Privacy Policy
for the content and functionalities
of the website www.joannaritz.com
(hereinafter the "Services")

April 2026

Introduction

Privacy policies are often difficult to read. We understand that—and we want to do things differently. With this privacy policy, we aim to provide users with a clear and easily understandable explanation of how we process personal data. To this end, we have structured our privacy policy in a transparent and user-friendly manner and indicate for each section whether and how we process users' personal data.

In this privacy policy, we explain whether and how we process personal data. In doing so, we present all processing activities carried out by us, by third-party service providers engaged or integrated by us, or by other third parties acting on our behalf in connection with the use of our website, our social media profiles and the respective functionalities available therein, as well as in connection with the performance of our contractual relationships (hereinafter collectively also referred to as the "Services").

Table of Contents

Our privacy policy is structured as follows:

1. **General Information – Brief introduction to the subject matter of this privacy policy, the data controller, and the data protection officer**
2. **General Information on Data Processing – Information on what personal data is, the legal basis on which we process it, and whether and how we share it with third parties**
3. **Data Subject Rights – Information on users' rights, including the right of access, erasure, or objection to our data processing**
4. **Information on Cookies and Other Technologies – Information on the use of cookies and other technologies by which or with which we process users' personal data**
5. **Data Processing in Connection with the Use of Our Services – Information on our data processing within our Services**
6. **Communication Services – Information on communication services and the associated processing of personal data**
7. **Payment Processing – Information on the processing of payments through the integration of payment service providers and the related processing of personal data**
8. **Provision of Our Services – Information on hosting providers and the services used by them**
9. **Tracking & Tools – Information on services through which we provide our Services and analyze their usage**
10. **Transactional Emails – Information on the integration of mailing service providers used to send transactional emails**
11. **Newsletter – Information on the integration of newsletter services used to provide users with regular information about our Services**
12. **Social Media Profiles – Information on our presence on social media platforms and the associated processing of personal data**
13. **Sharing Function – Information on the options to share content from our Services directly on social media platforms**

1. General

The protection of personal data and privacy is of utmost importance to us. Therefore, we aim to provide users with comprehensive transparency regarding the processing of personal data (GDPR) as well as the storage of information on users' terminal devices (TDDDG). Only if the processing of personal data and information is

understandable to users as data subjects are they sufficiently informed about the scope, purposes, and benefits of such processing.

This privacy policy applies to all processing of personal data carried out by us, as well as to the storage of information on terminal devices. It therefore applies both within the scope of the provision of our Services and within external online presences, such as our social media profiles.

The controller within the meaning of the General Data Protection Regulation (GDPR), the German Federal Data Protection Act (BDSG), and other applicable data protection regulations is:

Joanna Ritz (Freelancer)
Breite Straße 22
40213 Düsseldorf
Email: contact@joannaritz.com
Phone: +49 (0) 160 927 008 22

Hereinafter referred to as the “Controller” or “we”.

2. General Information

First of all, we would like to provide users with introductory information on what the protection of personal data means, what personal data is, how we process it, and which security measures we apply in this regard.

2.1 Processing of Personal Data

Personal data (hereinafter also referred to as “data”) means individual information relating to the personal or factual circumstances of an identified or identifiable natural person.

Individual information relating to personal or factual circumstances includes, for example, the following data, whereby it is clarified that not all of this data necessarily has to be processed by our Services:

· **Personal data** – name, age, marital status, date of birth
· **Communication data** – address, telephone number, email address
· **Account data** – bank account number, credit card number
· **Geodata** – IP address and location data

The “processing” of personal data includes, for example, the following activities:

· **Collection** – The collection of data via contact forms, by email, or through processes and services used by us
· **Transmission** – The transmission of data to our service providers, integrated services, or other third parties
· **Storage** – The storage of data in our databases or on our servers
· **Modification** – The modification of data due to changes in name, place of residence, or information provided in our Services
· **Deletion** – The deletion of data where we no longer have authorization to process it

2.2 Legal Bases for the Processing of Personal Data

We process personal data only within the legally permissible limits. We are already required to do so by law, in particular by the GDPR. Under the GDPR, we are obliged to always be able to base data processing activities on a legal basis. These legal bases are set out in Art. 6(1) GDPR. Below, we list all legal bases on which we may base the processing of personal data.

· **Consent – Art. 6(1)(a) GDPR:** Data is processed where users have actively consented to such processing, for example by way of an “opt-in”, after having previously been sufficiently informed by us about the scope and purposes of the processing. If users withdraw their consent or have not given consent, we will no longer process, or will not process, users’ data for purposes for which consent is required.

· **Performance of a contract – Art. 6(1)(b) GDPR:** Data is processed where such processing is necessary for the performance of a contract between us and the user or in order to take steps prior to entering into a contract. Where processing is no longer necessary for the performance of a contract, we will no longer process users' personal data.

· **Compliance with a legal obligation – Art. 6(1)(c) GDPR:** Data is processed where such processing is necessary for compliance with a legal obligation to which we, as the Controller, are subject.

· **Legitimate interest – Art. 6(1)(f) GDPR:** Data is processed where such processing is necessary for the purposes of a legitimate interest pursued by us, provided that the interests or fundamental rights and freedoms of users relating to the protection of data do not override such interest.

We process personal data only for specific purposes (Art. 5(1)(b) GDPR). As soon as the purpose of the processing no longer applies, users' personal data will be deleted or protected by technical and organizational measures, for example by pseudonymization.

The same applies upon expiry of a prescribed retention period, subject to cases in which further storage is necessary for the conclusion or performance of a contract. In addition, a statutory obligation to store data for a longer period or to disclose data to third parties, in particular law enforcement authorities, may arise. In all other cases, the retention period and the type of data collected, as well as the type of data processing, depend on which functions users use in each individual case. We will also be happy to provide users with information on this in individual cases, in accordance with Art. 15 GDPR.

2.3 Data Categories We Process

Data categories include, in particular, the following data:

· **Master data** (e.g. names, addresses, dates of birth),
· **Contact data** (e.g. email addresses, telephone numbers, messenger services),
· **Content data** (e.g. text entries, photographs, videos, contents of documents/files),
· **Contract data** (e.g. subject matter of the contract, terms, customer category),
· **Payment data** (e.g. bank details, payment history, use of other payment service providers),
· **Usage data** (e.g. history within our Services, use of certain content, access times),
· **Connection data** (e.g. device information, IP addresses, URL referrers).

2.4 Security Measures We Apply

In accordance with statutory requirements and taking into account the state of the art, implementation costs, and the nature, scope, circumstances, and purposes of processing, as well as the varying likelihood and severity of risks to rights and freedoms, we implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

These measures include, in particular, ensuring that users' data is stored and processed confidentially, with integrity, and in a manner that ensures availability at all times. Furthermore, controls relating to data access, access rights, input, disclosure, safeguarding availability, and separation from the data of other natural persons are among the security measures we implement. In addition, we have established procedures to ensure the exercise of data subject rights (see Section 3), the deletion of data, and responses in the event of a risk to users' data. Furthermore, we take the protection of personal data into account already during the development of our software and through procedures that comply with the principles of data protection by design and by default.

2.5 How We Transfer or Disclose Personal Data to Third Parties

In the course of our processing of personal data, such data may be transferred or disclosed to other bodies, companies, legally independent organizational units, or persons. Such third parties may include, for example, payment institutions in connection with payment transactions, service providers entrusted with IT tasks, or

providers of services and content that we have integrated into our Services. If we transfer or disclose users' personal data to third parties, we comply with the statutory requirements and, in particular, conclude appropriate contracts or agreements with the recipients of the data that serve to protect such data.

2.6 How Transfers to Third Countries Are Carried Out

If this privacy policy states that we transfer users' personal data to a third country, i.e. a country outside the EU or outside the EEA, the following applies. Any transfer to a third country takes place only in accordance with statutory requirements. We assure users that we have a contractual or statutory authorization to transfer and process data in the relevant third country. In addition, we only allow users' data to be processed by service providers in third countries that, in our view, provide a recognized level of data protection. This means, for example, that an adequacy decision exists between the EU and the country to which we transfer users' personal data. An "adequacy decision" is a decision adopted by the European Commission pursuant to Art. 45 GDPR determining that a third country, i.e. a country not bound by the GDPR, or an international organization ensures an adequate level of protection for personal data. Alternatively, for example where no adequacy decision exists, a transfer to a third country will only take place if, for instance, contractual obligations between us and the service provider in the third country exist on the basis of the so-called Standard Contractual Clauses of the European Commission and additional technical safeguards have been implemented to ensure a level of protection essentially equivalent to that in the EU, or if the service provider in the third country can demonstrate data protection certifications and processes users' data only in accordance with internal data protection rules (Arts. 44 to 49 GDPR. Information page of the European Commission: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_de).

Within the framework of the so-called "Data Privacy Framework" ("DPF"), the European Commission recognized the level of data protection for certain companies from the United States as adequate in its adequacy decision of 10 July 2023. Users can find a list of certified companies as well as further information on the DPF on the website of the U.S. Department of Commerce at https://www.dataprivacyframework.gov/ (in English). In this privacy policy, we inform users which Services used by us are certified under the Data Privacy Framework.

Please note: Certification under the EU-U.S. Data Privacy Framework (DPF) is company-specific and may change at any time. We regularly check whether the U.S. service providers used by us are certified under the DPF at the time of the respective data processing. The current list of certified companies is available at: https://www.dataprivacyframework.gov/list.

If a service provider used by us is not, or is no longer, certified under the DPF, personal data will be transferred exclusively on the basis of the European Commission's Standard Contractual Clauses and supplementary technical and organizational measures.

2.7 Deletion of Data

The data processed by us will be deleted in accordance with statutory requirements as soon as the consent permitting its processing is withdrawn or other permissions cease to apply, for example where the purpose of processing such data no longer applies or the data is no longer required for that purpose. Where data is not deleted because it is required for other legally permissible purposes, its processing will be restricted to those purposes. This means that the data will be blocked and not processed for other purposes. This applies, for example, to data that must be retained for commercial or tax law reasons or where storage is necessary for the establishment, exercise, or defense of legal claims or for the protection of the rights of another natural or legal person.

Within this privacy policy, we may provide information on the deletion and retention of data that specifically applies to the respective processing activities.

2.8 Storage of and Access to Data on the User's Terminal Device

Where we do not obtain users' consent for this, the storage of or access to information on the user's terminal device is carried out pursuant to Section 25(2) No. 2 of the German Telecommunications Digital Services Data Protection Act (TDDDG), because the storage of and access to such information is strictly necessary in order to provide the requested functions of our Services. Where we obtain consent for this, the legal basis is Section 25(1) TDDDG. Our Services use cookies, tokens, or other technologies that may be stored on terminal devices and without which the provision of our Services would not be possible.

Cookies, tokens, or other technologies are generally text files that are stored on the user's terminal device and can be read by us and third parties when our Services are accessed. Many of the aforementioned technologies contain their own ID. Such an ID is a unique identifier of the respective technology used. It consists of a string of characters that enables websites and servers to be assigned to the specific internet browser or the specific service or terminal device used in which cookies, tokens, or other technologies have been stored. This enables operators of websites and analytics services to identify users as users and distinguish them from others.

2.9 Data Processing on Behalf of the Controller

If we use external service providers to process data, these service providers are carefully selected and commissioned by us. If the services provided by these service providers constitute processing on behalf of the controller within the meaning of Art. 28 GDPR, the service providers are bound by our instructions and are regularly monitored. Our data processing agreements meet the strict requirements of Art. 28 GDPR as well as the requirements of the German data protection authorities.

3. Data Subject Rights

If personal data of our users is processed, users are data subjects within the meaning of the GDPR and have the following rights vis-à-vis the Controller.

3.1 Right of Access

Users may request confirmation from the Controller as to whether personal data concerning them is being processed.

If such processing takes place, users may request information from the Controller regarding the following:

- the purposes for which the personal data is processed;
- the categories of personal data that are processed;
- the recipients or categories of recipients to whom the personal data concerning the users has been or will be disclosed;
- the envisaged period for which the personal data concerning the users will be stored or, where specific information on this is not possible, the criteria used to determine that period;
- the existence of a right to rectification or erasure of personal data concerning the users, a right to restriction of processing by the Controller, or a right to object to such processing;
- the existence of the right to lodge a complaint with a supervisory authority;
- all available information as to the source of the data where the personal data has not been collected from the data subject;
- the existence of automated decision-making, including profiling, pursuant to Article 22(1) and (4) GDPR and—at least in those cases—meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;

- users also have the right to request information as to whether the personal data concerning them is transferred to a third country or to an international organization. In this context, users may request to be informed of the appropriate safeguards pursuant to Article 46 GDPR in connection with such transfer.

3.2 Right to Rectification

Users have the right to obtain from the Controller the rectification and/or completion of personal data concerning them, where such data is inaccurate or incomplete. The Controller shall carry out the rectification without undue delay.

3.3 Right to Restriction of Processing

Under the following conditions, users may request the restriction of processing of personal data concerning them:

- where users contest the accuracy of the personal data concerning them for a period enabling the Controller to verify its accuracy;
- where the processing is unlawful and users oppose the erasure of the personal data and request the restriction of its use instead;
- where the Controller no longer needs the personal data for the purposes of processing, but the users require it for the establishment, exercise, or defence of legal claims; or
- where users have objected to processing pursuant to Art. 21(1) GDPR and it has not yet been determined whether the legitimate grounds of the Controller override those of the users.

Where the processing of personal data concerning users has been restricted, such data may—apart from storage—only be processed with the user's consent or for the establishment, exercise, or defence of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or of a Member State.

Where the restriction of processing has been imposed under the above conditions, users shall be informed by the Controller before the restriction is lifted.

3.4 Right to Erasure

3.4.1 Users may request from the Controller that personal data concerning them be erased without undue delay, and the Controller shall be obliged to erase such data without undue delay where one of the following grounds applies:

- the personal data concerning the users is no longer necessary for the purposes for which it was collected or otherwise processed;
- users withdraw their consent on which the processing was based pursuant to Art. 6(1)(a) or Art. 9(2)(a) GDPR, and where there is no other legal basis for the processing;
- users object to the processing pursuant to Art. 21(1) GDPR and there are no overriding legitimate grounds for the processing, or users object pursuant to Art. 21(2) GDPR;
- the personal data concerning the users has been processed unlawfully;
- the erasure of personal data concerning the users is required for compliance with a legal obligation under Union or Member State law to which the Controller is subject;
- the personal data concerning the users has been collected in relation to the offer of information society services pursuant to Art. 8(1) GDPR.

3.4.2 Where the Controller has made personal data concerning users public and is obliged pursuant to Art. 17(1) GDPR to erase such data, the Controller shall, taking account of available technology and the cost of implementation, take reasonable steps, including technical measures, to inform other controllers processing the

personal data that users, as data subjects, have requested the erasure of any links to, or copies or replications of, those personal data.

3.4.3 The right to erasure shall not apply where processing is necessary

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing under Union law or the law of theMember States to which the Controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
- for reasons of public interest in the area of public health pursuant to Art. 9(2)(h) and (i) and Art. 9(3) GDPR;
- for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes pursuant to Art. 89(1) GDPR, insofar as the right referred to above is likely to render impossible or seriously impair the achievement of the objectives of that processing;
- or for the establishment, exercise, or defence of legal claims.

3.5 Right to Notification

If users have exercised their right to rectification, erasure, or restriction of processing vis-à-vis the Controller, the Controller shall be obliged to notify all recipients to whom the personal data concerning the users has been disclosed of such rectification, erasure, or restriction of processing, unless this proves impossible or involves disproportionate effort.

3.6 Right to Data Portability

Users have the right to receive the personal data concerning them, which they have provided to the Controller, in a structured, commonly used, and machine-readable format. Users also have the right to transmit those data to another controller without hindrance from the Controller to whom the personal data has been provided, where the 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. In exercising this right, users also have the right to have the personal data concerning them transmitted directly from one controller to another, where technically feasible. In doing so, the rights and freedoms of others must not be adversely affected. The right to data portability shall not apply to processing of personal data that 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.

3.7 Right to Object

Users have the right, on grounds relating to their particular situation, to object at any time to the processing of personal data concerning them which is based on Art. 6(1)(e) or (f) GDPR; this also applies to profiling based on those provisions. The Controller shall no longer process the personal data concerning the users unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the users, or the processing serves the establishment, exercise or defence of legal claims. Where personal data concerning users is processed for direct marketing purposes, users have the right to object at any time to the processing of such personal data for the purpose of such marketing; this also applies to profiling insofar as it is related to such direct marketing. Where users object to processing for direct marketing purposes, the personal data concerning users shall no longer be processed for such purposes. In the context of the use of information society services, users have the possibility—irrespective of Directive 2002/58/EC—to exercise their right to object by automated means using technical specifications.

3.8 Right to Withdraw Consent

Users have the right to withdraw their consent to the processing of personal data at any time. The withdrawal of consent shall not affect the lawfulness of processing carried out on the basis of consent prior to its withdrawal.

Processing shall remain lawful until the withdrawal; the withdrawal therefore only takes effect for processing after receipt of the withdrawal.

Users may declare the withdrawal informally, for example by post or email. The processing of personal data will then cease, unless it is permitted on the basis of another legal ground. If this is not the case, users' data must be deleted without undue delay following the withdrawal in accordance with Art. 17(2) GDPR. The right to withdraw consent under the above conditions is guaranteed.

The revocation shall be addressed to:

Joanna Ritz (Freelancer)
Breite Straße 22
40213 Düsseldorf
Email: contact@joannaritz.com
Phone: +49 (0) 160 927 008 22

3.9 Right to Lodge a Complaint

Without prejudice to any other administrative or judicial remedy, users shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of their place of residence, place of work, or the place of the alleged infringement, if users consider that the processing of personal data concerning them infringes the GDPR. The supervisory authority with which the complaint has been lodged shall inform the complainant of the status and outcome of the complaint, including the possibility of a judicial remedy pursuant to Art. 78 GDPR.

3.10 Automated Decision-Making

Automated decision-making in individual cases within the meaning of Art. 22 GDPR does not take place. However, we use automated processes in certain areas to structure or optimize content, communication, or workflows (e.g. statistical analyses or AI-assisted response suggestions). These processes do not produce legal effects for users and do not affect them in any comparable manner.

3.11 Notification Obligations

If personal data concerning users has been disclosed to other recipients (third parties) on a legal basis, we shall inform them of any rectification, erasure, or restriction of processing of such personal data (Art. 16, Art. 17(1), and Art. 18 GDPR). The obligation to provide such notification shall not apply if it proves impossible or involves disproportionate effort. We shall also inform users, upon request, about those recipients.

4. Information on Cookies and Other Technologies

We use cookies and other technologies to provide our Services, analyze them, and use the evaluated data for marketing purposes. Cookies are, for example, small text files that contain data from visited websites or domains and are stored on a device (computer, tablet, or smartphone). When users access a website, the cookie stored on the device sends information to the entity that placed the cookie.

4.1 How We Use Cookies and Other Technologies

We want users to be able to make an informed decision for or against the use of cookies and other technologies that are not strictly necessary for the technical functionality of the Services. Therefore, where we use cookies and other technologies that require consent, users are given the option—upon their first visit and at any time thereafter via the settings—to decide which cookies and technologies they wish to allow. Functional cookies and technologies are strictly necessary for the operation of our Services and are therefore enabled by default. Statistical and marketing cookies and technologies are optional. Users may allow them by giving their consent via the consent banner or may decline them.

4.2 Storage Period of Cookies and Other Technologies

The specific storage duration of cookies and comparable technologies depends on the respective service used and is transparently displayed in the consent banner or in the cookie overview available there. Where no specific duration is indicated, cookies will be deleted or expire at the latest after 24 months. If cookies and technologies are set on the basis of consent, users may withdraw their consent or object to the processing at any time (collectively referred to as “opt-out”).

4.3 Types of Cookies and Other Technologies

We distinguish between the following categories:

- **Functional cookies/technologies:** These are necessary for the basic technical functionality of the Services, for example enabling secure login, saving shopping cart content, or ensuring consistent display of website content.
- **Statistical cookies/technologies:** These enable us to analyze our Services to measure and improve performance. Users may change their statistical settings via the opt-out options provided.
- **Marketing cookies/technologies:** These are used to display advertisements that may be relevant to users’ interests. They also enable sharing content via social networks or interacting with content such as comments. Users may adjust their marketing preferences via the corresponding opt-out options.

4.4 Consent Management

We use a consent management tool (hereinafter “Consent Tool”) in connection with tracking and analytics activities in our Services. The Consent Tool collects log file and consent data and enables us to inform users about, obtain, manage, and document their consent to certain technologies within our Services. In doing so, we process the following data: (1) consent data (including anonymized log data such as consent ID, processor ID, controller ID, consent status, timestamp), (2) device data (including truncated IP addresses (IPv4, IPv6), device information, timestamp), (3) user data (including email address, ID, browser information, setting IDs, change log). The consent ID (containing the above information) and the consent status including timestamp are stored both in the browser’s local storage and on cloud servers used by us. Further processing only takes place in the event of a user request (e.g., access request) or withdrawal of consent. The legal basis for processing personal data via the Consent Tool is our legitimate interest and compliance with legal obligations pursuant to Art. 6(1)(f) and (c) GDPR. The purpose of using the Consent Tool is to comply with legal requirements related to data protection and tracking and to ensure a lawful and user-oriented operation of our systems.

Provider of the Consent Tool:

Usercentrics A/S
Havnegade 39
1058 Copenhagen
Denmark

5. Data Processing in Connection with the Use of Our Services

The use of our Services, including all of their functions, involves the processing of personal data. We explain to users below exactly how this takes place.

5.1 Informational Use of Our Services

The purely informational use of our Services requires the processing of the following personal data and information: device type and device version, operating system used, IP address of the end device with which users access our Services, and the time at which our Services are accessed. All of this information is automatically transmitted by the device unless users have configured the device in such a way that the transmission of this information is suppressed. This personal data is processed for the purpose of ensuring the

functionality and optimization of our Services, as well as ensuring the security of our information technology systems. These purposes also constitute legitimate interests pursuant to Art. 6(1)(f) GDPR; the processing is therefore carried out on a legal basis.

5.2 Coaching Services

In the course of providing our Coaching Services, we process users' personal data. We process users' personal data within the scope of the coaching agreement in order to be able to provide the contractually owed services. We only disclose the data entered by you to authorized third parties, in particular, on a case-by-case basis and insofar as agreed in the coaching agreement, to Hogan Assessment Systems, Inc., 11 South Greenwood Avenue, Tulsa, OK 74120, United States, and process such data for the performance of the contractual relationships entered into with users, in particular for the performance of the coaching agreement. The legal basis for the processing of your data is therefore Art. 6(1)(b) GDPR.

6. Communication Services

6.1 Contact Form / Contact by Email

We process the personal data that users provide to us when contacting us for the purpose of responding to an inquiry, an email, or a callback request. The categories of data processed in this context are master data, contact data, content data, and, where applicable, usage data, connection data, and contract data. In individual cases, we disclose this data to affiliated companies or third parties that are permitted to process such data in accordance with the agreement for the purpose of handling orders and bookings. The legal basis for the processing depends on the purpose of the contact. By submitting an inquiry via the contact form or by contacting us by email, users indicate that they wish to receive answers or information on specific topics. For this purpose, users also provide their data. We respond to the inquiry as requested and process users' data for this purpose. The authorization to process the data is therefore based on Art. 6(1)(b) GDPR, as we process it in order to respond to an inquiry and thus to perform the corresponding agreement.

6.2 Questionnaires and Surveys

For the implementation of questionnaires and surveys, we use the questionnaire and survey tools of the providers listed below. The categories of data typically processed in this context are contact data, master data, and content data. If a provider transfers this data to a third country, this will only take place on a case-by-case basis, on the basis of a data processing agreement concluded with that provider and in accordance with Standard Contractual Clauses agreed with that provider as well as other safeguards permitted under the GDPR, which ensure the security of the processing of personal data at a level of protection equivalent to that within the EU. Our legal basis for using the questionnaire and survey tools listed below is Art. 6(1)(f) GDPR (legitimate interest), as these tools enable us to fully automate the collection of information that is important to us and thereby make the process of preparing corresponding discussions more efficient. In addition, the legal basis for data processing by means of the questionnaire and survey tools is Art. 6(1)(b) GDPR insofar as the questionnaires and surveys are conducted within the scope of our contractual relationships.

Provider of the questionnaire and survey tools used by us

Wix Forms
Wix.com Ltd
40 Namal Tel Aviv St.
Tel Aviv 6350671
Israel

https://de.wix.com/about/privacy

6.3 Data Processing in the Event of Revocation of a Contract

If consumer users effectively revoke a contract concluded with us, for example pursuant to Sections 312g and 355 German Civil Code (BGB), we will no longer process their personal data for the performance of the effectively revoked contract. The revocation itself may be exercised via the methods specified in the revocation notice, i.e. by telephone, email, or post, and in particular also through the revocation process by clicking the revocation button. Despite the revocation, however, we will continue to process the user's data where this is necessary for handling the revocation, for example for refunding payments already made, for complying with statutory retention and documentation obligations, in particular under commercial and tax law, or for the establishment, exercise, or defense of legal claims. The legal basis for processing data in connection with the revocation of a contract is Art. 6(1)(c) GDPR (legal obligation) and Art. 6(1)(f) GDPR (legitimate interest in proper processing and legal protection). As soon as the user's personal data is no longer required for the aforementioned purposes and no statutory retention obligations apply, it will be permanently deleted.

6.4 Appointment Scheduling and Appointment Booking

We use the appointment scheduling tools listed below in our Services to arrange appointments with users. Through the appointment scheduling tools and their integrated online calendars, users can conveniently request and select an appointment for a conversation. When users click the corresponding button in our Services or wish to arrange an appointment via a link provided by us, for example in an email, users are automatically connected to our appointment account with the appointment scheduling tools integrated by us. After selecting the appointment, confirming it, and entering contact details and the subject matter, users receive an email confirming the appointment. If the appointment scheduling tools transfer this data to a third country, for example the USA, this will only take place on a case-by-case basis, on the basis of a data processing agreement concluded with them and in accordance with Standard Contractual Clauses agreed with them as well as other safeguards permitted under the GDPR, which ensure the security of the processing of personal data at a level of protection equivalent to that within the EU, in particular on the basis of the EU-US Data Privacy Framework (DPF). Information from the appointment scheduling tool form, including the data entered by users there, is stored by us for the purpose of processing an inquiry or handling a corresponding contractual relationship. Once an inquiry has been answered or the purpose no longer applies, for example because the contractual relationship has ended, we will delete users' data promptly, subject to contractual or statutory retention options. If users wish their data to be deleted earlier, they may request deletion from us or withdraw consent to storage. Mandatory statutory provisions, in particular retention periods, remain unaffected. Our legal basis for using the appointment scheduling tools is Art. 6(1)(f) GDPR (legitimate interest), as these tools enable us to fully automate appointment scheduling and thereby make the process for corresponding appointment requests and conversations more efficient. In addition, the legal basis for data processing by means of the appointment scheduling tools is Art. 6(1)(b) GDPR insofar as appointment scheduling is carried out within the scope of our contractual relationships.

Provider of the appointment scheduling tools used by us

Wix Bookings
Wix.com Ltd
40 Namal Tel Aviv St.
Tel Aviv 6350671
Israel

https://de.wix.com/about/privacy

6.5 Video Communication Tools

We use video communication tools to conduct telephone conferences, client meetings, online meetings, video conferences, and/or webinars (hereinafter "Online Meetings"). The scope of data processing depends on the

specific purpose for which we hold the Online Meeting and on the data provided by users before or during participation in an Online Meeting. Relevant categories of data may include master data, contact data, content data, and, where applicable, usage data, connection data, and contract data. The recipients of the data are the providers of video communication tools integrated by us and listed below. If these providers transfer data to a third country, for example the USA, this will only take place on a case-by-case basis, on the basis of a data processing agreement concluded with them and in accordance with Standard Contractual Clauses agreed with them as well as other safeguards permitted under the GDPR, which ensure the security of the processing of users' personal data at a level of protection equivalent to that within the EU, and, where data is transferred to the USA, in particular on the basis of the EU-US Data Privacy Framework (DPF). Our legal basis for using video communication tools is Art. 6(1)(b) GDPR (performance of a contract), provided that the Online Meeting takes place in connection with contract negotiations or for the performance of our contractual obligations. Where online communication or collaboration tools are used outside a specific contractual relationship or on a voluntary basis, data processing takes place on the basis of consent pursuant to Art. 6(1)(a) GDPR. Where we obtain consent for the use of video communication tools, our legal basis is Art. 6(1)(a) GDPR. By integrating video communication tools, we aim to fully digitalize communication between us. Video communication tools are intended to enable us to gain a personal impression of each other in an Online Meeting, which is, among other things, essential for a relationship of trust in a contractual relationship.

Provider of the video communication tools used by us

"Zoom"
Zoom Video Communications, Inc.
55 Almaden Blvd
Suite 600
San Jose
CA 95113
United States of America

https://www.zoom.com/de/trust/privacy/privacy-statement/

7. Payment Processing

To process payments, we offer various payment methods. For this purpose, we integrate the payment service providers described below. This is done to ensure the proper and needs-based provision of our Services. In this context, the data processed may include usage data, connection data, master data, payment data, contact data, as well as contract data, such as bank account numbers or credit card numbers, passwords, TANs, checksums, and information related to the contract, amounts, and recipients. This information is required to carry out the transactions. The data entered is processed and stored only by the respective payment service providers. We do not receive any account or credit card-related information, but only information regarding the confirmation or rejection of a payment. In some cases, payment service providers may transmit user data to credit agencies for identity and credit checks. For this purpose, we refer to the terms and conditions and privacy notices of the respective payment service providers. The legal basis for the use of payment service providers is Art. 6(1)(b) GDPR, as we can only provide our contractually agreed Services by using third parties such as payment service providers to process payments. Where a payment service provider transfers data to a third country, for example the United States, this will only take place in individual cases, on the basis of a data processing agreement and in accordance with Standard Contractual Clauses and other safeguards permitted under the GDPR, in particular on the basis of the EUUS Data Privacy Framework (DPF).

Payment Service Provider

PayPal

It is possible to process payments via the online payment service PayPal. PayPal enables online payments to third parties. The European operating company of PayPal is PayPal (Europe) S.à r.l. & Cie. S.C.A., 2224 Boulevard Royal, 2449 Luxembourg. If users select PayPal as a payment method, the data required for the payment process is automatically transmitted to PayPal. This typically includes the following data:
name, address, company name, email address, telephone number, mobile number, and IP address. The data transmitted to PayPal may be shared by PayPal with credit agencies for identity and credit checks. PayPal may also transfer user data to third parties where this is necessary for the performance of contractual obligations or where the data is to be processed on behalf of PayPal. Users may view PayPal's privacy policy at: https://www.paypal.com/de/webapps/mpp/ua/privacy-full/ The legal basis for this data processing is Art. 6(1)(b) GDPR, as the processing is necessary for payment via PayPal and thus for the performance of the contract.

8. Hosting

8.1 Provision of Our Services

In order to provide our Services, we use the hosting providers listed below. Our Services are accessed from the servers of these providers. For this purpose, we use infrastructure and platform services, computing capacity, storage space, database services, as well as security and technical maintenance services of the hosting providers. The processed data includes all data entered by users in connection with the use of and communication within our Services, as well as data collected during such use (e.g. IP address). The legal basis for using hosting providers is Art. 6(1)(f) GDPR (legitimate interest).

8.2 Sending and Receiving Emails

The services provided by hosting providers may also include the sending, receiving, and storage of emails. For these purposes, recipient and sender addresses, as well as additional information related to email transmission (e.g. involved providers) and the content of emails are processed. This data is also processed, in particular, for the detection of spam. Emails sent over the internet are generally not encrypted. While emails are typically encrypted during transmission, they are not encrypted on the servers from which they are sent and received unless end-to-end encryption is used. We therefore cannot assume responsibility for the transmission route of emails between sender and recipient. The legal basis is Art. 6(1)(f) GDPR (legitimate interest).

8.3 Collection of Access Data and Log Files

We (or our hosting providers) collect data on every access to the server (server log files). These log files include the name and address of accessed files, date and time of access, data volume transferred, notification of successful access, device type and version, operating system, referrer URL, IP address, and requesting provider. This data is used for security purposes and to ensure the stability and performance of the servers. The legal basis is Art. 6(1)(f) GDPR (legitimate interest).

Hosting Providers Used by Us

Website hosting:
Wix
Wix.com Ltd
40 Namal Tel Aviv St.
Tel Aviv 6350671
Israel

https://de.wix.com/about/privacy

Domain registrar:
Namecheap, Inc.

4600 East Washington Street
Suite 305, Phoenix
AZ 85034
United States

https://www.namecheap.com/legal/general/privacy-policy/

9. Tracking & Tools

To ensure a smooth technical operation and an optimal, user-friendly use of our Services, we use the following service:

TWIPLA

We use the web analytics service "TWIPLA Website Intelligence", operated by Arcanys, 10th Floor, i2 Building, Corner Gorordo Avenue & Salinas Drive, Lahug, Cebu City 6000. TWIPLA is used for the statistical analysis of the use of our website. The data processed in connection with the use of TWIPLA includes, in particular, usage data and connection data. Processing is carried out without the use of cookies and—since we have activated the "maximum privacy mode"—exclusively in anonymized and aggregated form. Individual users are not identified. According to TWIPLA, the technical processing and storage of data takes place on servers within the European Union. The use of TWIPLA is based on appropriate safeguards pursuant to Art. 44 et seq. GDPR, in particular a data processing agreement concluded with TWIPLA, Standard Contractual Clauses, and other safeguards permitted under the GDPR that ensure the security of the processing of personal data at a level of protection equivalent to that within the EU. The processing is carried out on the basis of Art. 6(1)(f) GDPR. Our legitimate interest lies in measuring reach and optimizing our website. Further information on data processing by TWIPLA can be found at:
https://www.twipla.com/en/support/legal-data-privacy-certificates/twipla-website/privacy-policy and on data processing by Arcanys at: https://www.arcanys.com/legal/privacy-policy.

10. Transactional Mailings

For administrative purposes, to confirm actions, and within the scope of our non-promotional customer communication, we send transactional notifications (hereinafter "transactional mailings") to users. These transactional mailings contain important administrative information regarding our Services. We do not use any external service providers for the management, creation, or sending of transactional mailings. When users access transactional mailings, technical information such as browser and system information, as well as the IP address and the time of access, may be collected. This information is used to analyze interaction with our transactional mailings based on technical data, user groups, and reading behavior. The legal basis for the use of transactional mailings is Art. 6(1)(b) GDPR, as the information contained therein serves the fulfillment of our contractual obligations towards users.

11. Newsletter Distribution

With user consent (typically by subscribing), we send newsletters, emails, and other electronic notifications (hereinafter "newsletters") to users. Our newsletters generally contain technical, commercial, and promotional information about our Services. For the management of newsletter subscribers and the creation and distribution of newsletters, we use the services listed below. To subscribe to the newsletter, it is generally sufficient for users to provide an email address. Subscription is carried out using a so-called double opt-in procedure. After registering, users receive an email requesting confirmation of their subscription via a confirmation link. This confirmation is necessary to prevent unauthorized registrations using third-party email addresses. We log newsletter subscriptions in order to demonstrate compliance with legal requirements. This includes storing the registration

and confirmation time as well as the IP address. Changes to data stored with the mailing service provider are also logged. Users may unsubscribe from the newsletter at any time by clicking the “unsubscribe” button in the footer of each newsletter. If users unsubscribe, their email address may be stored for up to three years based on our legitimate interest in demonstrating previously given consent before deletion. Where external service providers are used for sending emails, this is based on our legitimate interest in an efficient and secure mailing system. Our newsletters may contain so-called web beacons. A web beacon is a pixel-sized file that is retrieved from our server (or the server of a mailing service provider) when the newsletter is opened. In the course of such retrieval, technical information such as browser information, system information, IP address, and time of access is collected. This information is used to technically improve our newsletters based on technical data, target groups, reading behavior, access locations (determined via IP address), and access times. The analysis also includes whether newsletters are opened, when they are opened, and which links are clicked. Although this information may in some cases be associated with individual recipients for technical reasons, neither we nor, where applicable, the service provider aim to monitor individual users. Instead, the evaluations serve to understand reading habits and to tailor content accordingly. The evaluation of newsletters and performance measurement are carried out—subject to explicit user consent—on the basis of our legitimate interest in a user-friendly and secure newsletter system that meets both our business interests and user expectations. The legal basis for sending newsletters and the use of web beacons is consent pursuant to Art. 6(1)(a) GDPR. If users do not provide consent, no newsletters will be sent and web beacons will not be used. Where service providers are used, the legal basis is Art. 6(1)(f) GDPR. Our legitimate interest lies in standardizing and efficiently managing the distribution of newsletters, without disproportionately affecting users’ interests. Where providers transfer data to third countries (e.g., the USA), this is done only on the basis of data processing agreements, Standard Contractual Clauses, and further safeguards permitted under the GDPR, in particular on the basis of the EUUS Data Privacy Framework (DPF).

Provider of the newsletter services used by us

Wix EMail Marketing
Wix.com Ltd
40 Namal Tel Aviv St.
Tel Aviv 6350671
Israel

https://de.wix.com/about/privacy

12. Social Media Profiles

We maintain profiles on social media platforms and process personal data in this context in order to communicate with users active on those platforms or to provide information about us. We inform users that their data may be processed outside the European Union when visiting our profiles. Responsibility for such processing lies with the respective operators of the social networks. Detailed information on the respective forms of processing and the available options to object (e.g. opt-out) can be found in the privacy policies of the respective social network operators. When visiting our social media profiles, user behavior may be analyzed and the resulting information made available to us (“Insights”). This analysis is carried out for the purposes of economic optimization and the needs-based design of our Services. The categories of data processed may include master data, contact data, content data, usage data, and connection data. The recipient of the data is the provider of the respective social media platform acting as joint controller pursuant to Art. 26 GDPR. The legal basis for such processing is our legitimate interest pursuant to Art. 6(1)(f) GDPR. The respective social media platforms are responsible for implementing data subject rights. Information on data subject rights can be found below in connection with the respective platforms on which we maintain profiles. Users may also assert their rights against us, in which case we will forward the request promptly to the respective social media platform operator.

LinkedIn
LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland. Data subject rights: https://de.linkedin.com/legal/privacy-policy.

Google Scholar
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. Data subject rights: https://policies.google.com/privacy?hl=de.

13. Sharing Function in Our Services

Within our Services, users are provided with the option to share generated content directly on their own profiles in various social networks. This sharing function operates in such a way that, by clicking “Share”, the respective social networks receive and process an IP address via corresponding plug-ins. As a result, the social networks become aware that users have previously visited our Services. Some social networks use pixel tags (invisible graphics also referred to as “web beacons”) for statistical or marketing purposes. Through these pixel tags, information such as visitor traffic within our Services may be analyzed. Users may grant or refuse their consent to such processing within the context of the sharing function. Additional information may also be stored in cookies on a device and may contain, among other things, technical information about a browser, operating system, time of access, and further details about the use of our Services, which may be combined with data from other sources. The categories of data processed in this context include master data, contact data, content data, usage data, and connection data. The recipients of the data are the operators of the respective social networks. The legal basis for this processing is our legitimate interest pursuant to Art. 6(1)(f) GDPR. The respective social network operators are responsible for implementing data subject rights. We have integrated “share” links for the following platforms within our Services:

LinkedIn: LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland. LinkedIn is responsible for implementing data subject rights. Information on data subject rights is available at: https://de.linkedin.com/legal/privacy-policy.

Google Scholar: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. Google is responsible for implementing data subject rights. Information on data subject rights is available at: https://policies.google.com/privacy?hl=de.