

## Privacy Policy

Thank you for your interest in our online presence. Protecting your personal data is very important to us. We would therefore like to take this opportunity to inform you about how DGQ e.V. and DGQ Weiterbildung GmbH handle your personal data. It goes without saying that we comply with the statutory provisions of the General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (BDSG), as well as other data protection regulations, where applicable.

You can trust us with your personal data! Your data is encrypted by digital security systems and transferred to us. Our websites are protected by technical measures to prevent damage, destruction and unauthorised access.

More information about data protection is available here:

Table of contents

### Privacy Policy

1. Where data protection applies
2. Controller and data protection officer
3. Extent of data collection and processing when you visit our website
4. Extent of data collection and the processing of data for bookings via our webshop
5. Use of data for specific purposes and disclosure to third parties
6. General storage period and deletion (erasure)
7. Your rights as a data subject
8. Data processing for the online application
9. Use of cookies
10. Sending our newsletter and analysis of newsletter usage
11. DGQplus networking portal
12. Data processing when contacting us and using contact forms
14. Use of the blog functions
15. Conferences via GoToMeeting
16. Events using GoToTraining
17. Webinars using GoToWebinar
18. Webinars using Microsoft Teams
19. Conferences using Microsoft Teams
20. Events and e-training using Microsoft Teams
21. Online examinations using Easy LMS
22. Use of Matomo
23. Advertising campaigns and remarketing via Google Ads
24. Marketing using Microsoft Advertising
25. Use of Sleeknote
26. Social Plugins
27. LinkedIn Insight Tag

- 28. YouTube videos
- 29. Admiral Cloud
- 30. Competitions
- 31. Scope of this Privacy Policy
- 32. Policy subject to change
- 33. Note on gender

## 1. Where data protection applies

Data protection applies to personal data. According to Article 4 No. 1 GDPR, personal data means any information relating to an identified or identifiable natural person. For example, this includes details such as name, postal address, email address and phone number, but also usage data such as your IP address, if applicable.

## 2. Controller and data protection officer

- 2.1 The **German Association for Quality (DGQ e.V.)**, represented by its Board, is the controller for the data processing carried out in connection with operating this website and the DGQ networking portal "DGQplus", managing membership of DGQ, running examinations and certification and cooperating with regional groups across Germany.

The controller for data processing in connection with research activities relating to quality assurance, quality management and in related subject areas, including managing the relevant membership, is the **FQS Forschungsgemeinschaft Qualität e.V. (FQS e.V.)**, represented by its Board.

The data controller for the data processing that is carried out in the course of delivering training, courses and seminars, related events and consulting services as well as when operating the e-learning platform, including e-learning sessions and webinars that are provided on the platform, is **DGQ Weiterbildung GmbH**, represented by its Managing Director Claudia Welker.

DGQ e.V., FQS e.V. and DGQ Weiterbildung are hereinafter jointly referred to as "**DGQ**". Where statements are made regarding data protection at "DGQ" in this Privacy Policy (including with reference to "us"), such statements apply equally to DGQ e.V. and DGQ Weiterbildung.

You can contact DGQ e.V., FQS e.V. and DGQ Weiterbildung at:

August-Schanz-Str. 21 A  
D-60433 Frankfurt/Main, Germany  
Phone +49 (0)69-9 54 24-0  
Fax +49 (0)69-9 54 24-133  
[info@dgg.de](mailto:info@dgg.de)

- 2.2 You can contact the data protection officer for DGQ, who is appointed for all DGQ companies, at:

Data protection officer  
August-Schanz-Str. 21 A

D-60433 Frankfurt/Main, Germany  
Phone +49 (0)69-9 54 24-0  
Fax +49 (0)69-9 54 24-133  
[datenschutzbeauftragter@dgq.de](mailto:datenschutzbeauftragter@dgq.de)

**3. Extent of data collection and processing when you visit our website**

- 3.1 When you visit the DGQ website, information that your browser sends to us is logged automatically. This includes the IP address of the device you are using, the date and time (including time zone) of access to the website and information about which specific page or file has been requested, the domain via which the relevant request has been made (known as the referrer URL), the operating system you are using and the browser you are using on your device. This data is stored in our system log files. The above data is not stored with other personal data.
- 3.2 Our system has to store your IP address temporarily for the website to be provided to your computer. We have to save your IP address throughout the time you are using the website in order to do this. For your protection, we use IP anonymisation. This involves truncating your IP address so that it can no longer be clearly linked to you. This data is therefore saved in log files for the website to function. We also use this data to optimise our website and to secure our IT systems. The data is not used for marketing purposes in this case. The legal basis for the temporary storage of the data and the log files is Article 6(1)(f) GDPR, where our legitimate interest is in providing the website.
- 3.3 The data is stored while necessary to achieve the purpose for which it has been collected. Where data is required to provide the website, it ceases to be necessary at the end of the relevant session. Your data is then deleted automatically.

**4. Extent of data collection and the processing of data for bookings via our webshop**

- 4.1 If you place an order with us to provide a service or to send you goods, we only collect, store and use your personal data to the extent necessary to perform the service or the contract. This is also the case when we run events, training sessions, examinations and certifications that you have registered for. To use our webshop, you have to register for a customer account, which allows us to store your data for future purchases. Mandatory information required for registration is indicated specifically; other information is optional. The legal basis for the associated data processing is in each case Article 6(1)(b) GDPR. This may also require us to share your personal data with companies we use to perform the service or the contract. This includes, for example, transport companies and other service providers. This data is also sent to the service providers we use on the basis of Article 6(1)(b) GDPR.
- 4.2 Similarly, when you book and take part in e-learning sessions or webinars with DGQ Weiterbildung that are held on the e-learning platform, the associated processing of your personal data by DGQ Weiterbildung is solely for the purpose of fulfilling and processing the contract concluded with you, in accordance with Article 6(1)(b) GDPR. For more information on the nature and extent of data processing when using the e-learning platform, please see DGQ Weiterbildung's terms of use for e-learning and webinars.
- 4.3 In all cases in which data processing as described above is for the purpose of fulfilling a contract, providing your personal data is necessary for the conclusion of the contract (cf. Article 13(2)(e) GDPR). Without your personal data, we are unable to perform the contract.
- 4.4 Your data is deleted as soon as it is no longer required to achieve the

purpose for which it has been collected. This is usually the case for data collected during registration if you cancel registration or delete your access details. However, if this data is also required for the fulfilment of a contract or to take steps prior to entering into a contract, it can only be deleted immediately where there are no contractual or statutory obligations that prevent deletion. We may be contractually or legally obliged to store data even after the end of the contract (e.g. for tax purposes). The storage periods that apply in this case must be determined specifically for the relevant contracts and the parties to those contracts.

## **5. Use of data for specific purposes and disclosure to third parties**

5.1 We follow the principle of using data for specific purposes and we only collect, process and use your personal data for the purposes for which you have provided the data to us or for which we have collected the data. Please see the other sections of this Privacy Policy for details.

5.2 Your personal data is not disclosed to third parties without your express consent, unless this is necessary to perform the service or the contract (e.g. to carry out training or examinations). This means that your data is only transferred to third parties on the basis of your consent pursuant to Article 6(1)(a) GDPR or for the purposes of performing a contract pursuant to Article 6(1)(b) GDPR. Such data is also only sent to state institutions and authorities who are entitled to access the data where legal obligations to provide access apply or if we are obliged to provide access by a court decision. In this case, transferring your data is necessary pursuant to Article 6(1)(c) GDPR, to comply with a legal obligation to which we are subject.

5.3 We also take internal data protection very seriously. We have placed our employees and the service companies we use under obligation to maintain confidentiality and to comply with the provisions of data protection law.

## **6. General storage period and deletion (erasure)**

We store your personal data for as long as is necessary to fulfil the intended purpose (e.g. until the contract is performed or your membership with DGQ e.V. ends) or for as long as statutory retention periods make storage necessary. Where statutory retention obligations, such as under tax or commercial law, prevent your personal data from being deleted (erased), we restrict the processing of your data; your data is then deleted in accordance with the statutory regulations.

## **7. Your rights as a data subject**

7.1 According to Article 15(1) GDPR, you have the right to obtain access to the personal data we have stored relating to you, on request and free of charge.

7.2 You also have the right to have your personal data corrected (rectified) (Article 16 GDPR), deleted (erased) (Article 17 GDPR) and restricted (Article 18 GDPR), where the statutory requirements are met.

7.3 If the data processing is based on Article 6(1)(f) GDPR (legitimate interest), you have the right to object in accordance with Article 21 GDPR. If you object to data processing, we will no longer process your data in the future, unless we can demonstrate compelling legitimate grounds for further processing which override your interests in objecting.

- 7.4 If you have provided the processed data yourself, you have the right to data portability in accordance with Article 20 GDPR.
- 7.5 If the data processing is based on consent pursuant to Article 6(1)(a) or Article 9(2)(a) GDPR, you may withdraw your consent at any time with effect for the future without affecting the lawfulness of processing that has already taken place.
- 7.6 To exercise your rights as set out above, please contact us at the contact address above or email us or our data protection officer. We are always available and happy to answer any further queries you may have about our Privacy Policy and the processing of your personal data.

## **8. Data processing for the online application**

- 8.1 Deciding to apply online makes it easier for us to process your application and it speeds up the application process.
- 8.2 The personal data you provide to us as part of an application (typically: contact details, cover letter and application documents; together referred to as the "application data") is only stored and used electronically for the purpose of processing the application. The data is not disclosed to third parties outside DGQ. The following people have access to your data: Staff members in the human resources department, the responsible line manager, and the works council (if any). If your application leads to a second interview in person, future colleagues receive your CV so that they can prepare for the interview. All these people are under obligation to maintain data secrecy and shall treat your application as absolutely confidential.
- 8.3 Before you submit your binding application, you will be asked to consent to storage of your personal data for a period of one year after the end of the application process. The reason for this is so that we can contact you again at a later date. The data provided during an application for a vacancy at DGQ is collected and processed in accordance with Article 88 GDPR in conjunction with Section 26(1) BDSG. If we continue to store your personal data in our applicant management system for a period of one year after completion of the application process, the data is stored in accordance with Article 6(1)(a) GDPR on the basis of your consent provided voluntarily. Otherwise, your data (application data and interview results) shall be deleted in entirety from our applicant management system no later than six months after the end of the application process.

## **9. Use of cookies**

- 9.1 We use technical tools on our website for various functions. In particular, we use cookies, which may be stored on your device. When you access our website and at any time subsequently, you have the choice of whether you allow cookies to be set generally or you can choose which specific additional functions you want. You can make changes to your browser settings or via our Consent Manager. Below, we start by describing cookies from a technical point of view, before going into more detail about your individual choices by describing technically necessary cookies and cookies that you can optionally select or deselect.
- 9.2 Cookies are text files or information in a database that are stored on your hard drive and linked to the browser you are using, so that certain information can be sent to the operator who has set the cookie. Cookies cannot execute programs or transfer viruses to your computer. They are primarily used to make our website faster and more user-

friendly. This website uses the following types of cookies. How they function and the legal basis for the cookies is explained below:

- Transient cookies: These cookies, in particular session cookies, are automatically deleted when you close your browser or log out. They contain a session ID. This means that various requests from your browser can be assigned to the same session and we can recognise your computer when you return to our website.
- Persistent cookies: These cookies are deleted automatically after a predefined time, which varies depending on the cookie. You can view the cookies that have been set and the expiry times in the settings of your browser at any time and you can delete the cookies manually.

9.3 Mandatory functions that are technically necessary to display the website: The technical structure of the website requires us to use certain technologies, in particular cookies. Without these technologies, our website cannot be displayed (without errors) or it would not be possible to provide the support functions. These are transient cookies that are deleted after the end of your visit to our website, at the latest when you close your browser. You cannot opt out of these cookies if you wish to use our website. See the Consent Manager for details of the specific cookies. The legal basis for such processing is Section 25(2) No. 2 of the German Telecommunications and Telemedia Data Protection Act (TTDSG) in conjunction with Article 6(1)(f) GDPR.

9.4 Optional cookies when you give your consent: We only set various cookies after you have given your consent, which you can select on your first visit to our website using the cookie consent tool. The functions are only activated with your consent and may be used in particular so that we can analyse and improve visits to our website, make it easier for you to use the website via different browsers or devices, recognise you when you visit the website or to provide advertising (if applicable, also in order to tailor advertising to interests, to measure the effectiveness of ads or to display interest-based advertising). The legal basis for such processing is Section 25(1) of the German Telecommunications and Telemedia Data Protection Act (TTDSG) in conjunction with Article 6(1)(a) GDPR. You can withdraw your consent at any time, which does not affect the lawfulness of processing before you withdraw your consent.

The functions we use, which you can select and deselect individually via the Consent Manager, are described below.

[Change consent](#)

THE COOKIE TABLE IS DISPLAYED HERE

## 10. Sending our newsletter and analysis of newsletter usage

- 10.1 We are very happy to send you our newsletter, with your consent. You have to register for our newsletter before we can send it. Details of the content of the relevant newsletter are provided in the declaration of consent or on the registration page.
- 10.2 We use the double opt-in procedure when you register for our newsletter. After you register, we will send a message to the email address you have provided with a link that you can click on to confirm that you want to receive the newsletter. As evidence that you have registered for the newsletter, we store the time of registration and



confirmation, as well as your IP address at that time. After you have confirmed, we store your email address for the purpose of sending you the newsletter.

- 10.3 Please note that you only need to provide your email address when you register for the newsletter. Providing other data, which is indicated separately, is optional and will be used to address you personally.
- 10.4 As the newsletter is only sent to you with your consent, the legal basis for the related data processing is Article 6(1)(a) GDPR. You can withdraw your consent and unsubscribe from the newsletter at any time. You can withdraw by clicking the link provided in every newsletter email or by sending a message to our contact details provided at the start of this Privacy Policy and in our legal notice.
- 10.5 We analyse how you use the newsletter and use our findings to improve and personalise the newsletter, provided you have given your consent to this. For analysis, the newsletter emails that we send contain web beacons, which are used to record the email being opened and subsequent further use. To analyse use of the newsletter, we process the information from the web beacons and the technical data collected to send the email together with your email address and an individual identifier ("ID") and other data relating to the relevant user account. We also record when you click on a link received in the newsletter. By analysing this data, we can assess general use of the newsletter and gain insights into which content and parts should be further improved and developed, according to user habits. We also use the above data to determine which content and links individual users have viewed or clicked on, and draw conclusions from this about a user's individual habits, requirements and interests regarding the newsletter and its content. We use this data to tailor the newsletter to your individual needs and interests. We may also link the insights we gain to actions you take on our website in order to further customise and personalise the newsletter and website content.
- 10.6 We only analyse your use of the newsletter with your consent. The legal basis for such analysis is therefore Article 6(1)(a) GDPR and Section 25(1) of the German Telecommunications and Telemedia Data Protection Act (TTDSG). It is not possible for us to use the newsletter without the analysis function. However, you can withdraw your consent to such analysis of usage at any time by unsubscribing from the newsletter. You can withdraw by clicking the link provided in every newsletter email or by sending a message to our contact details provided at the start of this Privacy Policy and in our legal notice.
- 10.7 You can also prevent analysis using web beacons from the start by disabling images being displayed in your email program. In this case, the newsletter will not be displayed in full and you may not be able to use all the functions.
- 10.8 The newsletter is sent and use of the newsletter is analysed using Act-On, a service provided by the US provider, Act-On Software, Inc, 8300 SW Creekside Place, Suite 250, Beaverton, Oregon 97008, USA ("Act-On"). For these purposes, Act-On receives and uses the above information on our behalf. According to the information it has provided, Act-On may also use this data to optimise or improve its own services, e.g. to technically optimise sending and display of the newsletter. However, Act-On does not use the data from the recipients of our newsletter to write to them itself and does not disclose such data to third parties. For more details on the technologies used by Act-On and for more information about how Act-On handles personal data, please see Act-On's Privacy Policy.

- 10.9 Please note that there may be additional risks associated with transferring data to servers in the USA that are used by Act-On. For example, it may be more difficult to enforce your rights with regard to such data. For any transfer of data to the USA, we have concluded an agreement with Act-On as the processor who processes data on our behalf in accordance with Article 28 GDPR, as well as the standard contractual clauses for data protection from the EU Commission, which also require the implementation of appropriate protection measures for the specific case, which may also include encryption of the data, depending on the level of protection required. If data is transferred to the USA or another third country, such transfer to a third country is based on your consent in accordance with Article 49(1)(a) GDPR, which you give via the Consent Manager (or other forms, registrations, etc.).

## **11. DGQplus networking portal**

- 11.1 We provide an independent network and member portal called "DGQplus" (hereinafter also referred to as the "Portal"). This Portal is used as an optional platform for DGQ members and visitors to DGQ events where they can share information and find answers to frequently asked questions, find relevant information, e.g. about upcoming DGQ events and created documents or solutions to problems, and can share information with other users of the Portal.
- 11.2 To access DGQplus, you must register for the Portal and create a user profile. For registration, we collect some personal data from you (first and last name, email address and, if applicable, your postcode so that we can initially offer you the best possible selection of the DGQ regional groups or working groups relevant to you), which is necessary to complete registration and to accept the user agreement for the Portal. You can also optionally add further details, such as a profile photo to round out your user profile.
- 11.3 When registering, we also check whether you are a member of DGQ, using the data you enter, so we can give you access to exclusive member areas, if applicable. To simplify this matching process, we recommend that you use the same email address for the Portal as you used when joining DGQ.
- 11.4 Your user profile, which is created during registration, is only visible to other users logged on to DGQplus. Your profile also shows those users which groups you have joined on DGQplus (e.g. your DGQ regional group or a working group). Your user profile also contains an overview of some of your activities on the Portal, such as when you tag content from others as "interesting", when you share or when you comment. This information to other users is essential to make DGQplus a place for active, DGQ-wide networking, not least so that cross-regional events can be coordinated and as the basis for the active exchange of information on the Portal.
- 11.5 Certain people who are not members of DGQ ("Guests") may be given the opportunity to register for certain groups on the Portal, on special invitation by an administrator. The registered profiles of guests are only visible to other users logged on to DGQplus.
- 11.6 You can submit questions, post comments, documents and other content publicly on the Portal. The content is then generally available for access by any user logged on to DGQplus. You can also publish your content for specific groups only (e.g. your associated regional group), which gives access to your content to the members of the group only. Please note that, when publishing your content, it is not possible to rule out the possibility that the users authorised to access the content may process your content further, for example by copying or downloading documents you have provided and processing them further. We therefore recommend that you check your content before



publication to ensure that it contains only the absolute minimum of personal data, in particular confidential data. If you would like certain content to be visible only to a selected person, you also have the option of sending them a direct message.

- 11.7 If you respond to another user's content (for example, by tagging it as "interesting" or by commenting on it), the other user may – depending on your settings – be notified of your response.
- 11.8 You can also register and cancel your registration for certain events via DGQplus. We may forward your registration or cancellation to the applicable organisers of the event for the purpose of planning and running the event.
- 11.9 Every time you access the Portal – just as when visiting our websites – information set by your browser is automatically logged and processed to provide the Portal. For details, see the section above ("Extent of data collection and processing when you visit our website"). The Portal also sets certain cookies that are necessary to provide Portal functions, such as to save your login details so that you are automatically logged in the next time you visit the Portal. For more information on cookies, see the specific section above on the use of cookies ("Use of cookies"). To provide the core functions of the Portal, we also process the details you enter in your user profile and your posts on DGQplus to make this content available to other users of the Portal, according to your settings.
- 11.10 We carry out such processing activities to perform the contract with you regarding the use of DGQplus, in accordance with Article 6(1)(b) GDPR.
- 11.11 As a networking portal for the purpose of exchanging information, DGQplus also includes the function of sending you information by email from time to time about important changes to the Portal and about your activities, events in the groups you have joined and your booked events. This notification function on the Portal is designed to provide you with an overview of important events on the Portal and, if necessary, with reminders about upcoming events, thereby simplifying management of your activities. You can manage and restrict this function at any time in the settings for your profile. If you restrict this function, you will only receive limited information relating to your profile, but also relating to security events, such as changes to the password for your user profile. The legal basis for data processing using this function on the networking portal is also performance of the contract with you regarding the use of DGQplus, in accordance with Article 6(1)(b) GDPR.
- 11.12 Members of DGQ also receive the above notifications regarding important activities on the Portal and the applicable member's DGQ groups even before they register for the networking portal. This is so that members are kept informed at all times, in particular before registration is completed, of (what may be short-notice) events for their associated DGQ groups, as the Portal is the primary communication channel between DGQ and its members, particularly regarding the DGQ groups and their activities. These notifications are therefore only sent as part of DGQ membership and so on the basis of an agreement with the members, which is the basis for the data processing in accordance with Article 6(1)(b) GDPR. The processing of your personal data to send event- and service-related information is based on Article 6(1)(f) GDPR, whereby our legitimate interest is in informing our members via our Portal as the primary channel of communication. You can withdraw your consent and unsubscribe from the newsletter at any time. You can opt out of receiving these notifications at any time by clicking on the link provided in each notification to change the settings. Alternatively, you can opt out by sending a message to our contact details provided at the start of this Privacy Policy and in our legal notice.

- 11.13 We also collect general information about interactions on the Portal, such as which parts of the Portal are accessed and which functions are used. We analyse this information to gain insights into how our Portal is used and so that we can further develop the Portal according to how it is actually used. The legal basis for such data processing is Article 6(1)(f) GDPR, whereby our legitimate interest is in continuously improving the Portal so that we can provide the greatest possible user convenience and an appealing design for the Portal.
- 11.14 For the technical operation of DGQplus including the analysis of interactions on the Portal as described above, we use the services of mixxt GmbH, Adenauerallee 134, 52113 Bonn, Germany ("mixxt"). mixxt receives the data listed above in this context and processes it to provide the Portal. We have concluded a processor agreement with mixxt in accordance with Article 28 GDPR, so that mixxt only processes this data within the scope of and on the basis of our instructions.
- 11.15 The profile settings give you with various options for exercising your rights regarding your personal data on the Platform, such as settings to make your posts visible to other users and to change the details of your profile. If you wish to delete your profile in entirety, please notify us using the contact details above. We will then go ahead and delete your profile. We will make your posts on the Portal anonymous so that they can no longer be attributed to you, but will retain the valuable information on the Portal for other users (for example, if you publish an answer to a frequently occurring question from another user on the Portal).
- 11.16 Otherwise, your data will be stored in accordance with our criteria for the general storage period as described above (generally, for as long as is necessary for your use of DGQplus or as long as required by statutory retention obligations), then your data will be deleted in accordance with statutory requirements.

## **12. Data processing when contacting us and using contact forms**

- 12.1 If you send us enquiries via the contact form, your details from the enquiry form, including the contact details you provide on the form, are stored by us for the purpose of processing the enquiry and in the event of follow-up enquiries. We do not share this data without your consent.
- 12.2 If you contact us by email, phone or fax, your enquiry including all the personal data arising from your enquiry (name and enquiry) are stored and processed by us for the purpose of processing your request. We do not share this data without your consent.
- 13.3 This data is processed on the basis of Article 6(b) GDPR, insofar as your request is related to the performance of a contract or is necessary in order to take steps prior to entering into a contract. In all other cases, the processing is based on our legitimate interest in the effective handling of the enquiries made to us (Article 6(1)(f) GDPR) or on your consent (Article 6(a) GDPR) if this has been requested; your consent may be withdrawn at any time.
- 13.4 We shall keep the data you have entered on the contact form or sent with your contact query until you request that we delete it, withdraw your consent to it being stored or the purpose for storing the data no longer applies (e.g. after processing your query is complete). Mandatory statutory provisions – in particular, retention periods – remain unaffected.
- 13.5 To provide the Contact forms, we use a software solution provided by Act-On Software, Inc, 8300 SW Creekside Place, Suite 250, Beaverton, Oregon 97008, USA ("Act-On").

For these purposes, Act-On receives and uses the above information on our behalf. According to the information it has provided, Act-On may also use this data to optimise or improve its own services, e.g. to technically optimise sending and display of the newsletter. However, Act-On does not use the data from the recipients of our newsletter to write to them itself and does not disclose such data to third parties. For more details on the technologies used by Act-On and for more information about how Act-On handles personal data, please see Act-On's Privacy Policy.

- 13.6 Please note that there may be additional risks associated with transferring data to servers in the USA that are used by Act-On. For example, it may be more difficult to enforce your rights with regard to such data. For any transfer of data to the USA, we have concluded an agreement with Act-On as the processor who processes data on our behalf in accordance with Article 28 GDPR, as well as the standard contractual clauses for data protection from the EU Commission, which also require the implementation of appropriate protection measures for the specific case, which may also include encryption of the data, depending on the level of protection required. If data is transferred to the USA or another third country, such transfer to a third country is based on your consent in accordance with Article 49(1)(a) GDPR, which you give via the Consent Manager (or other forms, registrations, etc.).

#### **14. Use of the blog functions**

- 14.1 You can make public comments on our blog, where we publish various posts on topics related to our activities. Your comment is published with your entered username under the post. We recommend using a pseudonym instead of your real name. A username and an email address are required; all other information is optional.
- 14.2 If you post a comment, we continue to store your IP address, which we delete after one week. Storage is necessary to be able to defend ourselves against claims based on liability, in cases in which illegal content may be published. We need your email address to contact you if a third party objects to your comment as illegal. The comments and the associated data are stored and remain on the website until the commented content has been deleted completely or the comments have to be deleted for legal reasons.
- 14.3 The legal basis is your consent pursuant to Article 6(1)(a) GDPR. You can withdraw any consent you have given at any time. All you need to do is send us a simple message by email. The legality of the data processing operations that have already been carried out remains unaffected by your withdrawal of consent. The comments are not checked before publication. We reserve the right to delete comments if we or third parties object to them as illegal.
- 14.4 As a user of the website, you can subscribe to the blog after registering. You will receive a confirmation email to verify that you are the owner of the email address that has been provided. You can unsubscribe from this function at any time using a link in the info emails. For details, please see the information in section 10 of this Privacy Policy.

#### **15. Conferences via GoToMeeting**

- 15.1 We also use GoToMeeting, provided by GoTo Technologies Ireland Unlimited Company, The Reflector, 10 Hanover Quay, Dublin 2, Ireland ("GoTo"), to run internal digital meetings for DGQ and its members.
- 15.2 For this service, GoTo collects your participant data, your email address and, if applicable, further login data and technical data about your device, such as your IP address. It processes this data on our behalf in order to provide the virtual room for

participating in the meeting. During the meeting, your participant data is visible to the other participants, to make the interactive sharing of ideas and experience possible. You can change and stop your audio and video from being shared via the settings, which are available at all times during the meeting.

- 15.3 GoTo also provides a recording function, but we do not use it for these meetings. If, in exceptional cases, a recording is to be made (e.g. as minutes of the meeting), we will inform you of this in advance and obtain your consent.
- 15.4 Data is processed for the purposes of digital meetings for DGQ members so that you can exercise your rights as a DGQ member or member of the specialist and regional groups and it is therefore processed to performance a contract, in accordance with Article 6(1)(b) GDPR.
- 15.5 GoToMeeting also includes GoTo's analysis functions, which are used to analyse how the meetings are run and used. We cannot disable these analysis functions. However, we do not use this analysis function and do not via the collected data or reports provided by these functions. We also do not control the analyses via parameters or filter criteria.
- 15.6 For details of general data protection at GoTo, see GoTo's Privacy Policy.
- 15.7 We have concluded a processor agreement with GoTo, which means that LogMeIn processes the above data on our behalf on the basis of Article 28 GDPR. In connection with the online conference services, GoTo may also send the data that is processed in this case to servers used by GoTo outside the EU, in particular in the USA, insofar as this is necessary to provide these services. As we have already explained, there is no adequacy decision by the EU Commission for the USA and there is no consistently high level of data protection because of the difference in statutory provisions. Sending data to servers in the USA may therefore give rise to additional risks. For example, it may be more difficult to enforce your rights as data subject with regard to such data. We have therefore concluded the EU standard data protection clauses with GoTo, which also require the implementation of appropriate protection measures, which may also include encryption of the data, depending on the need for protection, and are improved in accordance with the statutory and technical conditions for adequate protection of the data. If data is transferred to the USA or another third country, such transfer to a third country is based on your consent in accordance with Article 49(1)(a) GDPR, which you give via the Consent Manager (or other forms, registrations, etc.).

## **16. Events using GoToTraining**

- 16.1 DGQ runs some events and courses digitally via the GoToTraining conference service provided by GoTo Technologies Ireland Unlimited Company, The Reflector, 10 Hanover Quay, Dublin 2, Ireland ("GoTo") to provide flexible event formats.
- 16.2 For this service, GoTo processes your participant data, your login data and technical data about your device, such as your IP address, in order to provide the virtual room for the event on our behalf.
- 16.3 During the event, your participant data may also be displayed to other participants to make active discussion possible, for example, when the participants are assigned to different, virtual group rooms to run the event. You can change and stop your audio and video from being shared via the settings, which are available at all times during the event. We do not record the event.

- 16.4 The processing of data for the conference service is necessary for performance of the contract for the event, in accordance with Article 6(1)(b) GDPR, provided that you have made a binding booking for the relevant course with us. Otherwise, the data is processed on the basis of our legitimate interests pursuant to Article 6(1)(f) GDPR, which are in running the event that is offered specifically as an online format. By using the online format, we can also offer a flexible event for participants, in your interest, for which you do not have to be present at a specific location.
- 16.5 We also use analytics tools provided by GoTo as part of these events to analyse how the events are run and used and to gain insights to improve the events. For this purpose, we need information about how the event was run generally and about the interactions of the participants. GoTo creates reports for us with general technical information about the course of the event and the devices that are used by participants, as well as data about joining the event and general participation in the event. We do not combine this data with any other information about the participants and we do not create any usage profiles from this data. The legal basis for data processing for such purely statistical analysis is Article 6(1)(f) GDPR. Our legitimate interest is in the continuous development and optimisation of our event formats for the best possible participant experience. You can object to the collection of your data in these reports, e.g. by sending a message to our contact details above, stating the email address you used to register for the event. If you object, we shall only use your data in accordance with the above paragraphs for the purpose of running the event, including verifying actual participation in the event and identifying and, where possible, correcting technical problems during the event.
- 16.6 For details of general data protection at GoTo, see GoTo's Privacy Policy.
- 16.7 We have concluded a processor agreement with GoTo, which means that GoTo processes the above data on our behalf on the basis of Article 28 GDPR. In connection with the online conference services, GoTo may also send the data that is processed in this case to servers used by GoTo outside the EU, in particular in the USA, insofar as this is necessary to provide these services. As we have already explained, there is no adequacy decision by the EU Commission for the USA and there is no consistently high level of data protection because of the difference in statutory provisions. Sending data to servers in the USA may therefore give rise to additional risks. For example, it may be more difficult to enforce your rights as data subject with regard to such data. We have therefore concluded the EU standard data protection clauses with GoTo, which also require the implementation of appropriate protection measures, which may also include encryption of the data, depending on the need for protection, and are improved in accordance with the statutory and technical conditions for adequate protection of the data. If data is transferred to the USA or another third country, such transfer to a third country is based on your consent in accordance with Article 49(1)(a) GDPR, which you give via the Consent Manager (or other forms, registrations, etc.).

## **17. Webinars using GoToWebinar**

- 17.1 We also use the GoToWebinar online webinar service provided by GoTo Technologies Ireland Unlimited Company, The Reflector, 10 Hanover Quay, Dublin 2, Ireland ("GoTo") to run certain webinars.
- 17.2 For this service, GoTo collects your participant data (i.e. your name, chat posts and any audio and video you may have shared), your email address and, if applicable, other login data, as well as technical data about your device such as your IP address, and it processes this data on our behalf in order to set up and provide the webinar.



- 17.3 During the webinar, depending on the webinar format, we as the organiser may make your participant data visible to all other participants so that you can submit and view questions and comments relevant to the webinar as a whole and so that participants can share information.
- 17.4 The processing of data for the webinar service is necessary for performance of the contract for training in the form of a webinar, in accordance with Article 6(1)(b) GDPR, provided that you have made a binding booking for the webinar with us. Otherwise, the data is processed on the basis of our legitimate interests pursuant to Article 6(1)(f) GDPR, which are in running the training courses that are offered specifically webinars. By using the webinar format, we can also offer a flexible training option for participants, in your interest, for which you do not have to be present at a specific location.
- 17.5 We also use analytics tools provided by GoTo within these webinars to analyse how the webinars are run and used. Using such analyses, we can gain insights into which aspects of the webinars can be improved, in the interest of users, to make participation in the webinar as convenient and straightforward as possible. For this purpose, we need information about how the webinar was run generally and about the interactions of the participants. GoTo creates reports for us with general technical information about the course of the webinar and the devices that are used by participants, as well as data about joining the event and general participation in the webinar. We do not combine this data with any other information about the participants and we do not create any usage profiles from this data. We also do not analyse the active participation of individual participants during the webinar using attention tracking. The legal basis for data processing for such purely statistical analysis is Article 6(1)(f) GDPR. Our legitimate interest is in the continuous development and optimisation of our webinar formats for the best possible participant experience. You can object to the collection of your data in these reports, e.g. by sending a message to our contact details above, stating the email address you used to register for the webinar. If you object, we shall only use your data in accordance with the above paragraphs for the purpose of running the webinar, including verifying actual participation in the webinar and identifying and, where possible, correcting technical problems during the webinar.
- 17.6 GoTo also provides the option of recording webinars. These recordings also include participant data you have disclosed during the webinar (name, chat posts and any audio and video you have shared). We only use this recording function with your consent to give you and other participants the option of repeating and referring back to the webinar content in its entirety at a later date. We also make the recordings available to people who are interested who were prevented from attending at short notice and to other customers, so that they can catch up on the webinar later on their own. The processing of your data for these recordings is based on your consent in accordance with Article 6(1)(a) GDPR. You can withdraw your consent for the future at any time. If you withdraw your consent, we will immediately remove or make unrecognisable any of your data that could be used to identify you.
- 17.7 You can change and stop your audio and video from being shared via the settings, which are available at all times during the webinar.
- 17.8 For details of general data protection at GoTo, see GoTo's Privacy Policy.
- 17.9 We have concluded a processor agreement with GoTo, which means that GoTo processes the above data on our behalf on the basis of Article 28 GDPR. In connection with the online conference services, GoTo may also send the data that is processed in this case to servers used by GoTo outside the EU, in particular in the USA, insofar as this is necessary to provide these services. As we have already explained, there is no



adequacy decision by the EU Commission for the USA and there is no consistently high level of data protection because of the difference in statutory provisions. Sending data to servers in the USA may therefore give rise to additional risks. For example, it may be more difficult to enforce your rights as data subject with regard to such data. We have therefore concluded the EU standard data protection clauses with GoTo, which also require the implementation of appropriate protection measures, which may also include encryption of the data, depending on the need for protection, and are improved in accordance with the statutory and technical conditions for adequate protection of the data. If data is transferred to the USA or another third country, such transfer to a third country is based on your consent in accordance with Article 49(1)(a) GDPR, which you give via the Consent Manager (or other forms, registrations, etc.).

## **18. Webinars using Microsoft Teams**

- 18.1 We also use Microsoft Teams, an online webinar service provided by Microsoft, to run certain webinars. Microsoft Teams is part of Microsoft Office 365. Microsoft Teams is a productivity, collaboration and sharing platform for individual users, teams, communities and networks that is used across the association. This includes a video conferencing function, as well as other functions. Microsoft Office 365 is software provided by Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland ("Microsoft").
- 18.2 For this service, Microsoft collects your participant data, i.e. communication data (e.g. your email address, if you provide a personal email address), log files, log data, metadata (e.g. IP address, time of participation, etc.), profile data (e.g. your username if you provide one yourself) and processes this data on our behalf in order to set up and provide the webinar.
- 18.3 During the webinar, depending on the webinar format, we as the organiser may make your participant data visible to all other participants so that you can submit and view questions and comments relevant to the webinar as a whole and so that participants can share information.
- 18.4 The processing of data for the webinar service is necessary for performance of the contract for training in the form of a webinar, in accordance with Article 6(1)(b) GDPR, provided that you have made a binding booking for the webinar with us. Otherwise, the data is processed on the basis of our legitimate interests pursuant to Article 6(1)(f) GDPR, which are in running the training courses that are offered specifically webinars. By using the webinar format, we can also offer a flexible training option for participants, in your interest, for which you do not have to be present at a specific location.
- 18.5 We also use analytics tools provided by Microsoft within these webinars to analyse how the webinars are run and used. Using such analyses, we can gain insights into which aspects of the webinars can be improved, in the interest of users, to make participation in the webinar as convenient and straightforward as possible. For this purpose, we need information about how the webinar was run generally and about the interactions of the participants. Microsoft creates reports for us with general technical information about the course of the webinar and the devices that are used by participants, as well as data about joining the event and general participation in the webinar. We do not combine this data with any other information about the participants and we do not create any usage profiles from this data. We also do not analyse the active participation of individual participants during the webinar using attention tracking. The legal basis for data processing for such purely statistical analysis is Article 6(1)(f) GDPR. Our legitimate interest is in the continuous development and optimisation of our webinar formats for the best possible participant experience. You can object to the collection of

your data in these reports, e.g. by sending a message to our contact details above, stating the email address you used to register for the webinar. If you object, we shall only use your data in accordance with the above paragraphs for the purpose of running the webinar, including verifying actual participation in the webinar and identifying and, where possible, correcting technical problems during the webinar.

- 18.6 Microsoft Teams also provides the option of recording webinars. These recordings also include participant data you have disclosed during the webinar (name, chat posts and any audio and video you have shared). We only use this recording function with your consent to give you and other participants the option of repeating and referring back to the webinar content in its entirety at a later date. We also make the recordings available to people who are interested who were prevented from attending at short notice and to other customers, so that they can catch up on the webinar later on their own. The processing of your data for these recordings is based on your consent in accordance with Article 6(1)(a) GDPR. You can withdraw your consent for the future at any time. If you withdraw your consent, we will immediately remove or make unrecognisable any of your data that could be used to identify you.
- 18.7 You can change and stop your audio and video from being shared via the settings, which are available at all times during the webinar.
- 18.8 For details about data protection at Microsoft, see Microsoft's Privacy Policy.
- 18.9 Data is processed by Office 365 on servers in data centres in the European Union in Ireland and the Netherlands. We have concluded a processor agreement for such processing with Microsoft in accordance with Article 28 GDPR. Microsoft can access the data for the purpose of remote maintenance. In this case, the data may also be accessed by affiliates of Microsoft from outside the European Union, including the USA. As we have already explained, there is no adequacy decision by the EU Commission for the USA and there is no consistently high level of data protection because of the difference in statutory provisions. Sending data to servers in the USA may therefore give rise to additional risks. For example, it may be more difficult to enforce your rights as data subject with regard to such data. We have therefore concluded the EU standard data protection clauses with Microsoft, which also require the implementation of appropriate protection measures, which may also include encryption of the data, depending on the need for protection, and are improved in accordance with the statutory and technical conditions for adequate protection of the data. If data is transferred to the USA or another third country, such transfer to a third country is based on your consent in accordance with Article 49(1)(a) GDPR, which you give via the Consent Manager (or other forms, registrations, etc.).

## **19. Conferences using Microsoft Teams**

- 19.1 We also use Microsoft Teams, provided by Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland, to run internal digital meetings for DGQ and its members.
- 19.2 For this service, Microsoft collects your participant data, your email address and, if applicable, further login data and technical data about your device, such as your IP address. It processes this data on our behalf in order to provide the virtual room for participating in the meeting. During the meeting, your participant data is visible to the other participants, to make the interactive sharing of ideas and experience possible. You can change and stop your audio and video from being shared via the settings, which are available at all times during the meeting.

- 19.3 Microsoft also provides a recording function, but we do not use it for these meetings. If, in exceptional cases, a recording is to be made (e.g. as minutes of the meeting), we will inform you of this in advance and obtain your consent.
- 19.4 Data is processed for the purposes of digital meetings for DGQ members so that you can exercise your rights as a DGQ member or member of the specialist and regional groups and it is therefore processed to performance a contract, in accordance with Article 6(1)(b) GDPR.
- 19.5 Microsoft Teams also includes Microsoft's analysis functions, which are used to analyse how the meetings are run and used. We cannot disable these analysis functions. However, we do not use this analysis function and do not via the collected data or reports provided by these functions. We also do not control the analyses via parameters or filter criteria.
- 19.6 For details about data protection at Microsoft, see Microsoft's Privacy Policy.
- 19.7 Data is processed by Office 365 on servers in data centres in the European Union in Ireland and the Netherlands. We have concluded a processor agreement for such processing with Microsoft in accordance with Article 28 GDPR. Microsoft can access the data For the purpose of remote maintenance. In this case, the data may also be accessed by affiliates of Microsoft from outside the European Union, including the USA. As we have already explained, there is no adequacy decision by the EU Commission for the USA and there is no consistently high level of data protection because of the difference in statutory provisions. Sending data to servers in the USA may therefore give rise to additional risks. For example, it may be more difficult to enforce your rights as data subject with regard to such data. We have therefore concluded the EU standard data protection clauses with Microsoft, which also require the implementation of appropriate protection measures, which may also include encryption of the data, depending on the need for protection, and are improved in accordance with the statutory and technical conditions for adequate protection of the data. If data is transferred to the USA or another third country, such transfer to a third country is based on your consent in accordance with Article 49(1)(a) GDPR, which you give via the Consent Manager (or other forms, registrations, etc.).

## **20. Events and e-training using Microsoft Teams**

- 20.1 DGQ runs some events and courses digitally via the Microsoft Teams conferencing service provided by Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland, to offer flexible event formats.
- 20.2 For this service, Microsoft processes your participant data, your login data and technical data about your device, such as your IP address, in order to provide the virtual room for the event on our behalf.
- 20.3 During the event, your participant data may also be displayed to other participants to make active discussion possible, for example, when the participants are assigned to different, virtual group rooms to run the event. You can change and stop your audio and video from being shared via the settings, which are available at all times during the event. We do not record the event.
- 20.4 The processing of data for the conference service is necessary for performance of the contract for the event, in accordance with Article 6(1)(b) GDPR, provided that you have made a binding booking for the relevant course with us. Otherwise, the data is

processed on the basis of our legitimate interests pursuant to Article 6(1)(f) GDPR, which are in running the event that is offered specifically as an online format. By using the online format, we can also offer a flexible event for participants, in your interest, for which you do not have to be present at a specific location.

- 20.5 We also use analytics tools provided by Microsoft as part of these events to analyse how the events are run and used and to gain insights to improve the events. For this purpose, we need information about how the event was run generally and about the interactions of the participants. Microsoft creates reports for us with general technical information about the course of the event and the devices that are used by participants, as well as data about joining the event and general participation in the event. We do not combine this data with any other information about the participants and we do not create any usage profiles from this data. The legal basis for data processing for such purely statistical analysis is Article 6(1)(f) GDPR. Our legitimate interest is in the continuous development and optimisation of our event formats for the best possible participant experience. You can object to the collection of your data in these reports, e.g. by sending a message to our contact details above, stating the email address you used to register for the event. If you object, we shall only use your data in accordance with the above paragraphs for the purpose of running the event, including verifying actual participation in the event and identifying and, where possible, correcting technical problems during the event.
- 20.6 For details about data protection at Microsoft, see Microsoft's Privacy Policy.
- 20.7 Data is processed by Office 365 on servers in data centres in the European Union in Ireland and the Netherlands. We have concluded a processor agreement for such processing with Microsoft in accordance with Article 28 GDPR. Microsoft can access the data For the purpose of remote maintenance. In this case, the data may also be accessed by affiliates of Microsoft from outside the European Union, including the USA. As we have already explained, there is no adequacy decision by the EU Commission for the USA and there is no consistently high level of data protection because of the difference in statutory provisions. Sending data to servers in the USA may therefore give rise to additional risks. For example, it may be more difficult to enforce your rights as data subject with regard to such data. We have therefore concluded the EU standard data protection clauses with Microsoft, which also require the implementation of appropriate protection measures, which may also include encryption of the data, depending on the need for protection, and are improved in accordance with the statutory and technical conditions for adequate protection of the data. If data is transferred to the USA or another third country, such transfer to a third country is based on your consent in accordance with Article 49(1)(a) GDPR, which you give via the Consent Manager (or other forms, registrations, etc.).

## **21. Online examinations using Easy LMS**

- 21.1 DGQ runs some online examinations digitally via the platform provided by Easy LMS B.V., Oude Delft 48, 2611 CD Delft, The Netherlands ("Easy LMS") in order to offer examinations efficiently.
- 21.2 For this service, Easy LMS processes your participant and access data, as well as technical data about your device, such as your IP address, in order to provide the examination on our behalf.
- 21.3 The processing of data for the examination platform is necessary for performance of the contract for the examination, in accordance with Article 6(1)(b) GDPR, provided that you have made a binding booking for the relevant course with us. Otherwise, the data

is processed on the basis of our legitimate interests pursuant to Article 6(1)(f) GDPR, which are in running the examination that is offered specifically as an online format. By using the online format, we can also offer a flexible examination for participants, in your interest, for which you do not have to be present at a specific location.

- 21.4 For details about data protection at Easy LMS, see Easy LMS's Privacy Policy.
- 21.5 Data is processed by Easy LMS on servers in data centres in the European Union in Germany. We have concluded a processor agreement for such processing with Easy LMS in accordance with Article 28 GDPR. Subcontractors may be involved in providing the service. In this case, the data may also be accessed by companies from outside the European Union, including the USA. As we have already explained, there is no adequacy decision by the EU Commission for the USA and there is no consistently high level of data protection because of the difference in statutory provisions. Sending data to servers in the USA may therefore give rise to additional risks. For example, it may be more difficult to enforce your rights as data subject with regard to such data. Easy LMS has therefore concluded the EU standard data protection clauses with processors outside the EEA, which also require the implementation of appropriate protection measures, which may also include encryption of the data, depending on the need for protection, and are improved in accordance with the statutory and technical conditions for adequate protection of the data. If data is transferred to the USA or another third country, such transfer to a third country is based on your consent in accordance with Article 49(1)(a) GDPR, which you give via the Consent Manager (or other forms, registrations, etc.).

## **22. Use of Matomo**

- 22.1 On this website, we use the Matomo web analytics service (formerly Piwik) to analyse and check use of our website. We can use the statistics from Google Analytics to improve our website and make it more interesting for you as a visitor.
- 22.2 For these purposes, the service records the third-party website from which you have accessed our site (the called referrer URL); information about the time of access and the location from which you have accessed the website; your language settings; which parts of our website you access; and how often and for how long you have viewed a particular part of our website. We run a version of Matomo that does not require cookies. No Matomo cookies are therefore stored on your computer for the purpose of web analysis. Only your IP address and the above information is recorded for the purpose of analysing website usage. We store the information collected in this way on our server in Germany.
- 22.3 This website uses Matomo with the "AnonymizeIP" extension. This means that IP addresses are only further processed after being truncated and any way of using them to identify you personally has been prevented. It is therefore no longer possible to use this information to identify you as a user. The IP address sent by your browser to Matomo is not combined with other data we collect; no data is passed on to third parties either. The processed data is not used to create profiles about individual users.
- 22.4 The Matomo program is an open source project. For more information about data protection, please see the Matomo Privacy Policy and further information about GDPR.
- 22.5 We use Matomo on the basis of our legitimate interests pursuant to Article 6(1)(f) GDPR. Our legitimate interest is in continuously improving our website to ensure the greatest possible user convenience, which we can only achieve on the basis of anonymised analyses of user behaviour. That is because this is the only way to know



e.g. which areas of our website were visited frequently and which have not been visited at all or only visited for a short time. You can prevent your data being analysed by Matomo by deselecting the following checkbox and thereby enabling the opt-out plug-in:

- 22.6 You can prevent actions you take here from being analysed and linked. This will protect your privacy, but will also prevent the operator from learning from your actions and improving usability for you and other users.



**Your visit to this website is currently recorded by Matomo web analytics. Deselect this checkbox to opt out.**

In this case, an opt-out cookie is stored in your browser, which prevents Matomo from storing usage data. Deleting your cookies will also delete the Matomo opt-out cookie. You will then have to re-enable the opt-out plug-in when you next visit our website.

## **23. Advertising campaigns and remarketing via Google Ads**

- 23.1 We have integrated the Google Ads advertising service on this website, which is provided by Google Ireland Limited, Google Building Gordon House, Barrow St, Dublin 4, Ireland (hereinafter referred to as "Google"). Google Ads is used to display ads in the search engine and on the websites of Google and Google partners (the Google Display Network). As part of this service, we use the conversion tracking function to analyse the ad campaigns, provided you have consented. We also display the ad via cross-device advertising and remarketing functions, which display our ads in a targeted way to users who, for example, have indicated a general interest in our offers from previously visiting our websites.
- 23.2 For this ads service, Google independently selects which ads are displayed to which specific user in the Google Display Network. We are not able to give instructions regarding this choice or influence this selection. We can only impose rough restrictions on where ads may potentially be displayed, in advance, when ordering the ads by pre-setting options provided by Google. In this context, we do not send any personal data to Google and do not receive the data processed by Google for the users who see ads and we do not have any further influence on the related data processing.
- 23.3 The ads are delivered by Google using ad servers. For this purpose, we and other websites use ad server cookies, which can be used to measure certain parameters of success, such as ads displayed or user clicks. Using the Google Ads cookies stored on our website, we can access information about the success of our ad campaigns. These cookies are not intended 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 (tag that a user no longer wishes to receive ads) are usually stored as values for analysis using this cookie. The cookies set by Google enable Google to recognise your internet browser when you return. If a user visits certain pages on a Google Ads customer's website and the cookie stored on their computer has not yet expired, Google and the customer can see that the user has clicked on the ad and been redirected to that page. A different cookie is assigned to each Google Ads customer, so that the cookies cannot be tracked across other Google Ads customers' websites. By integrating Google Ads, Google is informed that you have opened the corresponding part of our website or clicked on an ad from us. If you are registered with a Google service, Google can link the visit to your account. Even if you are not registered with Google or have not logged in, it is possible that the provider will



obtain and store your IP address. Given the marketing tools that are used, your browser automatically establishes a direct connection with Google's server. We do not collect personal data ourselves for the above ads, but only provide Google with the ability to collect such data. We only receive statistical analyses from Google that provide information about which ads have been clicked, how often and at what prices. We do not receive any further data from the use of advertising; in particular, we cannot identify users from such information.

- 23.4 We use Google Ads with the additional Google Conversion Tracking application. This is a process that allows us to check the success of our ad campaigns. For this purpose, the ads have a technical feature, such as an ID, which we can use to determine how a user interacts after clicking on the ads and whether one of our services is actually used. This provides us with statistical information about the total number of viewers of our ads, which ads are particularly popular and, if applicable, with further information about the impact of the ads. For conversion tracking, a conversion cookie is stored by Google on your device when you click on an ads from us on the Google Display Network. This cookie is deleted after 90 days at the latest. When you visit our websites, we and Google are informed that you have clicked on one of our ads and have been redirected to our websites. This information may be sent to Google servers in the USA. This means that contacts you have with ads on websites on the Google Display network (visual contacts and clicks on ad banners) are linked by Google to your subsequent interactions on our website. Google also collects your IP address, the specific advertising ID for your device and technical information about your device. The data collected in this way is analysed by Google and used to create statistical reports. In this context, Google also uses other data relating to you that Google has collected when you use Google services, such as your age, gender and general categories of topics in which you have shown an interest. For conversion tracking, we only receive aggregated data that we cannot link to any individual user, and under no circumstances do we receive data that can be used to identify users personally.
- 23.5 With your consent, we also use the remarketing function provided by Google to display ads in a more targeted way. When you visit our websites and thereby express your general interest in the content on our websites, the conversion cookie is used to display targeted ads about our offers on the Google Display Network. For this purpose, the conversion cookie is used to link whether you have already visited our websites and this information is forwarded with the cookie to Google servers, which may also be located in the USA. However, we do not receive any information that could identify you personally.
- 23.6 Even using this remarketing function, Google ultimately decides independently on the specific ad that is displayed. This include in particular the exact time it is displayed and the placement of the ad, as well as the choice of whether our ad is also specifically displayed to you among the various people who have visited our websites.
- 23.7 You can disable this Google remarketing function generally for all the websites that you visit via your browser by making the appropriate settings, as described here.
- 23.8 All of the above functions for the Google Ads services are only used with your consent and therefore on the basis of Article 6(1)(a) GDPR and Section 25(1) of the German Telecommunications and Telemedia Data Protection Act (TTDSG). You can withdraw such consent for the future at any time for the computer you are using, e.g. by clicking [here](#).

When providing the above functions, Google may also send the data that is processed to servers outside the EU, in particular in the USA, insofar as this is necessary to provide these services. As we have already explained, there is no adequacy decision

by the EU Commission for the USA and there is no consistently high level of data protection because of the difference in statutory provisions. Sending data to servers in the USA may therefore give rise to additional risks. For example, it may be more difficult to enforce your rights as data subject with regard to such data. We have therefore concluded the EU standard data protection clauses with Google, which also require the implementation of appropriate protection measures, which may also include encryption of the data, depending on the need for protection, and are improved in accordance with the statutory and technical conditions for adequate protection of the data. If data is transferred to the USA or another third country, such transfer to a third country is based on your consent in accordance with Article 49(1)(a) GDPR, which you give via the Consent Manager (or other forms, registrations, etc.).

- 23.9. All of the above functions for Google Ads are run by Google across all devices. Google can therefore recognise and link your usage in certain cases across different devices that you use. To do this, Google records when you have signed into your account for Google services (such as Gmail, YouTube or the Chrome browser) in the browser on a device and links your usage on those devices with your Google account. Using this kind of cross-device linking, Google can, for example, show you ads from us that are potentially of interest to you, e.g. after your visit to our website, even if you are using a different device. Google can also link your (return) visit to our website with any previous interactions with our ads and thereby more closely measure the success of our ad campaigns, regardless of which specific device you use to visit our website.
- 23.10 Cross-device linking is also automatically processed by Google in order to further analyse the routes by which you have reached our website. We cannot disable this automatic Google function on its own. However, we do not view the details of these specific analyses by Google and do not use them for our own purposes. If you do not want this data to be linked to your Google account, you can log out of your Google account before accessing our website and thereby prevent linking.
- 23.11 You can also prevent cross-device linking completely by ensuring that personalised advertising is disabled in your Google Account settings. For instructions on disabling personalised advertising, see the Google support website.
- 23.12 For more information about how Google processes your personal data for Google Ads, for contact details where you can exercise your related rights as a data subject against Google, and for Google's applicable privacy terms, please see Google's Privacy Policy and this Google help page.

## **24. Marketing using Microsoft Advertising**

- 24.1 We use the Microsoft Advertising service with Universal Event Tracking. This service is provided by Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland ("Microsoft").
- 24.2 We use Microsoft Advertising on our websites to place ads via Microsoft that are shown on Bing, on other Microsoft services and on the ad network of Microsoft's participating partners, and to obtain information about the acceptance, reach and success of such ads and use such information to gain insights to improve our ads.
- 24.3 For these purposes, the Microsoft Advertising service records whether you have been shown one of our ads via Microsoft and whether you have clicked on that ad. If you have, your subsequent usage behaviour on our websites, technical data about your browser and your IP address are also collected. Microsoft also determines whether different use of our websites across different devices is likely to have been by the same

user and attributable to one of our ads. Hence, Microsoft can also associate your use of our websites with you across different devices.

- 24.4 Cookies are also set by the Microsoft Advertising service for this purpose. If you are logged into your Microsoft account, the cookies can also be linked to your Microsoft account. The cookies set by Microsoft Advertising remain stored on your computer for a maximum of 13 months.
- 24.5 The information collected by the Microsoft Advertising service, including cookies, is sent to Microsoft servers in the EU and the USA. Microsoft uses this information independently to analyse the reach and success of our ads with the Microsoft Advertising service and to provide us with summary reports on the results of the analyses. Microsoft retains information about you that is collected via Microsoft Advertising for 180 days.
- 24.6 Please note that Microsoft selects, in particular, the ads to be displayed and the individual user for whom an ads from us is displayed on the pages and platforms of Microsoft or a Microsoft partner. The data in connection with choosing the user and displaying the ad is processed by Microsoft independently and without further instructions from us. We are only given the option by Microsoft, when ordering the ads, to choose from various settings provided by Microsoft to apply rough restrictions in advance about the user groups to whom ads could potentially be displayed. We do not sent any personal data to Microsoft to display the ads and do not view the data processed by Microsoft from the users for whom ads are display, and we do not have any further influence on the related data processing.
- 24.7 For more information about how Microsoft handles your personal data, please see Microsoft's Privacy Policy.
- 24.8 The basis for our use of Microsoft Advertising and the associated data processing is your consent pursuant to Article 6(1)(a) GDPR and Section 25(1) of the German Telecommunications and Telemedia Data Protection Act (TTDSG). Of course, you can withdraw your consent for the future at any time for the computer you are using and object to such data processing and the setting of cookies by Microsoft Advertising at any time, for example by clicking [here](#).
- 24.9 When providing the above functions, Microsoft may also send the data that is processed to servers outside the EU, in particular in the USA, insofar as this is necessary to provide these services. As we have already explained, there is no adequacy decision by the EU Commission for the USA and there is no consistently high level of data protection because of the difference in statutory provisions. Sending data to servers in the USA may therefore give rise to additional risks. For example, it may be more difficult to enforce your rights as data subject with regard to such data. We have therefore concluded the EU standard data protection clauses with Microsoft, which also require the implementation of appropriate protection measures, which may also include encryption of the data, depending on the need for protection, and are improved in accordance with the statutory and technical conditions for adequate protection of the data. If data is transferred to the USA or another third country, such transfer to a third country is based on your consent in accordance with Article 49(1)(a) GDPR, which you give via the Consent Manager (or other forms, registrations, etc.).

## **25. Use of Sleeknote**

- 25.1 To provide user-friendly access to specific content (such as downloads, feedback options and registration for newsletters and promotions) that is appropriate to your use of our website and quick to access, we use the Sleeknote service on this website, subject to your consent. This service is operated by Sleeknote ApS, Jens Baggesens Vej 90A, 8200 Aarhus, Denmark ("Sleeknote").
- 25.2 The Sleeknote service displays certain additional content to you as a visitor, depending on what content on our website you access and how you use our website, in order to make your visit as convenient and efficient as possible for you. In this context, Sleeknote collects and stores data about use of our website, from which user profiles are created using pseudonyms, in order to analyse acceptance of the displayed content and to be able to continuously improve and optimise the individual displayed content on the basis of user needs. For this purpose, the Sleeknote service also sets cookies on your computer. These are small text files that are stored locally on your computer. The cookies are stored on your computer for a maximum of 2 years. The pseudonymised usage profiles are not combined with other personal data without the express consent of the applicable data subject. Your personal data is also not passed on to third parties. Sleeknote stores the data collected via the Sleeknote service for up to 3 months and then deletes it.
- 25.3 We have entered into a processor agreement with Sleeknote. The disclosure of personal data concerning you is therefore based on Article 28 GDPR.
- 25.4 Please also see Sleeknote's Privacy Policy for further information about how Sleeknote protects your personal data.
- 25.5 We use the Sleeknote service with your consent. The legal basis for using the Sleeknote services is therefore Article 6(1)(a) GDPR and Section 25(1) of the German Telecommunications and Telemedia Data Protection Act (TTDSG). Of course, you can withdraw your consent for the future at any time for the computer you are using and object to such data processing and the setting of cookies by Sleeknote at any time. [You can change your consent here.](#)

## **26. Social Plugins**

- 26.1 We use social plugins provided by the following social networks and providers on our website:
- Facebook, provided by Meta Platforms Ireland Ltd, Grand Canal Square, Grand Canal Har-bour, Dublin 2, Ireland ("Facebook").
  - Twitter, provided by Twitter International Company, One Cumberland Place, Fenian Street, Dublin 2, D02 AX07, Ireland ("Twitter").
  - LinkedIn, provided by LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland ("LinkedIn")

The above companies are also referred to below as social media providers.

- 26.2 To increase the protection of the users' data when visiting our website, the plugins are each integrated into the website using the "Shariff solution" provided by Heise Verlag. This integration ensures that a connection is not established with the servers of the applicable social media provider when opening the parts of our website that contain

such plugins. Only if the user activates the plugins does the user's browser establish a direct connection to the servers of the applicable social media provider.

- 26.3 If the user activates a plugin and interacts with it in this way, the applicable social media provider is informed that the user's browser has accessed the corresponding parts of our website, even if the user does not have a profile with the applicable social network or is not currently logged into the service of the applicable social media provider. This information (including the user's IP address) is sent by the user's browser directly to a server belonging to the social media provider and is stored on the server. If you interact further with the applicable plugins, such as by clicking the Facebook "Like" button, this information is also sent directly to a server belonging to the relevant provider and stored on the server. In this case, user profiles can be created from the processed data.
- 26.4 If you are logged into one of the services provided by the social media providers, the social media provider can directly link your visit to our website to your account with the relevant social network. The information is also published on the social network or on your social media account and displayed to your contacts on the network.
- 26.5 However, we have no influence over the extent of the data that the social media provider collects using the relevant plugin and therefore provide information for you below to the best of our understanding.

## **26.6 Facebook plugin**

- 26.6.1 For the Facebook plugin, we assume that, when you activate it, Facebook registers your visit to our website, the IP address of your device and that the plugin has been activated. Facebook therefore knows, from integration of the plugin, that you have accessed our website and which parts you have accessed. If you are not a registered member of Facebook, it is still possible for Facebook to receive and store your IP address. This data is also sent to Facebook servers in the USA. According to Facebook, however, they only store an anonymised IP address for users in Germany.
- 26.6.2 For the purpose and extent of data collection and further processing and of use of the data by Facebook, as well as the related rights and setting options to protect the privacy of users, see Facebook's Privacy Policy.
- 26.6.3 You can change further settings and object to the use of data for advertising purposes in your Facebook profile settings or on the page for the USA or the page for the EU. The settings are platform-independent, i.e. they apply to all devices, such as desktop computers and mobile devices.
- 26.6.4 We process data in connection with use of the Facebook plugin on the basis of Article 6(1)(f) GDPR. Our legitimate interest in using the plugins is in improving and optimally designing our website based on the wishes and preferences of users, which we discover from interaction with the plugins in the context of our website and which we implement in line with the wishes of users. Your interests are taken into account by the fact that data is only sent to Facebook if you activate the plugin yourself by clicking on it. Where Facebook transfers data to the USA for our purposes in specific cases, we and Facebook shall ensure that this is done on the basis of appropriate safeguards, such as by agreeing the EU Commission standard data protection clauses that provide for appropriate safeguards in individual cases, such as encryption of data.



## **26.7 Twitter plugin**

- 26.7.1 We understand that, when you activate the Twitter plugin, your IP address and the fact that the plugin has been activated are recorded. Therefore, by integrating the plugin, Twitter is informed that you have accessed the corresponding parts of our website and links this information to your Twitter account. Twitter also sets cookies for this purpose. If you are not a registered for the Twitter services, it is still possible for Twitter to receive and store your IP address. This data is also sent to Twitter servers in the USA.
- 26.7.2 For the purpose and extent of data collection and further processing and of use of the data by Twitter, as well as the related rights and setting options to protect your privacy, see Twitter's Privacy Policy.
- 26.7.3 You can change further settings and object to the use of data for advertising purposes in your Twitter settings. More detailed information is available [here](#). You can also object to the use of data for advertising purposes on the page for the USA or on the page for the EU. The settings are platform-independent, i.e. they apply to all devices, such as desktop computers and mobile devices.
- 26.7.4 We process data in connection with use of the Twitter plugin on the basis of Article 6(1)(f) GDPR. Our legitimate interest in using the plugins is in improving and optimally designing our website based on the wishes and preferences of users, which we discover from interaction with the plugins in the context of our website and which we implement in line with the wishes of users. There are no circumstances to establish that you have any overriding interest, as you have to activate the plugin first before data is sent to Twitter. Where Twitter transfers data to the USA for our purposes in specific cases, we and Twitter shall ensure that this is done on the basis of appropriate safeguards, such as by agreeing the EU Commission standard data protection clauses that provide for appropriate safeguards in individual cases, such as encryption of data.

## **26.8 LinkedIn plugin**

- 26.8.1 We understand that, when you activate the LinkedIn plugin, your IP address and the fact that the plugin has been activated are recorded. Therefore, by integrating the plugin, LinkedIn is informed that you have accessed the corresponding parts of our website and links this information to your LinkedIn account. We cannot rule out the possibility that LinkedIn receives and stores your IP address when the plugin is activated, even if you do not have a profile on LinkedIn.
- 26.8.2 For the purpose and extent of data collection and further processing and of use of the data by LinkedIn, as well as the related rights and setting options to protect your privacy, see LinkedIn's Privacy Policy.
- 26.8.3 You can change further settings and object to the use of data for advertising purposes in the settings for your LinkedIn account. More detailed information is available [here](#). You can also object to the use of data for advertising purposes on the page for the USA or on the page for the EU. The settings are platform-independent, i.e. they apply to all devices, such as desktop computers and mobile devices.
- 26.8.4 We process data in connection with use of the LinkedIn plugin on the basis of Article 6(1)(f) GDPR. Where LinkedIn transfers data to the USA for our purposes in specific cases, we and LinkedIn ensure compliance with appropriate protection measures on the basis of which such transfer takes place, such as by agreeing the EU Commission standard data protection clauses, provide for appropriate protective measures, such as encryption of the data in specific cases.



## 27. LinkedIn Insight Tag

- 27.1 Our website also uses the LinkedIn Insight Tag provided by LinkedIn Ireland Unlimited Company ("LinkedIn"). By integrating this JavaScript tag, you as a user of our website may be shown interest-based ads relevant to you when visiting the LinkedIn social network or other websites that also use the process, and we get statistics about website visitors and demographics. We can also analyse your use of our LinkedIn ads and your interest in our offers using a Conversion Tracking function, and show you LinkedIn ads on other websites via retargeting as well. We do this in the interest of improving the effectiveness of LinkedIn ads and making our website more interesting for you.
- 27.2 By integrating the LinkedIn Insight Tag, your browser automatically establishes a direct connection with LinkedIn's server, when visiting both the LinkedIn website and websites that have integrated the LinkedIn Insight Tag. For this purpose, LinkedIn also sets cookies on your computer. These are small text files that are stored locally on your computer. We and LinkedIn are jointly responsible for collecting your usage data when you visit our website and for sending it to the provider, but LinkedIn is solely responsible for the relevant processing for the described purposes once the data has been sent. We have no influence on the extent or nature of the use of the data by LinkedIn. We therefore provide you with information to the best of our knowledge: By integrating LinkedIn Insight Tag, LinkedIn is informed that you have opened our corresponding page or clicked on an ad from us. If you are registered with a LinkedIn service, LinkedIn can link the visit to your account. Even if you are not registered with LinkedIn or have not logged in, it is possible that the provider will obtain your IP address, time period and other identifiers and will link them to the actions associated with you.
- 27.3 You can disable the LinkedIn Insight Tag and object to advertising under the settings for ads, and also here. For further setting options and information, go to the LinkedIn Privacy Center.
- 27.4 The legal basis for processing your data and setting cookies is Article 6(1)(a) GDPR and Section 25(1) of the German Telecommunications and Telemedia Data Protection Act (TTDSG), i.e. the Tag is only integrated after you have given your consent. You can withdraw any consent you have already given for your relevant device at any time with effect for the future by changing your consent. You can change your consent here.  
28.5 When providing the above functions, LinkedIn may also send the data that is processed to servers outside the EU, in particular in the USA, insofar as this is necessary to provide these services. As we have already explained, there is no adequacy decision by the EU Commission for the USA and there is no consistently high level of data protection because of the difference in statutory provisions. Sending data to servers in the USA may therefore give rise to additional risks. For example, it may be more difficult to enforce your rights as data subject with regard to such data. We have therefore concluded the EU standard data protection clauses with LinkedIn, which also require the implementation of appropriate protection measures, which may also include encryption of the data, depending on the need for protection, and are improved in accordance with the statutory and technical conditions for adequate protection of the data. If data is transferred to the USA or another third country, such transfer to a third country is based on your consent in accordance with Article 49(1)(a) GDPR, which you give via the Consent Manager (or other forms, registrations, etc.).

## 28. YouTube videos

- 28.1 Content (such as videos) from the YouTube platform may also be integrated into our website. This service is operated by YouTube, a subsidiary of Google. Google Ireland Limited, Gordon House, Barrow Street Dublin 4, Ireland is responsible for data processing within Europe. When you visit a part of our website that has YouTube content, a connection is established to the YouTube or Google servers, and they thereby receive your IP address. In the process, the fact that you have visited our website is also shared when you play the YouTube videos. If you are logged into your YouTube account at the same time, this information can also be directly linked to your personal profile. You can prevent this by logging out of your YouTube account first. For details about data protection at YouTube and Google, in particular regarding the nature, extent and purpose of data processing, see Google's Privacy Policy.
- 28.2 YouTube also analyses views of the videos statistically and provides us with reports on these analyses. However, they only contain general information about views, such as the total number of views. We therefore do not receive more detailed information about the individual users. We integrate the videos in a way that does not set YouTube cookies when you access the videos on our websites. We therefore assume that it is not possible to analyse individual users in more detail when YouTube analyses video views. YouTube also analyses the data automatically and independently, without us being able to disable or influence such analysis or obtain further insight into the analyses.
- 28.3 We use YouTube content to enhance the user experience when using our website. We have integrated the YouTube content in such a way that data is only sent when you click on the video and reload or enable the external content. The basis for integration of YouTube content is therefore Article 6(1)(a) GDPR. You are entitled to withdraw your consent with effect for the future at any time by disabling loading external content again by unchecking the checkbox.
- 28.4 When providing the above functions, YouTube may also send the data that is processed to servers outside the EU, in particular in the USA, insofar as this is necessary to provide these services. As we have already explained, there is no adequacy decision by the EU Commission for the USA and there is no consistently high level of data protection because of the difference in statutory provisions. Sending data to servers in the USA may therefore give rise to additional risks. For example, it may be more difficult to enforce your rights as data subject with regard to such data. We have therefore concluded the EU standard data protection clauses with YouTube/Google, which also require the implementation of appropriate protection measures, which may also include encryption of the data, depending on the need for protection, and are improved in accordance with the statutory and technical conditions for adequate protection of the data. If data is transferred to the USA or another third country, such transfer to a third country is based on your consent in accordance with Article 49(1)(a) GDPR, which you give via the Consent Manager (or other forms, registrations, etc.).
- 28.5 For more information about the purpose and extent of data collection and processing by YouTube, please see Google's Privacy Policy. The Privacy Policy also provides more information about your rights and setting options to protect your privacy.

## **29. Admiral Cloud**

- 29.1 Our website uses the AdmiralCloud digital asset management system provided by AdmiralCloud AG, Fidicinstraße 3, 10965 Berlin, Germany. AdmiralCloud is a software-as-a-service platform which is used to provide content is made available on this website, including: videos, images, audio and documents.
- 29.2 To transfer videos, images, audio and documents technically, a connection to AdmiralCloud may be established when you open individual pages on this website. The connection is established as soon as you click on an applicable file. When this connection is established, data is transferred from us to the provider, AdmiralCloud AG. The data collected by the AdmiralCloud server includes details of how you use the AdmiralCloud services, your IP address, details of your browser type, browser language, date and time of viewing and the URL of the page where the content is stored. This data is used by AdmiralCloud to display customer statistics and to charge for use of storage and for traffic. This data is also stored to maintain system security. This data is stored until the end of the limitation period for claims arising such use. When a video is played via the AdmiralCloud player, the following data is also stored and processed for the statistical analysis of usage behaviour: start time of the video, end time of the video, user engagement ("how long the user was watching"). This data is presented to us as aggregated statistics that we cannot use to identify individuals.
- 29.3 The legal basis for using AdmiralCloud is Article 6(1)(f) GDPR. Our legitimate interest is in making our website as appealing and informative as possible and enhancing the functionality of the homepage. You can prevent data being passed on to AdmiralCloud by activating the "Do no track" (DNT) option in your browser. In this case, data is not stored or processed.
- 29.4 For information about the extent and purpose of data collection, further processing and use of the data by AdmiralCloud AG, as well as your rights and the settings that you can configure to protect your privacy, see AdmiralCloud AG's statement on data protection. For more general information, see the AdmiralCloud website and their Privacy Policy.

## **30. Competitions**

- 30.1 From time to time, you may have the opportunity to enter competitions on our website. During competitions for the purpose of running and managing the competitions, the following personal data may be collected, stored and used:

- first and last name;
- email address;
- postal address;

and, where applicable, the data and information you provide voluntarily as part taking part in the competition. The personal data that is collected is used exclusively for the purpose of running and managing the competition, e.g. to find out who has won the prize, to notify the winner and to send the prize. The winner's name or place of residence is not published.

- 30.2 Taking part in a DGQ competition is, of course, optional. In the conditions of taking part in the applicable competition, you will be informed both about the data required to take part in the competition and whether the competition is being organised by DGQ e.V. or DGQ Weiterbildung. If you then decide to take part, you give us your consent

to process your personal data, as required for this purpose. When you take part, you will be informed specifically about giving consent. The data is then processed based on your consent in accordance with Article 6(1)(a) GDPR. The processed data is deleted after the end or expiry of the competition or the promotion and after the prizes have been sent.

### **31. Scope of this Privacy Policy**

- 31.1 This Privacy Policy only applies to the content on DGQ websites, including the e-learning platform, and on the member Portal, as well as to the data processing on the servers we use. It does not apply to any third party content and websites that our website only provides links to. This applies, for example, to social networks such as Facebook, Twitter, Xing, YouTube and LinkedIn. Your personal data is processed via these social networks by the relevant operator of the network and we have no influence on such processing. For information on how your personal data is handled and protected on such platforms, please see the privacy policy of the relevant platform.
- 31.2 However, if we store your personal data that you have provided to us via a social network or that we receive from a social network on our own servers and use it for the purpose of processing your enquiry or request or for other purposes, our statements in this Privacy Policy, of course, then apply.

### **32. Policy subject to change**

Please note that data protection regulations and practices are subject to change. We also reserve the right to change the measures and provisions in this Policy – under prevailing statutory rules – insofar as this is required, for example, as the result of new technical developments or changes to case law or our business operations. It is therefore advisable and necessary to keep up to date with changes in statutory regulations and the practices at companies, both our own company and e.g. Google. We therefore ask you always to observe the current version of this Privacy Policy.

### **33. Note on gender**

DGQ also considers that it is important to write in a way that treats all genders equally. After extensive review, we have reached the following conclusion: There is currently no one standout solution that treats all gender identities equally. DGQ has explored and tried out various options. On this basis, it has decided to use the generic masculine in editorial articles, on the website, in flyers, emails and all other publications, including in this Privacy Policy. The reason for this is that the text is significantly easier to read and more practical, given the large number of publications. The only exception to this is the DGQ blog, where each author decides on their own approach. The DGQ sees the generic masculine as a neutral grammatical expression which – where not otherwise indicated – explicitly includes all genders.