



EVIDENTIQ

## Privacy Policy

We, EvidentIQ GmbH (“EvidentIQ /we“), are pleased about your visit to our website and your interest in our products and services. In the following provisions, we inform you about the type, scope and purpose of the collection and use of your personal data on our website. Personal data is any information relating to an identified or identifiable natural person. This includes in particular your name and e-mail address.

The use of our website is generally possible without providing personal data. You are neither obliged to call up this website nor to provide personal data. However, the active provision of personal data is required, for example, in the case of registration for a newsletter or an application. If you do not provide us with personal data for the purposes listed below, you may not be able to use the functions of this website or some of its services.

### 1. Provider and data protection officer

Provider of the website and controller in the sense of data protection law is the

EvidentIQ

Grosse Johannisstr. 7, 20457 Hamburg, Germany

Managing director: Andreas Weber

Phone: +43 660 514 8792

E-mail: [info@xclinical.com](mailto:info@xclinical.com)

You can reach EvidentIQ’s data protection officer at

krupna LEGAL

Dr. Karsten Krupna

Am Sandtorkai 77

20457 Hamburg

Phone: +49 (0) 40 31976927

E-mail: [karsten-krupna@xclinical.com](mailto:karsten-krupna@xclinical.com)

### 2. Data processing for enabling website use

Every time you access content on our website, connection data is transmitted to our webserver. This connection data includes:

- the IP address (Internet Protocol address) of the respective users,
- the date and time of the request,

- the referrer URL,
- device numbers such as UDID (Unique Device Identifier) and comparable device numbers, device information (e.g. device type) and
- the browser type / the browser version.

This connection data is not used to draw conclusions about the person of the user or merged with data from other data sources, but serve to provide the website. After 7 days at the latest, the data will be anonymized by shortening the IP address at domain level. The legal basis for the processing of your data is Art. 6 para. 1 sentence 1 lit. f GDPR.

### **3. Newsletter**

If you have expressly consented, you will receive a newsletter on EvidentIQ products and services via e-mail. To receive our newsletter, only your e-mail address is required. This is marked accordingly (\*). The entry of any additional information about your person is voluntary and serves only to personalize the newsletter for you.

In connection with your registration to receive the newsletter, we use the so-called double-opt-in procedure. This means that after your registration we will send you an e-mail to the e-mail address you provided, in which we ask you to confirm that you wish to receive the newsletter. If you do not confirm your registration within 7 days, your information will be blocked and automatically deleted after one month.

The processing of your personal data in connection with the newsletter is based on your consent pursuant to Art. 6 para. 1 sentence 1 lit. a GDPR.

You can revoke your consent to receive newsletters at any time with effect for the future towards EvidentIQ. The revocation of consent does not affect the lawfulness of the processing carried out on the basis of the consent until the revocation. To exercise the revocation, you will find a corresponding link at the end of each e-mail newsletter. Alternatively, you can revoke your consent at any time, e.g. by sending an e-mail to [info@xclinical.com](mailto:info@xclinical.com).

When you register for the newsletter, we also store your IP address and the time of registration in order to fulfill our legal documentation obligations. The legal basis for data processing in this case is Art. 6 para. 1 sentence 1 lit. c GDPR.

### **4. Online application**

On our linked separate website (please note the separate privacy policy for this website) you can apply for a position at EvidentIQ. You have the option of using our online application form. Alternatively, you can also apply by e-mail or by post.

As part of the online application, you will be asked to provide personal information (e.g. name and contact details). For the establishment and implementation of a possible employment relationship, the provision of certain data is required. If you do not provide this data, which is separately marked as mandatory, your application is incomplete and cannot be considered further in the application process. The provision of other information and the upload of files or documents (e.g. CV or application photo) is not mandatory at

this stage of the application process, but optional. If you only provide mandatory information, there will be no disadvantages for your application.

After receipt of your online application, you will receive an automatic confirmation of receipt from us. Further communication regarding the application process will then be handled by our HR department.

Your data will be processed by EvidentIQ for the purpose of deciding on the establishment of an employment relationship. The legal basis for data processing by EvidentIQ is § 26 para. 1 sentence 1 BDSG. If special categories of personal data are involved, the processing is governed by § 26 para. 3 BDSG.

## **5. Data processing for the demand-oriented design of the website / cookies**

The tracking tools and other services used by us are listed in sections 6 ff. The legal basis for the processing of your data follows from Art. 6 para. 1 sentence 1 lit. f GDPR, unless otherwise stated in sections 6 ff. Our legitimate interest then consists in the demand-oriented design of the website.

In order to make the use of our website as pleasant as possible for you, we use so-called "cookies", i.e. small text files that are sent to your browser by a web server and stored on the hard drive of your end device. This enables us to recognize the end device you are using when you use our website.

Most browsers are set in such a way that cookies are automatically accepted. You can deactivate the storage of cookies in your browser and have the option of deleting them from your hard drive at any time. However, you can also use your browser to prevent the setting of certain cookies only (e.g. cookies from third parties), for example if you wish to prevent web tracking. You can find more information on this in the help function of your browser.

We would further like to point out that you can also install a plugin in your browser to protect your privacy, which offers the possibility of preventing tracking - e.g. AdBlock, Ghostery or NoScript (please refer to the data protection information of the respective plugin provider).

Finally, please note that if you disable cookies, you may not be able to use all the features of this website to their full extent.

Details of the cookies used on the website can be found in the cookie banner and in the following provisions.

## **6. Cookie consent with Usercentrics**

This website uses the cookie consent technology of Usercentrics to obtain your consent to the storage of certain cookies on your end device and to document this in a data protection compliant manner. The provider of this technology is Usercentrics GmbH, Rosental 4, 80331 Munich, website: <https://usercentrics.com/de/> ("Usercentrics").

When you access our website, the following personal data will be transferred to Usercentrics:

- Your consent(s) or revocation of your consent(s)

- Your IP address
- Information about your browser
- Information about your end device
- Time of your visit on the website

Furthermore, Usercentrics stores a cookie in your browser in order to be able to attribute the given consents or their revocation to you. The data collected in this way is stored until you request us to delete it, delete the Usercentrics cookie yourself or the purpose for storing the data no longer applies. Mandatory legal storage obligations remain unaffected.

Usercentrics is used to obtain the legally required consent for the use of cookies. The legal basis for this is Art. 6 para. 1 sentence 1 lit. c GDPR.

## **7. Tracking tools / Other services**

### **7.1. Google Analytics**

Our website uses the tracking tool "Google Analytics". This is a service provided by Google Ireland Limited, a company incorporated and regulated under Irish law with its registered office at Gordon House, Barrow Street, Dublin 4, Ireland ("Google"). This tracking tool helps us to make the website more interesting for you and to improve the user experience. In doing so, data on the use of our website is stored in pseudonymous user profiles. Cookies can also be used for this purpose. In addition, data from various devices, sessions and interactions can be linked to a so-called "user ID". The generated information is usually transferred to a Google server in the USA and stored there. We would like to point out that on our website Google Analytics has been extended by the "anonymizelp" function. This means that your IP address is first shortened by Google within member states of the European Union or in other contracting states of the Agreement on the European Economic Area and only then transferred to a Google server in the USA. The shortening of the IP address is an additional measure pursuant to Art. 25 para. 1 GDPR for the protection of users, but it does not result in anonymization of the complete data processing. Thus, when Google Analytics is used, in addition to the IP address, other usage data is also collected that is to be assessed as personal data, such as identification features of the individual users, which also allow a link to an existing Google account, for example. On our behalf, Google will use the information obtained via Google Analytics to evaluate your use of our website, to compile reports on website activity and to provide us with other services related to website and internet usage. The pseudonymized usage profiles are not merged with personal data about the bearer of the pseudonym without a separately granted consent.

For more information about Google Analytics, see:

<https://support.google.com/analytics/answer/2790010?hl=de>

Please note that Google also has independent access to your data collected via Google Analytics and can also use this data for its own purposes. For example, Google may combine this data with other data about you, such as your search history, personal account, usage data from other devices and any other data that Google has about you.

The legal basis for our processing of your data is your consent in accordance with Art. 6 para. 1 sentence 1 lit. a GDPR. You give your corresponding consent via our cookie banner. Please note that Google is a company from the USA. According to a recent ruling of the European Court of Justice (ECJ), there is no adequate level of data protection in the USA and thus a risk to the protection of your data. For example, under certain circumstances your data may be processed by US authorities for control and monitoring purposes. If you still wish to give your consent to the use of this tool, you can select this via the cookie banner.

## **7.2. Google Ads Conversion**

In order to advertise our products and services on external websites with the help of advertising media and to determine the success of our advertising measures, we use the "Google Ads Conversion" service. These advertising media are delivered by Google via so-called "Ad Servers". If you access our website via a Google ad, Google Ads will store a cookie on your end device. These cookies usually lose their validity after 30 days and do not serve to identify you personally. The unique cookie ID, number of ad impressions per placement (frequency), last impression (relevant for post-view conversions) and opt-out information (marking that the user no longer wishes to be addressed) are usually stored as analysis values for this cookie.

The aforementioned cookies enable Google to recognize your internet browser. Therefore, provided that you have visited certain websites of an Ads customer and the cookie stored on your computer has not yet expired, Google and the Ads customer can recognize that you have clicked on the ad and were redirected to this page. Cookies cannot be tracked through Ads customer websites. We ourselves do not collect or process any personal data in the aforementioned advertising measures. We also only receive statistical evaluations from Google. Based on these evaluations, we can see which of the advertising measures used are particularly effective. We do not receive any further data from the use of the advertising media, in particular we cannot identify you on the basis of this information.

Due to the marketing tools used, your browser automatically establishes a direct connection with the Google 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 knowledge as follows: Through the integration of Ads Conversion, Google receives the information that you have called up the relevant part of our internet presence or clicked on an advertisement from us. If you are registered at a Google service, Google can assign the visit to your account. Even if you are not registered at Google or have not logged in, there is the possibility that the provider learns your IP address and stores it.

You can find more information about data privacy at Google here: <https://support.google.com/google-ads/answer/93148> [https://ads.google.com/intl/de\\_de/home/faq/gdpr/](https://ads.google.com/intl/de_de/home/faq/gdpr/)

The legal basis for our processing of your data is your consent pursuant to Art. 6 para. 1 sentence 1 lit. a GDPR. You give your corresponding consent via our cookie banner. Please note that Google is a company from the USA. According to a recent ruling by the European Court of Justice (ECJ), there is no adequate level of data protection in the USA and thus a risk to the protection of your data. For example, under certain conditions, your

data may be processed by US authorities for control and monitoring purposes. If you nevertheless wish to consent to the use of this tool, you can do so via the cookie banner.

### **7.3. HubSpot**

For our online marketing activities, we use the service of HubSpot Inc., a software company based in the USA, 25 First Street, Cambridge, MA 02141 USA, with an office in Ireland, Ground Floor, Two Dockland Central, Guild St, North Dock, Dublin, D01 K2C5, Ireland (“HubSpot”).

HubSpot is an integrated software solution that we use to cover various aspects of our online marketing. These include: E-mail marketing, contact management (e.g. user segmentation & CRM) and data processing via contact forms. We use all collected information exclusively to optimize our marketing measures.

The legal basis for the processing of your data is your consent pursuant to Art. 6 para. 1 sentence 1 lit. a GDPR. You give your corresponding consent via our cookie banner. Please note that HubSpot is a company from the USA. According to a recent ruling by the European Court of Justice (ECJ), there is no adequate level of data protection in the USA and thus a risk to the protection of your data. For example, under certain conditions, your data may be processed by US authorities for control and monitoring purposes. If you nevertheless wish to consent to the use of this tool, you can select this via the cookie banner.

### **7.4. ShareThis**

In order to be able to share content from this website on social media channels such as Instagram or Twitter, we use the ShareThis tool from ShareThis Inc. (4005 Miranda Ave, Suite 100, Palo Alto, 94304 California, USA). ShareThis collects information via technical cookies placed on your browser, pixel tags, HTTP headers (or other communication protocols) and browser identifiers.

For detailed information about ShareThis privacy and the technology used, please see the following [link](#).

The legal basis for the processing of your data is your consent pursuant to Art. 6 para. 1 sentence 1 lit. a GDPR. You give your corresponding consent via our cookie banner. Please note that ShareThis Inc. is a company from the USA. According to a recent ruling by the European Court of Justice (ECJ), there is not an adequate level of data protection in the USA and thus a risk to the protection of your data. For example, under certain conditions, your data may be processed by US authorities for control and monitoring purposes. If you nevertheless wish to consent to the use of this tool, you can select this via the cookie banner.

### **7.5. YouTube**

Our website uses plugins from the YouTube site operated by Google. When you visit one of our websites equipped with a YouTube plugin, a connection to the YouTube servers is established. In the process, the YouTube server is informed which of our websites you have visited. If you are logged into your YouTube account, you enable YouTube to assign your surfing behavior directly to your personal profile. You can prevent this by logging out of your YouTube account. The use of YouTube is based on your consent in accordance with Art. 6 para. 1 sentence 1 lit. a GDPR. You give your corresponding consent via our cookie banner. Please note that Google is a company from the USA. According to a re-

cent ruling by the European Court of Justice (ECJ), there is no adequate level of data protection in the USA and thus a risk to the protection of your data. For example, under certain circumstances, your data may be processed by US authorities for control and monitoring purposes. If you nevertheless wish to consent to the use of this tool, you can select this via the cookie banner.

For more information on the handling of user data, please refer to Youtube's privacy policy at: <https://www.google.de/intl/de/policies/privacy>

## **7.6. LinkedIn Insight-Tag**

On our website we use the conversion tool "LinkedIn Insight-Tag" of LinkedIn Ireland Unlimited Company ("LinkedIn Ireland"). This tool creates a cookie in your web browser, which enables the collection of, among other things, the following data: IP address, device and browser properties and page events (e.g. page views). LinkedIn Ireland does not transmit any personal data to us, but provides anonymized reports on website audience and viewing performance. In addition, LinkedIn Ireland offers the possibility of retargeting via the Insight-Tag. With the help of this data, we can display targeted advertising outside our website without identifying you as a user of the website. Our legal basis for processing your data is your consent pursuant to Art. 6 para. 1 sentence 1 lit. a GDPR. You give your corresponding consent via our cookie banner.

Please note that LinkedIn Ireland may also process your data outside the EU/EEA. According to a recent ruling by the European Court of Justice (ECJ), there is no adequate level of data protection in the USA and thus a risk to the protection of your data. For example, under certain conditions, your data may be processed by US authorities for control and monitoring purposes. If you nevertheless wish to consent to the use of this tool, you can select this via the cookie banner.

For more information about the LinkedIn Insight-Tag, please see the following [link](#). For more information about privacy at LinkedIn Ireland, please see the LinkedIn Ireland [Privacy Policy](#).

## **7.7. Google reCAPTCHA**

We use Google reCAPTCHA ("reCAPTCHA") on our website. This is a service of the provider Google. reCAPTCHA is used to check whether the data entry on our website (e.g. when registering for a newsletter) is made by a human or by an automated program. For this purpose, reCAPTCHA analyzes the behavior of the website visitor based on various characteristics. This analysis begins automatically as soon as the website visitor calls up or enters the website. For the analysis, reCAPTCHA evaluates various information (e.g. IP address, time spent by the website visitor on the website or mouse movements made by the user). The data collected during the analysis is forwarded to Google. The reCAPTCHA analyses run completely in the background. You will not be informed separately that an analysis is taking place. Please note that Google is a company from the USA. According to a recent ruling by the European Court of Justice (ECJ), there is no adequate level of data protection in the USA and thus a risk to the protection of your data. For example, under certain conditions, your data may be processed by US authorities for control and monitoring purposes.

For more information about reCAPTCHA and Google's privacy policy, please see the following links: <https://www.google.com/intl/de/policies/privacy/> and <https://www.google.com/recaptcha/intro/android.html>.

## **7.8. Google Tag Manager**

We use the Google Tag Manager. Through this service from Google, website tags can be managed via an interface. However, the Google Tag Manager only implements tags. In this respect, no cookies are used and no personal data is collected. The Google Tag Manager merely triggers other tags, which in turn may collect data. However, the Google Tag Manager does not access this data. The data is analyzed exclusively in the respective tool (see the aforementioned explanations in section 7).

## **8. Social media presence**

### **8.1. Links to social networks**

Our website contains links to social networks (Instagram, LinkedIn and Twitter). These websites are operated exclusively by third parties. If you follow the links, the respective provider may process personal data about you. Please note the data protection information of the provider in this regard.

### **8.2. Data processing by EvidentIQ and legal basis**

Our social media presences and links to third-party providers (Instagram, LinkedIn and Twitter) serve the purpose of informing you about EvidentIQ as well as new developments, services and products of EvidentIQ. Depending on the offer of the respective providers, you have the possibility of different interaction (comments, recommendations etc.) e.g. in connection with our social media presence. The interaction of the users is an important criterion for us in order to carry out targeted marketing. For example, we can determine which articles are read preferentially. We therefore also use the statistics determined by the providers in this regard for our own purposes. Insofar as we process personal data of users in this context, the legal basis for this is Art. 6 para. 1 sentence 1 lit. f GDPR. Our legitimate interest then consists in particular in targeted information / advertising. The providers will inform you separately about the legal basis on which they process your data for their own purposes.

### **8.3. Joint responsibility**

In some cases, we are jointly responsible with the social media providers for processing your personal data. In this case you can assert your rights (see section 14) generally either against us or against the social media provider. However, the social media provider is the first point of contact.

We have concluded a joint responsibility agreement with LinkedIn Ireland for the processing of personal data. This applies in relation to so-called "page insights". These are aggregated page statistics, whereby LinkedIn does not provide us with any personal data from you. Details on the insights data and our agreement with LinkedIn can be found at the following [link](#).

With regard to the storage period of the data we process from you for our own purposes, please refer to our explanations under section 12. Otherwise, please observe the data protection provisions of the respective social media provider.

## 9. Telephone and video conferences via teams

We use the online platform teams (“teams“) for interactive communication. Teams is a service provided by Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, based in the USA (“Microsoft“). For more information from Microsoft about team’s privacy practices, please click [here](#).

### 9.1. Microsoft’s own responsibility

If you access Microsoft's website for the use of teams, Microsoft is responsible for the data processing. However, you only need to access the website to download the software for the use of teams. You can also use teams if you enter the respective meeting ID and, if necessary, other access data for the meeting directly in the teams app. If you do not wish to use the teams app, the basic functions can also be used via a browser version.

To the extent that Microsoft processes personal data in connection with its own legitimate business operations, as described in the [Microsoft Online Services Terms of Use](#), Microsoft is an independent data controller for such processing, whose legal basis, according to its [own declaration](#), is "legitimate interests". "Microsoft's legitimate business transactions" in this context are, as evidenced by [Microsoft's statement](#), the following, each as an incident involving the provision of teams to us (1) billing and account management; (2) compensation (e.g., calculation of employee commissions and partner incentives); (3) internal reporting and modeling (e.g., forecasts, revenue, capacity planning, product strategy); (4) combating fraud, cybercrime or cyber attacks that may affect Microsoft or Microsoft products; (5) improving core accessibility, privacy, or energy efficiency functionality; and (6) financial reporting and compliance with legal obligations.

Microsoft's statement on the storage of personal data can be found [here](#).

### 9.2. Purpose of processing and types of personal data

We use teams to conduct telephone conferences and/or video conferences, particularly in connection with online seminars for prospects and professionals and/or employment relationships (“online meetings”).

When using teams, various types of personal data are processed by us. The type and scope of the data depends in particular on the information you provide before or during participation in an online meeting. However, in order to identify you as an authorized participant, you must at least provide your name. You can deactivate the video or microphone function at any time via the teams application.

Personal data processed in connection with teams include:

- **Profile data:** First name, surname, telephone number (optional), e-mail address, password (if “Single-Sign-On” is not used), profile picture (optional), department (optional)

- **Meeting metadata:** Subject, description (optional), participant IP addresses, device/hardware information
- **Call history data:** Information on incoming and outgoing telephone number, country name, start and end time. If necessary, other connection data such as the IP address of the device can be saved.
- **Content data:** You may be able to use chat, question or survey functions during an online meeting. Your text entries and other approved data are processed to display them in the online meeting.

For further details on data processing by Microsoft, please refer to Microsoft's [explanations](#) von Microsoft.

### 9.3. Data processing by EvidentIQ and legal basis

To the extent that personal data of employees is processed by us, the legal basis for data processing is generally § 26 para. 1 BDSG. If special categories of personal data are involved, the processing is governed by § 26 para. 3 BDSG.

If, however, in connection with the use of teams, personal data is not required for the establishment, implementation or termination of the employment relationship, the legal basis for data processing is generally Art. 6 para. 1 sentence 1 lit. f GDPR. In these cases, our interest lies in the effective implementation of online meetings. In addition, the legal basis for data processing when conducting online meetings is Art. 6 para. 1 sentence 1 lit. b GDPR, insofar as the meetings are conducted in the context of contractual relationships. In special cases (e.g. a recording of online meetings) in which you are asked in advance for a declaration of consent, the legal basis is Art. 6 para. 1 sentence 1 lit. a GDPR.

### 9.4. Data transfer to countries outside the EU

Teams is a service provided by a provider from the USA. A processing of personal data therefore also takes place in a third country. We have concluded a data processing agreement with Microsoft in accordance with Art. 28 GDPR. An adequate level of data protection is ensured by the conclusion of the so-called EU standard model clauses. If law enforcement authorities contact Microsoft with a request, Microsoft, according to its [own statement](#), tries to redirect law enforcement authorities to request the personal data directly from us. If Microsoft is required to disclose personal information to law enforcement authorities, Microsoft will (also at Microsoft's [own statement](#)) notify us immediately and provide a copy of the request unless prohibited by law. For more information about the data that Microsoft discloses in response to requests from law enforcement and other government agencies, please refer to [Microsoft's Law Enforcement Requests Report](#).

## 10. Data transfer

We only transfer your personal data to third parties or other recipients if this is necessary for the provision of services, if you have given your consent, if there is a legal obligation or if the transfer of data is permitted by another legal basis. Where necessary, we have concluded data processing agreements with the recipients of your data, such as Google,

Usercentrics or other service providers, in accordance with Art. 28 GDPR. We will only transfer your data to government bodies within the scope of legal obligations or on the basis of an official order or court decision.

## **11. Data transfer to countries outside the EU**

As far as necessary for our purposes, we will also transfer your data to recipients outside the EU if you have given your consent, if there is a legal obligation or if the transfer of data is permitted on another legal basis. Your data will also be transferred to recipients based in the USA within the scope of data processing. An adequate level of data protection is generally ensured by the conclusion of the so-called EU standard contract clauses. Please note, however, that according to a recent ruling of the European Court of Justice (ECJ), there is no adequate level of data protection in the USA and thus a risk to the protection of your data. For example, under certain circumstances your data may be processed by US authorities for control and monitoring purposes. In addition, we refer to Art. 49 GDPR with regard to the legal basis for the transfer of data.

## **12. Duration for which personal data is stored / criteria for determining the duration**

Your personal data will be stored by EvidentIQ for as long as it is necessary for the aforementioned purposes of processing, in the event of an objection no compelling reasons worthy of protection oppose EvidentIQ or in the event of a revocation no other legal basis for data processing exists. In certain cases, e.g. if there is a legal obligation to retain data, your personal data will not be deleted immediately, but blocked initially.

If an application (e.g. via our online application form, see section 4) is successful, your data will be transferred to the personnel file and stored beyond the period of the application process in accordance with the statutory provisions. If your application is not successful, we will store your data beyond the period of the application process for a maximum of 6 months, unless you have given your consent to further data processing.

## **13. Data security**

To protect your personal data on this website, we use a secure online transmission procedure, the so-called "Secure Socket Layer" (SSL) transmission. You can recognize this by the fact that a closed padlock symbol is displayed on the address <https://>. By clicking on the symbol, you will receive information about the SSL certificate used. The display of the symbol depends on the browser version you are using. The SSL encryption guarantees the encrypted and complete transmission of your data.

## **14. Your rights**

Within the framework of the legal requirements, you have a fundamental claim against EvidentIQ for

- confirmation as to whether personal data concerning you is processed by EvidentIQ,
- information about these data and the circumstances of processing,

- correction, if this data is incorrect,
- deletion, unless the processing is not justified and there is no (longer an) obligation to keep the data,
- restriction of processing in special cases determined by law,
- objection in case of data processing on the basis of Art. 6 para 1 sentence 1 lit. f GDPR and
- transmission of your personal data – if you have provided it – to you or a third party in a structured, common and machine-readable format.

Insofar as the processing of your personal data is based on your consent, you have the right to revoke this consent at any time, with the consequence that the processing of your personal data will become inadmissible for the future. However, this does not affect the lawfulness of the processing carried out on the basis of the consent up to the point of revocation.

Please address your specific request in writing or by e-mail to our data protection officer (see section 1), clearly identifying yourself.

Insofar as we process your data in joint controllership with third parties within the meaning of Art. 26 GDPR (see section 8.3), the third party is centrally responsible for the exercise of all rights of the persons concerned. However, you are free to assert your rights against us as well.

Finally, we would like to draw your attention to your right of appeal to the supervisory authority.

e.g. supervisory authority in Bavaria:

Bavarian State Office for Data Protection Supervision (BayLDA)  
 Promenade 18 / 91522 Ansbach

## **15. No automated individual decision**

We do not use your personal data for automated individual decisions.

## **16. Amendment of the privacy policy**

New legal requirements, business decisions or technical developments may require changes to our privacy policy. The privacy policy will then be adjusted accordingly. You will always find the latest version on our website.