

Privacy Policy Prianto GmbH

Data protection has a high priority for the management of Prianto GmbH. Therefore, we strictly adhere to the rules of data protection laws and other data protection relevant regulations according to the General Data Protection Regulation (GDPR) as well as applicable country-specific data protection regulations. Hereby we would like to give you, as a visitor of our website, an overview of the measures we have taken to protect personal data and to inform about the nature, scope and purpose of the personal data collected, used and processed by us. Furthermore, data subjects are informed of their rights under this privacy policy.

Prianto GmbH, as controller, has implemented numerous technical and organizational measures to ensure the most complete protection possible for the processed personal data. Nevertheless, in particular Internet-based data transmissions, there might be security gaps so that absolute protection cannot be guaranteed in principle. For this reason, every person concerned is free to submit personal data to us in alternative ways, for example by telephone.

Definitions

The data protection declaration of the Prianto GmbH is based on the terms used by the European legislator for the adoption of the General Data Protection Regulation (GDPR). Our data protection declaration should be legible and understandable for the general public, as well as our customers and business partners. To ensure this, we would like to first explain the terminology used.

In this data protection declaration, we use, inter alia, the following terms:

a) Personal data

Personal data means any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

b) Data subject

Data subject is any identified or identifiable natural person, whose personal data is processed by the controller responsible for the processing.

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

f) Pseudonymisation

Pseudonymisation 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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

g) Controller or controller responsible for the processing

Controller or controller responsible for the processing 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

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

i) Recipient

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; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

j) Third party

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 of the data subject 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.

Name and Address of the controller:

Prianto GmbH
Barthstr. 18
80339 München
E-Mail: kontakt@prianto.com
www.prianto.com
Tel: +49 89 416148 210

The Data Protection Officer of the controller is:

Franz Obermayer
Compliment AG
Edt 4, 84558 Kirchweidach
E-Mail: franz.obermayer@compliment.de
Tel: +49 8623 98739 00

Any data subject may, at any time, contact our Data Protection Officer directly with all questions and suggestions concerning data protection.

Collection of general data and information

The website of the Prianto GmbH collects a series of general data and information when a data subject or automated system calls up the website. This general data and information are stored in the server log files.

- the browser types and versions used
- the operating system used by the accessing system,
- the website from which an accessing system reaches our website (so-called referrers),
- the sub-websites,
- the date and time of access to the Internet site,
- an Internet protocol address (IP address),
- the Internet service provider of the accessing system, and
- any other similar data and information that may be used in the event of attacks on our information technology systems.

When using these general data and information, the Prianto GmbH does not draw any conclusions about the data subject. Rather, this information is needed to

- deliver the content of our website correctly,
- optimize the content of our website as well as its advertisement,
- ensure the long-term viability of our information technology systems and website technology, and
- provide law enforcement authorities with the information necessary for criminal prosecution in case of a cyber-attack.

Therefore, the Prianto GmbH analyses anonymously collected data and information statistically, with the aim of increasing the data protection and data security of our enterprise, and to ensure an optimal level of protection for the personal data we process. The anonymous data of the server log files are stored separately from all personal data provided by a data subject.

In addition, in some cases, visiting our website requires to provide additional personal data (such as name, address, company, position, e-mail address or telephone number). This is the case, for example, if you register for an event / promotion / webinar, request the postal mailing of information material or the submission of a concrete and individual offer or register as a new customer of Prianto GmbH.

By registering, a business relationship comes into existence, according to which, according to the UWG §7, contact via e-mail is permitted.

At events / webinars / promotions, we protect the personal data of the participant and take all necessary measures for its security. The participant data will be collected and used for processing, support and evaluation of the offered events / webinars / promotions and for the purpose of optimizing the offer, but will not be passed on to third parties. Our manufacturer sponsors are also subject to the aforementioned provisions. By registering, the participant / manufacturer representative gives us the specific permission to pass on the corresponding data to the manufacturer sponsors, who use them for follow-up activities of the respective event / webinar / promotion, but are not allowed to pass them on to third parties. By registering, the participant authorizes Prianto to use the photos / videos taken by Prianto for media-independent use and to publish his/her name and company.

You can always update your contact preferences by sending an e-mail to kontakt@prianto.com. Likewise, event participants agree with their registration to publish their name, position and company regarding the respective event. Order processing requires automated data processing. The reseller partner acknowledges and agrees that we may require personal data from its employees to be used or stored in automated data processing and internally by or at Prianto, Prianto subsidiaries or to transfer to suppliers. Such processing, storage and transmission is required to enable us to comply with the obligation to sell products, licenses or services to the reseller partner, as well as for commercial use based on local personal data protection laws. Data may be used in any of the countries in which Prianto and its affiliates do business, including third countries outside the European Union.

We reserve the right, for the purpose of the credit check of the customer to obtain information from credit reporting agencies or credit insurance organizations, regarding the creditworthiness of the customer. We reserve the right to report data in the case of non-contractual settlement e.g. request for payment of a claim in the case of undisputed claim, order of execution issued, enforcement measures. The transfer of data only takes place if this is necessary to safeguard legitimate interests of Prianto and the interests of the customer that are worthy of protection are not impaired. In doing so, Prianto will comply with the relevant data protection regulations. The provision of the data referred to is necessary for the fulfilment of the contract (Art. 13 para. 2 DSGVO). Without this, the contract cannot be concluded or brokered.

Subscription to our newsletters

On the website of Prianto GmbH, users are given the opportunity to subscribe to our enterprise's newsletter. The input mask used for this purpose determines what personal data are transmitted, as well as when the newsletter is ordered from the controller.

Prianto GmbH informs its customers and business partners regularly by means of a newsletter about enterprise offers. The data subject may only receive the enterprise's newsletter if

- the data subject has a valid e-mail address and
- the data subject registers for the newsletter

A confirmation e-mail will be sent to the e-mail address registered by a data subject for the first time for newsletter shipping, for legal reasons, in the double opt-in procedure. This confirmation e-mail is used to prove whether the owner of the e-mail address as the data subject is authorized to receive the newsletter.

During the registration for the newsletter, we also store the IP address of the computer system assigned by the Internet service provider (ISP) and used by the data subject at the time of the registration, as well as the date and time of the registration. The collection of this data is necessary in order to understand the (possible) misuse of the e-mail address of a data subject at a later date, and it therefore serves the aim of the legal protection of the controller.

The personal data collected as part of a registration for the newsletter will only be used to send our newsletter. In addition, subscribers to the newsletter may be informed by e-mail, as long as this is necessary for the operation of the newsletter service or a registration in question, as this could be the case in the event of modifications to the newsletter offer, or in the event of a change in technical circumstances. There will be no transfer of personal data collected by the newsletter service to third parties. The data subject may terminate the subscription to our newsletter at any time. The consent to the storage of personal data, which the data subject has given for shipping the newsletter, may be revoked at any time.

For the purpose of revocation of consent, a corresponding link can be found in each newsletter. It is also possible to unsubscribe from the newsletter at any time directly on the website of the controller, or to communicate this to the controller in a different way.

Newsletter Tracking

The newsletter of Prianto GmbH contains so-called tracking pixels. A tracking pixel is a miniature graphic embedded in such e-mails, which are sent in HTML format to enable log file recording and analysis. This allows a statistical analysis of the success or failure of online marketing campaigns. Based on the embedded tracking pixel, Prianto GmbH may see if and when an e-mail was opened by a data subject, and which links in the e-mail were called up by data subjects.

Such personal data collected in the tracking pixels contained in the newsletters are stored and analyzed by the controller in order to optimize the shipping of the newsletter, as well as to adapt the content of future newsletters even better to the interests of the data subject. These personal data will not be passed on to third parties.

Data subjects are at any time entitled to revoke the respective separate declaration of consent issued by means of the double-opt-in procedure. After a revocation, the controller will delete this personal data. Prianto GmbH automatically regards a withdrawal from the receipt of the newsletter as a revocation.

Contact possibility via the website

The website of Prianto GmbH contains information that enables a quick electronic contact to our enterprise, as well as direct communication with us, which also includes a general address of the so-called electronic mail (e-mail address). If a data subject contacts the controller by e-mail or via a contact form, the personal data transmitted by the data subject are automatically stored. Such personal data transmitted on a voluntary basis by a data subject to the data controller are stored for the purpose of processing or contacting the data subject. There is no transfer of this personal data to third parties.

Comments function in the blog on the website

The Prianto GmbH offers users the possibility to leave individual comments on individual blog contributions on a blog, which is on the website of the controller. A blog is a web based, publicly accessible portal, through which one or more people called bloggers or web bloggers may post articles or write down thoughts in so-called blogposts. Third parties may usually comment blogposts.

If a data subject leaves a comment on the blog published on this website, the comments made by the data subject are also stored and published, as well as information on the date of the commentary and on the user's (pseudonym) chosen by the data subject.

In addition, the IP address assigned by the Internet service provider (ISP) to the data subject is also logged. This storage of the IP address takes place for security reasons, and in case the data subject violates the rights of third parties, or posts illegal content through a given comment. The storage of these personal data is, therefore, in the own interest of the data controller, so that he can exculpate in the event of an infringement. This collected personal data will not be passed to third parties, unless such a transfer is required by law or serves the aim of the defense of the data controller.

Subscription to comments in the blog on the website

Third parties may subscribe to the comments made in the blog of Prianto GmbH. In particular, there is the possibility that a commenter subscribes to the comments following his comments on a particular blog post.

If a data subject decides to subscribe to the option, the controller will send an automatic confirmation e-mail to check the double opt-in procedure as to whether the owner of the specified e-mail address decided in favour of this option. The option to subscribe to comments may be terminated at any time.

Routine erasure and blocking of personal data

We base the protection of your personal data on the three pillars:

1. Full **transparency** of what happens to your data and when and how you handle it
2. **Data economy**, meaning minimization of the amount of required data
3. Strict **purpose limitation** for the use of the data provided by you

In no case will collected data be sold or passed on to third parties, except the latter is required for the performance of the contract or the provision of services. A transmission to authorities or state institutions with information right only takes place, if these are subject to a legal obligation to provide information or judicially. In such cases, the transmission is generally limited to the minimum extent required.

After the purpose of the data retention is abolished (and after expiration of possibly relevant tax and commercial retention periods) all stored personal data is deleted immediately, if at that time no explicit agreement to a further data use exists.

Basically, you can assert your legal rights according to the General Data Protection Regulation (GDPR) free of form and charge:

a) Right of confirmation

Each data subject shall have the right granted by the European legislator to obtain from the controller the confirmation as to whether or not personal data concerning him or her are being processed. If a data subject wishes to avail himself of this right of confirmation, he or she may, at any time, contact our Data Protection Officer or another employee of the controller.

b) Right of access

Each data subject shall have the right granted by the European legislator to obtain from the controller free information about his or her personal data stored at any time and a copy of this information. Furthermore, the European directives and regulations grant the data subject access to the following information:

- the purposes of the processing
- the categories of personal data concerned
- 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 organisations
- 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 the right to lodge a complaint with a supervisory authority
- where the personal data are not collected from the data subject, any available information as to their source
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.

Furthermore, the data subject shall have a right to obtain information as to whether personal data are transferred to a third country or to an international organisation. Where this is the case, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer. If a data subject wishes to avail himself of this right of access, he or she may at any time contact our Data Protection Officer or another employee of the controller.

c) Right to rectification and Right to erasure (Right to be forgotten)

Each data subject shall have the right granted by the European legislator to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. If a data subject wishes to exercise this right to rectification, he or she may, at any time, contact our Data Protection Officer or another employee of the controller.

Each data subject shall have the right granted by the European legislator 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:

- The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- The data subject withdraws consent to which the processing is based according to point (a) of Article 6(1) of the GDPR, or point (a) of Article 9(2) of the GDPR, and where there is no other legal ground for the processing.
- The data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR.
- The personal data have been unlawfully processed.
- The personal data must be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.
- The personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the GDPR.

If one of the aforementioned reasons applies, and a data subject wishes to request the erasure of personal data stored by the Prianto GmbH, he or she may at any time contact our Data Protection Officer or another employee of the controller. The Data Protection Officer of

the Prianto GmbH or another employee shall promptly ensure that the erasure request is complied with immediately.

Where the controller has made personal data public and is obliged pursuant to Article 17(1) to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other controllers processing the personal data that the data subject has requested erasure by such controllers of any links to, or copy or replication of, those personal data, as far as processing is not required. The Data Protection Officer of Prianto GmbH or another employee will arrange the necessary measures in individual cases.

d) Right of restriction of processing

Each data subject shall have the right granted by the European legislator to obtain from the controller restriction of processing where one of the following applies:

- The data subject contests the accuracy of the personal data, 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 instead the restriction of their use instead.
- The controller no longer needs the personal data for the purposes of the processing, but the data subject for the establishment, exercise or defence of legal claims requires them.
- The data subject has objected to processing pursuant to Article 21(1) of the 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 the Prianto GmbH, he or she may at any time contact our Data Protection Officer or another employee of the controller. The Data Protection Officer of the Prianto GmbH or another employee will arrange the restriction of the processing.

e) Right to data portability (Art. 20 DSGVO)

Each data subject shall have the right granted by the European legislator, to receive the personal data concerning him or her, which was provided to a controller, in a structured, commonly used and machine-readable format.

He or she shall have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, as long as the processing is based on consent pursuant to point (a) of Article 6(1) of the GDPR or point (a) of Article 9(2) of the GDPR, or on a contract pursuant to point (b) of Article 6(1) of the GDPR, and the processing is carried out by automated means, as long as the processing is not 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 his or her right to data portability pursuant to Article 20(1) of the GDPR, the data subject shall have the right to have personal data transmitted directly from one controller to another, where technically feasible and when doing so does not adversely affect the rights and freedoms of others.

In order to assert the right to data portability, the data subject may at any time contact the Data Protection Officer designated by the Prianto GmbH or another employee.

f) Right to object

Each data subject shall have the right granted by the European legislator 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.

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

If the Prianto GmbH processes 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 applies to profiling to the extent that it is related to such direct marketing. If the data subject objects to the Prianto GmbH to the processing for direct marketing purposes, the Prianto GmbH 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 the Prianto GmbH 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.

In order to exercise the right to object, the data subject may directly contact the Data Protection Officer of the Prianto GmbH or another employee. In addition, the data subject is free in the context of the use of information society services, and notwithstanding Directive 2002/58/EC, to use his or her right to object by automated means using technical specifications.

g) Automated individual decision-making, including profiling

Each data subject shall have the right granted by the European legislator 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, as long as the decision (1) is not necessary for entering into, or the performance of, a contract between the data subject and a data controller, or (2) is not authorised 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 not 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, the Prianto GmbH 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 the data subject wishes to exercise the rights concerning automated individual decision-making, he or she may at any time directly contact our Data Protection Officer of the Prianto GmbH or another employee of the controller.

h) Right to withdraw data protection consent

Each data subject shall have the right granted by the European legislator to withdraw his or her consent to processing of his or her personal data at any time.

If the data subject wishes to exercise the right to withdraw the consent, he or she may at any time directly contact our Data Protection Officer of the Prianto GmbH or another employee of the controller.

- The right of opposition with effect for the future
- The right to complain to a supervisory authority (Article 77 GDPR)

You may revoke your consent to data collection, storage and use at any time without giving reasons. Please direct your inquiries or your general suggestions or complaints regarding data protection to the following contact options:

Prianto GmbH
Barthstr. 18
80339 Munich
E-mail: kontakt@prianto.com
www.prianto.com
Tel: +49 89 416148 210

Data protection at Prianto GmbH is achieved, among other things, through training, active communication and the written obligation to keep data confidential and to comply with the data protection requirements of all employees and external service providers.

All technical and organizational, physical and logical facilities and measures in the area of data protection, IT and information security serve to protect against damage, destruction and unauthorized access to stored data and to achieve the confidentiality, availability and integrity protection goals.

Changes to the privacy policy

We reserve the right to modify our privacy practices and this policy to adapt it to changes in relevant laws or regulations, or to better serve your needs. Possible changes to our privacy practices will be announced accordingly. Please note the current version number of the privacy policy.

More information:

Persons under 18 years

Persons under the age of 18 should not submit any personal data to us without the consent of their parents or guardians. We do not require any personal data from children and adolescents do not collect them and do not pass them on to third parties.

Cookies

If you visit one of our websites, we may store information in the form of a cookie on your computer. Cookies are small text files sent from a web server to your browser and stored on your computer's hard drive. Besides the internet protocol address no personal data of the user are stored. This information is intended to automatically recognize you on your next visit to our websites and to make navigation easier for you. Cookies allow us, for example, to customize a website according to your interests or to store your password so that you do not have to re-enter it every time.

External links

If you use external links that are offered within the framework of our Internet pages, this Privacy Policy does not extend to these links. Insofar as we offer links, we affirm that at the time of the link setting no violations of the applicable law on the linked websites were identified. However, we have no influence on the compliance of other providers with privacy and security regulations. Therefore, please inform yourself on the websites of the other providers also about the privacy statements provided there.

In-house tools and systems

The data collected through the website or other collaborations are recorded during in-house storage and retention in in-house tools and systems. The third-party tools we use have contracted in advance to secure the data in accordance with the requirements of the GDPR. Even specially programmed systems meet this safety standard without exception.

Privacy policy for the use and application of Matomo

We utilize Matomo, an open-source analytics platform. Unlike other analytics services, our implementation of Matomo is self-hosted, which means all analytics data is stored on our own servers and not shared with any third-party providers.

When you visit our website, Matomo collects information about your interactions, such as pages visited, duration of visit, and the actions taken on the site. It may also collect anonymized IP addresses, browser information, and device type to help us understand how our website is used and how we can improve user experience. Importantly, since we self-host Matomo, this data is processed and stored securely on our servers and is subject to our stringent data protection and privacy standards.

Matomo creates usage profiles based on pseudonyms. For this purpose, permanent cookies are stored on your terminal device and read by us. In this way, we are able to recognize and count returning visitors. We also use the heatmap & session recording modules. Matomo's heatmap service shows us the areas of our website where the mouse is most frequently moved or clicked. The session recording service records individual user sessions. We can replay recorded sessions and thus analyze the use of our website. Data entered in forms is not recorded and is not visible at any time.

The data processing is based on your consent in accordance with § 25 para. 1 TTDSG, Art. 6 para. 1 lit. a DSGVO, provided that you have given your consent via our banner. You have the right to opt-out of being tracked by our Matomo analytics. To exercise this right, you can disable cookies in your browser settings at any time or make the appropriate settings via our banner.

The operating company behind Matomo is InnoCraft Ltd., 7 Waterloo Quay PO625, 6140 Wellington, New Zealand. For more information on Matomo's terms of use and data protection regulations, please visit: <https://matomo.org/privacy/>

Privacy Policy for the use and application of Mautic

To provide a seamless and efficient registration process for our events and to deliver personalized communication, we utilize Mautic, an open-source marketing automation platform. This platform enables us to manage event registrations, send emails, and track interactions to ensure that we meet the needs and interests of our participants.

By registering for our events through our website, you will be asked to provide personal information such as your name, email address, Company Information, and preferences regarding the event. This information is collected and processed through Mautic, enabling us to manage your registration, communicate important event information, and offer personalized content based on your interests.

Our Mautic implementation may use cookies to enhance the registration process and to understand how users interact with our website and emails. These cookies help us improve our website's functionality and your overall experience.

The information collected through Mautic is stored securely on our servers. As a self-hosted solution, we have full control over this data, and it is not shared with any third-party providers. We implement robust security measures to protect your information from unauthorized access, disclosure, alteration, or destruction.

If you prefer not to have your activity tracked by our Mautic platform, you can opt-out by adjusting your browser settings to refuse cookies, by contacting us directly to express your preferences or make the appropriate settings via our banner.

For more information about Mautic and its commitment to privacy, please visit Mautic's Privacy Policy under <https://www.mautic.org/privacy-policy>.

Privacy Policy for the use and application of CRM Systems – SuiteCRM, Pipedrive and Zoho CRM

As part of our commitment to providing you with personalized and efficient service, our website utilizes Mautic, an open-source marketing automation platform, which is integrated with our Customer Relationship Management (CRM) systems. This integration allows us to manage and analyze customer interactions and data throughout the customer lifecycle, enhancing our customer service and improving our marketing efforts.

When you interact with our website or participate in our events, the personal information you provide, including but not limited to your name, email address, and interaction history, may be processed by Mautic and subsequently shared with our CRM systems.

This integration facilitates a seamless flow of your information between our marketing platform and CRM systems, enabling us to tailor our communications and offers more effectively to your needs and preferences.

Use of Pipedrive

To ensure efficient management of customer relationships and to provide tailored services and communications, we utilize Pipedrive, a leading Customer Relationship Management (CRM) platform. This section of our Privacy Policy outlines how we collect, use, and protect data within Pipedrive.

Through interactions with our website, contact forms, and event registrations, we collect information such as names, email addresses, telephone numbers, and any other data you provide. This information is directly entered into our Pipedrive CRM to facilitate customer management, sales tracking, and personalized communication based on your interests and needs.

The primary purpose of using Pipedrive is to streamline our sales processes, enhance customer service, and ensure that we can respond effectively to your inquiries and requests.

Data Sharing and Security:

- The data stored in Pipedrive is for internal use only and is accessed by authorized personnel who are committed to upholding your privacy and security.
- We have implemented appropriate technical and organizational measures to protect your data from unauthorized access, disclosure, alteration, or destruction. Pipedrive employs robust security protocols to safeguard data stored on its platform.

You have the right to access the personal information we hold about you in Pipedrive, to request corrections, or to have your data deleted. If you wish to exercise these rights, please contact us at kontakt@prianto.com.

The operating company behind Pipedrive is Pipedrive OÜ, Mustamäe tee 3a, 10615 Tallinn, Estonia.

As Pipedrive is a third-party service, we advise reviewing Pipedrive's Privacy Policy for comprehensive details on their data protection and privacy practices under <https://www.pipedrive.com/en/privacy>.

Use of Zoho CRM

We gather personal information including names, email addresses, phone numbers, and other details through interactions on our website, contact forms, and service sign-ups. This data is partly stored in Zoho CRM to enhance customer management, personalize our services, and ensure communications are tailored to your needs and preferences.

Our integration of Zoho CRM aims to elevate our service standards by effectively organizing customer data, streamlining communication, and empowering our team with advanced tools for superior service.

Data Sharing and Security:

- Data stored in Zoho CRM is exclusively for internal use, accessible only to authorized staff trained in data protection, ensuring your privacy.
- We commit to rigorous security measures to prevent unauthorized data access, including continuous software updates, encrypted data storage, and restricted data access protocols. Zoho employs robust security protocols to safeguard data stored on its platform.

You have the right to access the personal information we hold about you in Zoho CRM, to request corrections, or to have your data deleted. If you wish to exercise these rights, please contact us at kontakt@prianto.com.

As Zoho CRM is a third-party service, we advise reviewing Zoho's Privacy Policy for comprehensive details on their data protection and privacy practices under <https://www.zoho.com/en-uk/privacy.html>.

Use of SuiteCRM

In our commitment to maintaining strong and transparent customer relationships, we utilize SuiteCRM, an open-source Customer Relationship Management (CRM) platform. This portion of our Privacy Policy elaborates on our practices regarding data collection, usage, and protection within SuiteCRM.

We collect personal information such as names, email addresses, telephone numbers, and any other information you provide through our website interactions, contact forms, and

service registrations. This information is entered into SuiteCRM to facilitate efficient customer management, service customization, and to ensure responsive communication tailored to your preferences and requirements.

The goal of integrating SuiteCRM into our operations is to improve our service delivery by organizing customer information effectively, automating communication processes, and providing our team with the tools needed to offer exceptional service.

Data Sharing and Security:

- Data input into SuiteCRM is strictly for internal use and accessed only by authorized personnel who are trained in data protection and committed to safeguarding your privacy.
- Despite SuiteCRM being an open-source platform that we host and manage, we adhere to stringent security measures to prevent unauthorized access, disclosure, or misuse of your personal data. Our security protocols include regular software updates, secure data encryption, and restricted data access.

Use of Personal Data for Event Logistics

In addition to the uses described above, we may also utilize the personal information you provide to facilitate event logistics, such as hotel bookings and transportation arrangements for events you have registered for through our website. This section details how we handle your data for these purposes.

Purpose and Sharing:

- To ensure your participation in our events is seamless and enjoyable, we may need to share relevant personal data (e.g., name, contact details, and booking preferences) with third-party service providers, such as hotels, transport companies, and event venues.
- The sharing of this information is strictly limited to what is necessary to complete the bookings and arrangements on your behalf. We select service providers who demonstrate compliance with data protection laws and commit to respecting the confidentiality of your information.
- You will have the option to manage your preferences and opt-out of these services if you wish to make your arrangements independently. In such cases, please contact us at kontakt@prianto.com.

Privacy Policy for the use and application of Mailchimp

We use Mailchimp, a marketing platform operated by Intuit Inc., with its mailing address at 2700 Coast Ave., Mountain View, CA 94043, United States, as our service provider for email marketing campaigns.

When you subscribe to our newsletter, we collect personal information that you voluntarily provide to us. This typically includes your email address and your name, and gender to tailor our communications to suit your needs better.

By subscribing, you acknowledge and consent that the information you provide will be transferred to Mailchimp for processing in accordance with their privacy practices and terms. Mailchimp employs various security measures to protect your data, ensuring its confidentiality and integrity.

You have the right to access, correct, or delete your personal information at any time. Should you wish to exercise these rights, or if you decide to unsubscribe from our newsletter, you can do so by clicking the 'unsubscribe' link available in the footer of every email we send through Mailchimp, or by contacting us directly.

Please be aware that our newsletters may use Mailchimp's tracking technologies to monitor engagement and effectiveness, such as open rates and click-through rates of our emails. This helps us to continuously improve our offerings and ensure the content is relevant to you.

Your data may be stored and processed in countries different from your country of residence, including the United States where Mailchimp's servers are located. We and Mailchimp are committed to safeguarding your privacy and ensuring your personal data is protected, regardless of where it is processed.

We reserve the right to update our privacy policy to reflect changes in our practices or service providers' policies. Rest assured, any significant changes will be communicated to you through our website or via a direct notification.

For more detailed information on Mailchimp's privacy practices, please visit Mailchimp's Privacy Policy <https://www.intuit.com/privacy/statement/>.

Data protection provisions about the application and use of Facebook

On this website, the controller has integrated components of the enterprise Facebook. Facebook is a social network.

A social network is a place for social meetings on the Internet, an online community, which usually allows users to communicate with each other and interact in a virtual space. A social network may serve as a platform for the exchange of opinions and experiences, or enable the Internet community to provide personal or business-related information. Facebook allows social network users to include the creation of private profiles, upload photos, and network through friend requests.

The operating company of Facebook is Meta Platforms, Inc. 1 Hacker Way Menlo Park California 94025. If a person lives outside of the United States or Canada, the controller is the Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland.

The plugins are marked with a Facebook logo or the addition "Facebook Social Plugin".

With each call-up to one of the individual pages of this Internet website, which is operated by the controller and into which a Facebook component (Facebook plug-ins) was integrated,

the web browser on the information technology system of the data subject is automatically prompted to download display of the corresponding Facebook component from Facebook through the Facebook component. An overview of all the Facebook Plug-ins may be accessed under <https://developers.facebook.com/docs/plugins/>. During the course of this technical procedure, Facebook is made aware of what specific sub-site of our website was visited by the data subject.

If the data subject is logged in at the same time on Facebook, Facebook detects with every call-up to our website by the data subject—and for the entire duration of their stay on our Internet site—which specific sub-site of our Internet page was visited by the data subject. This information is collected through the Facebook component and associated with the respective Facebook account of the data subject. If the data subject clicks on one of the Facebook buttons integrated into our website, e.g. the "Like" button, or if the data subject submits a comment, then Facebook matches this information with the personal Facebook user account of the data subject and stores the personal data.

Facebook always receives, through the Facebook component, information about a visit to our website by the data subject, whenever the data subject is logged in at the same time on Facebook during the time of the call-up to our website. This occurs regardless of whether the data subject clicks on the Facebook component or not. If such a transmission of information to Facebook is not desirable for the data subject, then he or she may prevent this by logging off from their Facebook account before a call-up to our website is made.

The data protection guideline published by Facebook, which is available at <https://facebook.com/about/privacy/>, provides information about the collection, processing and use of personal data by Facebook. In addition, it is explained there what setting options Facebook offers to protect the privacy of the data subject. In addition, different configuration options are made available to allow the elimination of data transmission to Facebook. These applications may be used by the data subject to eliminate a data transmission to Facebook.

If you do not want Facebook to collect data about you via our website, you must log out of Facebook before visiting our website.

Data protection provisions about the application and use of Google-Ads

On this website, the controller has integrated Google Ads. Google Ads is a service for Internet advertising that allows the advertiser to place ads in Google search engine results and the Google advertising network. Google Ads allows an advertiser to predefine specific keywords with the help of which an ad on Google's search results only then displayed, when the user utilizes the search engine to retrieve a keyword-relevant search result. In the Google Advertising Network, the ads are distributed on relevant web pages using an automatic algorithm, taking into account the previously defined keywords.

The operating company of Google Ads is Google LLC., 1600 Amphitheatre Pkwy, Mountain View, CA 94043-1351, United States.

The purpose of Google Ads is the promotion of our website by the inclusion of relevant advertising on the websites of third parties and in the search engine results of the search engine Google and an insertion of third-party advertising on our website.

If a data subject reaches our website via a Google ad, a conversion cookie is filed on the information technology system of the data subject through Google. The definition of cookies is explained above. A conversion cookie loses its validity after 30 days and is not used to identify the data subject. If the cookie has not expired, the conversion cookie is used to check whether certain sub-pages, e. g, the shopping cart from an online shop system, were called up on our website. Through the conversion cookie, both Google and the controller can understand whether a person who reached an Ads ad on our website-generated sales, that is, executed or cancelled a sale of goods.

The data and information collected through the use of the conversion cookie is used by Google to create visit statistics for our website. These visit statistics are used in order to determine the total number of users who have been served through ads to ascertain the success or failure of each ad and to optimize our ad in the future. Neither our company nor other Google Ads advertisers receive information from Google that could identify the data subject.

The conversion cookie stores personal information, e.g. the Internet pages visited by the data subject. Each time we visit our Internet pages, personal data, including the IP address of the Internet access used by the data subject, is transmitted to Google in the United States of America. Google in the United States of America stores these personal data. Google may pass these personal data collected through the technical procedure to third parties.

The data subject may, at any time, prevent the setting of cookies by our website, as stated above, by means of a corresponding setting of the Internet browser used and thus permanently deny the setting of cookies. Such a setting of the Internet browser used would also prevent Google from placing a conversion cookie on the information technology system of the data subject. In addition, a cookie set by Google Ads may be deleted at any time via the Internet browser or other software programs.

The data subject has a possibility of objecting to the interest-based advertisement of Google. Therefore, the data subject must access from each of the browsers in use the link www.google.de/settings/ads and set the desired settings.

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

Data protection provisions about the application and use of LinkedIn

The controller has integrated components of the LinkedIn Corporation on this website. LinkedIn is a web-based social network that enables users with existing business contacts to connect and to make new business contacts. Over 400 million registered people in more than

200 countries use LinkedIn. Thus, LinkedIn is currently the largest platform for business contacts and one of the most visited websites in the world.

The operating company of LinkedIn is LinkedIn Corporation, 1000 W. Maude Avenue, Sunnyvale, CA 94085 United States. For privacy matters outside of the UNITED STATES LinkedIn Ireland, Privacy Policy Issues, Wilton Plaza, Wilton Place, Dublin 2, Ireland, is responsible.

With each call-up to one of the individual pages of this Internet site, which is operated by the controller and on which a LinkedIn component (LinkedIn plug-in) was integrated, the Internet browser on the information technology system of the data subject is automatically prompted to the download of a display of the corresponding LinkedIn component of LinkedIn. Further information about the LinkedIn plug-in may be accessed under <https://developer.linkedin.com/plugins>. During the course of this technical procedure, LinkedIn gains knowledge of what specific sub-page of our website was visited by the data subject.

If the data subject is logged in at the same time on LinkedIn, LinkedIn detects with every call-up to our website by the data subject—and for the entire duration of their stay on our Internet site—which specific sub-page of our Internet page was visited by the data subject.

This information is collected through the LinkedIn component and associated with the respective LinkedIn account of the data subject. If the data subject clicks on one of the LinkedIn buttons integrated on our website, then LinkedIn assigns this information to the personal LinkedIn user account of the data subject and stores the personal data.

LinkedIn receives information via the LinkedIn component that the data subject has visited our website, provided that the data subject is logged in at LinkedIn at the time of the call-up to our website. This occurs regardless of whether the person clicks on the LinkedIn button or not. If such a transmission of information to LinkedIn is not desirable for the data subject, then he or she may prevent this by logging off from their LinkedIn account before a call-up to our website is made.

LinkedIn provides under <https://www.linkedin.com/psettings/guest-controls> the possibility to unsubscribe from e-mail messages, SMS messages and targeted ads, as well as the ability to manage ad settings. LinkedIn also uses affiliates such as Eire, Google Analytics, BlueKai, DoubleClick, Nielsen, Comscore, Eloqua, and Lotame. The setting of such cookies may be denied under <https://www.linkedin.com/legal/cookie-policy>. The applicable privacy policy for LinkedIn is available under <https://www.linkedin.com/legal/privacy-policy>. The LinkedIn Cookie Policy is available under <https://www.linkedin.com/legal/cookie-policy>.

Data protection provisions about the application and use of Twitter / X

For the purposes of this Privacy Policy, references to 'Twitter' shall encompass the services provided by the social media platform, which, as of April 2023, operates under X following its acquisition. This terminology is used to maintain clarity and recognizability for our users.

On this website, the controller has integrated components of Twitter. Twitter is a

multilingual, publicly accessible microblogging service on which users may publish and spread so-called 'tweets,' e.g. short messages, which are limited to 140 characters. These short messages are available for everyone, including those who are not logged on to Twitter. The tweets are also displayed to so-called followers of the respective user. Followers are other Twitter users who follow a user's tweets. Furthermore, Twitter allows you to address a wide audience via hashtags, links or retweets.

The operating company of Twitter is X Corp, 1355 Market Street, Suite 900, San Francisco, CA 94103, United States. For privacy matters outside of the United States Twitter International Unlimited Company, One Cumberland Place, Fenian Street Dublin 2, D02 AX07 IRLAND is responsible.

With each call-up to one of the individual pages of this Internet site, which is operated by the controller and on which a Twitter component (Twitter button) was integrated, the Internet browser on the information technology system of the data subject is automatically prompted to download a display of the corresponding Twitter component of Twitter. Further information about the Twitter buttons is available under <https://about.twitter.com/de/resources/buttons>. During the course of this technical procedure, Twitter gains knowledge of what specific sub-page of our website was visited by the data subject. The purpose of the integration of the Twitter component is a retransmission of the contents of this website to allow our users to introduce this web page to the digital world and increase our visitor numbers.

If the data subject is logged in at the same time on Twitter, Twitter detects with every call-up to our website by the data subject and for the entire duration of their stay on our Internet site, which specific sub-page of our Internet page was visited by the data subject. This information is collected through the Twitter component and associated with the respective Twitter account of the data subject. If the data subject clicks on one of the Twitter buttons integrated on our website, then Twitter assigns this information to the personal Twitter user account of the data subject and stores the personal data.

Twitter receives information via the Twitter component that the data subject has visited our website, provided that the data subject is logged in on Twitter at the time of the call-up to our website. This occurs regardless of whether the person clicks on the Twitter component or not. If such a transmission of information to Twitter is not desirable for the data subject, then he or she may prevent this by logging off from their Twitter account before a call-up to our website is made.

The applicable data protection provisions of Twitter may be accessed under <https://twitter.com/privacy?lang=en>.

Data protection provisions about the application and use of Xing

On this website, the controller has integrated components of XING. XING is an Internet based social network that enables users to connect with existing business contacts and to create

new business contacts. The individual users can create a personal profile of themselves at XING. Companies may, e.g. create company profiles or publish jobs on XING.

The operating company of XING is New Work SE, Am Strandkai 1, 20457 Hamburg, Germany.

With each call-up to one of the individual pages of this Internet site, which is operated by the controller and on which a XING component (XING plug-in) was integrated, the Internet browser on the information technology system of the data subject is automatically prompted to download a display of the corresponding XING component of XING. Further information about the XING plug-in may be accessed under <https://dev.xing.com/plugins>. During the course of this technical procedure, XING gains knowledge of what specific sub-page of our website was visited by the data subject.

If the data subject is logged in at the same time on XING, XING detects with every call-up to our website by the data subject—and for the entire duration of their stay on our Internet site—which specific sub-page of our Internet page was visited by the data subject. This information is collected through the XING component and associated with the respective XING account of the data subject. If the data subject clicks on the XING button integrated on our Internet site, e.g. the "Share"-button, then XING assigns this information to the personal XING user account of the data subject and stores the personal data.

XING receives information via the XING component that the data subject has visited our website, provided that the data subject is logged in at XING at the time of the call to our website. This occurs regardless of whether the person clicks on the XING component or not. If such a transmission of information to XING is not desirable for the data subject, then he or she can prevent this by logging off from their XING account before a call-up to our website is made.

The data protection provisions published by XING, which is available under <https://www.xing.com/privacy>, provide information on the collection, processing and use of personal data by XING. In addition, XING has published privacy notices for the XING share button under https://dev.xing.com/plugins/share_button/privacy_policy

Data protection provisions about the application and use of You Tube

On this website, the controller has integrated components of You Tube. YouTube is an Internet video portal that enables video publishers to set video clips and other users free of charge, which also provides free viewing, review and commenting on them. You Tube allows you to publish all kinds of videos, so you can access both full movies and TV broadcasts, as well as music videos, trailers, and videos made by users via the Internet portal.

The operating company of You Tube is You Tube, LLC, 901 Cherry Ave., San Bruno, CA 94066, United States. The You Tube, LLC is a subsidiary of Google LLC., 1600 Amphitheatre Pkwy, Mountain View, CA 94043-1351, United States.

With each call-up to one of the individual pages of this Internet site, which is operated by the controller and on which a YouTube component (You Tube video) was integrated, the Internet

browser on the information technology system of the data subject is automatically prompted to download a display of the corresponding YouTube component. Further information about YouTube may be obtained under <https://www.youtube.com/yt/about/en/>. During the course of this technical procedure, YouTube and Google gain knowledge of what specific sub-page of our website was visited by the data subject.

If the data subject is logged in on YouTube, YouTube recognizes with each call-up to a subpage that contains a YouTube video, which specific sub-page of our Internet site was visited by the data subject. This information is collected by YouTube and Google and assigned to the respective YouTube account of the data subject.

YouTube and Google will receive information through the YouTube component that the data subject has visited our website, if the data subject at the time of the call to our website is logged in on YouTube; this occurs regardless of whether the person clicks on a YouTube video or not. If such a transmission of this information to YouTube and Google is not desirable for the data subject, the delivery may be prevented if the data subject logs off from their own YouTube account before a call-up to our website is made.

YouTube's data protection provisions, available at <https://www.google.com/intl/en/policies/privacy/>, provide information about the collection, processing and use of personal data by YouTube and Google. (Version 1.0)

Legal basis for the processing

Art. 6(1) lit. 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, the processing is based on Article 6(1) lit. b GDPR. The same applies to such processing operations, which are necessary for carrying out pre-contractual measures, for example in the case of inquiries concerning our products or services. Is our company subject to a legal obligation by which processing of personal data is required, such as for the fulfilment of tax obligations, the processing is based on Art. 6(1) lit. c GDPR. In rare cases, the processing of personal data may be necessary to protect the vital interests of the data subject or of another natural person. This would be the case, for example, if a visitor were injured in our company and his name, age, health insurance data or other vital information would have to be passed on to a doctor, hospital or other third party. Then the processing would be based on Art. 6(1) lit. d GDPR. Finally, processing operations could be based on Article 6(1) lit. 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 company 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. Such processing operations are particularly permissible because the European legislator has specifically mentioned them. He considered that a legitimate interest could be assumed if the data subject is a client of the controller (Recital 47 Sentence 2 GDPR).

The legitimate interests pursued by the controller or by a third party

Where the processing of personal data is based on Article 6(1) lit. f GDPR our legitimate interest is to carry out our business in favour of the well-being of all our employees and the shareholders.

Period for which the personal data will be stored

The criteria used to determine the period of storage of personal data is the respective statutory retention period. After expiration of that period, the corresponding data is routinely deleted, as long as it is no longer necessary for the fulfilment of the contract or the initiation of a contract.

Provision of personal data as statutory or contractual requirement; Requirement necessary to enter into a contract; Obligation of the data subject to provide the personal data; possible consequences of failure to provide such data

We clarify that the provision of personal data is partly required by law (e.g. tax regulations) or can also result from contractual provisions (e.g. information on the contractual partner). Sometimes it may be necessary to conclude a contract that the data subject provides us with personal data, which must subsequently be processed by us. The data subject is, for example, obliged to provide us with personal data when our company signs a contract with him or her. The non-provision of the personal data would have the consequence that the contract with the data subject could not be concluded. Before personal data is provided by the data subject, the data subject must contact our Data Protection Officer. Our Data Protection Officer clarifies to the data subject 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 the consequences of non-provision of the personal data.

Existence of automated decision-making

As a responsible company, we do not use automatic decision-making or profiling.