



Privacy Notice

13.07.2026

When you visit a website, register for a service, handle contracts, or interact with us in other ways, personal data is processed. This happens both automatically (e.g. your IP address) and when you actively provide data (e.g. when you place an order). The General Data Protection Regulation (GDPR) requires us to inform you about this processing. For example, you should know what purposes we pursue, how long your information is stored, which legal basis the processing is based on, and which recipients of data there may be. This is what this privacy policy is about.

As a rule, Zeitverlag Gerd Bucerius GmbH & Co. KG, Buceriusstraße, entrance Speersort 1, 20095 Hamburg, is the controller responsible for the processing of personal data. Further information about the company as well as contact options can be found at the end of this Privacy Notice.

DIE ZEIT Customer Service

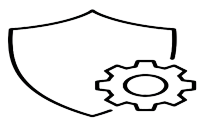
If you have any questions about your subscription, cancellations, or a withdrawal, please contact only our



Companies of the ZEIT publishing group

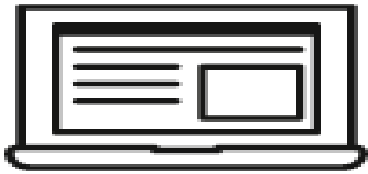
The ZEIT publishing group includes the following companies: Zeitverlag Gerd Bucerius GmbH & Co. KG, ZEIT Sprachen GmbH, ZEIT Akademie GmbH, Studio ZX GmbH, ZEIT Weltkunst Verlag GmbH, academics GmbH, Good Jobs GmbH, and e-fellows.net GmbH & Co. KG.

For example, we offer journalistic content, travel, products, seminars, events, and special offers for subscribers.



Privacy settings

This is how you can change your privacy settings: click on “Withdraw consent” or delete the cookies in your browser. The next time you visit zeit.de, the consent banner will appear again, where you can choose between access with advertising tracking and the paid zeit.de ad-free subscription.



Use of the website

Websites have different functions and ways to interact. Sometimes you can view content or use an online form to contact us. On other pages, you can register. Depending on the website, the scope of data processing varies.

Logfiles

When you visit a website, technical usage data (so-called log data) is processed temporarily. This data is transmitted by your browser and includes, among other things, your computer's IP address, the client request (file name and URL), the HTTP response code, and the website from which you came to our website.

The data processing described is permitted to protect legitimate interests (Art. 6(1)(f) GDPR). We depend on achieving the greatest possible reach for our companies and content. Operating a website is essential for this. The processing happens automatically and cannot be prevented. It is technically necessary in order to access a website.

The log data is deleted or anonymized as soon as it is no longer needed.

Requests via the Website

We offer various ways to contact us (e.g., online contact form, email contact address, feedback form). We process the data and information you provide in order to respond to your request. We use feedback on our products or reports of errors to improve them and to fix errors.

The data processing in a (pre-)contractual context, for communication and for fixing errors is permitted by law (Article 6(1)(b), (f) GDPR, Section 25(2) TDDDG). Providing your personal data is necessary in

order to communicate with us and, in the case of feedback, to enable error correction.

We store the data for a period of 6 months. If you register with us or if there is another type of further contact, your data will continue to be stored and will only be deleted after the applicable statutory retention obligations have expired.

Registration

You have the option to register using your email address and gain access to extended functions and content of the website. In this process, a user account linked to the email address is created, to which the actions you carry out on the website can be assigned.

The legal basis for the processing of personal data is the user relationship created by the registration (Art. 6(1)(b) GDPR). Providing your data is necessary for the registration, as otherwise no user account can be created for you.

Your data will be stored for the duration of the user relationship and any statutory retention obligations.

Study Interest Assessment

As a registered user, you can take our Study Interest Assessment and receive detailed feedback on suitable degree programmes. The test is multi-dimensional and takes into account both your interests and your own self-assessment regarding strengths and weaknesses.

The processing of personal data to provide a service is legally permitted (Art. 6(1)(b) GDPR). Providing your personal data is necessary in order to complete the Study Interest Assessment and receive a result.

We store the test result for the duration of your registration. If you delete your profile, the related data will also be deleted.



Use of zeit.de

On www.zeit.de you will find a selection of editorial content from the ZEIT editorial team and ZEIT Verlag, as well as games, videos and podcasts. In order to finance the provision of this content, we offer our advertising customers advertising space for usage-based advertising. The data generated when you access the website is used to create a user profile and to display advertising that is as relevant to you as possible.

If you do not want to see personalised advertising and would like to prevent ad tracking, you can alternatively use our paid zeit.de ad-free subscription. This gives you access to the same content, but without personalised ad tracking and without the display of usage-based advertising.

Before you access www.zeit.de, you can actively choose between using the website with ad tracking or the zeit.de ad-free subscription.

Usage options

You can choose between the two usage options. Before you can access the website, the following is displayed to you:

Willkommen auf ZEIT ONLINE

Für die Verbesserung und zur Finanzierung unseres Angebotes erheben und verarbeiten wir und unsere bis zu 157 Partner personenbezogene Daten. Dazu speichern wir Cookies auf Endgeräten, nutzen persönliche Identifikationsmerkmale wie Gerätekennungen oder IP-Adressen und erfassen individuelles Nutzungsverhalten.

Die Verarbeitungszwecke für diese Daten sind: personalisierte Werbung mit Profilbildung, externe Inhalte anzeigen, technisch erforderliche Cookies (Sicherheit, Anmeldung, Kommentarbereich), Push-Benachrichtigungen/Kommunikation, Optimierung des Angebots (Marktforschung, A/B-Testing, Inhaltsempfehlungen).

Mit Werbung lesen

Durch das Klicken des Buttons „Zustimmen und weiter“ stimmen Sie der Verarbeitung der auf Ihrem Gerät bzw. Ihrer Endeinrichtung gespeicherten Daten wie z.B. persönlichen Identifikatoren oder IP-Adressen für diese Verarbeitungszwecke gem. § 25 Abs. 1 TTDSG sowie Art. 6 Abs. 1 lit. a DSGVO zu.

Zustimmen und weiter

Werbefrei-Abo

Oder nutzen Sie zeit.de ohne Werbettracking und nahezu ohne Werbung, indem Sie zeit.de Pur abonnieren oder sich hier mit ihrem [bestehenden Pur-Abo einloggen](#). Informationen zur Datenverarbeitung im Pur-Abo finden Sie in [unserer Datenschutzerklärung](#) und in den [FAQ](#).

zeit.de Pur abonnieren

Details zum Tracking finden Sie in der [Datenschutzerklärung](#) und im [Privacy Center](#). Einzelnen Zwecken der Datenverarbeitung können Sie über den Button „Einstellungen“ oder den Menüpunkt Cookies & Tracking am Ende jeder Seite zustimmen oder sie teilweise ablehnen. Ihre Zustimmung insgesamt können Sie jederzeit über den Link Privacy Einstellungen am Ende jeder Seite entziehen.

Einstellungen

[Mit Pur-Abo anmelden](#)

[PUR-Abo-FAQ](#)

[Impressum](#)

[AGB](#)

[Datenschutz](#)

Consent Management Platform

To manage data processing on the website in compliance with data protection law, we use the Transparency and Consent Framework of IAB Europe (TCF). This set of rules comes from an online marketing industry association, the Interactive Advertising Bureau Europe (IAB Europe). It defines the purposes and legal bases for processing and provides technical standards for obtaining consent. Implementation

takes place via the consent prompt shown before you access the website, which we implement using the Sourcepoint tool (provided by Sourcepoint Technologies, Inc., 228 Park Avenue South, #87903, New York, NY 10003-1502, USA). We store the settings you have selected by setting cookies.

The data processing that takes place on your end device is permitted or necessary to safeguard our legitimate interests or to provide our service (Art. 6(1)(f) GDPR, Section 25(2) no. 2 TDDDG). In order to operate our website in compliance with data protection law, we must electronically document whether consent has been given and whether it has been withdrawn. Otherwise, in case of doubt, we cannot prove that you have consented to certain processing activities. In this respect, the data processing is necessary in order to use our website.

The cookie is stored until you withdraw your consent and is deleted after 13 months at the latest.

Ad-supported access

If you want to use the selection of editorial content without an additional payment, we finance our journalism by displaying personalised advertising and political advertising based on your usage behaviour and your inferred interests. Our advertising partners and we use various technologies for ad tracking, which also involve data processing on your end device (in particular through cookies). You can find detailed information on which specific data processing takes place when you access www.zeit.de in the Privacy Center.

The data processing described is based on your consent (Art. 6(1)(a) GDPR, Art. 18(1)(b) TTVO, Section 25(1) TDDDG). In order to use the service, you must consent to the analysis for the purpose of presenting our personalised advertising. Otherwise, you cannot access the website or the content. You can withdraw your consent at any time. This means that you can then only use the service after taking out a

PUR subscription. This also applies to the paid ZEIT Digital subscription.

You can see the storage periods of the data generated and the cookies set on your end device in the Privacy Center.

zeit.de ad-free subscription

As a zeit.de ad-free subscriber, you can use the service without ad tracking and personalised advertising. However, non-personalised advertising may still be displayed.

The processing of personal data when you use our website with a zeit.de ad-free subscription is permitted for the performance of the user contract (Art. 6(1)(b) GDPR). Providing the data requested during paid registration is necessary in order to grant you access and to bill for the service.

We store the contractual data that arises for as long as this is necessary to comply with statutory retention obligations. Depending on the date and document, these are 6 or 8 years.

Content from social networks

We integrate content and features from social media platforms on our website (e.g. Facebook, YouTube, Instagram or TikTok). If you use a share button or read an article with embedded content, usage data such as your IP address is transmitted to these social media platforms.

These services are inactive by default and must be activated by you. The legal basis for the data processing is therefore your consent (Art. 6(1)(a) GDPR, Section 25(1) TDDDG). Providing your data is voluntary and not required to use www.zeit.de. However, you will then not be able to view content from social media platforms or use their embedded features.

You can find the storage periods of the data generated and the cookies set on your end device in the Privacy Center.

Personalised editorial content recommendations

We use various technologies to create a publisher-specific reading profile for the device you use. We use the data generated about your reading behaviour to suggest personalised editorial content to you in selected places. This means you will see more content that matches your specific interests.

The legal basis for processing in connection with personalised content recommendations is your consent (Art. 6(1)(a) GDPR, Section 25(1) TDDDG). Providing your data is not required. You can also use the selection of editorial content on www.zeit.de if you do not give consent.

You can find information on data storage and the lifetime of the cookies set on your end device in the Privacy Center.

Measurement of usage

We carry out statistical analyses of how our content is used in order to improve our service and make it more interesting. The measurement relates, for example, to which content was read and which page a user came from.

The permissibility of the processing carried out is based on our legitimate interests (Art. 6(1)(f) GDPR). In order to maintain and improve our service, we rely on these statistical analyses. The processing that takes place on your end device is necessary in order to use the service (Section 25(2) no. 2 TDDDG).

You can find information on the storage period in the Privacy Center.

Secure operation of the website

Our digital services and subscriptions may only be used in accordance with the respective applicable contractual agreements. In order to detect misuse and respond appropriately, personal data (e.g., login data, devices, login frequency, date and time) is processed in our database to protect our rights and to identify unusual usage. In particular, we defend against credential stuffing (automated testing of leaked access data), brute-force/password-spraying attacks, session hijacking/session fixation, cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection/injection attacks on backend systems, and the scraping of our journalistic content by AI bots.

The legal basis for this processing is the user relationship that has been established and our legitimate interests (Art. 6(1)(b), (f) GDPR, Section 25(2) No. 2 TDDDG). The content on zeit.de embodies the journalistic work of our company and is our most important economic asset. We must protect it through technical measures in order to maintain our business model. The data processing is automated and cannot be prevented.

No separate data storage takes place for these purposes.

A/B testing

We carry out so-called A/B testing, in which we show you our website with slightly varied content. This allows us to analyse our service, improve it on a regular basis and make it more interesting.

The legal basis for carrying out A/B testing is your consent (Art. 6(1)(a) GDPR, Section 25(1) TDDDG).

No separate data storage takes place for this processing.

Online games

We offer various online games. The entries made by logged-in users are stored in the database under their user account so that game progress can be retrieved. The game progress of users who are not logged in is stored in a session cookie. In some cases, you can choose a username of your choice to be displayed in a high score table.

The data processing that takes place is legally permitted within the scope of the user relationship and the provision of the service (Art. 6(1) (b) GDPR, Section 25(2) no. 2 TDDDG). In order to use the online games, the entry of data and/or the processing of data on your end device is necessary.

The cookies set expire after 10 months at the latest.

Comments

As a registered user, you can leave comments on our articles. These are published on the website together with the username you provide. When choosing a username, we recommend using a pseudonym instead of your real name.

In addition, you can respond to other users' comments and, for example, mark them with "Like".

We want to give our users the opportunity to actively participate in discourse and the formation of opinions. For this, it is necessary that comments and reactions are published and can be read by others. As digital letters to the editor, comments fall under the media privilege.

They remain publicly accessible for an unlimited period of time, even if a user account is deleted (the username will then also no longer be available). In the event of a breach of the Netiquette, comments may be deleted or edited by the editorial team.

Podcasts on third-party platforms

You can also use our Z+ podcast offering on third-party platforms (e.g. Apple Music or Spotify). To make this possible, personal data must be shared in pseudonymised form. This only happens if you actively enable your Z+ offerings on the third-party platform. No further personal data relating to your ZEIT user account is processed.

The data processing is legally permitted for the performance of the contract that is concluded (Art. 6(1)(b) GDPR). The transfer of the personal data mentioned above is necessary to give you the option to use content on third-party platforms.

Information on the storage period can be found on the respective third-party platform.

Contact between users

Via an online contact form you can send messages directly to other users. The message you enter will be transmitted, and the receiving user will see your email address so they can reply. Further data that is technically necessary may be generated when the form is submitted (e.g. a timestamp). Before you send a message, you will be explicitly informed that your email address will be disclosed to the recipient.

The legal basis is the user relationship pursuant to Art. 6(1)(b) GDPR. Providing the email address and the message is necessary in order to use this function. Without this information, delivery to the other user is not possible.

Messages are not stored on zeit.de. They are stored exclusively by the respective recipients in their mailboxes.

ZEIT single sign-on account

Some services require you to have a so-called single sign-on account. This requires an email address and a password of your choice. With

this account, you can access various services.

The data processing carried out as part of the resulting user relationship is permitted by law (Article 6(1)(b) GDPR). Providing the requested data is necessary for registration.

Your data is stored for the duration of your account's existence.

HeyStudium AI chatbot

We provide an AI-powered chatbot that users can use to get advice on study programmes and universities and to interact directly. For this purpose, we process the content entered in the chat as well as usage data required for session management in order to generate suitable answers and provide the consultation.

The legal basis for this processing is the performance of the user relationship (Article 6(1)(b) GDPR) on zeit.de. Providing the data entered in the chat is necessary to understand and answer your request. Without this information, the chatbot cannot be used. Chat histories are analysed and used for optimisation (Article 6(1)(f) GDPR). This is about improving the quality of the chatbot's answers and consultation. For example, if users end the chat and leave the page because of certain answers or questions, this should be detected and, if possible, fixed.

We store chat histories for 2 months and then delete them.

Liveblog

On zeit.de, we have embedded a live blog to display content, provide a live ticker, and report on current events in real time for journalistic purposes. In doing so, usage data and device data are processed (also on the end device).

The legal basis for the processing is the user relationship (Art. 6(1)(b) GDPR) and the legitimate interest in providing current journalistic content in a user-friendly format that is continuously updated (Art. 6(1)(f) GDPR). The data processing on the end device is legally permitted for the provision and embedding of the live blog on zeit.de (Section 25(2) TDDDG). The processing takes place automatically when the live blog is accessed and cannot be prevented.

There is no separate storage period for this purpose. The data is therefore processed only for as long as this is necessary to provide and operate the live blog.

Community AI Feature

We have integrated an AI community feature on zeit.de to summarise user comments on our articles and display them in a clear format. In addition, comments with a particularly high number of reactions are highlighted. In particular, the content of the comments, the usernames used, and the number of reactions may be displayed.

The processing is carried out to safeguard our legitimate interests (Article 6(1)(f) GDPR). This consists of presenting discussions on our pages in a clearer way and enabling users to get a quick overview of comments that are particularly frequently supported or relevant. The AI community feature cannot be deactivated.

The comments are processed via the community feature for the duration of their publication on zeit.de.



Promotions, contracts, and subscriptions

The companies of the ZEIT publishing group offer various products and services. If you, for example, take out a subscription, book a trip, or participate in a competition, different personal data will be collected, used, and passed on to other companies for the purpose of contract fulfillment.

Taking out a subscription

When you take out a subscription, we collect various data from you. We use this data to provide the subscription and to invoice you.

The data processing is permitted by law for the performance of the resulting contract (Article 6(1)(b) GDPR). Providing the requested data is required in order to conclude the subscription.

Your data record is stored in our customer database for the duration of your subscription. Any storage beyond this period serves to comply with the statutory retention obligations applicable to us.

Taking out a trial subscription

We regularly offer the option of taking out a trial subscription so that you can test our services. Depending on the product, different data is collected and used to provide the offer.

The data processing is permitted for the performance of resulting contracts as well as for the purposes of our legitimate interests (Article 6(1)(b), (f) GDPR). Providing your data is voluntary, but necessary for us to provide our offer. If taking out a trial subscription is a prerequisite for participating in a competition, failure to provide your data will result in you being unable to participate.

Contract documents inevitably include tax-relevant commercial and business correspondence, which is subject to a statutory retention period of up to 8 years. In order to be able to trace all processes and

provide information in the event of an official audit, we store all documents and data for at least this period.

Shared subscription

As a digital subscriber, you have the option to share your subscription with another person. The co-usage authorization ends no later than the end of the digital subscription, but you may withdraw a shared access at any time.

The data processing takes place for the provision of the shared subscription and for the purposes of legitimate interests (Article 6(1)(b), (f) GDPR). Our subscribers should have the opportunity to let others benefit from our content. Providing the email address of the beneficiary is necessary to grant access. The invited person may object to receiving an invitation at any time.

If the email address of the invited person may not be stored for other purposes for a longer period, it will be deleted upon expiration of the invitation after 3 months or stored until the end of the co-usage right.

Payment (service providers)

We use payment service providers to offer you as many payment methods as possible with a single click. These providers are responsible in particular for forwarding the amounts paid to us and for controlling payment flows.

The integration of payment service providers and the transfer of your data that takes place in this context is permitted for the purposes of our legitimate business interests (Article 6(1)(f) GDPR). We are not able to map the necessary processes in a legally compliant manner ourselves. For this reason, we have chosen external payment service providers. Data processing occurs automatically when you select one

of the payment methods offered and complete the payment on the provider's website. The data processing is necessary for the payment.

We do not store any bank details in our systems. We only retain information on the amounts to be paid and whether they have been settled.

Protection against bad debt

We process personal data in order to decide on the conclusion of contracts. In particular, we check whether claims existing in our favour have been duly settled in the past. The result of this check is taken into account in our decision.

The legal basis for the processing is Article 6(1)(f) GDPR. Our legitimate interest is to protect ourselves against bad debt losses and fraudulent conclusions of contracts. This also serves the economically responsible exercise of our private autonomy. We use only the data provided when placing an order as well as the information already stored in our database about previous orders.

We store data on unpaid claims beyond the expiry of statutory retention obligations.

Protection against multiple trial subscriptions

We store data about individuals and orders to prevent multiple trial subscriptions and to reject the conclusion of (renewed) contracts for economic or legal reasons. In doing so, we flag records with attributes.

The processing is lawful because it is necessary for the purposes of our legitimate interests (Art. 6(1)(f) GDPR). We offer trial subscriptions so that our products can be tested. We may prevent excessive use of this offer on the basis of the applicable principle of freedom of contract and

thereby protect our business interests. For this purpose, we compare the data with previous orders and transactions.

We store the data for as long as necessary to review and prevent abusive orders.

Prize draw

We regularly conduct prize draws and collect various data for this purpose. We process this data to verify eligibility, determine and notify the winner, send the prize, and, if applicable, publish a winner list.

The data processing carried out in the context of a prize draw is permitted by law (Article 6(1)(b) GDPR). Participation constitutes a type of contract for which the data we request is necessary. If you do not provide the requested data, you cannot participate in the prize draw.

The data collected in connection with our prize draws is stored until the process has been fully completed (determination and notification of the winners, dispatch of the prize). Further storage may occur as part of associated processing activities (e.g., taking out a trial subscription or signing up for a newsletter, if this was a prerequisite for participating in the prize draw). Any publications are not subject to a time limit.

Surveys

We conduct online surveys to assess the quality of our services or to gather information about interests. Opinions and views are collected, which we analyze and use to improve our services. If prizes are drawn among survey participants, we additionally collect contact details that are not linked to the survey results.

The data processing carried out serves the purposes of our legitimate business interests (Article 6(1)(f) GDPR). We want to take our customers' opinions into account when developing our services and need data that is as meaningful as possible for this. Participation in our surveys is voluntary. Providing contact details is necessary in order to be considered for a prize draw.

We store the anonymized survey results for an unlimited period. Non-anonymizable data is stored for a period of 6 months from the time of collection. Contact details are stored for the duration of their subsequent use.



Events and seminars

We regularly organise events and seminars on various topics. Registration is usually done online and, depending on the event, requires the provision of different data.

In-Person Events

If you would like to register for one of our events, you can usually do so online. Depending on the event, different data is requested and passed on to our partners and sponsors (e.g. to create participant lists or name badges, or to enable the transmission of documents). If members of the constitutional bodies of the Federal Republic of Germany (e.g. politicians) are guests at an event or give a presentation, we are obliged to pass data on to the Federal Criminal Police Office (Bundeskriminalamt) and other authorities. This allows potential sources of danger to be identified and, if necessary, appropriate risk-prevention measures to be taken. For some event formats, a list of participants is published in the printed programme at the conference.

The data processing that takes place in the course of running the event is permitted to enable your participation and to safeguard legitimate interests (Art. 6(1)(b) and (f) GDPR). Our partners and sponsors are your subject-matter contacts and need the participants' data for handling the event. The information marked with an asterisk is required for the organisation of our events and entitles you to attend. Any additional information is voluntary.

We store the data relating to your participation at least for the duration of the applicable statutory retention obligations. As a rule, this is 8 years.

Online Events

We conduct our digital events on online platforms. Depending on the event and how participants use it, different personal data is processed (e.g. name, video, audio). Participation generally does not require you to create an account with the platform used. It is usually sufficient to log in via the web interface using your access data. During participation, metadata (e.g. IP address, device/hardware information), connection data (e.g. phone number, country name, start and end time) and—depending on the event—also content data (e.g. chat history, audio, video) are processed.

The lawfulness of the processing is based on our legitimate interest (Art. 6(1)(f) GDPR). Digital events are an alternative and supplement to traditional in-person events. The interactive design and running of events is only possible with software that provides the necessary functions and capacity. The meta and connection data are information that is necessarily generated when the service is used. Otherwise, no connection can be established to the device used. You decide yourself which content data is processed. You can switch off the camera or microphone at any time and prevent the processing of data in this way. Using the other functions is also voluntary.

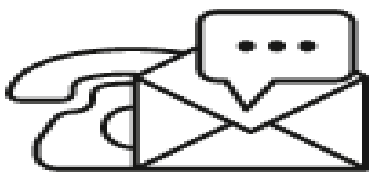
As a rule, our digital events are not recorded.

Video and Photo Recordings

Video and photo recordings are regularly made at our events. We, as well as our partners and sponsors, use them to document the event and present it to the public. The recordings may be published in print or digital form (e.g. on websites or social networks).

The processing of video and photo recordings is permitted to safeguard legitimate interests (Art. 6(1)(f) GDPR). We organise events that attract public attention, featuring personalities from business, politics and culture. There is an increased public interest in receiving information about the content of the event, the people attending, and the general conditions. As a rule, both group and individual recordings are made. As a participant, you can leave the recording area at any time.

Video and photo recordings are generally stored without any time limit. If they are published on the internet, they may also remain accessible there for an unlimited period.



Communication

We use various communication channels to get in touch with you, to receive messages, or to provide you with interesting offers and information. Advertising communication is important for our company in order to be economically successful. You can object to the use of your personal data for advertising purposes at any time and/or unsubscribe from our email newsletters via the unsubscribe link at the end of each newsletter.

Newsletter

We offer various newsletters that you can subscribe to by providing your email address. You will then receive information about various offers (from us or from third parties).

Using your email address to send our newsletters depends on your consent (Art. 6(1)(a) GDPR). Providing your data is voluntary and has no effect on any contractual relationship you may have with us. If subscribing to a newsletter is a requirement for participating in a prize draw or receiving editorial content (e.g. in the form of an eBook), failure to provide the data means that you cannot participate or will not receive the content.

Your email address will be stored in our newsletter database for as long as your consent exists and afterwards to document your subscription and unsubscription. If you withdraw your consent, you will no longer receive newsletters.

Editorial Newsletters

We offer various editorial newsletters, which you can in some cases subscribe to separately or receive automatically as an additional part of a subscription.

We use your email address to send our editorial newsletters either based on your consent (Art. 6(1)(a) GDPR) or because this is legally permitted on the basis of a contract (Art. 6(1)(b) GDPR). Where consent is used, providing your data is voluntary. If the sending takes place as part of a contract, providing your data is required.

Your email address will be stored in our newsletter database for as long as your consent or a contract exists and afterwards to document your subscription and unsubscription. If you withdraw your consent, you will no longer receive newsletters.

Recommendation of Similar Offers

We use the email address you provide when you log in, register, place an order, or make a booking to send you advertising for our own similar offers.

The use of email addresses to send our own similar offers is expressly permitted by law and does not depend on consent (Section 7(3) UWG). However, providing your personal data in this context is voluntary, and you can object at any time (either by contacting us or via the link at the end of each advertising email).

If you object to the use for advertising purposes, your data will be deleted or blocked for advertising. Deletion is usually not possible because we must continue to store the data collected during a login, registration, order, or booking in order to comply with statutory retention obligations.

Newsletter Performance Measurement

For newsletter performance measurement, we process open and click rates and create recipient profiles. We use the resulting data to improve the newsletter and tailor it to your interests and reading habits.

The processing is carried out to safeguard our legitimate interests and is therefore lawful (Art. 6(1)(f) GDPR). We need to be able to understand whether our marketing measures are successful. Providing your data is voluntary. You can disable performance measurement separately at any time.

The resulting data is pseudonymised or anonymised and stored for an unlimited period.

Postal Advertising

We use the postal addresses stored by us, as well as addresses provided by contractual partners, to send offers and information by post.

The use of data for sending postal advertising is permitted in order to safeguard legitimate interests (Article 6(1)(f) GDPR). From an economic perspective, we rely on offering our services to existing and potential customers. In all areas, it is important to actively approach people and send information.

The retention period for postal addresses depends on whether you are a customer or whether we purchased the address. We must store customer data for up to 8 years to comply with statutory retention obligations. Purchased data is used for advertising mailings and is then deleted.

Advertising by third parties

We provide the postal addresses stored by us to companies and donation organisations so that they can send you offers and information.

The disclosure for the purpose of advertising is carried out to safeguard legitimate interests (Art. 6(1)(f) GDPR). All companies involved are economically dependent on acquiring new customers and retaining existing customers. You can object to the transfer of your postal address to third parties at any time, without this having any impact on any existing contractual relationship.

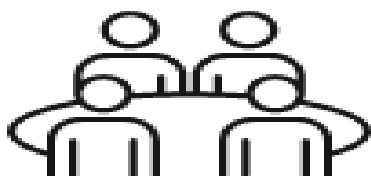
We must store customer data for up to 8 years in order to comply with statutory retention obligations. However, in the event of an objection, we will no longer transfer your postal address to third parties for advertising purposes.

Marketing Calls

We use your phone number to inform you about offers and news.

Processing is based on your consent (Art. 6(1)(a) GDPR, Section 7a(1) UWG). We are legally required under Section 7a UWG to document your consent to telephone advertising and to keep it for 5 years from the time it is given and after each use. This applies regardless of whether you gave us your consent online, in writing, by email, by phone, or in any other way. If you give your consent by phone, we will, with your consent, make a recording of you giving your consent and store it together with your contact and contract data. Providing your phone number for advertising purposes is voluntary. Your consent expires automatically 2 years after the end of your last active subscription.

Storage ends no later than 7 years after the end of your last active subscription. After that, the data will be deleted (we are legally required to retain it).



Joint controllers

ZEIT publishing group

Due to the close cooperation within the ZEIT publishing group, mutual data exchange as well as the shared use of systems and applications are unavoidable. For this reason, some processing operations take place under joint controllership. The agreement concluded accordingly between the involved ZEIT companies pursuant to Article 26 GDPR regulates in particular who is responsible for complying with the various obligations under the GDPR.

General infrastructure and communication

The companies of the ZEIT publishing group use a shared infrastructure and communicate via centrally managed devices. Zeitverlag Gerd Bucerius GmbH & Co. KG provides the essential telecommunications services and applications and, together with the other companies, is jointly responsible for the data processing that takes place.

Joint controllers: Zeitverlag Gerd Bucerius GmbH & Co. KG, ZEIT Akademie GmbH, Studio ZX GmbH, ZEIT Sprachen GmbH, academics GmbH, ZEIT Weltkunst Verlag GmbH

Data Warehouse

To analyze, monitor, and optimize advertising measures, we process personal data in a data warehouse that is separate from the production systems. The information is pseudonymized there and used for specific questions, for group profiling, and for creating engagement and propensity scores.

If we have obtained consent for the collection of the data, any further processing is also carried out on this basis (Art. 6(1)(a) GDPR). Otherwise, the analysis and internal provision of the pseudonymised data are carried out to safeguard our legitimate corporate interests (Art. 6(1)(f) GDPR). In order to make economically sound decisions and remain competitive, we need to understand our customers' requirements, identify changes, and be able to respond to them.

The duration of pseudonymized storage in the data warehouse is based on the retention periods in our other systems (e.g., newsletter database, event database). When the data can be deleted there, it can no longer be accessed via the data warehouse.

Joint controllers: Zeitverlag Gerd Bucerius GmbH & Co. KG, ZEIT Sprachen GmbH, academics GmbH, Studio ZX GmbH, ZEIT Akademie GmbH

Customer care and service center

To process questions and complaints, as well as to provide our vacation and relocation services, subscribers' personal data is made available to the responsible employees in a central system. We use your data to communicate with you and to set up the services you request.

The processing takes place within the framework of a contractual relationship and is therefore permitted by law (Article 6(1)(b) GDPR). Providing your data is necessary for us to deliver our services.

The storage of your personal data, in the case of an existing or former subscription, is based on the statutory retention periods required for compliance with tax and commercial obligations. The data arising from customer care and the use of our services is subject to the same retention period.

Joint controllers: Zeitverlag Gerd Bucerius GmbH & Co. KG, ZEIT Akademie GmbH

Subscription management and marketing

We process the personal data of our subscribers for the initiation and performance of subscription contracts as well as for carrying out various marketing activities. In addition to master data, information about services received and past contractual relationships is also processed. In our marketing activities, we take into account what may be of interest to the recipients and provide suitable offers.

The processing carried out as part of subscription management serves the performance of a contractual relationship and is therefore permitted by law (Article 6(1)(b) GDPR). Providing your data is necessary for us to deliver our services. We base marketing activities either on our legitimate business interests (Article 6(1)(f) GDPR), the UWG exemption (§ 7(3) UWG), or your consent (Article 6(1)(a) GDPR).

The data stored for managing your subscription is subject to various statutory retention obligations. We store all contract data for a period of at least 8 years. If you object to the use of your data for marketing purposes, the data will be processed in a restricted manner and marked with a marketing block.

Joint controllers: Zeitverlag Gerd Bucerius GmbH & Co. KG, ZEIT Akademie GmbH

Other companies

The use of some services takes place jointly with the respective provider, so that an agreement on joint controllership pursuant to Article 26 GDPR must also be concluded here. As a rule, this is an integral part of the terms of use and is provided by the provider in a standardized form. In some cases, the joint controllership also concerns the organization of events or joint projects.

Criteo SA

We use cookies and process data on your device in order to obtain information for the delivery of advertising. Among other things, we analyze which content you have viewed on our website and display matching recommendations (on our site and on the sites of other operators).

Data processing takes place only with your consent (Article 6(1)(a) GDPR). Providing your data is voluntary and is not a requirement for accessing the website.

The processing described is carried out under joint controllership with the provider of the analytics service (Criteo SA, 32 Rue Blanche, 75009 Paris, France). We have concluded an agreement with the company pursuant to Article 26 GDPR and defined who must fulfill which GDPR obligations. Among other things, we are obliged to inform you about

the joint controllership with Criteo SA and to point out that technologies such as cookies and pixels are used on our website. It is also our responsibility to obtain valid consent.

You can reach the Data Protection Officer of Criteo SA at dpo@criteo.com. The data protection supervisory authority responsible for the company is the [Commission Nationale de l'Informatique et des Libertés \(CNIL\)](#) in France.

Further information on data processing can be found in the [Criteo SA privacy notice](#).

Outbrain UK Ltd.

A pixel is integrated on our website, which is used, among other things, to process cookie IDs, user IDs and IP addresses in truncated form. The resulting usage data is used for advertising tracking and for displaying personalised recommendations.

Data processing via the pixel only takes place with your consent (Art. 6(1)(a) GDPR). Providing your data is voluntary and is not a requirement for accessing the website.

The processing described takes place under joint controllership with the provider of the pixel (Outbrain UK Limited, 121 Kingsway, First Floor, London WC2B6PA, United Kingdom). In an agreement pursuant to Art. 26 GDPR, the provider and we have set out our respective obligations regarding compliance with data protection requirements. As the website operator, we are in particular obliged to ensure that a legal basis for the processing exists, to use a consent management platform to obtain consent, and not to use usage data to discriminate against individuals. Outbrain UK Limited must, among other things, provide transparent privacy information about the pixel, ensure that an appropriate agreement is concluded with us, and comply with data subject requests. Furthermore, there is a mutual obligation to cooperate in data protection matters.

You can contact Outbrain UK Limited directly via the email address privacy@outbrain.com. You can reach Outbrain UK Limited's Data Protection Officer at ePrivacy GmbH, Burchardstraße 14, 20095 Hamburg, and at privacy@eprivacy.eu. The data protection supervisory authority responsible for Outbrain UK Limited is the [Information Commissioner's Office](#).

Further information on the processing of data can be found in the [Outbrain UK Limited Privacy Notice](#).

Utiq SA/NV

The Utiq technology is provided by Utiq SA/NV, a European AdTech company that works with participating telecommunications network operators (see the list [here](#)), who contribute to operating the technology. The Utiq technology enables websites such as ours that use the Utiq technology to carry out our digital marketing activities.

We use the Utiq technology on our website. If you consent to activating this technology, we will use it to recognise you as the same website visitor and to collect insights about your usage behaviour on our website. This allows us to offer you personalised content and advertising or to carry out analyses, depending on which additional consents you have given us for these purposes.

The Utiq technology is switched off by default and requires your consent in order to be activated and used. The technology is only available if you are a customer of one of the participating telecommunications network operators.

For certain phases of the data processing, we act as joint controllers together with Utiq. As part of this joint controllership:

- we obtain your consent to use the Utiq technology; this also applies to the processing operations carried out by Utiq and your telecommunications network operator;

- we provide you with a specific link at the bottom of our website through which you can obtain information about the technology and how to manage it;
- UtIQ provides you with a privacy portal ([consenthub](#)) to facilitate the exercise of your data protection rights and to enable you to easily manage your consents with UtIQ; at any time, in one place.
- Regardless of the fact that you can exercise your rights in relation to each controller, UtIQ acts as the joint contact point for all questions or concerns you may have in connection with the UtIQ technology.

Via the UtIQ privacy portal ([consenthub](#)) you can view and withdraw all consents you have given for the use of the UtIQ technology across all websites participating in UtIQ. You can also withdraw your consent that applies only to this website [here](#).

You can find more information about the UtIQ technology in the [UtIQ Privacy Statement](#).

iq digital media marketing GmbH

We work together with iq digital media marketing GmbH to manage our advertising partners on zeit.de. This specialised service provider markets the advertising space for us and takes care of integrating advertisers on our pages. In doing so, iq digital media marketing GmbH processes personal data that is collected on zeit.de. This is also done via other parties involved, in particular providers of marketing tools, agencies and advertisers. Depending on their specific role and depending on the purpose of the processing, these parties involved act as joint controllers within the meaning of Art. 26 GDPR.

The personal data jointly processed by us and iq digital media marketing GmbH includes cookie IDs, IP addresses, MAC addresses, device IDs, the browser used and data from the browser (e.g. resolution or language setting), the operating system used and data about the operating system (e.g. version number, screen resolution),

the end device used, the user's behaviour on zeit.de and/or movement data (which articles were read, which offers were visited, which links were clicked, etc.), referrer URL, date and time of the visit and time spent on zeit.de, geographic location, user data (email addresses, mobile phone numbers, but also IP addresses and other online identifiers) and profile-identifying identifiers generated on the basis of partner-specific IDs or identifiers. Not all of this data is processed in every case. This depends on which marketing tools were active in the individual case.

We and iq digital media marketing GmbH have undertaken to be bound by the respective current rules of the IAB TCF. These rules precisely define which personal data is processed in the specific individual case by the providers of marketing tools, agencies and advertisers involved.

When you access zeit.de, you have the option of determining, via the appropriate settings in the consent banner, the scope of the processing of personal data and access to and/or the storage of information on your end device. You can withdraw your consent at any time. Depending on the settings, technical signals about the existence of the legal basis are transmitted to the parties involved in the processing. iq digital media marketing GmbH markets zeit.de on this basis.

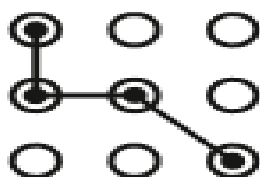
The following processing operations fall under joint controllership:

- Create a personalised ads profile
- Select personalised ads
- Create a personalised content profile (content profiles)
- Select personalised content (content)
- Measure ad performance
- Measure content performance
- Apply market research to generate audience insights
- Develop and improve products
- Store and/or access information on a device (if specified in the IAB TCF)
- Deliver and present ads and content (Special Purpose 2)

We have agreed with iq digital media marketing GmbH that we will take care of the notification and communication obligations under Art. 33, 34 GDPR as well as compliance with the information obligation under Art. 13 GDPR.

Providers of social media platforms

We maintain profiles on various social media platforms in order to present our services and to interact with users. The data processing that takes place when you visit our profiles is partly carried out under joint controllership with the platform operator. Further information on this can be found in the section Social Media Profiles.



Recipients and Place of Processing

We process personal data in various systems and, depending on the processing activity, transfer it to other companies, public authorities or individuals. The location of the processing depends on our registered office as well as the locations of our service providers.

Processors

We use various processors, such as software providers, data centre operators, call centres and IT service providers. We have carefully selected these companies and concluded a data processing agreement pursuant to Art. 28 GDPR. If, in addition to the companies listed in the Privacy Center, other processors are involved in the processing of data, they are listed below.

List of companies

- Sourcepoint Technologies, Inc. (SaaS provider for Consent Management Platform)
- Webtrekk GmbH (SaaS provider tracking tool)
- Mailjet GmbH (newsletter tool)
- Google Ireland Ltd. (SaaS provider)
- Brightcove, Inc. (hosting and video platform)
- DPV Deutscher Pressevertrieb GmbH (subscription processing)
- Optimizely GmbH (SaaS newsletter tool provider)
- ferret go GmbH (comment review)
- Tickaroo GmbH (live blog integration)
- Audio Ventures Inc. (SimpleCast audio hosting)
- Salesforce, Inc. (Heroku web hosting)
- Snowplow Analytics Ltd. (SaaS provider for tracking tool)
- Freshworks Inc. (SaaS ticketing system provider)
- Meta Platforms Ireland Ltd. (Social Media Platform)
- MaxMind, Inc. (geolocation)
- Fastly, Inc. (content delivery network provider)
- StorifyMe GmbH (SaaS provider for social media stories)
- Amazon Web Services, Inc. (hosting provider)
- Kilkaya AS (SaaS provider for analytics tool)
- SpeedCurve Ltd (SaaS provider for page speed performance)
- 7 Points Sp. z o.o. (SaaS provider for survey tool SurveyLab)
- Piano Software Norway (SaaS provider for personalisation and user engagement)
- Stripo Inc. (SaaS provider for newsletter templates)
- Friendly Captcha GmbH (SaaS provider of an anti-bot solution)
- Centinel Analytica GmbH (SaaS provider for an anti-AI-bot solution)
- Snap Inc. (Social Media Platform)

Third parties

Some activities involve the disclosure of personal data to third parties. These may include providers of website tools, cooperation partners, shipping service providers or suppliers. These companies independently determine the purposes of further processing and must ensure compliance with data protection law. If, in addition to the companies already mentioned elsewhere, other third parties are involved in the processing of data, they are listed below.

List of companies

- MapTiler AG (visual display of geoinformation)
- Hola Org Ltd. (Spark video preview)
- Meta Platforms Ireland Ltd. (Social Media Platform)
- Snap Inc. (Social Media Platform)

Place of processing

As a rule, data processing takes place in the European Union and/or the European Economic Area. However, we also use applications and tools where a transfer of data to third countries cannot be ruled out. In such cases, we ensure that appropriate safeguards are in place to guarantee an adequate level of data protection in these third countries. As a rule, the Standard Contractual Clauses provided by the European Commission have been agreed with the providers, or the provider is certified under the Data Privacy Framework.



Rights of the data subject and Contact

Under the GDPR, data subjects generally have a number of rights. You can exercise these at any time. However, we are not always obliged to grant a right. For example, a request for erasure may be refused due to statutory retention obligations. Where processing is carried out under joint controllership, you may exercise your rights against any of the companies involved.

Rights of the data subject

You have the right of access (Art. 15 GDPR), rectification (Art. 16 GDPR), erasure (Art. 17 GDPR), restriction of processing (Art. 18 GDPR) and data portability (Art. 20 GDPR).

Right to object

We have checked whether we are allowed to process your personal data. This applies in particular to all processing carried out for the purposes of legitimate interests (Art. 6(1)(f) GDPR). If you believe that a specific processing activity is not permissible, you can let us know. If, in your individual case, we come to the conclusion that we are indeed not permitted to process your data, we will stop doing so. If your objection relates to advertising messages, we will of course implement it immediately.

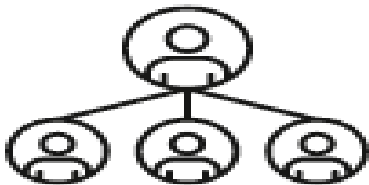
Right to withdraw consent

Some processing activities are based on consent you have given. You can withdraw this consent at any time with effect for the future. However, this does not affect the lawfulness of the processing carried out up to that point.

Contact details

To exercise your data protection rights and for questions and complaints regarding data protection, please use exclusively the email address datenschutz@zeit.de or our postal address.

You can reach our external data protection officer by post at Herting Oberbeck Datenschutz GmbH, Hallerstr. 76, 20146 Hamburg, or via the email address dsb@zeit.de. You also have the right to lodge a complaint at any time with a supervisory authority.



Social Media

We maintain profiles on various social networks to publish our content and engage with users. Like you, we have created an account for this purpose and agreed to the respective social network's terms of use. In addition, we use the tools provided by these social networks for our online marketing to define target groups and run campaigns.

Responsibilities for data processing vary from network to network. It may involve controller status or joint controllership under Article 26 GDPR, and in some cases even processor status under Article 28 GDPR. This assessment is based on the terms of use and integrated contracts of the platform providers, which we are required to use as the basis for our information.

The data processing that occurs when social networks are accessed is determined by the providers. We can only inform you about the processes that fall within our sphere of influence and can be controlled by us.

Meta profiles

Joint controllership

We use our Meta profile to make information publicly available, place advertisements and communicate with users. The data processing that takes place when a profile is accessed is carried out under joint controllership between us and the platform provider. For this reason, we have concluded an agreement pursuant to Art. 26 GDPR, which in particular governs the fulfilment of data subject rights.

The various Meta platforms are operated by Meta Platforms Ireland Limited, Block J, Serpentine Avenue, Dublin 4, Ireland. The provider is responsible for the lawfulness of the data processing via the respective social network. The company is represented by director Gareth Lambe. Meta Platforms Ireland Limited has appointed a Data Protection Officer, whom you can contact at any time.

You can exercise your data subject rights at any time against us or Meta Platforms Ireland Limited. As a rule, however, these rights can usually only be fulfilled by the latter, so we will forward such requests.

Insights data

When you access our profile, Insights data is collected and analysed. These are aggregated statistics created based on certain actions logged by Meta Platforms Ireland Limited. This mainly concerns how you interact with our profile and other content. We have no way to identify you via the Insights data or to assign it to a profile. Insights data is also collected from people who do not have an account. In that case, however, the user is asked for consent when accessing the platform – without it, no content can be viewed.

Meta Platforms Ireland Limited bases the lawfulness of processing Insights data on legitimate interests in the form of optimising advertisements (Art. 6(1)(f) GDPR). We use it ourselves to improve our profile and to provide content that is read by many people. To improve our reach, we need many views and a lot of traffic on our profile. The

more we tailor the content to the interests of our users, the more likely we are to achieve this.

For us, the Insights data is part of the functions provided by the social network. The processing is governed by the terms of use that all profile owners must accept. When you created your own account, you therefore contractually permitted the processing. If you do not accept the terms of use, you cannot maintain a profile. In this respect, providing the Insights data is necessary for use.

The Insights data collected via our profile is processed in anonymised form. This means that the data is modified so that it can no longer, or only with a disproportionately large amount of time, cost and labour, be attributed to a specific or identifiable natural person.

Direct messages and likes

We use our account to get in touch with you and to interact with you. This is possible via direct messages, the like function or comments. In this context, the name stored in your profile is always displayed.

The lawfulness of this processing is based on legitimate interests (Art. 6(1)(f) GDPR). Communicating with you is important to us in order to answer questions, address criticism and exchange information. This is the only way we can improve our services. You can use the various options for communication, but you do not have to. The content of our profile can be viewed independently of this.

Comments are stored on our profile for an unlimited period of time and can be viewed by other users until you delete the comment yourself. The same applies to using the like function. Direct messages are also stored, but are deleted at regular intervals.

Objection to the processing of Insights data

Since Insights data is also used for advertising purposes, there is generally a right to object pursuant to Art. 21 GDPR. Meta Platforms Ireland Limited provides various forms for exercising rights in its privacy policy. There you can object to the processing of data. You can

also exercise this right against us, and we will then forward the request to the provider.

Please note that, if you object to the processing of Insights data, use of the platform may be limited or may no longer be possible at all.

Data disclosure and third-country transfers

Data processing takes place on servers of Meta Platforms Ireland Limited. Direct messages are seen and answered by our employees. All other actions are publicly visible.

Our profile on the social network can be accessed worldwide via the internet, meaning that access from countries without an adequate level of data protection is possible. Meta Platforms Ireland Limited has taken various measures to ensure an adequate level of data protection.

Meta Platforms Ireland Ltd.

Responsibilities

We use Meta Business Tools to better understand how our website is used, to optimize advertising measures on Facebook and Instagram, and to measure their success. Meta Business Tools include, among other things, the Facebook Pixel, the Meta Conversions API, Social Plugins, and functions for logging in or sharing via Meta services.

Meta Business Tools are provided by Meta Platforms Ireland Ltd., Block J, Serpentine Avenue, Dublin 4, Ireland. You can contact the Data Protection Officer via an online form.

Depending on which Meta Business Tools we use and which processing operations we carry out, different data of users are processed. The responsibility for the processing varies. Part of the processing is carried out under joint controllership between us and Meta Platforms Ireland Ltd. For this reason, we have concluded an agreement pursuant to Art. 26 GDPR, which primarily regulates the

fulfilment of data subject rights. When using certain functions, the social network acts on our behalf and in accordance with our instructions. In these constellations, this is processing on behalf pursuant to Art. 28 GDPR, which we have regulated contractually. Sometimes the processing also takes place under separate controllership, so that we and Meta Platforms Ireland Ltd. must each ensure compliance with the GDPR ourselves. Which company is responsible in which way results from the table below.

Purpose	Data categories	Responsibility
Matching with user IDs and combination with event data	Contact information	Processing on behalf
Excluding users from delivered ads, creating Custom Audiences, creating reports on the impact of advertising campaigns and other content, creating analyses and insights about people and their use of apps, websites and products	<u>Event Data</u>	Processing on behalf
Targeting advertising campaigns to people who interact with us, creating Custom Audiences	<u>Event Data</u> , user IDs	Joint controllership
Delivery of commercial and	<u>Event Data</u> , user IDs	Joint controllership

Purpose	Data categories	Responsibility
transactional messages		
Improving ad delivery, for personalising functions and content, and for improving, providing and securing the products of the Meta companies	<u>Event Data</u> , user IDs	Joint controllership
Lead generation	Data collected individually via lead form	Separate controllership

Processed data

Personal data are processed with Meta Business Tools. Meta Platforms Ireland Ltd. specifies how these data are referred to overall. This distinction is relevant for understanding the processing situations shown in the table.

Contact information are information that can be used to identify individuals. This includes, for example, names, email addresses and phone numbers.

Event Data are other information that users generate through their actions on the internet. This includes, for example, visits to websites, installations of apps and purchases in an online shop.

More detailed information can be found in the [Terms for Meta Business Tools](#).

Custom Audiences

An important component of Meta Business Tools are Custom Audiences. These are audiences based on various data, which we use to deliver offers in a targeted manner. Meta Business Tools distinguish between several Custom Audiences:

- Website Custom Audiences (people who visited the website)
- App Activity Custom Audiences (people who used an app)
- Customer List Custom Audiences (people whose contact details we uploaded)
- Engagement Custom Audiences (people who interacted with posts or ads)
- Shopping Custom Audiences (people who viewed an online shop or product catalogue)

Custom Audiences are not directly personal to us. We cannot see or find out whether specific people are in an audience or not.

Legal basis

Processing under joint controllership and separate controllership is carried out on the basis of your consent (Art. 6(1)(a) GDPR, Section 25(1) TDDDG). We obtain this consent via a consent management platform.

Processing in which we use Meta Platforms Ireland Ltd. as a processor is based on our legitimate interests (Art. 6(1)(f) GDPR). When we deliver campaigns via Meta platforms, this is intended to be particularly efficient and cost-saving. In order to exclude active subscribers from these campaigns, we match subscriber data with data of users of Meta services (name and email address).

TikTok profiles

Controllership

We have profiles on the social network TikTok. This is a social media platform where users can create, share and watch short videos. TikTok

is provided by TikTok Technology Limited, 10 Earlsfort Terrace, Dublin, D02 T380, Ireland, and TikTok Information Technologies UK Limited, One London Wall, London, EC2Y 5EB, United Kingdom. The TikTok companies can be contacted via the email address dach@tiktok.com and [various online contact forms](#). You can also reach the Data Protection Officer via an [online form](#).

Depending on which actions we perform via a profile and which features we use, different data of TikTok users is processed. Responsibility for the processing varies. Some processing is carried out under joint controllership between us and the TikTok companies. For this reason, we have concluded an [agreement pursuant to Art. 26 GDPR](#), which mainly governs the fulfilment of data subject rights. This agreement is part of the “Jurisdiction Specific Terms”, which are unilaterally specified for us. Other processing is carried out under separate controllership, so both we and the TikTok companies must ensure compliance with the applicable data protection requirements. When using some features, the social network acts on our behalf and on our instructions. In these cases, this is so-called [processing by a processor pursuant to Art. 28 GDPR](#), which is also governed in the “Jurisdiction Specific Terms”. Which company is responsible in which way results from the table below.

Purpose	Data categories	Responsibility
Collection and transfer of developer data and/or event data by (and to) TikTok	Developer data and/or event data	Joint controllership
Measurement and insights reporting	Event data	Joint controllership
Audience creation and ad targeting	Event data	Separate controllership

Purpose	Data categories	Responsibility
Improving, optimising and personalising ads	<u>Event data</u>	Separate controllership
Security, protection, fraud prevention and development	Developer data and/or <u>event data</u>	Separate controllership
Matching contact details	Contact data	Processing by a processor
Functionality of the developer tool	Developer data	Processing by a processor
Custom Audiences (Customer File) product	Contact data	Processing by a processor
Lead Generation product	Lead generation data (as defined in the <u>Lead Generation Terms</u>)	Processing by a processor

Under the “Jurisdiction Specific Terms”, we are required to inform users about the existence of joint controllership with the TikTok companies and the key provisions of the agreement pursuant to Art. 26 GDPR.

Use of TikTok

We use our TikTok profiles to make information publicly available, place advertising and communicate with users. You can contact us via direct messages, the like function or comments. As part of this contact, the name stored in your profile as your username is displayed. If you have uploaded a picture, it is also visible.

The lawfulness of the processing described is based on our legitimate interests (Art. 6(1)(f) GDPR). Interaction with users is particularly

important to us in order to answer questions, respond to criticism and exchange information. We can also present our content in a way that is appreciated by younger people.

Comments are stored on the channel for an unlimited period of time and can be viewed by other users. The same applies to the use of the like function and direct messages. If we delete our profile, the content generated via it will also be deleted.

When you use TikTok, various data is processed by the social network. This includes, among other things, IP address, location data, time zone settings, advertising IDs, app and browser versions, and device information (system, network type, device ID, screen resolution, operating system, audio settings and connected audio devices). The TikTok profiles and channels you access, likes, messages and other information about usage are also processed. If you are logged in with your own TikTok account, this data is assigned to your account. You can find more information on the processing of your data in TikTok's [Privacy Policy](#). The processing described is carried out under the sole responsibility of the TikTok companies.

Insights data

The collection and transfer of developer data and event data by (and to) the TikTok companies as well as measurement and insights reporting take place under joint controllership. The processed insights data provides information about how many users accessed our channel or posts at what time. The data is made available to us in aggregated form as statistics. We have no way to personally identify you via these statistics or to assign certain actions to your account. Please note that insights data may also be collected if you do not have your own TikTok account.

From our perspective, the collection and use of insights data is permitted for the purposes of safeguarding legitimate interests (Art. 6(1)(f) GDPR). Based on the anonymised insights data, we can optimise the content of our channel and thus increase our revenue.

We store the aggregated insights data for an unlimited period of time, or for as long as we operate the respective TikTok profile.

TikTok companies' privacy policy

Information about how the TikTok companies process personal data (including the legal basis and options to exercise data protection rights) can be found in TikTok's Privacy Policy.

Exercising data subject rights

In the joint controllership agreement, it was agreed that the TikTok companies are responsible for fulfilling data subject rights under Art. 15–20 GDPR in relation to the personal data stored or otherwise processed by the social network as part of the joint processing. If you want to assert data subject rights, it is best to use the provided online form. You can also assert your data subject rights towards us. We will then forward your request.

Data disclosure and third-country transfers

Data processing takes place on servers of the TikTok companies. Direct messages are seen and answered by our employees. All other actions are publicly visible.

TikTok can be accessed via the internet worldwide, so access from countries without an adequate level of data protection is also possible. The platform operators have taken various measures to ensure an adequate level of data protection. The standard contractual clauses contained in the "Jurisdiction Specific Terms" govern international data transfers and ensure that the companies involved in the data processing act in compliance with data protection law.

X profiles

Controllership

The short messaging service X is offered and operated by Twitter International Unlimited Company, One Cumberland Place, Fenian Street Dublin 2, D02 AX07, Ireland. Responsibility under data protection law lies solely with that company. The company belongs to X Corp., 1355 Market Street, Suite 900, San Francisco, CA 94103, USA.

Use of X

We use X and the functions provided there to share information and to communicate with other users. In doing so, we comply with the terms of use that we agreed to when we created our profile.

We have no influence on the data processing that takes place. You can find information about this in the [X Privacy Policy](#). You use the short messaging service at your own responsibility and must decide for yourself whether you agree to the data processing by Twitter International Unlimited Company. This applies in particular to the use of interactive functions (e.g. reposting, liking) and data processing in countries outside the EU and the EEA.

Privacy settings

In your account's general settings and under "Privacy and safety", you have the option to restrict the processing of your data. In addition, you can restrict X's access on your mobile device to contacts and calendar data, photos and location data (depending on the operating system used). Further information on these points is available from the platform provider.

WhatsApp channels

Controllership

The WhatsApp messenger service is offered and operated by WhatsApp Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland. Sole responsibility under data protection law lies there. The

company belongs to Meta Platforms, Inc., 1601 Willow Road, Menlo Park, CA 94025, USA.

Use of WhatsApp

We operate a WhatsApp channel to provide information. There is no individual communication with users. In particular, we can neither view the phone number nor the profile name.

We have no influence on the data processing that takes place when using WhatsApp. You decide for yourself whether you want to use the service in the form offered. Please read the provider's WhatsApp Privacy Policy.

Privacy settings

You have the option to adjust data processing when using WhatsApp. To do so, use the privacy settings within the app.

LinkedIn profiles

LinkedIn account and communication with users

We maintain various LinkedIn accounts in order to network with companies and individuals. There we present ourselves, share posts and interact with other LinkedIn users. In doing so, we can see the content published on your profile and use it to communicate with you. For example, we share and comment on posts, tag LinkedIn users or use the messaging function.

The data processing carried out directly by us is for the purposes of our legitimate business interests (Art. 6(1)(f) GDPR). We rely on the widest possible reach and therefore on professional networks such as LinkedIn. Making contact is facilitated by ongoing interaction with users and the information available in profiles. Communication with us and interaction with our profile is voluntary.

If you would like to learn more about data processing when using LinkedIn, please read the provider's [LinkedIn Privacy Policy](#) (LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland).

Page Insights

When you visit our LinkedIn profile, follow the page or engage with it, LinkedIn Ireland Unlimited Company processes personal data in order to provide us with statistics and insights in anonymised form. This gives us insights into the types of actions people take on our page (so-called Page Insights). For this purpose, the social network processes in particular data that you have made available in your profile (e.g. job function, country, industry, seniority, company size and employment status). In addition, information is processed about how you interact with our LinkedIn company page. The processing serves our legitimate interest in analysing the types of actions taken on our LinkedIn company page and improving our company page based on these insights (Art. 6(1)(f) GDPR).

With Page Insights, LinkedIn Ireland Unlimited Company does not provide us with any of your personal data. We only have access to aggregated and anonymised Page Insights. Nor is it possible for us to draw conclusions about individual members via Page Insights. The processing described is carried out by LinkedIn Ireland Unlimited Company and us as joint controllers. For this reason, there is a [joint controllership agreement pursuant to Art. 26 GDPR](#) with the provider, which stipulates the following:

LinkedIn Ireland Unlimited Company is responsible for enabling you to exercise your rights under the GDPR. You can [contact the company online](#) or reach it via the [contact details provided in the privacy policy](#). You can contact the [Data Protection Officer](#) via an online form. You can also contact us regarding the exercise of your rights in connection with the processing of personal data as part of Page Insights. In such a case, we will forward your request to the social network.

LinkedIn Ireland Unlimited Company and we have agreed that the Irish Data Protection Commission is the lead supervisory authority for

monitoring the processing of data via Page Insights. You always have the right to lodge a complaint with the Irish Data Protection Commission (see www.dataprotection.ie) or with any other supervisory authority.

Recipients of data

We use LinkedIn only as a platform and comply with the provider's terms of use. We ourselves have no influence on which data is processed when our profile is accessed or who can see your profile. In this respect, like you, we are only a user.

However, we have employees who take care of our LinkedIn profiles. Incoming messages are viewed and processed by them. Depending on how you interact with our content, your profile and your publications may be seen by other users. When using LinkedIn, data is transferred to third countries outside the European Union and the European Economic Area. According to the provider, this is legitimised by Standard Contractual Clauses.

Storage period

If you leave a comment, it will be stored on our profile for an unlimited period of time (until you delete it). The same applies to using the like function. Direct messages to us are also stored, but are deleted at regular intervals.

SnapChat profiles

Controllershship

The social media platform SnapChat is offered and operated by Snap Inc., with its address at 3000 31st Street, Santa Monica, California 90405, USA. Responsibility under data protection law lies solely there.

Use of SnapChat

We use SnapChat and the functions provided via it to share information and to communicate with other users. In doing so, we comply with the terms of use that we agreed to when creating our profile.

We have no influence on the data processing that takes place. You can find information about this in SnapChat's [Privacy Notice](#). You use the social media platform at your own responsibility and must decide for yourself whether you agree with the data processing by Snap Inc. This applies in particular to the use of the functions (e.g. reactions, stories, chatting, SnapMap) and the data processing in countries outside the EU and the EEA.

Advertising campaigns

We run advertising campaigns on various social networks and place our ads using the features provided by these platforms (e.g., Meta, Google, or SnapChat). In doing so, we enter our campaign and advertising content into the provider's system, configure the settings we require, and define which user categories should see the content and for how long. The social network, as an independent controller, is responsible for delivering the content and uses its own database to select the recipients.

To enable even more precise targeting, we may provide the social network with additional data (e.g., IP addresses, cookie and device identifiers, browser and device information, visited pages, or registrations). For data processing in advertising campaigns where we do not supply any additional data, the respective social network is solely responsible. If we provide further data, we do so only with the consent of the data subjects (Art. 6(1)(a) GDPR, § 25(1) TTDSG). We obtain this additional data in particular through the use of cookies and pixels or other processing operations on users' devices. You can find details of the specific processing activities in our Privacy Center.

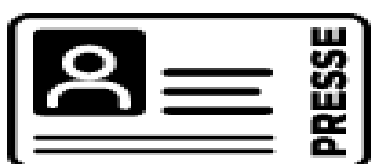
The social networks themselves determine the retention period for data processed under their responsibility. In our Privacy Center, you can find information on how long data is stored on your device.

Customer matching

To avoid targeting existing customers with advertising and acquisition campaigns, we compare selected customer master data (in particular email addresses) with user data from social media platforms (e.g., Meta, LinkedIn, Google, SnapChat). The goal is to exclude active existing customers from new customer campaigns (so-called suppression/exclusion audiences), minimize wastage, use advertising budgets efficiently, and avoid unnecessary contact with existing customer relationships.

The legal basis for this processing is either consent (Article 6(1)(a) GDPR) or legitimate interest (Article 6(1)(f) GDPR), depending on the requirements set by the social media platforms in their terms and conditions. Our legitimate interest lies in the efficient management of marketing measures, the avoidance of misdirected communication to existing customers, and the economically sensible use of advertising budgets.

The provision of the data used for the comparison is carried out within the framework of the existing customer relationship. There is no separate storage of the data beyond the comparison process. The data uploaded to the social media platforms for the matching process is deleted by the platforms after the matching has been completed.



Media privilege

We also process personal data via our website and other channels for journalistic purposes. In doing so, we pursue the aim of disseminating information, opinions and ideas to the public and objectively contributing to the formation of opinions.

In this case, the so-called media privilege applies, with the result that not all requirements of the GDPR have to be complied with. For example, we do not need a legal basis for the processing of personal data and do not have to provide a privacy policy. This is also understandable. It would be harmful to freedom of the press and freedom of expression if, when publishing articles, we had to consider a legal basis or inform all persons affected by research about the processing of their personal data. This would endanger independent reporting and the personal rights of sources.

Of course, the media privilege does not exempt us from all legal obligations. All persons involved in processing have been bound to confidentiality, appropriate technical and organisational measures are taken to protect personal data, and we comply with the State Media Treaty, the applicable press laws and the Press Code.