

ULTIMAMEDIA

PART OF  Süddeutscher Verlag

Privacy policy

05.02.2025

If you use the offers of Ultima Media Germany GmbH your personal data will be processed. With this privacy policy we would like to inform you how and why we process your data and how we ensure that it remains confidential and protected.

We take data protection seriously: as a matter of principle, we only process personal data if this is necessary for the provision of a service or offer or if it is provided voluntarily by the user. We also use technical and operational security measures to protect personal data against accidental or intentional manipulation, loss, destruction or access by unauthorized persons. We regularly review and modernize these precautions.

Data protection information for applications

If you have applied to us, you will find the necessary data protection information [here](#).

Data protection at a glance

What data do we collect from you?

- Inventory data (e.g. names, addresses)
- Contact data (e.g. email, phone numbers)
- Content data (e.g. entries in online forms)
- Payment data (e.g. bank details, invoices, payment history)
- Contract data (e.g. subject matter of contract, term)
- Utilization data (e.g. web pages visited, interest in content, access times)
- Meta/communication data (e.g. device information, IP addresses)

How do we collect your data?

We automatically collect the data that is generated when you access our digital offerings. Otherwise, we collect data on the basis of your input or communications or through the use of cookies or similar technologies.

What do we use your data for?

Providing digital offerings:

- Cookies and similiar technologies
- technical provision ans security
- Essential technology
- Push notifications
- Embeds (video, audio, map services, Twitter, Instagram, etc.)

Product optimization:

- Further development of user-friendliness
- usage analysis
- Surveys

Events:

- Order tickets for events
- Online events

Communication:

- Contact by e-mail, contact form, phone or letter

Promotion & Marketing:

- Direct marketing
- Newsletter
- Self-advertisement
- Personalized product recommendations
- Company presences in the social media

Do we share your data?

If you have consented or if we are otherwise legally authorized to do so, we will share your personal data with service providers (e.g. hosting, marketing, sales partners) for the above purposes. In such cases, we strictly comply with the legal requirements and, in particular, conclude appropriate contracts or agreements that serve to protect your data with the recipients of your data.

We may transfer personal data to other companies within our group of companies or grant them access to this data. Insofar as this transfer is for administrative purposes, the transfer of data is based on our legitimate corporate and business interests or is conducted insofar as it is necessary for the fulfillment of our contract-related obligations or if the consent of the data subjects or a legal permission exists.

Do we transfer data to third countries?

In order to use our digital offerings, it may be necessary to transfer certain personal data to third countries, i.e. countries in which the GDPR is not applicable law. However, we only permit processing of your data in a third country if the special requirements of Art. 44 GDPR and consequently the guarantee of an adequate level of data protection in the country are met. This means that the third country must either have an adequacy decision from the European Commission or appropriate safeguards pursuant to Art. 46 GDPR or one of the requirements of Art. 49 GDPR. **Unless otherwise stated below, we use as appropriate guarantees the applicable Standard Contractual Clauses for the transfer of personal data to processors in third countries.**

How do we protect your data?

In order to protect your privacy and to ensure a level of protection appropriate to the risk, we take technical and organizational measures. We take these measures in accordance with the legal requirements, considering the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing, as well as the different probabilities of occurrence and the extent of the threat to the rights and freedom of natural persons, which are reviewed and adapted on a regular basis. The measures ensure the confidentiality, integrity, availability and resilience of your data. This includes, among other things, the use of recognized encryption methods (SSL or TLS) and pseudonymization.

However, we would like to point out that due to the structure of the Internet, it is possible that the rules of data protection and the above-mentioned security measures are not observed by other persons or institutions not within our sphere of responsibility. In particular, data disclosed unencrypted - e.g., if this is done by e-mail - can be read by third parties. We have no technical influence on this.

When do we delete your data?

We delete or anonymize your personal data as soon as it is no longer required for the purposes for which we collected or used it.

However, if necessary, we must continue to store your data until the expiry of the retention obligations and periods issued by the legislator or supervisory authorities, which may result from the German Commercial Code, the German Fiscal Code and the German Money Laundering Act (usually 6 to 10 years). In addition, we may retain your data until the expiry of the statutory limitation periods (i.e. usually 3 years; in individual cases, however, up to 30 years), insofar as this is necessary for the assertion, exercise or defense of legal claims. After that, the corresponding data will be deleted.

What are your rights?

- Information
- Deletion
- Correction
- Objection

You can contact the data protection officer with your request by mail or e-mail, swmh-datenschutz@atarax.de, with your request.

This privacy notice will be adjusted from time to time. The date of the last update can be found at the beginning of this information.

Privacy settings

You can obtain an overview of all the tools and cookies we use as well as a withdrawal option by clicking on Privacy Settings in the footer of the respective website.

In the following, you will receive data protection information in detailed form.

Providing the content

Cookies and similar technology

We use cookies and similar technologies to provide you with the best experience when using our digital offerings and to help fund us. We use them i.a. für ensuring functionality, for IT security and fraud prevention, usage analysis in order to be able to optimize the products and for marketing and advertising.

For an overview of the technologies used and withdrawal or objection options, click on Privacy Settings in the footer of the website you are visiting.

If cookies, device identifiers or other personal data are stored or accessed on your terminal for processing operations, this is in accordance with the legal basis stated in Art. 6 of the General Data Protection Regulation.

In order to be able to provide the telemedia service you expressly requested, we also take into account the regulations in Section 25 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) and, in particular, on absolute necessity in accordance with Section 25 (2) No. 2 TDDDG.

Technical deployment and security

When you use our offerings, we automatically use absolutely necessary technologies to enable the usability of the functions provided and to ensure the security and stability of our offer:

- Information about the accessing terminal device and the software used
- Date and time of access

- Websites from which you access our website or which you access via our website
- IP address

The processing of the IP address is absolutely necessary to enable the delivery of our offerings to your end device and to measure the efficiency and performance of our offerings. Usage profiles are not created in the process. Our servers store your IP address for up to seven days for the purpose and interest of being able to guarantee the security of our offer. The other data is deleted after 30 days.

The legal basis for the data processing operations is our legitimate interest.

Essential technology

We cannot do without certain cookies and similar technologies, as they are indispensable for our telemedia service and business model - as requested by the user. In addition to data, we need to provide and ensure functionality and security. The following tools and cookies are essential technologies.

The legal basis for the data processing operations is our legitimate interest.

Paid content model

We have introduced a registration model for our online content, i.e. the content of our websites and apps is only made available against registration. Our paid content model stipulates that initially selected content or a certain number of articles can be accessed without having to take out a subscription (metering model) and then the content is restricted and only made available against the provision of data. In addition, access to individual, exclusive “Plus” articles is only granted to subscribers.

The setting of cookies is absolutely necessary for this function, as otherwise it would not be possible for readers to access all journalistic content.

If you have registered with us via Login, these reading authorizations will be associated with the personal data in your user account.

Piano Composer

Name	Purpose	Duration	Type
xbc	Controlling the paid content model	2 years	Cookie
_tbc	Identification of the user's browser; contains encrypted browserId, userId, isNew-Flag	2 years	Cookie
_tac	Access token containing an encrypted payload with current permissions; updated when a user's access status changes (login, conversion, expired access permissions, cookie deletion)	90 days	Cookie
_tae	Expiration timestamp for _tac; indicates when the _tac cookie was last updated.	2 years	Cookie

Name	Purpose	Duration	Type
_tp-customVariables	During a payment: redirection to and from a 3D-Secure bank page	2 days	local storage
_tp-customVariables-expiration	During a payment: redirection to and from a 3D-Secure bank page	2 days	local storage

Google Tag Manager

The Google Tag Manager service is an organizational tool and allows us to control services. The tool only uses the IP address to connect to the server and to function technically. Otherwise, no personal data is processed by way of the tool itself. The Tag Manager ensures that other services are only executed if the conditions (tags) set in the Tag Manager are met for them. In this way, we ensure that, for example, tools that require consent are only loaded after you have given your consent. The Tag Manager does not access the data processed by the tools.

Datawrapper

We use Datawrapper (Datawrapper GmbH, Raumerstraße 39, 10437 Berlin) to create interactive charts from statistics. We do not store any personal data and do not perform any tracking. For embedding and display absolutely necessary are the transmission of the IP address, which is used only for the provision of the service, and a cookie. This data is only required for the technical implementation of the embedding and is deleted from all systems after a maximum of 24 hours.

Google reCaptcha

We use Google reCaptcha to determine whether a person or computer is making a certain entry in our contact or newsletter form. Google (Google LLC, 1600 Amphitheatre Parkway Mountain View, CA 94043. USA) uses the following data to determine whether you are a human or a computer: IP address of the terminal device used, the website you visit with us and on which the captcha is integrated, the date and duration of the visit, the identification data of the type of browser and operating system used, the Google account if you are logged in at Google and mouse movements on the reCaptcha areas. Based on this data, reCaptcha analyzes your actions on the website and evaluates them with a score between 0 and 1. The lower this value is, the more likely reCaptcha considers the respective user to be a bot.

Legal basis for the described data processing is our legitimate interest. We use reCaptcha solely for the purpose of ensuring the security of our websites, to protect us from automated input (such as bot attacks) and to ensure an exclusively private, non-commercial use by human users.

You can find the opt-out for this under [this link](#).

You can find Google's privacy policy [here](#).

Mouseflow

We use Mouseflow, a web analytics tool from Mouseflow ApS, Flaesketoerret 68, 1711 Copenhagen, Denmark, to record randomly selected individual visits (with anonymized IP address only). The data processing is for the purpose of analyzing this website and its visitors. This creates a log of mouse movements and clicks with the intention of randomly replaying individual website visits and deriving potential improvements for the website. The information is not personal and will not be disclosed. The processing is based on Art. 6 para. 1 p. 1 lit. f) GDPR from the legitimate interest in direct customer communication and in the design of the website according to needs.

If you do not wish to be recorded, you can deactivate this on all websites that use Mouseflow using the following link: www.mouseflow.de/opt-out/.

Einwilligungsmanagement

In order to obtain and store your consent under data protection law, we use the consent management platform from Sourcepoint (Sourcepoint Technologies, Inc., 228 Park Avenue South, #87903, New York, NY 10003-1502,

United States). This sets cookies that are absolutely necessary in order to query the consent status and thus to be able to play out corresponding content.

Cookie	Purpose	Duration	Type
consentUUID	UniqueUserID to store the consent status of the user	12 months	Cookie
_sp_su	Marking of users for the sample of the reporting of the consent rates	12 months	Cookie
_sp_user_consent	UUniqueUserID to retrieve the user's consent status stored in our database when needed	12 months	local storage
_sp_local_state	Determine if a user has seen the Consent banner so that it is shown only once	12 months	local storage
_sp_non_keyed_local_state	Information about the metadata and the UniqueUserID of the user	12 months	local storage

Registration and login

We would like to offer you our content and services as conveniently as possible and provide you with a web offer that is tailored to you and your

personal wishes and expectations. We therefore offer you the opportunity to create a free customer profile, which allows you to use a variety of personalized services (Art. 6 para. 1 S.1 lit. b) GDPR).

Your data will be deleted when you delete your user account or in case of inactivity after two years.

Your data will be passed on to our hosting and technical service providers.

"stay logged in" feature

You have the option of using a "stay logged in" feature after logging in, so that you do not have to log in again after ending the session and visiting again later. For this purpose, we use cookies that automatically recognize you when you visit again with your consent. After 30 days of inactivity, the function is deleted. After the "Stay logged in" function expires, you will be prompted to log in again.

Embeds

We use embeds to provide you with content of interest. The respective embedding is performed by the technical procedure of so-called framing. Framing is the process of simply inserting a provided HTML link into the code of a website to create a playback frame on our pages, thereby enabling playback of the content stored on the third-party platform's servers.

This third-party content is loaded subsequent to your consent.

Some of such content also originates from social networks or other companies in the USA. By integrating their content, cookies and similar technologies may be used by them and data may also be transmitted to them in the USA (e.g. your IP address, browser information, cookie ID, pixel ID, page accessed, date and time of access). Details on the integrated content of the individual networks or these companies, which is stored on their servers and for the provision of which your IP address is transmitted to these companies, as well as on the data processing taking place at these companies, which may also include advertising purposes, can be found in the following lines.

You can withdraw your consent in the privacy settings.

- **Vimeo** You can find further information on data protection [here](#).

YouTube

The embedding of a YouTube video is done by the technical process of so-called framing. Framing involves simply inserting an HTML link provided by YouTube into the code of a website to create a playback frame on the third-party site, thus enabling the video stored on YouTube servers to be played. We use the generated framing codes in the so-called "extended data protection mode", so that the cookie activity and the data collection initiated by it is only linked to the use of the playback function of the video itself. Against this background, the collection of data by merely using the website with framed content is prevented.

The playing of the videos and the analysis and optimization of our video offer is based on your consent to a secure and efficient provision of this service.

In order to generate the embedding link based on the extended data protection mode, a click on "Share" below the desired embed and then on "Embed" is required. The adoption of this link ensures that cookies are only set when the embedded video is played by the user YouTube videos from the social network of YouTube, (Google Inc., Amphitheater Parkway, Mountain View, CA 94043, USA).

[Here](#) you will find more detailed information on the purpose and scope of data processing by Google and the settings you can make to protect your privacy.

- **Google Maps** Further information on data protection can be found [here](#).

Push notifications

You can sign up to receive our push notifications, which we use to inform you about new news and posts on our digital offerings. To do this, we display a push-up when you visit the website, asking you to consent to the notifications. If you agree, we store the login time and your browser ID or device ID. If you opt-out of notifications, we also store that decision so that you are not notified again.

We statistically evaluate the push notifications to see if and when they were displayed and clicked on.

You can withdraw your consent at any time with effect for the future by unsubscribing from the respective push notification by right-clicking on it in the settings that appear there. The unsubscribe process is explained in detail under the following link: <https://cleverpush.com/faq>.

Your data will therefore be stored as long as the subscription to our push notifications is active.

Your data will be processed on the basis of your consent.

Contentpass

On our website we offer you a service for ad- and tracking-free access. This service is called contentpass and is an offer of Content Pass GmbH, Wolfswerder 58, 14532 Kleinmachnow, Germany. When you sign up for the Service, contentpass becomes your contractual partner. For more information about this service, please visit contentpass.net.

In order to display and offer this service on our website, contentpass, on our behalf, processes your IP address at the beginning of your website visit. For the registration as well as the contract processing of contentpass and the associated data processing, contentpass is the controller in the sense of the GDPR. We are exclusively responsible for the processing of your IP address. The processing is necessary for technical reasons in order to display and offer you the service of contentpass. For more information regarding data processing at contentpass, please read the [Privacy Policy](#) there.

The basis for the data processing of the IP address, within the scope of our commissioned processing with contentpass, is our legitimate interest in offering you the opportunity to access our website free of advertising and tracking and your legitimate interest in using our website practically without advertising and tracking Art. 6 para. 1 p. 1 lit. f) GDPR in conjunction with § 25 para. 2 no. 2 TDDDG. In addition, we hereby fulfill the legal obligation to obtain legally compliant consent to data processing requiring consent Art. 6 para. 1 lit. c) DSGVO in conjunction with § 25 para. 2 No. 2 TDDDG.

Podcasts

We use the podcast hosting service **Podigee** of the provider Podigee GmbH, Schlesische Straße 20, 10997 Berlin, Germany to play out podcasts. The podcasts are thereby loaded by Podigee or transmitted via Podigee. Podigee processes IP addresses and device information on our behalf in order to enable podcast downloads/playbacks and to determine statistical data, such as retrieval figures. This data is anonymized or pseudonymized before being stored in Podigee's database unless it is necessary for the provision of the podcasts. The Podigee player and the social media links used are pure links and do not set cookies or communicate with external services without user interaction.

The playing of the podcasts and the associated counting of how often the podcast has been played is based on our legitimate interest under Art. 6 (1) p. 1 lit. f) DSGVO in the secure and efficient provision of these services.

We have contractually obligated Podigee neither to use your data for our own purposes nor to pass it on to others, and we regularly monitor compliance with data protection regulations.

Further information can be found in the [Privacy Policy of Podigee](#).

How we optimize our products

Further development of user-friendliness

We use cookies and tracking tools to optimize our digital offerings based on your utilization. To do this, we measure the development of reach as well as the use of content and function and we use A/B testing to check which variants users like better.

Reach measurement

Our website uses the multi-stage measurement procedure "INFOnline Measurement" from INFOnline GmbH (NFOnline GmbH, Brühler Str. 9, D-53119 Bonn, Germany) to determine statistical parameters (page impression, visit, technical client) about the use of our digital offering. The aim of usage measurement is to determine the number of visits to our website, the number of website visitors and their surfing behavior statistically - on the basis of a uniform standard procedure - and thus to obtain values that are comparable across the market. The purpose of the data processing is thus the creation of digital performance values (page impression, visit and technical client) in order to be able to track and prove the use of our offer.

As a member of the Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V., the usage statistics are regularly updated by IVW with the "Page Impression" and "Visits" in the IVW Report.

As a participant in the agof daily digital facts study, the usage statistics of our digital offerings are regularly collected by the Arbeitsgemeinschaft Online-Forschung e.V. and the Arbeitsgemeinschaft Media-Analyse e.V. and published with the key figure "unique user."

Due to the nature of the data and the volume of data, the data collected with INFOnline Measurement does not permit any clear assignment of a user to a person. A JavaScript code (so-called "Measurement Manager") is used that automatically integrates and executes the necessary measurement sensors for anonymous and/or pseudonymous data processing to determine the key figures when called up via the user's browser or terminal device (client) on the basis of the consent information from our Consent Management Platform (CMP). INFOnline Measurement is designed as an anonymous system (without customer identifier) and as a pseudonymous system (with customer identifier).

Type of data

Due to the nature of the data and the data volume, the data collected with INFOnline Measurement do not permit any clear assignment of a user to a person. A JavaScript code (so-called "Measurement Manager") is used which, when called up via the browser or the user's end device (client), automatically integrates and executes the necessary measurement sensors for anonymous and/or pseudonymous data processing to determine the key figures on the basis of the consent information from the Consent Management Platform (CMP) used by the provider for the digital offering. INFOnline Measurement is designed as an anonymous system (without

customer identification) and as a pseudonymous system (with customer identification).

Anonymous Census Method (IOMb)

In the anonymous counting procedure (IOMb), no personal data is processed, especially not the IP address. It is completely removed from communication and processing. For this purpose, a communication interface, the so-called "service platform," as the measurement end point, prevents the exchange of the user's IP address with the INFOnline systems as part of the INFOnline measurement. The IP address as personal data is discarded in the counting process on the service platform before the measurement call is forwarded to INFOnline. There is also no geolocation via the IP address. The data record generated in the counting process is a pure PI data collection.

Pseudonymous measurement method (IOMp)

With the pseudonymized measurement method (IOMp), the following data is collected with the 3rd party cookie 'i00' (ioam.de) and the 1st party cookie 'ioma2018', which has a personal reference according to GDPR:

- IP address
On the Internet, every device needs a unique address for the transmission of data, the so-called IP address. The storage of the IP address, at least for a short time, is technically necessary due to the way the Internet works. The IP addresses are shortened by 1 byte before any processing and are only processed anonymously. further processed. The untruncated IP addresses are not stored or processed.
- A randomly generated client identifier
The range measurement uses for the recognition of computer systems unique identifiers of the end device, a "Local Storage Object" (LSO) or a "signature", which is created from various automatically transmitted information from your browser. This identifier is unique to a browser as long as the cookie or Local Storage Object is not deleted. The measurement of the data and the subsequent assignment to the respective identifier may also be possible under certain circumstances if you call up other websites that also use the pseudonymized measurement procedure of INFOnline GmbH.

The following unique identifiers can be transmitted to INFOnline GmbH as a hash:

- shortened client IP or X-Forwarded-For (XFF)
- user agent (as hash)

Personal data within the meaning of the EU-DSGVO is used for measurement only to the extent that a JavaScript is used vis-à-vis a user to whom an individual IP address and a randomly generated client identifier have been assigned for retrieving web content.

anonymous measurement method (IOMa)

The anonymous measurement method (IOMa) uses a measurement sensor (JavaScript) that calculates the metrics in the user's browser (LocalStorage (LSO)), automatically encrypts them, and transmits the aggregated usage data to a communication interface, the so-called 'service platform'. In the service platform identifiers required for Internet communication (e.g., IP address of the client) are removed and the encrypted anonymized measurement data is supplemented by geolocation and transmitted to the central server component at INFOnline.

Insofar as the collected measurement data is enriched with a geolocation of the browser, an IP address is also used only for the purpose of collecting the geolocation and the enrichment with the collected measurement data. An IP address required for this is discarded immediately after the enrichment.

During the implementation phase of IOMa a 1st party cookie is used to store the timestamps (Unix Epoch Timestamp) of the last usage per offer and per page code. These values are added as a benchmark for the formation of time-related metrics such as the visit when the HTTP origin changes. No other personal data/IDs are stored in the cookie. After the implementation phase, it should then be dropped, so that the measurement then takes place completely without cookies.

Personal data within the meaning of the GDPR are used for measurement only to the extent that the use of a JavaScript takes place vis-à-vis a user who has been assigned an individual IP address for calling up web content.

In this respect we do not permanently process any personal data about you through the use of the anonymous measurement method (IOMa) in INFOnline Measurement.

Data usage

The INFOnline GmbH measurement procedure used on this website determines usage data. This is done in order to collect the performance values page impression, visit and client.

- **Geolocation**

In the pseudonymized measurement procedure (IOMp) and in the anonymized measurement procedure (IOMa), a web page call is assigned to the location of the call exclusively on the basis of the anonymized IP address and only down to the geographic level of the federal states/regions. Under no circumstances can the geographical information obtained in this way be used to draw conclusions about the specific place of residence of a user.

- **Merging of usage data across offerings**

The usage data of a technical client (e.g., a browser on a device) is collected using the pseudonymized measurement method (IOMp) and stored in a database.

Duration of data storage

The complete IP address is not stored by INFOnline GmbH. The IP address is used only to receive the data packets and is subsequently shortened by 1 byte. In the counting procedure (IOMb), the shortened IP address is discarded; in the pseudonymous (IOMp) and anonymous procedure (IOMa), the shortened IP address is stored for a maximum of 60 days. In the pseudonymous (IOMp) and (IOMa) procedure, the usage data is stored in conjunction with the unique identifier for a maximum of 6 months.

The validity of the cookie "i00" used in the pseudonymous procedure (IOMp) and the cookie "ioma2018" on the user's terminal device is limited to a maximum of 1 year.

Legal basis

Measurement with INFOnline Measurement (pseudonymous system: IOMp) as well as the measurement with INFOnline Measurement (anonymous system: IOMa) is taken place with consent.

Usage analysis

We aim to constantly develop and improve our products. For this purpose, we require usage analysis that goes beyond mere reach measurement. Usage analysis serves to evaluate the flow of visitors to our online offerings and

may include behavior, interests or demographic information about visitors, such as age or gender, as pseudonymous values. With their help, we can recognize, for example, when our digital offerings are most frequently used or which functions are readily reused. This allows us to identify which areas need optimization.

In addition to usage analysis, we also use test procedures, for example, to test different versions of our online offerings or their components.

For these purposes, profiles, i.e. data summarized for a usage process are created and information is stored in and read from a browser or terminal device. The information collected includes, in particular, websites visited and elements used there, as well as technical information such as the browser used, the computer system used, and information on usage times. Only if you have consented to the collection of your location data will it be processed.

The IP addresses of the users are also stored. We use an IP masking method (i.e. pseudonymization by shortening the IP address) for your protection. Generally, the data stored in the context of web analytics, A/B testing and optimization is not clear user data (such as e-mail addresses or names), but pseudonyms, so that neither we nor the providers of the software used, who act for us as processors, know the actual identity of the users.

Google Analytics

We use Google Analytics (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland) to measure and analyze the use of our online offer on the basis of a pseudonymous user identification number. This identification number does not contain any unique data, such as names or e-mail addresses. It is used to assign analysis information to a terminal device in order to recognize which content users have accessed within one or various usage processes, which search terms they have used, have accessed again or have interacted with our online offer. Likewise, the time of use and its duration are stored, as well as the sources of users referring to our online offer and technical aspects of their end devices and browsers. In the process, pseudonymous profiles of users are created with information from the use of various devices, whereby cookies may be used. Google Analytics does not log or store individual IP addresses for EU users. However, Analytics provides coarse geographic location data by deriving the following metadata from IP addresses: City (and the derived latitude and

longitude of the city), Continent, Country, Region, Subcontinent (and ID-based counterparts). For EU traffic, IP address data is used exclusively for this derivation of geolocation data before being immediately deleted. They are not logged, are not accessible, and are not used for any other purpose. When Google Analytics collects measurement data, all IP queries are performed on EU-based servers before traffic is forwarded to Analytics servers for processing.

The storage period of the data is 14 months (concerns user and event level data). Aggregated data is anonymized and is not deleted.

Google is our processor, with whom we have concluded the necessary agreements for this purpose. We have also taken measures to ensure appropriate and adequate safeguards for the protection of personal data during third-country data transfers by concluding EU standard contractual clauses and observing additional measures to protect data subjects' rights where necessary.

If you have agreed to Google and linked your devices to your Google account, it is possible that Google can track your usage behavior across multiple devices ("Google Signals"). Google uses the log-ins in the Google network for these statistics and thus performs cross device tracking. Cross device tracking is intended to enable different visits to a website to be assigned to one visitor, even if the visitor accesses the content via different devices. Google uses Signals to provide reports on cross-device user numbers, as well as on different groups of users based on different device combinations used. For this purpose, Google uses the data of users who have activated the "personalized advertising" option in their Google account settings. This means that you can also be shown interest-based advertising when you change end devices.

You can find more information on terms of use and data protection at.

- [User Terms](#),
- [Privacy Policy Overview](#),
- [Privacy Policy](#).

You may refuse the use of cookies by selecting the appropriate settings on your browser, however please note that if you do this you may not be able to use the full functionality of this website. You can also prevent the collection of data generated by the cookie and related to your use of the website (including your IP address) to Google and the processing of this data by

Google by downloading and installing the browser plugin available at the following link: <http://tools.google.com/dlpage/gaoptout?hl=de>.

Your data will be processed on the basis of your consent.

Scaloper ABM-Campaign Targeting

Our website uses services provided by MBmedien Group GmbH (“MBmedien”). When connecting to MBmedien servers, the standard information is transmitted, namely the website visited including URL and path, date and time of access, time zone difference to Greenwich Mean Time (GMT), content of the request for the specific page, access status/HTTP status code, amount of data transferred in each case, website from which you came to this website, browser type used, language and version of the browser software, operating system and user interface used, IP address used. The transfer takes place exclusively to servers in the EU. MBmedien compares the transmitted data with its own database of non-personal IP addresses. Personal data is discarded as a result of this comparison and is not processed. The processing that then takes place relates exclusively to non-personal information and serves to optimize the display of our website. The transmission of the information to MBmedien serves to safeguard our legitimate interests in an optimized presentation of our online offers in accordance with Art. 6 para. 1 subpara. 1 lit. f GDPR, which predominate in the context of a balancing of interests.

Details on the data protection provisions of MBmedien Group GmbH can be viewed here <https://mbmedien.group/datenschutz-dsgvo>

Translated with DeepL.com (free version)

Surveys

To find out how satisfied you are with our products, you can take part in our surveys. You decide individually for each survey whether you want to participate and what information you want to give us.

To enable participants to interrupt a survey embedded on the website and resume it with the same browser, a session cookie is created at the start of the survey participation. This also prevents you from being shown the same survey more than once.

You can delete this cookie at any time in the data protection settings of your browser. However, this means that you will no longer be able to continue a partially completed survey at the point where it was interrupted and you will no longer be protected against the survey being displayed again.

If personal data is collected in a survey, it will be deleted at the latest at the end of the year in which the survey and its evaluation were completed.

For our surveys we use the online survey tool Happy Contests. Information on data protection can be found [here](#). All data is stored on the Happy Contests servers.

When you visit events

Order tickets for events

If you purchase tickets for events, you must provide us with your address, contact and communication details when concluding the contract, as well as your credit card details if applicable.

After termination of the contract, we will delete or block your data, unless we are required by law to retain such data. The deletion usually takes place after ten years.

The legal basis for the data processing operations is our legitimate interest.

Payment processing Payone GmbH

We transmit your data (name, address and, if applicable, date of birth) to infoscore Consumer Data GmbH ("ICD"), Rheinstr. 99, 76532 Baden-Baden, Germany, for the purpose of credit assessment, obtaining information to assess the risk of non-payment based on mathematical-statistical methods using address data, and to verify your address (check for deliverability).

The legal basis for these transmissions is our legitimate interest, because only by transmitting and checking the data can we assess whether the payment obligations can be met, so that we can carry out the contractual activities in a secure manner. Transmissions on the basis of these regulations may only take place if this is necessary to safeguard the legitimate interests of our company or third parties and does not outweigh the interests or fundamental rights and freedoms of the person concerned, which require the protection of personal data.

Detailed information on the ICD, i.e. information on the business purpose, on the purposes of data storage, on the data recipients, on the right of self-disclosure, on the right to deletion or correction etc. can be found under [this link](#).

Online events

In order to be able to offer our events online, we use the tools listed below. Details on the data processed in the process can be found under the respective section.

Calendly

We use the tool Calendly (Calendly, LLC, BB&T, Tower 271 17th St NW, Atlanta, GA 30363) to schedule appointments for, among other things, technology checks at digital events.

When using Calendly, various types of data are processed. The scope of the data here also depends on what information about data you provide before or when responding to an appointment request where we use Calendly.

The following personal data are subject to processing:

- **Appointment Data:** A Calendly user, invitee or third party may voluntarily provide Calendly with certain information. This may include names, email addresses and phone numbers, email addresses of other individuals, the subject of the meeting, and any other information
- **Calendar Information:** For Calendly users, the duration and free/busy status of events in the calendar is checked

The data processing is necessary for the fulfillment of the contract.

Your personal data processed in connection with the response to an appointment request via Calendly will not be disclosed to third parties as a matter of principle, unless they are specifically intended for disclosure. The service provider Calendly necessarily receives knowledge of the above-mentioned data insofar as this is provided for in the context of our order processing agreement with them. If you are registered as a user with calendly, then reports on your scheduling (duration and free/busy status) may be stored at calendly.

You can find more information in the data protection notice of calendly: <https://calendly.com/de/pages/privacy>

Clickmeeting

We use the Clickmeeting tool (ClickMeeting Sp. z o.o., Arkonska 6/A4, 80-387 Gdansk, Poland) to conduct webinars or other events.

We log the chat content in order to optimize our webinars. For this purpose, we process the questions asked by webinar participants for the follow-up of the webinars. The fact of the recording is also displayed to you.

The following personal data are subject to processing:

- User details: First name, last name, phone (optional), email.
- Meeting metadata: Topic, description (optional), attendee IP addresses, device/hardware information.
- For cloud recordings (optional): Mp4 of all video, audio, presentations, M4A of all audio, text file of all in meeting chats, audio log file
- IM chat logs
- Telephony usage data (optional): Call in number, call out number, country name, IP address, start time, end time, host name, host email, MAC address of device in use
- Text, audio and video data: you may have the opportunity to use the chat, question or poll functions in an "online meeting". The text entries you make there will be logged. To enable the display of video and the playback of audio, the data from the microphone of your terminal device and from any video camera of the terminal device will be processed accordingly for the duration of the meeting. You can turn off or mute the camera or microphone yourself at any time via ClickMeeting.

- Location data.

The data processing is carried out in accordance with Art. 6 para. 1 p. 1 lit. b) DSGVO, any recording is only carried out with prior consent.

Your personal data processed in connection with participation in our online events will generally not be disclosed to third parties, unless they are specifically intended for disclosure. The service provider ClickMeeting necessarily obtains knowledge of the above-mentioned data to the extent provided for in our order processing agreement with them. If you are registered as a user with ClickMeeting, then reports of online events (meeting metadata, telephone dial-in data, questions and answers in webinars, survey function in webinars) may be stored by ClickMeeting for up to one month.

Your personal data will be deleted at the latest at the end of the year in which the webinar and their evaluation was completed.

Do

You can register for events on our website. When you register for and participate in an event, we process your data provided during registration and collected during participation in the respective event for the purpose of carrying out the registration and participation in the event.

The personal data processed during a registration belong to the following data categories:

- Name
- Your address
- e-mail address
- Movement data at events ("session tracking")
- Payment data (for paid events)
- Reaction behavior with Invitee Data
- Other data transferred to the event management platform or requested as part of registration for an event.

The personal data processed on behalf of us do not regularly include special categories of data, unless special categories of data are transferred to the event management platform or queried as part of a registration for an event.

We send information by post and/or e-mail to the contact details you have provided as part of the registration and participation in an event. The legal basis for this is Art. 6 (1) lit. b DSGVO, i.e. the fulfillment of the contract for participation in the respective event or the implementation of pre-contractual measures, which take place at your request. For the registration and management of events, we use the service provider doo GmbH, Hultschiner Str. 8, 81677 Munich. Detailed information on data processing and data protection at doo can be found in doo's privacy policy at the following link: <https://doo.net/de/about/datenschutzerklaerung.html>

ExpolP

We use the EXPO-IP tool (EXPO-IP GmbH, Robert-Bosch-Str. 7, 64293 Darmstadt, Germany) to conduct digital events and trade fairs. If we want to record such an online event, we will transparently inform you in advance and - if necessary - ask for consent.

Various types of data are processed when using EXPO-IP. In this context, the scope of the data also depends on the data you provide before or when participating in an online event.

The following personal data are subject to processing:

- Authentication data
- Usage data, e.g. log files (esp. names of users of IT systems or applications, IP addresses)
- Master data
- System access data

The data processing is carried out in accordance with Art. 6 para. 1 p. 1 lit. b DSGVO. A recording of the online event is only made if we have informed you of this in advance and you have consented to the recording. The legal basis in this case is Art. 6 para. 1 lit. a DSGVO.

As a matter of principle, your personal data processed in connection with your participation in our online events will not be disclosed to third parties unless it is specifically intended for disclosure. The service provider EXPO-IP necessarily receives knowledge of the above-mentioned data insofar as this is provided for under our order processing agreement with it. If you are registered as a user with EXPO-IP, then reports of online events (meeting metadata, questions and answers in webinars, survey function in webinars, chat histories) may be stored at EXPO-IP.

Your data will be deleted as soon as it is no longer necessary for the purpose for which it was collected.

We have concluded an order processing agreement with EXPO-IP that complies with the requirements of Art. 28 DSGVO.

For more information, please refer to the [data protection notice of EXPO-IP](#).

GoTo Webinar

We use the GoTo Webinar tool (GoTo Technologies Ireland Unlimited Company, Ireland) to conduct webinars or other events.

We log the chat content in order to be able to optimize our webinars. For this purpose, we process the questions asked by webinar participants for the follow-up of the webinars. The fact of the recording is also displayed to you.

The following personal data are subject to processing:

- User details: First name, last name, phone (optional), email.
- Meeting metadata: Topic, description (optional), attendee IP addresses, device/hardware information.
- For cloud recordings (optional): Mp4 of all video, audio, presentations, M4A of all audio, text file of all in meeting chats, audio log file
- IM chat logs
- Telephony usage data (optional): Call in number, call out number, country name, IP address, start time, end time, host name, host email, MAC address of device in use
- Text, audio and video data: you may have the opportunity to use the chat, question or poll functions in an "online meeting". The text entries you make there will be logged. In order to enable the display of video and the playback of audio, the data from the microphone of your terminal device and from any video camera of the terminal device will be processed accordingly for the duration of the meeting. You can turn off or mute the camera or microphone yourself at any time via GoTo.
- Location data.

The data processing is carried out in accordance with Art. 6 para. 1 p. 1 lit. b) DSGVO.

As a matter of principle, your personal data processed in connection with participation in our online events will not be disclosed to third parties

unless they are specifically intended to be disclosed. The service provider GoTo necessarily obtains knowledge of the above-mentioned data insofar as this is provided for in the context of our order processing agreement with it. If you are registered as a user with GoTo, then reports on online events (meeting metadata, telephone dial-in data, questions and answers in webinars, survey function in webinars) may be stored by GoTo for up to one month.

Your personal data will be deleted at the latest at the end of the year in which the webinar and their evaluation was completed.

Hopin

For our online events we use the online event platform Hopin (Hopin Ltd of Seedcamp Office, 5 Bonhill Street, Shoreditch, London, England), which is operated on the website hopin.to, for the purpose of handling the registration process, the organization, implementation and possibly also for billing of the event.

The following personal data are subject of the processing:

- user data: first name, last name, phone (optional), e-mail, password (if SSO is not used), profile picture (optional), department (optional)
- Meeting metadata: Topic, description (optional), participant IP addresses, device/hardware information
- for cloud recordings (optional): Mp4 of all video, audio and presentations, M4A of all audio recordings, text file of all in meeting chats, audio log file
- IM Chat Logs
- Telephony usage data (optional): call in number, call out number, country name, IP address, 911 address (registered service address), start and end time, host name, host e-mail, MAC address of the used device
- Text, audio and video data: You may be able to use the chat, question or survey functions in an "event". In this respect, the text entries you make are processed in order to display them in the "event" and, if necessary, to log them. In order to enable the display of video and the playback of audio, the data from the microphone of your terminal device and from any video camera of the terminal device will be processed for the duration of the event. You can switch off or mute the

camera or microphone yourself at any time using the zoom applications.

In these cases, we process your personal data on the basis of the consent given during registration for participation in an event (Art. 6 para. 1 sentence 1 lit. a DSGVO) or on the basis of the event contract concluded with you (Art. 6 para. 1 sentence 1 lit. b DSGVO).

We will store your data until the event has been fully processed and settled and until no more claims can be made under the participant contract, i.e. until the statute of limitations. As a rule, the statute of limitations shall apply within three years from the end of the event, starting on 31 December of the year in question.

If you have given your consent, we will store the data until you withdraw this consent, which you can do informally at any time with effect for the future. As a rule, however, we delete such data after a maximum of three years if there has been no further contact between us during this period.

The following data may be processed when using Hopin:

- contact details: Address, e-mail address, telephone
- Identity data: First name, last name, username, birthday, gender and marital status
- transaction data: Product information and payments from other Hopin products and services
- Technical data: IP address, login data, browser type and version, browser plug-ins, hardware information, time zone, location, operating system, start and end time
- profile data: Username and Password
- usage data: User behavior

Hopin may also process your data in third countries. The transfer is based on EU standard contract clauses.

Here you can find the [data protection regulations](#) of Hopin.

MS Teams

We use the tool "Microsoft Teams" to conduct telephone conferences, online meetings, video conferences and/or web conferences (hereinafter: "Online Meetings").

"Microsoft Teams" is a service of Microsoft Corporation (Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA). If we want to record online meetings, we will transparently inform you in advance and - if necessary - ask for consent. The fact of recording will also be displayed to you in the MS Teams app.

Note: Insofar as you call up the "Microsoft Teams" website, the "Microsoft Teams" provider is responsible for data processing. However, calling up the Internet page is only necessary for the use of "Microsoft Teams" in order to download the software for the use of "Microsoft Teams". If you do not want to or cannot use the "Microsoft Teams" app, you can also use "Microsoft Teams" via your browser. The service will then to that extent also be provided via the "Microsoft Teams" website.

Data

The scope of the data depends on the information on data you provide before or when participating in an "online meeting". The following personal data are subject to processing:

- User details: e.g. display name ("Display name"), e-mail address if applicable, profile picture (optional), preferred language.
- Meeting metadata: e.g. date, time, meeting ID, phone numbers, location
- Text, audio and video data: you may have the option of using the chat function in an "online meeting". To this extent, the text entries you make are processed in order to display them in the "online meeting". In order to enable the display of video and the playback of audio, the data from the microphone of your terminal device and from any video camera of the terminal device will be processed accordingly for the duration of the meeting. You can turn off or mute the camera or microphone yourself at any time via the "Microsoft Teams" applications.

Chat content is logged when using Microsoft Teams. Files that users share in chats are stored in the OneDrive for Business account of the user who shared the file. Files that team members share in a channel are stored on the team's SharePoint site.

--Legal basis for data processing

--

Insofar as personal data of employees is processed, Section 26 of the German Federal Data Protection Act (BDSG) is the legal basis for data processing.

If, in connection with the use of "Microsoft Teams", personal data is not required for the establishment, implementation or termination of the employment relationship, but is nevertheless an elementary component in the use of "Microsoft Teams", Art. 6 (1) lit. f) DSGVO is the legal basis for data processing. In these cases, our interest is in the effective implementation of "online meetings".

Otherwise, the legal basis for data processing when conducting "online meetings" is Art. 6 (1) lit. b) DSGVO.

Online meetings are only recorded if we have informed you of this in advance and you have consented to the recording. The legal basis in this case is Art. 6 para. 1 lit. a) DSGVO.

Storage period

We generally delete personal data when there is no need for further storage. A requirement may exist in particular if the data is still needed to fulfill contractual services, to check and grant or defend against warranty and, if applicable, guarantee claims. In the case of statutory retention obligations, deletion will only be considered after expiry of the respective retention obligation.

__Data transfer __

Personal data that is processed in connection with participation in "Online Meetings" is generally not passed on to third parties unless it is intended for transfer. Please note that, as in the case of face-to-face meetings, the content of online meetings is often used to communicate information to customers, prospects or third parties and is therefore intended for disclosure.

__Other recipients: __

The provider of "Microsoft Teams" necessarily receives knowledge of the above-mentioned data, insofar as this is provided for in the context of our order processing agreement with "Microsoft Teams". In principle, no data processing takes place outside the European Union (EU), as we have limited our storage location to data centers in the European Union. However, we cannot exclude the routing of data via Internet servers that are located outside the EU. This may be the case in particular if participants in "Online Meeting" are located in a third country.

__Data transfer outside the EU/EEA __

Since Microsoft is based in the USA, we have concluded an order processing agreement with Microsoft that complies with the requirements of Art. 28 DSGVO. An adequate level of data protection is guaranteed on the one hand by the conclusion of the so-called EU standard contractual clauses. As supplementary protective measures, we have also configured our system in such a way that only data centers in the EU, the EEA or secure third countries such as Canada or Japan are used to conduct "online meetings".

For more information, please see Microsoft's privacy notice:

<https://privacy.microsoft.com/de-de/privacystatement>

<https://www.microsoft.com/de-de/trust-center>

The data is encrypted during transport over the Internet and thus protected against unauthorized access by third parties.

Slido

We use the tool Slido (sli.do s. r. o., Vajnorská 100/A, 831 04 Bratislava, Slovakia (European Union)) to conduct surveys and questions at digital events. If we want to record online events, we will transparently inform you in advance and - if necessary - ask for consent.

If it is necessary for the purposes of logging the results of an online meeting, we will log the content. However, this will generally not be the case.

When using Slido, different types of data are processed. The scope of the data also depends on the data you provide before or during participation in an online event where we use Slido.

The following personal data are subject to processing:

- User details: Username (optional)
- Text data: You have the option to use the chat, question or survey functions. To this extent, the text entries you make are processed in order to display them in the "online meeting" and to log them if necessary.

The data processing is carried out for the fulfillment of the contract.

Your personal data processed in connection with participation in our online events will not be disclosed to third parties as a matter of principle, unless they are specifically intended for disclosure. The service provider Slido necessarily obtains knowledge of the above-mentioned data insofar as this is

provided for in the context of our order processing agreement with it. If you are registered as a user with Slido, then reports on online events (meeting metadata, questions and answers at events, survey function at events) may be stored at Slido.

For more information, please see Slido's privacy notice:

<https://www.sli.do/terms#privacy-policy>

Wonder.me

We use the tool Wonder (Yotribe GmbH, Kommandantenstraße 77, 10117 Berlin, Germany) to conduct conference calls, online meetings, video conferences, webinars or other events. If we want to record online events, we will transparently inform you in advance and - if necessary - ask for consent.

If it is necessary for the purposes of logging the results of an online meeting, we will log the chat content. However, this will generally not be the case.

In the case of webinars, we may also process questions asked by webinar participants for purposes of recording and following up on webinars. When using Wonder, various types of data are processed. In this context, the scope of the data also depends on the information on data you provide before or when participating in an online event.

The following personal data are subject to processing:

- User details: User name, profile picture, e-mail (optional),
- Room metadata: Room name, description (optional), participant IP addresses, device/hardware information.
- IM chat logs
- Text, audio and video data: you may have the option to use chat, question or poll functions in an "online meeting". To this extent, the text entries you make are processed in order to display them in the "online meeting" and, if necessary, to log them. To enable the display of video and the playback of audio, the data from the microphone of your terminal device and from any video camera of the terminal device will be processed accordingly for the duration of the meeting. You can turn off or mute the camera or microphone yourself at any time through the Wonder applications
- Location data.

In order to participate in an online event or to enter the "meeting room", you must at least provide information about your name. The data processing is carried out in accordance with Art. 6 para. 1 p. 1 lit. b DSGVO.

We store your personal information in a form that permits identification only for as long as it is needed for those business purposes for which it was collected or is needed to comply with our legal obligations, resolve disputes and enforce our agreements.

As a matter of principle, your personal data processed in connection with your participation in our online events will not be disclosed to third parties unless they are specifically intended to be disclosed. The service provider Wonder necessarily obtains knowledge of the above-mentioned data insofar as this is provided for in the context of our order processing agreement with them. If you are registered as a user with Wonder, then reports of online events (meeting metadata, questions and answers in webinars, survey function in webinars, chat histories) may be stored at Wonder. We have entered into a contract for order processing with Wonder, which complies with the requirements of Art. 28 DSGVO.

For more information, please see [Wonder's privacy notice](#).

Zoom

We use the Zoom tool (Zoom Video Communications, Inc., 55 Almaden Blvd, Suite 600, San Jose, California, USA) to conduct conference calls, online meetings, video conferences, webinars or other events. If we want to record online events, we will inform you transparently in advance and - if necessary - ask for your consent. The fact of the recording will also be displayed in the zoom app.

If it is necessary for the purpose of logging the results of an online meeting, we will log the chat content. However, this will usually not be the case.

In the case of webinars, we can also process the questions asked by webinar participants for the purposes of recording and follow-up of webinars.

When using Zoom, different types of data are processed. The extent of the data also depends on the information you provide before or during participation in an online event.

The following personal data are subject to processing:

- user data: First name, last name, telephone (optional), e-mail, password (if SSO is not used), profile picture (optional), department (optional)
- Meeting metadata: Topic, description (optional), participant IP addresses, device/hardware information
- for cloud recordings (optional): Mp4 of all video, audio and presentations, M4A of all audio recordings, text file of all in meeting chats, audio log file
- IM Chat Logs
- Telephony usage data (optional): call in number, call out number, country name, IP address, 911 address (registered service address), start and end time, host name, host e-mail, MAC address of the used device
- Text, audio and video data: You may be able to use the chat, question or survey functions in an "online meeting". To this extent, the text entries you make are processed in order to display and, if necessary, log them in the "online meeting". In order to enable the display of video and the playback of audio, the data from the microphone of your terminal device and from any video camera of the terminal device will be processed for the duration of the meeting. You can switch off or mute the camera or microphone yourself at any time using the zoom applications
- location data.

In order to participate in an online event or to enter the "meeting room", you must at least provide information about your name.

The data processing is carried out in accordance with Art. 6 para. 1 sentence 1 lit. b DSGVO.

Your personal data, which is processed in connection with your participation in our online events, is generally not passed on to third parties, unless it is specifically intended to be passed on. The service provider Zoom necessarily obtains knowledge of the above-mentioned data to the extent that this is provided for in our contract processing agreement with him. If you are registered as a user at Zoom, reports on online events (meeting meta data, data on telephone dial-in, questions and answers in webinars, survey function in webinars) can be stored at Zoom for up to one month. Furthermore Zoom reserves the right to pass on your data to third parties with your consent.

Since Zoom is based in the USA, we have concluded a contract with Zoom that meets the requirements of Art. 28 DSGVO. An appropriate level of data protection is guaranteed on the one hand by the conclusion of the so-called EU standard contract clauses. As additional protective measures, we have also configured our Zoom in such a way that only data centers in the EU, the EEA or safe third countries such as Canada or Japan are used for "online meetings".

You can find further information in Zoom's data protection notice:
<https://zoom.us/de-de/privacy.html>

When you get in contact with us

Contact

When you contact us, we only collect personal data (e.g. name, e-mail address, telephone number) if you provide us with this information voluntarily. You can send this information to us by email or letter, for example. Your personal data will only be used to contact you or for the purpose for which you have provided us with this data, e.g. to process your inquiries, technical administration of the website and customer management.

Any communication of this information (including information on communication channels such as e-mail address, telephone number) is expressly on a voluntary basis. The data will be used exclusively to process your request if the data processing is necessary for the fulfillment of the contract or if there is a legitimate interest to do so. In the case of a telephone inquiry, your data will also be processed by telephone applications and, in some cases, by a voice dialogue system in order to support us in the distribution and processing of the inquiries.

This data is passed on to our service providers for customer service and is deleted if it is no longer required.

Contact form

When you use our contact form, we process the following data:

- Salutation, first name, last name, company (voluntary information).
- E-mail.

This data processing is carried out with predominantly legitimate interest (Art. 6, para. 1 lit. f DSGVO) or, as far as it concerns voluntary information, with your consent (Art. 6, para. 1 lit. a DSGVO).

The data will be deleted when your request has been processed.

Messaging

To facilitate communication with you, we use the messenger service Userlike (Userlike UG (haftungsbeschränkt), Probsteigasse 44-46, 50670 Cologne, Germany). For this purpose, we have integrated a widget on our website <https://aufträge.fertigung.de>, which you can use to chat with us. To protect your privacy, we have deactivated the collection of personal data and tracking. The functionality requires the setting of a cookie (uslk-umm-{134853}-s), which is deleted after 30 days. Consequently, we only process the personal data that you enter in the chat. The legal basis for this is your consent (Art.6 para.1 p.1 lit.a) GDPR).

If the communication contains personal data and is terminated, we delete it at the latest at the end of the year in which the communication was terminated. You can request earlier deletion at any time at datenschutz@mi-connect.de.

If we promote our products

Direct marketing

We also use your contact data for advertising purposes in addition to contract-related use. This is only done if you have expressly consented (Art. 6 para. 1 lit. a) GDPR) or on the basis of our legitimate interest in direct advertising (Art. 6 para. 1 lit. f) GDPR), for example for information about the same and similar products of our company (Section 7 para. 3 UWG).

The data processed by us will be deleted as soon as it is no longer required for its intended purpose and the deletion does not conflict with any statutory retention obligations. Deletion generally takes place after two years of inactivity.

We store the proof of your consent, which we provide via the double opt-in procedure, for 3 years even if you withdraw your consent (Art. 6 para. 1 lit. c), Art. 5 para. 1 lit. a), Art. 7 para. 1, Art. 6 para. 1 lit. f) GDPR)

If you no longer wish to receive advertising, you can withdraw your respective consent or object to advertising at any time.

- by clicking on the unsubscribe link at the end of the mail
- by mail to datenschutz@ultimamedia.de
- in writing to Ultima Media Germany GmbH, Hultschiner Straße 8, 81677 München, Germany (please include your e-mail address or telephone number and the name from the registration)
- or by phone via +49 (0)8191 125-570.

Newsletter

You will receive newsletters from us if you order them explicitly via a so-called "double-opt-in procedure", i.e. the specification of your e-mail address is verified by means of a confirmation e-mail sent to it. A processing of your personal data then takes place with your consent.

If you have consented, we evaluate your clicks in newsletters with the help of so-called tracking pixels, i.e. invisible image files. These are assigned to your mail address and are linked to a separate ID to uniquely assign clicks in the newsletter to you. The usage profile is intended to tailor the newsletter offer to your interests. We record when you read newsletters and which links you click on, and derive an interest profile from this.

The deletion takes place at the end of the year in which you unsubscribed from the newsletter.

You can unsubscribe from any newsletter at any time and withdraw your consent to the sending and evaluation.

Data processing in detail

Data	Purpose of processing	Legal basis of processing	Storage period
e-mail address	sending the newsletter	consent	until withdrawal
IP address for opt-in	proof of double opt-in	consent	until withdrawal
time of DOI verification	proof of double opt-in	consent	until withdrawal
salutation*	direct address	consent	until withdrawal
first name*	direct contact	consent	until withdrawal
Surname*	Direct contact	Consent	until withdrawal
usage data	further development and improvement of the service	consent	until withdrawal
End devices	correct playing of the newsletter	consent	until withdrawal

* voluntary information

Self-promotion

In order to show you advertising for our own products, we use the services of advertising partners or cooperate with advertising partners and

advertising networks. These use cookies, pixels or similar technical means to display and evaluate advertisements.

Advertisements may be customized for each user, for example, by using browser usage information (such as pages visited, hours of use, length of stay). However, user-related advertisements are also possible. Furthermore, evaluations of the range or for billing purposes can be carried out in pseudonymized form. The details of the services used, cooperation partners and individual possibilities of objection are described below.

Your data will be processed on the basis of your consent.

Adjust

We use the usage evaluation and analysis technology Adjust.io of adjust GmbH, Saarbrücker Str. 36, D-10405 Berlin, Germany. We collect data on interaction with our advertising materials, install and event data of the website and use it for anonymized evaluations. We use this information to measure the success of our marketing campaigns and use it for our own market research and optimization.

The data processing is carried out with your consent according to Art. 6 para. 1 p. 1 lit. a) DSGVO.

Your data will be stored from the time of consent until a maximum of 25 months thereafter.

The Adjust service has been tested and certified according to the [ePrivacyseal](#) (European Seal for your Privacy).

You can prevent future data collection and storage at any time by revoking your consent in the privacy settings - in the footer of the visited website.

Meta Platforms Conversion API

Within our online offer and also for newsletters and podcasts, we use the "Conversion API" of the social network Meta Platforms and Instagram, which is operated by Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland, for the analysis, optimization and economic operation of our online offer.

In order to ensure appropriate and adequate safeguards for the protection of personal data, we have concluded EU standard contractual clauses with Meta Platforms and observe additional measures for the protection of data subjects' rights as required.

The "Conversion API" is an interface to which conversion information can be sent on the server side. With the help of the data transfer via the API, we want to ensure that our Meta Platforms and Instagram ads correspond to the potential interest of the users and do not have a harassing effect.

Furthermore, we can track the effectiveness of the Meta Platforms and Instagram ads for internal performance measurement purposes by seeing whether users were redirected to our website after clicking on a Meta Platforms or Instagram ad and possibly performed an action (so-called "conversion").

User data is generated, read or sent at the following points:

User clicks on an SZ ad on Meta Platforms or Instagram

- Meta Platforms/Instagram registers the click
- The target URL is assigned a click ID "fbclid" (unique identifier that Meta Platforms/Instagram can use to match information about user, ad, campaign, etc.)

User reaches target page

If consent exists: fbclid information is read from URL and stored in a cookie ("szpay_fbclid", runtime: 7 days)

If a user performs a certain action on the target page (e.g. purchase of a subscription), it is checked whether the fbclid cookie is present. Only in the case that the cookie is present, the information is passed to Meta Platforms.

We store the click ID for 7 days, after which we only see the total number of actions.

In addition to the information of the purchase completion, the following information is also transmitted to Meta Platforms:

- Promotion (e.g. type of subscription, etc.) or product.
- Price of the promotion

In the case of newsletters and podcasts, only the name of the newsletter/podcast is transmitted.

At no time is any user-related information other than the click ID "fbclid" transferred to Meta Platforms.

The processing of data by Meta Platforms is carried out within the framework of Meta Platforms' Data Usage Policy. Accordingly, general information on the display of Meta Platforms ads, in the Meta Platforms Data Usage Policy: <https://de-de.facebook.com/policy.php>. Specific information and details about the "Meta Platforms Conversion API" and how it works can be found in the Meta Platforms help section: <https://www.facebook.com/business/help/2041148702652965?id=818859032317965>.

Google Ads advertising and remarketing

To draw attention to our offers, we place ads on Google's search network and banner ads on Google's display network (banners on third-party websites) and use Google Ads or Analytics remarketing. In doing so, we may combine ads with search terms or use custom ads to advertise products and services that you have viewed on our site. Ads remarketing lists allow us to optimize search and display campaigns if you have visited our site before.

For this interest-based advertising, Google analyzes your user behavior with cookies that are set when you click on ads or visit our websites. We and Google then receive information that you clicked on an ad and were redirected to us. Based on these evaluations, we can see which of the advertising measures used are particularly effective and can optimize them as a result.

The statistics that Google provides us with include the number of users who clicked on one of our ads and show which of our websites you were redirected to. In addition, we can target you more specifically if you have already been to our website. We can also track which search terms were clicked on particularly often and which ads lead to the purchase of a subscription, for example.

Due to the marketing tools used, your browser automatically establishes a direct connection with Google's server. We have no influence on the scope and further use of the data collected by Google through the use of this tool and therefore inform you according to our state of knowledge: Through the integration of Ads Advertising, Google receives the information that you have called up the corresponding part of our website or clicked on an

advertisement from us. If you are registered with a Google service, Google can assign the visit to your account. Even if you are not registered with Google or have not logged in, there is the possibility that the provider learns your IP address and stores it.

More information on this can also be found in the notes on website statistics and in the privacy policy of Google.

You can prevent this technology by disabling the use of cookies via your browser settings, deselecting individual types of ads in Google's ad settings, disabling interest-based ads on Google, or disabling cookies from advertising providers using the respective deactivation help of the network advertising initiative. We and Google then only receive the statistical information about how many users have visited a page and when. This can only be prevented by appropriate browser extensions.

The legal basis for the aforementioned data processing is Art.6 para.1 p.1 lit.a) DSGVO.

Personalized product recommendations

We analyze the use of our website in order to provide you with personalized product recommendations and use the Web Extend technology of our service provider Emarsys (emarsys eMarketing Systems GmbH, Märzstrasse 1, 1150 Vienna) for this purpose. We synchronize the data that we collect based on your interactions on our websites, as well as historical and offline sales data, with our Emarsys contact database. This allows us to see which email advertising has led to a purchase and to display sales data, provide personalized product recommendations in real time on websites and in emails and create customer lifecycle scoring.

If you have given us your consent for personalized online advertising, we use a cookie (scarab.visitor) to create affinity models for products and generic recommendations (for example, the most viewed or best-selling products). As soon as you have registered and logged in, we can assign your usage behavior to you as a registered user and enrich your contact data profile. To do this, we use either the hashed e-mail address or an external ID. The same explicit identification takes place when you click on a link in an email sent to you. We use the identifiers to assign you to your existing contact in our database. This allows us to log each of your interactions with

the website and synchronize them with the contact database, regardless of whether you are logged in or not.

If you are explicitly identified on multiple devices (you log in on desktop and later click on an email link on a mobile device), then the visitor cookies from both devices will be linked to the same explicit identifier, and all future visits by the user on both devices will be successfully identified and logged by the data collection scripts.

Your data is processed on the basis of Art. 6 para. 1 lit. a) GDPR with your consent. The cookies set with your consent will be deleted after one year at the latest.

You can revoke your consent at any time in the privacy settings in the footer of the website by generally refusing the creation and use of a personalized ad profile or by revoking the use of Emarsys eMarketing Systems AG.

Company presence in social media

We maintain presences in the "social media". To the extent that we have control over the processing of your data, we will ensure that applicable data protection regulations are complied with. In the following, you will find the most important information on data protection law with regard to our company websites.

Responsible for the company appearances in the sense of the General Data Protection Regulation as well as other data protection regulations are besides us:

- **Meta Platforms Ireland Limited** (4 Grand Canal Square, Grand Canal Harbour, D2 Dublin, Ireland); further informationen about privacy you can find [here](#).
- **LinkedIn** (LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Irland); further informationen about privacy you can find [here](#).
- **X** (Twitter International Unlimited Company, One Cumberland Place, Fenian Street, Dublin 2, D02 AX07 Ireland); further informationen about privacy you can find [here](#).

- **Xing** (New Work SE, Am Strandkai 1, 20457 Hamburg); further informationen about privacy you can find [here](#).

The processing of data that we use for statistical purposes in order to further develop and optimize the content and to make our offer more attractive is based on our legitimate interests in effective information and communication pursuant to Art. 6 para. 1 sentence 1 lit. f) DSGVO. This data includes the total number of page views, page activities, and data and interactions provided by visitors. These are processed and made available by the social networks. We have no influence on the generation and presentation.

In addition, your personal data will be processed for market research and advertising purposes with your consent (Art. 6 para. 1 sentence 1 lit. a) DSGVO). It is possible, for example, that usage profiles are created based on your usage behavior and the resulting interests. This allows, among other things, advertisements to be placed within and outside the platforms that presumably correspond to your interests. Cookies are usually stored on your computer for this purpose. Independently of this, data that is not collected directly from your end devices may also be stored in your usage profiles. The storage and analysis also takes place across devices; this applies in particular, but not exclusively, if you are registered as a member and logged in to the respective platforms.

Beyond that, we do not collect or process any personal data.

Since we do not have complete access to your personal data, you should contact the providers of the social media directly when asserting your data subject rights, because they each have access to the personal data of their users and can take appropriate measures and provide information.

For a detailed description of the respective processing and revocation options, please refer to the information linked below:

- **Meta Platforms** [Optout](#)
- **LinkedIn** [Optout](#)
- **X** [Optout](#)
- **Xing** Optout in den Xing-Einstellungen im Xing-Konto

What else you need to know

Controller and data protection officer

Controller is

Ultima Media Germany GmbH

Hultschiner Straße 8
D-81677 München
Germany

You can reach our **data protection officer** at

atarax Unternehmensgruppe

Luitpold-Maier-Str. 7
D-91074 Herzogenaurach
Phone: +49 9132 79800
Email: swmh-datenschutz@atarax.de.

Contact for your privacy request

Here you can ask your questions about data protection.

datenschutz@ultimamedia.de

Joint controllership

We are joint controller in the following cases.

Joint controllership Industrie-Medien-Netzwerk

The companies

- Hüthig GmbH, Im Weiher 10, D-69121 Heidelberg
- Ultima Media Germany GmbH, Hultschiner Str. 8, D-81677 Munich and
- verlag moderne industrie GmbH, mi connect, Justus-von-Liebig-Straße 1, D-86899 Landsberg

are jointly responsible for the processing of the following personal data

- name
- Business or private contact details
- Function in the company
- Area of responsibility within the company
- contact history.

for the following processing purposes

- logins
- webinars
- white papers
- Marketing and supporting companies with successful brand strategies,
- advertising campaigns and
- in product marketing through access to high-caliber target groups in high-quality environments and successful, efficient communication.

Legal basis:

- Direct advertising by email, telephone and post - the legal basis for this data processing is Art. 6 para. 1 lit. f) or Art. 6 para. 1 lit. a) GDPR. The legitimate interest in data processing is the presentation of the company, products and services for your information.
- Profiling for interest-based direct advertising - the legal basis for this data processing is Art. 6 para. 1 lit. a) GDPR.
- Creating a user account - The legal basis for this data processing is Art. 6 para. 1 lit. b) GDPR or Art. 6 para. 1 lit. a) GDPR.
- Webinars and whitepapers - The legal basis for this data processing is Art. 6 para. 1 lit. b) GDPR.
- Events - The legal basis for this data processing is Art. 6 para. 1 lit. b) GDPR.

We fulfill the data protection obligations as follows:

- The information required in accordance with Art. 13 and 14 GDPR is accessible in the respective data protection notices.
- The parties shall inform each other immediately of any legal positions asserted by data subjects. They shall provide each other with all information necessary to respond to requests for information.
- Data protection rights can be asserted with all controllers. Data subjects will generally receive the information from the office where the rights were asserted.

The data controllers store the above-mentioned data until the purposes for which it was collected or otherwise processed cease to apply or until objection or revocation, provided that there are no statutory retention periods to the contrary. The objection will be stored for a period of 3 years for the purpose of preserving evidence.

joint controllership Meta Platforms

When you visit our Meta Platforms Fanpage, we are jointly responsible with Meta Platforms for the processing of your personal data. In the following, we inform you about the associated data processing on our fan page, of which the terms of use of Meta Platforms remain unaffected:

contact details of the controllers and joint responsibility according to Art. 26 DS-GVO.

Joint controllers:

The entity responsible for this website (see information about us mentioned at the beginning).

and

Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, D2 Dublin, Ireland.

We are jointly responsible with Meta Platforms for the processing of your personal data according to the European Court of Justice (ECJ).

Appearance on the Meta Platforms Fanpage.

Scope of data collection and storage

Data	Purpose	Legal basis
User interactions (postings, likes, etc)	User communication via social media	Art. 6 para. 1 a DS-GVO

Data	Purpose	Legal basis
Meta Platforms cookies	Target group advertising	Art. 6 para. 1 a DSGVO
Demographic Data (based on age, place of residence, language or gender)	Target Group Advertising	Art. 6 para. 1 a DSGVO
Statistical data on user interactions in aggregated form, i.e. without personal reference (e.g. page activities, page views, page previews, likes, recommendations, posts, videos, page subscriptions incl. origin, times of day)	Target group advertising	Art. 6 para. 1 a DSGVO

The promotional use of your personal data is in the foreground, especially for Meta Platforms. We use the statistics function to learn more about the visitors to our Fanpage. The use of the function enables us to adapt our content to the respective target group. In this way, we also use demographic information on the age and origin of users, for example, although no personal reference is possible for us here. In order to provide the social media service in the form of our Meta Platforms fan page and to use the Insight function, Meta Platforms generally stores cookies on the user's end device. These include session cookies, which are deleted when the browser is closed, and persistent cookies, which remain on the end device until they expire or are deleted by the user. As a user, you can decide for yourself via your browser settings whether and which cookies you want to allow, block or delete. You can find instructions for your browser here: Internet Explorer, Firefox, Google Chrome, Google Chrome mobile, Microsoft Edge, Safari, Safari mobile (links). Alternatively, you can also install so-called ad blockers, such as Ghostery.

According to Meta Platforms, the cookies used by Meta Platforms are for authentication, security, website and product integrity, advertising and measurement, website features and services, performance, and analysis and

research. Details of the cookies used by Meta Platforms (e.g. cookie names, function duration, content collected and purpose) can be viewed [here](#) by following the links there. There you will also find the option to disable the cookies used by Meta Platforms. In addition, you can also change the settings for your advertising preferences there.

The collection and storage of data through the use of the above-mentioned cookies by Meta Platforms can additionally, but also at any time with effect for the future, be objected to via [this opt-out link](#).

Under the aforementioned link, you can manage your preferences regarding usage-based online advertising. If you object to usage-based online advertising with a particular provider using the preference manager, this will only apply to the particular business data collection via the web browser you are currently using. The preference management is cookie-based. Deleting all browser cookies will also remove the preferences you have set using the preference manager.

Note about Meta Platforms Insights

We use the Meta Platforms Insights function for statistical analysis purposes. In this context, we receive anonymized data on the users of our Meta Platforms fan page. However, using the filters provided by Facebook Meta Platformsook, we specify the categories of data according to which Meta Platforms provides anonymized statistics. Meta Platforms provides us with the following criteria or categories for evaluating the activities of the appearance anonymously, provided that the relevant information has been provided by the user or is collected by Meta Platforms:

- Age range
- gender
- Place of residence (city and country)
- language
- mobile or stationary page view (YouTube additionally individual device types)
- Interactions in the context of posts (e.g., reactions, comments, shares, clicks, views, video usage time)
- Time of use

This anonymized data is used to analyze user behavior for statistical purposes so that we can better tailor our offerings to the needs and interests of its audience.

We see our legitimate interest (Art. 6 para.1 f DSGVO) for data processing in the presentation of our company and our products as well as services for your information.

Sharing and use of personal data

Insofar as you interact within the framework of Meta Platforms, Meta Platforms naturally also has access to your data.

Your rights

- According to Art. 15 GDPR you have the right to request **information** about your personal data processed by us. In this context, you also have the right to obtain a copy of the personal data processed by us, in accordance with Art. 15, par. 3-4 GDPR
- In accordance with Art. 16 GDPR, you can immediately request the **correction** of incorrect data or the completion of your personal data stored by us.
- In accordance with Art. 17 GDPR, you can request the **deletion** of your personal data stored with us.
- In accordance with Art. 18 GDPR, you can demand the **restriction of processing** of your personal data.
- In accordance with Art. 20 GDPR, you can request to receive your personal data that you have provided us in a structured, common and machine-readable format and you can request the **transfer** to another person responsible.
- In accordance with Art. 7 (3) GDPR, you can **withdraw** your consent, once granted, to us at any time. As a result, we may no longer continue to process the data based on this consent in the future.
- In accordance with Art. 77 GDPR you have the right to **complain** to a supervisory authority. As a rule, you can contact the supervisory authority of your usual place of residence, your place of work or our registered office for this purpose.

Right of objection

If your personal data is processed on the basis of legitimate interests pursuant to Art. 6 (1) f GDPR or pursuant to Art. 6 (1)e GDPR, you have the right to object to the processing of your personal data pursuant to Art. 21 GDPR. In the event of such an objection, we will no longer process your personal data, unless we can prove compelling reasons for processing

worthy of protection that outweigh the interests, rights and freedoms of the person concerned or the processing serves to assert, exercise or defend legal claims.

In the case of direct marketing, you have the right to object to the processing of personal data relating to you at any time. If you object to processing for the purposes of direct marketing, the personal data will no longer be processed for those purposes.

Data protection information in the GTC

With this privacy policy, we fulfill the information requirements according to the GDPR. Our General Terms and Conditions also contain data protection information. In these, it is once again described in detail how in particular the processing of your personal data is carried out, which we require for the execution of the contracts and for the purpose of an identity and credit check.

Links to other websites

Our websites can contain links to websites of other providers. We have no influence on this and do not monitor the compliance of other providers with applicable data protection provisions.

Alterations of the privacy policy

We reserve the right to alter and/or adjust this data protection declaration at any time, taking into consideration the current applicable data protection provisions.