the browser. This applies in particular to personal data if users have activated functions such as intelligent tracking prevention, the automatic completion of forms or synchronization via iCloud. The data processed includes IP addresses, device information, operating system versions, browser types and browser versions, language settings, timestamps, location information, websites visited and entries in form fields.

Safari can also be used in conjunction with other Apple services, e.g., to synchronize bookmarks, passwords and browsing history across different devices. Depending on the configuration of the browser, synchronization with the Apple ID account can also take place, especially when using iCloud services. Control over these functions lies with the user, who can adjust them in the privacy settings of their device.

The company that operates the service and thus the recipient of personal data is:

Apple, Inc., One Apple Park Way, Cupertino, CA 95014, USA. For data subjects in the EU and EEA, Apple Distribution International Ltd., Hollyhill Industrial Estate, Hollyhill, Cork, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: APPLE (UK) LIMITED, 280 Bishopsgate, London, EC2M 4AG, United Kingdom. The representative under Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Apple Switzerland AG. Löwenstrasse 29 8001 Zürich, Switzerland.

Purposes for which personal data are to be processed and the legal basis for the processing: The purpose of processing is to provide web browser functions for displaying and interacting with web content, to support security functions and convenience functions and to synchronize browser data between different Apple devices. The processing is carried out on the basis of Art. 6 (1) (f) GDPR. The legitimate interest lies in the provision of a technically sophisticated, secure and user-friendly web browser as well as in improving the user experience and ensuring system security.

The company that operates the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company that operates the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate safeguards from us.

The criteria for determining the duration for which the personal data is processed are the contractual relationship between us and the company that operates the service or statutory or contractual retention periods. The provision of personal data is not required by law or contract, nor is it necessary for the conclusion of a contract. You are not obliged to provide personal data to the company that operates the service. However, if you do not provide personal data, certain functions of the browser may not be fully usable.

Further information and the applicable data protection provisions of Apple may be retrieved under <https://www.apple.com/>.

20. Data protection provisions about the application and use of DATEV

DATEV eG is a provider of software solutions and services for tax consultants, auditors, lawyers and companies and offers comprehensive solutions in the areas of accounting, human resources, corporate management, digital ecosystems and IT security. The use of DATEV products enables us to optimize our business processes, ensure tax and legal compliance and guarantee efficient processes in finance and human resources.

When using DATEV services, Personal Data such as names, address data, tax-relevant information, salary data and other business data are processed. This Processing is necessary to make use of the services offered, to comply with legal requirements and to obtain individual solutions.

The company operating the service and therefore the recipient of the Personal Data is: DATEV eG, Paumgartnerstr. 6-14, 90429 Nuremberg, Germany.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is the use of software solutions and services in the areas of tax consulting, accounting, human resources and corporate management. Processing is based on Art. 6 (1) (b) GDPR for the performance of a contract to which the Data Subject is party and Art. 6 (1) (c) GDPR for compliance with a legal obligation, in particular under tax law and labor law.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

Further information and the applicable data protection provisions of DATEV can be found at <https://www.datev.de>.

21. Data protection provisions about the application and use of DeepL

We use the translation service DeepL to translate content into other languages efficiently and with high quality. DeepL offers powerful AI-based translation technology that enables us to translate texts from different sources into different target languages, both manually via the web portal and automatically via interfaces (APIs). This may involve the processing of personal data, in particular when users enter content for translation that contains personal information. In addition, DeepL automatically processes various metadata during technical use, including IP addresses, browser information, timestamps and usage data.

When texts are submitted for translation, data processing is usually temporary. According to DeepL, content entered via the web application is only used to carry out the translation and is not stored permanently, unless the user uses additional functions such as saved translation histories or user accounts. When using the Pro version, account data, billing information, preferred language settings and contractual usage details may also be processed. DeepL uses this data to provide contractually agreed services, for quality assurance, for user analysis and for the further development of its own technologies. The processing is fully automated.

The company that operates the service and therefore the recipient of personal data is: DeepL SE, Maarweg 165, 50825 Cologne, Germany.

Purposes for which personal data are to be processed and the legal basis for the processing: The purpose of processing is the provision of machine translation services, the management of user accounts, the improvement of translation quality and the safeguarding of technical operations. Processing is carried out on the basis of Art. 6 (1) (b) GDPR, i.e., for the performance of a contract to which the data subject is party, and Art. 6 (1) (f) GDPR.

The legitimate interest lies in the user-friendly, secure and efficient provision of translation functions and in the continuous further development of the technology used.

The criteria for determining the duration for which the personal data is processed are the contractual relationship between us and the company that operates the service or statutory or contractual retention periods. The provision of personal data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company that operates the service with personal data. However, if you do not provide personal data, you may not be able to use our services or those of the company that operates the service.

Further information and the applicable data protection provisions of DeepL may be retrieved under <https://www.deepl.com/privacy>.

22. Data protection provisions about the application and use of Firefox

We use the Firefox web browser in our company for Internet use and to run certain web applications. Firefox is developed by Mozilla and offers various functions for the protection of privacy, secure display of websites and the management of Internet data. When using Firefox, personal data may be processed, especially when users use synchronized services such as Firefox Sync, add-ons, Pocket or the Mozilla account. Information such as IP addresses, location data, device identifiers used, installed extensions, language settings, bookmarks, websites visited, and usage data are collected and processed.

If functions such as automatic updates, telemetry data transmission or crash reports are activated, Firefox transmits diagnostic data to Mozilla in order to improve the stability and security of the browser. No website content is recorded, only technical information such as browser configuration, device model, operating system version or error codes. In addition, Firefox enables the use of protection functions such as tracking protection or phishing protection, in which data can also be transmitted to Mozilla or linked third-party providers in certain cases. The use of these functions is usually optional and can be adjusted or deactivated via the settings.

The company that operates the service and therefore the recipient of personal data is: Mozilla Corporation, 2 Harrison Street, Suite 175, San Francisco, CA 94105, USA. For data subjects in the EU and EEA, Mozilla Firefox GmbH, Weinmeisterstr. 8, 10178 Berlin, Germany is the contact person within the meaning of Art. 27 GDPR.

Purposes for which personal data are to be processed and the legal basis for the processing: The processing is carried out to provide a secure and efficient web browser, to technically optimize the user experience, to synchronize user-specific settings and for error analysis. It is carried out on the basis of Art. 6 (1) (b) GDPR, i.e., for the performance of a contract to which the data subject is party, and Art. 6 (1) (f) GDPR. The legitimate interest lies in the secure, stable and user-friendly use of web services, in the further development of the browser and in securing the system environment against potential security risks.

The company that operates the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual

clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company that operates the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate safeguards from us.

The criteria for determining the duration for which the personal data is processed are the contractual relationship between us and the company that operates the service or statutory or contractual retention periods. The provision of personal data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company that operates the service with personal data. However, if you do not provide personal data, you may not be able to use our services or those of the company that operates the service.

Further information and the applicable data protection provisions of Mozilla Firefox can be retrieved at <https://www.mozilla.org/>.

23. Data protection provisions about the application and use of Google Chrome

We use Google Chrome web browser to use web-based applications, to display Internet content and to integrate browser-based business services. Google Chrome is provided by Google and offers numerous functions, including synchronization via Google accounts, integration with other Google services, automated form entries, voice control and the use of extensions and security technologies. When using Google Chrome, personal data may be processed, especially if the browser is linked to a Google account or users voluntarily activate synchronization services and extensions. The processed data includes IP addresses, search queries, browsing history, installed extensions, location data, language settings and technical device information.

If the user is logged in with a Google account, Chrome activities such as the history of visited pages, bookmarks, passwords and other browser settings can be synchronized across devices and stored on Google servers. In addition, Chrome collects diagnostic data and usage statistics to improve the stability, security and performance of the browser, if this function is activated. Personal data is also processed locally or on the server when forms are automatically completed (e.g., addresses or credit card details). Chrome can also use third-party tools such as Safe Browsing or translation services, which also trigger data processing operations.

The company that operates the service and thus the recipient of personal data is: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. For data subjects in the EU and EEA, Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Google UK Limited, Belgrave House, 76 Buckingham Palace Road, London SW1W 9TQ, United Kingdom. The representative under Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Google Switzerland GmbH, Brandschenkestrasse 110, 8002 Zurich, Switzerland.

Purposes for which personal data are to be processed and the legal basis for the processing: The processing serves the secure, stable and personalized use of the web browser, the synchronization of user preferences, the improvement of browser performance, the protection against harmful content and the integration with other Google services. Processing is carried out on the basis of Art. 6 (1) (b) GDPR, i.e., for the performance of a contract to which the data subject is party, and Art. 6 (1) (f) GDPR. The legitimate interest lies in the secure provision of Internet functions, technical stability, user-friendliness and the integration of services to optimize online experience.

The company that operates the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company that operates the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate safeguards from us.

The criteria for determining the duration for which the personal data is processed are the contractual relationship between us and the company that operates the service or statutory or contractual retention periods. The provision of personal data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company that operates the service with personal data. However, if you do not provide personal data, you may not be able to use our services or those of the company that operates the service.

Further information and the applicable data protection provisions of Google Chrome can be retrieved at <https://policies.google.com/privacy>.

24. Data protection provisions about the application and use of Microsoft Edge

We use the Microsoft Edge web browser. When using the browser, personal data may be processed by Microsoft, in particular when using functions such as synchronization with the Microsoft account, the use of extensions, search integration via Bing or the personalized display of content. When you visit a website, Microsoft Edge processes various technical information that is required to display content and interact with online services. This includes IP addresses, browser types and versions, language settings, operating systems used, device identifiers, location data, cookies, stored form data and URLs visited.

Microsoft Edge can also be linked to other Microsoft services, e.g., for protection against malicious websites (SmartScreen), the use of Microsoft 365 accounts or the synchronization of bookmarks and passwords. Personal data may be transmitted to Microsoft for identification, usage analysis and security enhancement. Users can activate or deactivate these functions in the browser settings.

The company that operates the service and thus the recipient of personal data is: Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA. For data subjects in the EU and EEA, Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland, acts as contact and

representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Microsoft Limited, Microsoft Campus, Thames Valley Park, Reading, RG6 1WG, United Kingdom. The representative under Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Microsoft Schweiz GmbH, Seestrasse 356, 8038 Zurich, Switzerland.

Purposes for which personal data are to be processed and the legal basis for the processing: The purpose of processing is to provide a modern web browser with advanced features for display, interaction and security when using online content. The processing is carried out on the basis of Art. 6 (1) (f) GDPR. The legitimate interest lies in the secure, convenient and feature-rich use of web services, the synchronization of cross-device settings and the improvement of browser performance and browser security.

The company that operates the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company that operates the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate safeguards from us.

The criteria for determining the duration for which the personal data is processed are the contractual relationship between us and the company that operates the service or statutory or contractual retention periods. The provision of personal data is not required by law or contract, nor is it necessary for the conclusion of a contract. You are not obliged to provide the company that operates the service with personal data. However, if you do not provide personal data, certain functions of the browser may not be fully usable.

Further information and the applicable data protection provisions of Microsoft may be retrieved under <https://privacy.microsoft.com/>.

25. Data protection provisions about the application and use of Facebook Messenger

Facebook Messenger is an instant messaging service. The service allows users to exchange messages, photos, videos and voice messages as well as make video calls. Messenger is available both as a standalone app and within Facebook and offers functions such as group chats, sending stickers and GIFs as well as integration with other services and applications.

When using Facebook Messenger, Personal Data such as names, contact details, message content, call and video chat data, location information (if shared) and usage data are processed. This information is necessary to provide communication services, ensure user security, prevent misuse and develop new functions.

The company operating the service and therefore the recipient of the Personal Data is: Meta Platforms, Inc., 1 Meta Way, Menlo Park, CA 94025, USA.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is to use and improve the instant messaging service. Processing is based on Art. 6 (1) (b) GDPR for the performance of a contract to which the Data Subject is party and Art. 6 (1) (f) GDPR, whereby our legitimate interest lies in the provision and use of a secure, efficient and user-friendly communication service.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

Further information and the applicable data protection provisions of Facebook Messenger can be found at <https://www.facebook.com>.

26. Data protection provisions about the application and use of Google Meet

Google Meet is a video conferencing service developed by Google LLC that enables users to conduct video conferences and online meetings. As part of Google Workspace, Google Meet provides a secure and reliable platform for businesses, educational institutions and individuals to promote communication and collaboration. The service supports features such as screen sharing, real-time captioning and integration with Google Calendar to make it easier to plan and conduct virtual meetings.

When using Google Meet, Personal Data such as names, email addresses, video images and audio recordings, as well as meeting data (such as participant lists, date and time of the meeting) are processed. This information is necessary to provide the video conferencing service, improve the user experience and ensure the security of the meetings.

The company that operates the service and thus the recipient of personal data is: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. For data subjects in the EU and EEA, Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Google UK Limited, Belgrave House, 76 Buckingham Palace Road, London SW1W 9TQ, United Kingdom. The representative under Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Google Switzerland GmbH, Brandschenkestrasse 110, 8002 Zurich, Switzerland.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is the use and optimization of the video conferencing service. Processing is based on Art. 6 (1) (b) GDPR for the performance of a contract to which the Data Subject is party and Art. 6 (1) (f) GDPR, whereby our legitimate interest lies in the promotion of digital communication and collaboration.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

Further information and the applicable data protection provisions of Google Meet may be retrieved under <https://policies.google.com/privacy>.

27. Data protection provisions about the application and use of Microsoft Teams

Microsoft Teams is a communication and collaboration tool within the Microsoft 365 suite designed specifically for business use. It enables teams to work together effectively, no matter where they are, through features such as chat, video calls, meetings, file sharing and integration with other Microsoft products and services. Microsoft Teams promotes teamwork through digital spaces that enable seamless communication and collaboration, regardless of whether team members are in the same office or spread across different locations worldwide.

When using Microsoft Teams, Personal Data such as names, email addresses, telephone numbers, usage data (e.g. time and duration of meetings, chat logs), content data (e.g. files, notes, messages) and location data are processed. This information is necessary to provide the services, improve the user experience, provide support and ensure the security and compliance of the services.

The company that operates the service and thus the recipient of personal data is: Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA. For data subjects in the EU and EEA, Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Microsoft Limited, Microsoft Campus, Thames Valley Park, Reading, RG6 1WG, United Kingdom. The representative under Art. 14 of the Federal Act on

Data Protection (FADP) in Switzerland is: Microsoft Schweiz GmbH, Seestrasse 356, 8038 Zurich, Switzerland.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is to use, provide, manage and improve Microsoft Teams for communication. Processing is based on the performance of a contract (Art. 6 (1) (b) GDPR) to which the Data Subject is party and on legitimate interests (Art. 6 (1) (f) GDPR), such as the improvement of our services and the use and provision of modern communication tools.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

Further information and the applicable data protection provisions of Microsoft Teams can be found at <https://privacy.microsoft.com>.

28. Data protection provisions about the application and use of WhatsApp

WhatsApp LLC offers a widely used instant messaging service that enables users to send and receive text messages, voice messages, images, videos and documents. Users can also make voice and video calls. WhatsApp is characterized by end-to-end encryption, which ensures the security and privacy of communication between users.

When using WhatsApp, Personal Data such as telephone numbers, profile names, profile pictures, online status information and location data are processed. In addition, information about interactions between users, such as messages and call data, is transmitted in encrypted form and can be used by WhatsApp to improve the service and ensure security.

The company operating the service and therefore the recipient of the Personal Data is: WhatsApp LLC, 1 Meta Way, Menlo Park, CA 94025, USA.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of data processing lies in the use of the messaging service and the associated functions. Processing is based on the performance of a contract pursuant to Art. 6 (1) (b) GDPR, to which the Data Subject is a party, and on legitimate interests pursuant to

Art. 6 (1) (f) GDPR, such as the use of an efficient platform, the improvement of our services and ensuring the security of users and their data.

The company operating the service is located in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

Further information and the applicable data protection provisions of WhatsApp can be found at <https://www.whatsapp.com>.

29. Data protection provisions about the application and use of Google Cloud

Google Cloud is a comprehensive suite of cloud computing services offered by Google LLC. It enables companies, developers and organizations to use scalable infrastructure, platform services and specialized applications for data Processing, storage, analysis and much more. Google Cloud includes products such as Compute Engine, App Engine, Google Kubernetes Engine, BigQuery, Cloud Storage and many others that run on Google's own infrastructure. These services help customers manage their IT resources efficiently, develop innovative applications and analyze data securely and reliably.

When using the Google Cloud, Personal Data such as names, email addresses, payment information, usage data and, in some cases, content data is processed. This information is necessary to create and manage user accounts, provide services, make support requests and offer customized solutions.

The company that operates the service and thus the recipient of personal data is: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. For data subjects in the EU and EEA, Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Google UK Limited, Belgrave House, 76 Buckingham Palace Road, London SW1W 9TQ, United Kingdom. The representative under Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Google Switzerland GmbH, Brandschenkestrasse 110, 8002 Zurich, Switzerland.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is the use and optimization of cloud computing services. Processing is based on Art. 6 (1) (b) GDPR for the performance of a contract to

which the Data Subject is party and on Art. 6 (1) (f) GDPR, where our legitimate interest lies in the provision and use of efficient, secure and scalable cloud services.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

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

30. Data protection provisions about the application and use of Google Drive

Google Drive is a cloud storage service from Google LLC that allows users to store, synchronize and share files. With Google Drive, users can store documents, photos, videos and other file types in the cloud, access them from any device and share them with others. Drive integrates seamlessly with other Google services such as Google Docs, Sheets and Slides to create a collaborative work environment where users can work on documents simultaneously.

When using Google Drive, Personal Data such as names, email addresses, contents of stored files and activities relating to file uploads, file views and file shares are processed. This information is necessary to provide storage service, enable collaboration between users and offer a personalized user experience.

The company that operates the service and thus the recipient of personal data is: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. For data subjects in the EU and EEA, Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Google UK Limited, Belgrave House, 76 Buckingham Palace Road, London SW1W 9TQ, United Kingdom. The representative under Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Google Switzerland GmbH, Brandschenkestrasse 110, 8002 Zurich, Switzerland.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is the use and optimization of the cloud storage service. Processing is based on Art. 6 (1) (b) GDPR for the performance of a contract to which the Data Subject is party and Art. 6 (1) (f) GDPR, whereby our legitimate interest lies

in the provision and use of an efficient, secure and user-friendly storage and collaboration service.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

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

31. Data protection provisions about the application and use of IONOS

IONOS is a web hosting and domain services company. As a provider in this area, IONOS not only provides the technical infrastructure for our online presence, but also offers a range of related services, such as email hosting, SSL certificates and data backup. Through use of IONOS, various types of data are processed, in particular data generated during the registration of domains, such as the name of the domain owner, contact details and technical information about the domain.

In addition, IONOS collects data about website traffic to ensure IT security and ward off attacks such as DDoS attacks. This information may include IP addresses, timestamps and pages accessed. The purpose of Processing of this data is to provide and optimize the hosting services, to ensure network and information security and to improve the user-friendliness of our website.

The company operating the service and therefore the recipient of the Personal Data is IONOS SE, Elgendorfer Str. 57, 56410 Montabaur, Germany.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is the use of web hosting services and related services. Processing is based on Art. 6 (1) (f) GDPR. Our legitimate interest lies in the reliable and secure provision of our website and related services.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if

you do not provide it, you may not be able to use our services or those of the company operating the service.

Further information and the applicable data protection provisions of IONOS SE can be found at <https://www.ionos.de>.

32. Data protection provisions about the application and use of STRATO

STRATO is a provider of web hosting services, domain registrations, cloud storage, online stores and other internet-based services. With an extensive portfolio of products, STRATO supports both private individuals and companies in effectively designing and managing their online presence. STRATO's services are designed to provide users with reliable, secure and user-friendly solutions for their web projects.

When using STRATO services, Personal Data such as names, addresses, email addresses, telephone numbers, payment information and usage data of the services offered are processed. This information is necessary to provide the services, manage user accounts, make support requests and ensure the security of user data.

The company operating the service and therefore the recipient of the Personal Data is: STRATO AG, Otto-Ostrowski-Straße 7, 10249 Berlin, Germany.

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

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

Further information and the applicable data protection provisions of STRATO may be retrieved under <https://www.strato.de>.

33. Data protection provisions about the application and use of Google Fonts

Google Fonts is a free service from Google LLC that provides web developers with a wide range of fonts to improve the design and aesthetics of websites. By integrating Google Fonts, web developers can ensure that texts on their websites are displayed consistently and as intended on different devices and browsers. Google Fonts is provided via Google servers, ensuring high availability and fast loading times.

When using Google Fonts, Personal Data such as IP addresses and browser information may be processed, as a request is sent to the Google servers when the fonts are loaded. This data is used to provide the service, optimize performance and prevent misuse.

The company that operates the service and thus the recipient of personal data is: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. For data subjects in the EU and EEA, Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Google UK Limited, Belgrave House, 76 Buckingham Palace Road, London SW1W 9TQ, United Kingdom. The representative under Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Google Switzerland GmbH, Brandschenkestrasse 110, 8002 Zurich, Switzerland.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is to use and optimize the font service for web developers and end users. Processing is based on Art. 6 (1) (f) GDPR, whereby our legitimate interest lies in improving the user experience on websites by providing a variety of fonts and ensuring fast loading times.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

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

34. Data protection provisions about the application and use of jQuery

jQuery is a widely used JavaScript library used by web developers to simplify and speed up HTML document management, event handling, animation and Ajax interactions. The use of jQuery on our website serves to create a smoother and more interactive user experience. When visiting our website, jQuery can be used to collect certain data, such as information about user behavior and interactions on the site.

The Processing takes place indirectly and is primarily aimed at improving website performance and user-friendliness. jQuery itself, as a client-side library, stores or processes

Personal Data on its own servers. jQuery is executed in the user's browser and can be used for dynamic content updates by also transmitting data to external servers.

The operating company of jQuery is the OpenJS Foundation, 1 Letterman Dr, Ste D4700, San Francisco, California, USA.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of using jQuery is to improve the user experience on our website through an efficient interaction experience. Processing is based on Art. 6 (1) (f) GDPR, whereby our legitimate interest lies in the provision and use of a functional, user-friendly and visually appealing website.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

jQuery's Privacy Policy is available at <https://jquery.com/>.

35. Data protection provisions about the application and use of Google Calendar

Google Calendar is a comprehensive online calendar service from Google LLC that allows users to plan appointments, organize events, set reminders and manage their schedule. The platform supports synchronization across different devices and offers features such as sharing calendars with others, inviting participants to events and integration with other Google services to improve productivity and organization in everyday and professional environments.

When using Google Calendar, Personal Data such as names, email addresses, calendar events, participant lists, and reminder details are processed. This information is necessary to provide the calendar service, to offer users a personalized experience and to facilitate communication and coordination between event participants.

The company that operates the service and thus the recipient of personal data is: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. For data subjects in the EU and EEA, Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Google UK Limited, Belgrave House, 76 Buckingham Palace Road, London SW1W 9TQ, United Kingdom. The representative under

Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Google Switzerland GmbH, Brandschenkestrasse 110, 8002 Zurich, Switzerland.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is to use and improve the calendar service and scheduling. Processing is based on Art. 6 (1) (b) GDPR for the performance of a contract to which the Data Subject is party or for the initiation of a contract, and on Art. 6 (1) (f) GDPR, whereby our legitimate interest lies in the optimization of scheduling and organization of appointments.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

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

36. Data protection provisions about the application and use of Google Docs

Google Docs is part of Google Workspace, a comprehensive suite of cloud-based productivity tools that allows users to create, edit and collaborate on documents in real time. Google Docs offers features such as word Processing, spreadsheets, presentation creation and more, all within an online environment. It supports collaboration between users through commenting features, editing history and the ability to manage access rights.

When using Google Docs, Personal Data such as names, email addresses, document content and editing activities are processed. This information is necessary to provide the service, enable collaboration between users and offer a personalized user experience.

The company that operates the service and thus the recipient of personal data is: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. For data subjects in the EU and EEA, Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Google UK Limited, Belgrave House, 76 Buckingham Palace Road, London SW1W 9TQ, United Kingdom. The representative under Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Google Switzerland GmbH, Brandschenkestrasse 110, 8002 Zurich, Switzerland.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is to use and optimize the document editing and collaboration service. Processing is based on Art. 6 (1) (b) GDPR for the performance of a contract to which the Data Subject is party and Art. 6 (1) (f) GDPR, where the legitimate interest is to promote productivity and collaboration and to provide an efficient and secure document management service.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

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

37. Data protection provisions about the application and use of Google Gmail

Gmail is a widely used email service. It allows users to send and receive emails, organize messages in folders and use various productivity tools directly within the platform. Gmail is known for its powerful search capabilities, extensive storage capacity and integration with other Google services such as Google Drive and Google Calendar.

When using Gmail, Personal Data such as names, email addresses, email content, contacts and calendar events are processed. This information is necessary to enable email communication, filter spam, identify security risks and offer users a personalized experience.

The company that operates the service and thus the recipient of personal data is: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. For data subjects in the EU and EEA, Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Google UK Limited, Belgrave House, 76 Buckingham Palace Road, London SW1W 9TQ, United Kingdom. The representative under Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Google Switzerland GmbH, Brandschenkestrasse 110, 8002 Zurich, Switzerland.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is to use and improve the email service and the

integration with other Google services. Processing is based on Art. 6 (1) (b) GDPR for the performance of a contract to which the Data Subject is party and Art. 6 (1) (f) GDPR, whereby our legitimate interest lies in the provision and use of an efficient, secure and user-friendly email service.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

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

38. Data protection provisions about the application and use of Google Sheets

Google Sheets is an online spreadsheet program that is part of Google Workspace. It allows users to create, edit and collaborate on spreadsheets in real time, regardless of their location. Google Sheets supports a variety of features, including formulas, charts, tables and script automation with Google Apps Script to simplify complex data analysis tasks.

When using Google Sheets, Personal Data such as names, email addresses, content of the created or edited spreadsheets and user interactions within the spreadsheets are processed. This information is necessary to provide and use the service, to enable collaboration between users and to offer a personalized user experience.

The company that operates the service and thus the recipient of personal data is: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. For data subjects in the EU and EEA, Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Google UK Limited, Belgrave House, 76 Buckingham Palace Road, London SW1W 9TQ, United Kingdom. The representative under Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Google Switzerland GmbH, Brandschenkestrasse 110, 8002 Zurich, Switzerland.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is the use and optimization of the spreadsheet service. Processing is based on Art. 6 (1) (b) GDPR for the performance of a contract to which the Data Subject is party and Art. 6 (1) (f) GDPR, where the legitimate interest is to

promote productivity and collaboration and to provide an efficient and user-friendly spreadsheet management service.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

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

39. Data protection provisions about the application and use of Google Workspace

Google Workspace is a comprehensive suite of cloud-based productivity and collaboration tools. It includes a variety of applications such as Gmail, Google Docs, Google Sheets, Google Slides, Google Drive, Google Calendar and Google Meet that enable businesses, educational institutions and teams to collaborate, communicate and manage projects efficiently. Google Workspace provides seamless integration between its various services to create a productive work environment that is accessible from anywhere.

When using Google Workspace, Personal Data such as names, email addresses, calendar events, document content and communication data are processed. This information is necessary to provide the services, to enable collaboration and communication between users and to offer a personalized user experience.

The company that operates the service and thus the recipient of personal data is: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. For data subjects in the EU and EEA, Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Google UK Limited, Belgrave House, 76 Buckingham Palace Road, London SW1W 9TQ, United Kingdom. The representative under Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Google Switzerland GmbH, Brandschenkestrasse 110, 8002 Zurich, Switzerland.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is to use and optimize productivity and collaboration services. Processing is based on Art. 6 (1) (b) GDPR for the performance of a

contract to which the Data Subject is party and Art. 6 (1) (f) GDPR, whereby our legitimate interest lies in promoting the efficiency, productivity and collaboration of teams and organizations.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

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

40. Data protection provisions about the application and use of Google Analytics

Google Analytics is a tool from Google LLC that provides website and app operators with detailed statistics on traffic and user behavior. It enables the collection and analysis of data on website visits, user interactions and conversion rates, which helps operators to understand and optimize their online presence. Google Analytics uses cookies to collect information about user behavior, including page views, time spent on the site and the paths users take on the site.

When using Google Analytics, Personal Data such as IP addresses, browser information and interaction data are processed. This data helps website operators to measure the performance of their website, improve the user experience and develop targeted marketing strategies.

The company that operates the service and thus the recipient of personal data is: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. For data subjects in the EU and EEA, Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Google UK Limited, Belgrave House, 76 Buckingham Palace Road, London SW1W 9TQ, United Kingdom. The representative under Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Google Switzerland GmbH, Brandschenkestrasse 110, 8002 Zurich, Switzerland.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is the analysis and optimization of websites and apps and advertising. Processing is based on Art. 6 (1) (f) GDPR, whereby our legitimate

interest lies in improving the website, increasing user-friendliness and the effectiveness of online marketing.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

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

41. Data protection provisions about the application and use of Google Tag Manager

Google Tag Manager is a tag management system from Google LLC that allows website and app operators to easily implement and manage tags for web analytics and marketing optimization tools without having to change the source code of their websites or apps. Tags are small snippets of code that are used to analyze website data, understand user behavior, and monitor the effectiveness of online marketing campaigns. Google Tag Manager supports the integration of a variety of tags, including Google Analytics, Google Ads and many third-party tags.

The service allows users to manage and trigger tags that can collect data. This data is processed and stored by the respective tags and not by the Google Tag Manager.

The company that operates the service and thus the recipient of personal data is: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. For data subjects in the EU and EEA, Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Google UK Limited, Belgrave House, 76 Buckingham Palace Road, London SW1W 9TQ, United Kingdom. The representative under Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Google Switzerland GmbH, Brandschenkestrasse 110, 8002 Zurich, Switzerland.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of using Google Tag Manager is to simplify tag implementation and tag management. Processing is based on Art. 6 (1) (f) GDPR, whereby our legitimate

interest lies in optimizing and increasing the efficiency of tag management and the associated web analysis and marketing activities.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

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

42. Data protection provisions about the application and use of Google Site Kit

Google Site Kit is an official WordPress plugin from Google that provides website owners with an easy way to integrate and manage various Google services and tools such as Google Analytics, Search Console, AdSense and PageSpeed Insights directly in their WordPress dashboard. It allows users to see key performance indicators and insights about their website directly in the dashboard, making it easier to analyze and optimize the website.

When using Google Site Kit, Personal Data such as website usage statistics, visitor interactions and performance data are processed. This information is necessary to provide the integrated Google services, generate detailed reports and analyses and provide users with recommendations to improve website performance.

The company that operates the service and thus the recipient of personal data is: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. For data subjects in the EU and EEA, Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR. The representative under national law in the United Kingdom is: Google UK Limited, Belgrave House, 76 Buckingham Palace Road, London SW1W 9TQ, United Kingdom. The representative under Art. 14 of the Federal Act on Data Protection (FADP) in Switzerland is: Google Switzerland GmbH, Brandschenkestrasse 110, 8002 Zurich, Switzerland.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is the use and optimization of the website analysis and website performance improvement services as well as the monetization of content. Processing is based on Art. 6 (1) (f) GDPR, whereby our legitimate interest lies in the analysis, monitoring and optimization of our website and in the monetization of content.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

Further information and the applicable data protection provisions of Google Site Kit may be retrieved under <https://policies.google.com/privacy>.

43. Data protection provisions about the application and use of Polylang

Polylang is a WordPress plugin that offers extensive multilingual functions for websites. It enables website operators to create and manage multiple language versions of their content, allowing users to access different versions of the website depending on their language preference. Polylang does not store any Personal Data of website visitors unless they interact through language-specific settings, which can store the preferred language in a cookie.

The application is installed on our own IT infrastructure. We are the company operating the service.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of using Polylang is to use multilingual capabilities for WordPress websites, which improves accessibility and usability for an international audience. Processing is based on Art. 6 (1) (f) GDPR. Our legitimate interest lies in promoting user-friendliness and the use of content in different languages to meet the needs of a diverse audience.

The criteria for determining the duration for which the Personal Data is processed are internal, statutory or contractual retention periods. The use of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us with Personal Data. If you do not provide it, you may not be able to use our services, functionality or the plugin.

Further information about Polylang can be found at <https://polylang.pro/>.

44. Data protection provisions about the application and use of WP-Optimize

WP-Optimize is a WordPress plugin that integrates database optimization, image compression and caching into a single solution. It helps clean up the WordPress database

by removing unnecessary data such as old revisions of posts and comments that are spam. The plugin can also compress images to reduce loading times and offers caching features to improve the overall performance of the website. WP-Optimize does not store any Personal Data but interacts with database content that may contain such information.

The application is installed on our own IT infrastructure. We are the company operating the service.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of using WP-Optimize is to improve website performance through database cleaning, image optimization and caching. Processing is based on Art. 6 (1) (f) GDPR. Our legitimate interest lies in the use of a more efficient, faster loading website, which improves the user experience and optimizes the use of resources.

The criteria for determining the duration for which the Personal Data is processed are internal, statutory or contractual retention periods. The use of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us with Personal Data. If you do not provide it, you may not be able to use our services, functionality or the plugin.

Further information about WP-Optimize can be found at <https://getwpo.com/>.

45. Data protection provisions about the application and use of Facebook

Facebook is a social network that offers people the opportunity to connect, share content and communicate online. Users can create profiles, post photos and videos, exchange messages and organize themselves into groups. Facebook also offers companies and organizations a platform for advertising and interacting with their target group.

When using Facebook, Personal Data such as names, email addresses, telephone numbers, usage data, location information and information on shared content is processed. This data is necessary to provide the platform, offer personalized content and advertising, ensure user safety and develop new services.

The company operating the service and therefore the recipient of the Personal Data is: Meta Platforms, Inc., 1 Meta Way, Menlo Park, CA 94025, USA.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is to use and improve the social network functions and network services. Processing is based on Art. 6 (1) (b) GDPR for the performance of a contract to which the Data Subject is party and Art. 6 (1) (f) GDPR, whereby our legitimate interest lies in improving the user experience, providing personalized content and advertising and ensuring the security of the network.

The company operating the service is located in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You

can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

Further information and the applicable data protection provisions of Facebook can be found at <https://facebook.com>.

46. Data protection provisions about the application and use of Instagram

Instagram is a widely used social network that allows users to share photos and videos, post stories, and interact with followers and friends. Instagram offers a variety of features, including direct messages, IGTV for longer videos, Instagram Live for real-time broadcasts and a Discover page to find new content and users.

When using Instagram, Personal Data such as names, email addresses, telephone numbers, user content (photos, videos, comments, etc.), location data, usage information and, in some cases, payment information is processed. This data helps to provide the service, ensure the security of the platform, offer personalized advertising and improve the user experience.

The company operating the service and therefore the recipient of the Personal Data is: Meta Platforms, Inc., 1 Meta Way, Menlo Park, CA 94025, USA.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is the use and optimization of the social network functions. Processing is based on Art. 6 (1) (b) GDPR for the performance of a contract to which the Data Subject is party and Art. 6 (1) (f) GDPR, where our legitimate interest lies in the improvement and personalization of the user experience, the provision of customer support and ensuring the security and integrity of the platform, as well as in the use of the platform and marketing.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not

obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

Further information and the applicable data protection provisions of Instagram can be viewed at <https://instagram.com>.

47. Data protection provisions about the application and use of LinkedIn

LinkedIn is a social network for professional contacts and career development. The platform allows users to create a professional profile, network with colleagues, business partners and potential employers, share professional experiences and skills, and keep up to date with industry news. LinkedIn also provides tools for companies and recruiters to source talent, post job ads and build a brand presence.

When using LinkedIn, Personal Data such as names, email addresses, professional titles and experience, educational background, skills, interests and platform usage data are processed. This information is necessary to provide and use the service, to create networking opportunities, to present personalized content and job offers and to ensure the security of user data.

The company operating the service and thus the recipient of the Personal Data is: LinkedIn Corporation, 1000 W. Maude Avenue, Sunnyvale, CA 94085, USA.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is the use and optimization of network and career services. Processing is based on the Consent of the user (Art. 6 (1) (a) GDPR), the performance of a contract (Art. 6 (1) (b) GDPR) to which the Data Subject is party and on legitimate interests (Art. 6 (1) (f) GDPR), such as marketing and recruitment.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

Further information and the applicable data protection provisions of LinkedIn Corporation can be found at <https://www.linkedin.com>.

48. Data protection provisions about the application and use of Meta Platforms

Meta Platforms is a technology company that operates several social networks and communication platforms, including Facebook, Instagram, WhatsApp and Messenger. These services enable billions of users worldwide to connect, share content, communicate and build communities around their interests.

When using Meta Platforms' services, Personal Data such as names, email addresses, telephone numbers, profile information, posts, comments, messages, interactions with content and advertising, location data and payment information are processed. This information is used to provide services, ensure user security, offer personalized content and advertising and improve the user experience.

The company operating the service and therefore the recipient of the Personal Data is: Meta Platforms, Inc., 1 Meta Way, Menlo Park, CA 94025, USA.

Purposes for which the Personal Data is to be processed and the legal basis for the Processing: The purpose of processing is to use, provide, manage and improve the social networks and communication services. Processing is based on the Consent of the user (Art. 6 (1) (a) GDPR), the performance of a contract (Art. 6 (1) (b) GDPR) to which the Data Subject is party and on legitimate interests (Art. 6 (1) (f) GDPR), such as the use and improvement of the services.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may be a certified member of one or more of the data privacy frameworks. You can find more information at <https://www.dataprivacyframework.gov/list>. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

Further information and the applicable data protection provisions of Meta Platforms, Inc. can be found at <https://www.facebook.com>.

49. Data protection provisions about the application and use of Pinterest

Pinterest is a platform for visual discoveries that allows us to share and save images, ideas and content. When using Pinterest, personal data such as usage data, search queries, IP addresses and interaction data with content are processed in order to personalize the user experience and suggest content. This data is used to improve recommendations, provide personalized advertising and optimize the use of the platform.

The company that operates the service and thus the recipient of personal data is: Pinterest, Inc., 651 Brannan Street, San Francisco, CA 94107, USA. For data subjects in the EU and EEA, Pinterest Europe Ltd., Palmerston House, 2nd Floor, Fenian Street, Dublin 2, Ireland, acts as contact and representative within the meaning of Art. 27 GDPR.

Purposes for which personal data are to be processed and the legal basis for the processing: The purpose of the processing is to improve the user experience through personalized content and recommendations as well as advertising. The processing is based on Art. 6 (1) (f) GDPR, whereby the legitimate interest lies in the provision of relevant content and personalized advertising.

The company that operates the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company that operates the service may have concluded one of the EU standard contractual clauses with us. You can request a copy of the suitable or appropriate safeguards from us.

The criteria for determining the duration for which the personal data is processed are the contractual relationship between us and the company that operates the service or statutory or contractual retention periods. As a rule, the provision of personal data is neither legally nor contractually required, nor is it necessary for the conclusion of a contract. You are not obliged to provide us or the company that operates the service with personal data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

Further information and the applicable data protection provisions of Pinterest may be retrieved under <https://www.pinterest.com/>.

50. Data protection provisions about the application and use of X (formerly Twitter)

X (formerly known as Twitter) is a global platform for public self-expression and real-time conversation. Users can create and share short messages, called tweets, which can include text, images, videos and links. The platform allows users to follow breaking news, interact with others and participate in global discussions.

When using X, various types of Personal Data are processed, including usernames, email addresses, telephone numbers and location data. This information can be used for account creation, personalization of content, provision of advertising, security purposes and for analytical evaluations.

The operating company of the platform and therefore the recipient of the Personal Data is X Corp, Suite 900, 1355 Market Street, San Francisco, California, 94103, USA.

The Processing of Personal Data takes place, among other things, on the basis of the user's Consent (Art. 6 (1) (a) GDPR), for the performance of a contract (Art. 6 (1) (b) GDPR) to which the Data Subject is a party, or on the basis of legitimate interests (Art. 6 (1) (f)

GDPR), such as the use of the platform and the improvement of communication with the public.

The company operating the service is based in a third country, namely the USA. Transfers to third countries may be based on the conclusion of standard contractual clauses or other suitable or appropriate safeguards referred to in Art. 46 (2) GDPR. The company operating the service may have concluded one of the EU standard contractual clauses with us. You can request a copy of the suitable or appropriate guarantees from us.

The criteria for determining the duration for which the Personal Data is processed are the contractual relationship between us and the company operating the service or statutory or contractual retention periods. The provision of Personal Data is generally not required by law or contract, nor is it necessary for the conclusion of a contract. As a rule, you are not obliged to provide us or the company operating the service with Personal Data. However, if you do not provide it, you may not be able to use our services or those of the company operating the service.

Further information and the applicable data protection provisions of X can be found at <https://twitter.com/>.