RIB Website Privacy Policy

We are pleased that you visit our website and thank you for your interest. In the following, we inform you about how we handle your personal data when using this service. Personal data is all data that can be personally related to you, e.g., name, address, email addresses, user behavior. We have taken extensive technical and operational security measures to protect your data from accidental or intentional manipulation, loss, destruction, or access by unauthorized persons. Our security procedures are regularly reviewed and adapted to technological advances.

1. Data Processing Controller

The controller according to Art. 4 Para. 7 GDPR is:

RIB Software GmbH
Epplestraße 225, Haus 2
70567 Stuttgart, Germany
Email: Datenschutz@rib-software.com

(see our legal notice)

You can reach our Data Protection Officer at:
Datenschutz@rib-software.com

2. Purpose and Legal Basis for Processing

Personal data is only collected if you provide it to us voluntarily, such as when concluding a contract via our website or filling out the contact form. We use this data exclusively for the purpose for which you entered your data. It is used for other purposes only after explicit notification or after obtaining your consent, Art. 6 Para. 1 lit. a) GDPR. In certain cases, personal data is processed based on a legitimate interest according to Art. 6 Para. 1 lit. f) GDPR.

3. Collection of Personal Data When Visiting Our Website

When using the website for purely informational purposes, we only collect the personal data that your browser transmits to our server. If you wish to view our website, we collect the following data that is technically necessary for us to display our website to you and to ensure stability and security:

- Browser type and browser version
- Operating system used
- Referrer URL
- Hostname of the accessing computer
- Time of the server request
- IP address

The legal basis for this data processing is Art. 6 Para. 1 lit. f) GDPR. The legitimate interest lies in the proper display of its internet presence as well as ensuring the stability and security of our website.

4 Use of Cookies

4.1 General Information

Cookies are data that are stored on your computer by a website you visit and allow your browser to be re-identified. Through cookies, information is transmitted to the entity that sets the cookie. Cookies can

store various information, such as your language settings, the duration of your visit to our website, or your inputs made there. This avoids, for example, having to re-enter required form data each time you use it. The information stored in cookies can also be used to recognize preferences and align content according to areas of interest.

There are different types of cookies: Session cookies are amounts of data that are only temporarily kept in the working memory and deleted when you close your browser. Permanent or persistent cookies are automatically deleted after a predetermined duration, which can vary depending on the cookie. The information can also be stored in text files on your computer with this type of cookie. However, you can also delete these cookies at any time via your browser settings.

First-party cookies are set by the website you are currently visiting. Only this website is allowed to read information from these cookies. Third-party cookies are set by organizations that are not the operator of the website you are visiting. These cookies are used, for example, by marketing companies.

The legal bases for possible processing of personal data using cookies and their storage duration may vary. If you have given us consent, the legal basis is Art. 6 Para. 1 lit. a) GDPR and § 25 Para. 1 TDDDG. If data processing is carried out on the basis of our overriding legitimate interests, the legal basis is Art. 6 Para. 1 lit. f) GDPR and § 25 Para. 2 TDDDG. The stated purpose then corresponds to our legitimate interest.

We use cookies to ensure the proper operation of the website, to provide basic functionalities, to measure reach, and – with your consent – to tailor our services to preferred areas of interest. For this, we use both transient cookies and persistent cookies.

4.2 The Cookies Used on This Website

You can view the complete list of cookies used in our Usercentrics Consent Management HERE. Their scope and functionality are also explained there.

You can delete cookies already stored on your device at any time. If you want to prevent cookies from being stored, you can do this via the settings in your internet browser. Alternatively, you can also install so-called ad blockers. Please note that some functions of our website may not work if you have deactivated the use of cookies.

5. Website Analysis

For purposes of analyzing and optimizing our websites, we use various services, which are described below. This allows us to analyze, for example, how many users visit our site, which information is most in demand, or how users find the offer. Among other things, we collect data about which website a data subject came from to a website (known as the referrer), which subpages of the website were accessed, or how often and for what length of stay a subpage was viewed. This helps us to design our offers in a user-friendly manner and to improve them. The data collected for this purpose is not used to personally identify individual users.

5.1 Advertising

We use cookies for marketing purposes to address our users with interest-based advertising. In addition, we use cookies to limit the probability of an advertisement being displayed and to measure the effectiveness of our advertising measures. This information can also be shared with third parties, such as ad networks. The legal basis for this is Art. 6 Para. 1 a) and f) GDPR.

6. Your Rights

You have the following rights against us regarding the personal data concerning you:

6.1 General Rights

You have the right to information, correction, deletion, restriction of processing, objection to processing, and data portability. Insofar as processing is based on your consent, you have the right to revoke this to us with effect for the future.

6.2 Rights in Data Processing Based on Legitimate Interest

You have the right, according to Art. 21 Para. 1 GDPR, to object at any time, for reasons arising from your particular situation, to the processing of personal data concerning you which is carried out on the basis of Art. 6 Para. 1 e GDPR (data processing in the public interest) or on the basis of Article 6 Para. 1 f GDPR (data processing to safeguard a legitimate interest); this also applies to profiling based on this provision. In the event of your objection, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights, and freedoms, or the processing serves the establishment, exercise, or defense of legal claims.

6.3 Rights Regarding Direct Marketing

If we process your personal data to operate direct marketing, you have the right, according to Art. 21 Para. 2 GDPR, to object at any time to the processing of personal data concerning you for the purpose of such advertising; this also applies to profiling insofar as it is related to such direct marketing.

In the event of your objection to processing for direct marketing purposes, we will no longer process your personal data for these purposes.

6.4 Right to Lodge a Complaint with a Supervisory Authority

You also have the right to lodge a complaint with a competent data protection supervisory authority about the processing of your personal data by us.

The supervisory authority responsible for us is:

The State Commissioner for Data Protection and Freedom of Information Baden-Württemberg
Lautenschlagerstraße 20
70173 Stuttgart
P.O. Box 10 29 32
70025 Stuttgart

7. Contact via Email or Contact Form

When you contact us by email or through a contact form, the data you provide (your email address and your name) will be stored by us to answer your questions. Insofar as we request inputs via our contact form that are not required for contacting us, we have always marked these as optional. This information helps us to specify your request and to better handle your concern. The provision of this information is expressly voluntary and with your consent, Art. 6 Para. 1 lit. a) GDPR. If this involves information on communication channels (for example, email address, telephone number), you also consent that we may contact you via this communication channel to answer your request. You can, of course, revoke this consent at any time for the future.

We delete the data collected in this context when storage is no longer necessary, or we restrict processing if there are statutory retention obligations.

8. Contact via Chatmarshal and “Live Chat”

You have the voluntary option to contact us via the Live Chat. The Live Chat is provided by Chatmarshal, a service of Chatmarshal, Bevan Road, Rivonia, Gauteng, South Africa. To provide the live chat functionality, ChatMarshal uses the service LiveChat (Text Inc., One International Place, Suite 1400, Boston, MA 02110-2619, USA) as a sub-processor.

If you consent to the use of the “Live Chat” service, you can contact us via the Live Chat function. As part of the use of the service, the following personal data from you is processed:

• IP address
• Browser type
• Geographic location
• User ID
• Browser language
• Domain name
• Device operating system
• Username
• Contact details
• Chat content

Your inquiries are processed either by the agent “Chatmarshal” (a technical system) or qualified specialists from RIB, depending on the complexity. For the execution of the Live Chat, data may be transmitted to Chatmarshal. We have concluded a DPA in accordance with Art. 28 GDPR as well as EU Standard Contractual Clauses (SCC) with ChatMarshal.

As part of our customer support service, we store your data to process your concerns. The legal basis is Art. 6 Para. 1 lit. b) GDPR, insofar as the processing is necessary for the initiation or fulfillment of a contract with you (e.g., for complaints or product demo requests). In other cases, processing is carried out on the basis of Art. A Para. 1 lit. f) GDPR, as we have a legitimate interest in corresponding with you for business purposes. The data is processed by RIB via the Salesforce Marketing Cloud as described above.

Please note that when using this service, your data may be transmitted to the service provider Text, Inc. in the USA. The purpose of this processing is to provide the chat function, the proper processing of your request, and quality control. The legal basis for this data processing is your consent in accordance with Art. 6 Para. 1 lit. a) GDPR. Your data will only be transmitted to Text. Inc. if you actively consent to the use of the service. You can revoke your consent at any time by changing your cookie settings (LINK to the cookie settings). If you do not wish to give consent, you can alternatively contact us via the contact form or by email.

We have concluded a data processing agreement with the mentiond provider in accordance with Art. 28 GDPR.
Insofar your Data is processed outside the EU or the EEA, we rely for that on the standard contractual Clauses (“SCCs”) published by the European Commission or an adequacy decision by the European Commission. When data is transferred to the USA, we rely in particular on providers that are certified under the data privacy framework.

For more information, please consult the following links:
For information about the SCCs: Implementing decision – 2021/914 – EN – EUR-Lex,
For information about the applicable adequacy decisions: Data protection adequacy for non-EU countries

Data processing by Text, Inc. takes place in the USA. Text, Inc. is certified under the EU-U.S. Data Privacy Framework, so that for data transfers to Text, Inc., there is an adequacy decision of the European Commission within the meaning of Art. 45 GDPR. The status of the certification can be accessed via the following website: https://www.dataprivacyframework.gov/list.

More information on data protection at Text, Inc. can be found at: https://www.livechatinc.com/legal/privacy-policy/.

9. Orders in the RIB Shop

9.1 Ordering a Training or Webinar

On our website, you can order a webinar or training. The following personal data is requested for this:

• First and last name
• Email address
• Company name
• Billing address
• Company address
• Information about the ordered webinar or training (e.g., product line, current program version, build number, and service number)

The data is recorded in the RIB CRM and stored in the customer's contact history.

In the RIB shop, you can pay by SEPA direct debit. For payment processing, we use the bank details stored with us. This data is processed exclusively for the execution of the payment and for the processing of the SEPA direct debit mandate.

The legal basis for the processing and disclosure of your personal data is Art. 6 Para. 1 lit. b GDPR. This processing is essential for the fulfillment of the contract.

9.2 Registration with Email Address

After concluding a contract, you have the opportunity to register on our website for a webinar or training.

As part of the registration, we collect and store the following data:

• First and last name
• Email address
• Company name
• Name and date of the desired webinar or training
• Address
• Phone number (optional)

After completing the registration, you will receive a confirmation email from us. Registration is necessary to be able to use some of our services.

The legal bases for these data processing operations are Art. 6 Para. 1 lit. a), b), and f) GDPR.

9.3 Use of October CMS

The RIB shop website uses the content management system (CMS) October CMS, offered by October CMS Inc., 601 108th Ave NE, Bellevue, WA 98004, USA, for the management and optimization of content. October CMS is an open-source platform that allows us to efficiently create, update, and provide content.

When using our website, the following data may be processed in this context:

• IP address of the visitor,
• Date and time of access,
• Information about the browser used and the operating system,
• Visited pages and clicked links.

This data is usually automatically stored in so-called server log files and is used exclusively for the technical optimization of our website and to ensure its security and functionality. This data is not merged with other data sources. The processing is carried out in accordance with Art. 6 Para. 1 lit. f GDPR based on our legitimate interest in maintaining and optimizing our digital content.

We have concluded a data processing agreement with the above mentiond provider in accordance with Art. 28 GDPR.
Insofar your Data is processed outside the EU or the EEA, we rely for that on the standard contractual Clauses ("SCCs") published by the European Commission or an adequacy decision by the European Commission. When data is transferred to the USA, we rely in particular but on providers that are certified under the data privacy framework.
For more information, please consult the following links:
For information about the SCCs: Implementing decision – 2021/914 – EN – EUR-Lex,
For information about the applicable adequacy decisions: Data protection adequacy for non-EU countries
For information about the companies listed under the data privacy framework: https://www.dataprivacyframework.gov/list

The collected server log files are usually automatically deleted after 6 months, unless there are further legal retention obligations.

10. Processing Your Data as a New and Existing Customer of RIB

When you place an order with us, whether via an order form, by email, telephone, live chat, or in person at one of our exhibition stands, we will include you in our customer file. The scope of the data corresponds to the required data for the specific request, which are marked as such in the respective forms, etc.

Our customer file is maintained uniformly for the entire RIB Group, so your data is also visible to employees of all RIB locations. Your data is maintained in systems from Salesforce, Microsoft Dynamics, VIS, or RIB 4.0. RIB remains responsible for the processing of your data. Your data will be stored in our customer file until the necessity for processing, including legal retention periods, has expired. The legal basis for the processing is Art. 6 Para. 1 S.1 lit. b) GDPR when we process your data for the execution of an order, and Art. 6 Para. 1 S.1 lit. f) GDPR for the further processing of your data as existing customer data. Insofar as we are obliged to legally retain your data (e.g., due to German

Commercial Code, tax law, etc.), the legal basis is Art. 6 Para. 1 S.1 lit. c) GDPR.

We have concluded a data processing agreement with the above mentiond provider in accordance with Art. 28 GDPR.
Insofar your Data is processed outside the EU or the EEA, we rely for that on the standard contractual Clauses ("SCCs") published by the European Commission or an adequacy decision by the European Commission. When data is transferred to the USA, we rely in particular but on providers that are certified under the data privacy framework. For more information, please consult the following links:
For information about the SCCs: Implementing decision – 2021/914 – EN – EUR-Lex,
For information about the applicable adequacy decisions: Data protection adequacy for non-EU countries
For information about the companies listed under the data privacy framework: https://www.dataprivacyframework.gov/list

For customers with an existing business relationship (B2B), we consider you as an existing customer. In this case, we also process your contact and customer data without separate consent to provide you with information about new products and services or about our own similar products and services. The legal basis for this is Art. 6 Para. 1 lit. f GDPR in conjunction with § 7 Para. 3 UWG. You can object to the use of your data for these purposes at any time without incurring any costs other than the transmission costs according to the basic rates. To do this, you can either use the unsubscribe link in the corresponding emails or alternatively send us an email to the contact details mentioned under 1.

11. Salesforce Marketing Cloud (Account Engagement)

Data that you provide to us through some of our websites (e.g., in forms for purchases, newsletter registration, contact, and the fact that you participate in a contest) will be stored in the Salesforce Sales Cloud of salesforce.com, Salesforce Tower Dublin, 60 R801, North Dock, Dublin, Ireland, currently on servers in the EU, and used for sending order confirmations and shipping notifications. The parent company of salesforce.com Ireland is salesforce.com Inc., One Market Street, Suite 300, San Francisco, CA 94105, USA.

For sending our newsletters, for automated mailings (e.g., welcome mailing), and for advertising campaigns on social networks, we use the Salesforce Marketing Cloud (Account Engagement). For this purpose, the newsletter subscriber's data is transferred from the Salescloud to the Marketing Cloud.

We have concluded a data processing agreement with the above mentiond provider in accordance with Art. 28 GDPR.
Insofar your Data is processed outside the EU or the EEA, we rely for that on the standard contractual Clauses ("SCCs") published by the European Commission or an adequacy decision by the European Commission. When data is transferred to the USA, we rely in particular but not always on providers that are certified under the data privacy Framework.
For more information, please consult the following links:
For information about the SCCs: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de,
For information about the applicable adequacy decisions: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

The data in the Salesforce Marketing Cloud (Account Engagement) is stored and processed on Salesforce servers in the USA. For data transfers to the USA, the provider has joined the EU-US Data Privacy Framework, which ensures compliance with European data protection standards based on an

adequacy decision by the European Commission. Further documents on Salesforce's compliance with the EU GDPR can be found at https://compliance.salesforce.com/en/gdpr.

Data collection and storage only takes place after explicit consent according to § 25 Para. 1 TDDDG, Art. 6 Para. 1 S. 1 lit. a GDPR. This consent can be revoked at any time with effect for the future.

Using so-called web beacons and pixels, we receive information about users' clicking behavior through the Marketing Cloud. Interaction data is stored directly on the user in the Marketing Cloud so that we can target advertising more specifically, e.g., via social networks, through the Ad Studio. If you do not want this, you have the option to turn off personalized ads in your account settings on the social networks. Additionally, you can use a different email address for newsletters or your customer account with us than the one you use for your social media accounts. Further information about opting out can be found under "Use of Cookies".

For more information about data processing by Salesforce, please visit: https://www.salesforce.com/de/company/privacy/.

12. Inxmail Email Marketing

For sending newsletters for RIB eVergabe & RIB Tender platforms and the RIB service customer newsletter, we use the Inxmail service from Inxmail GmbH, Wentzingerstr. 17, 79106 Freiburg, Germany.

Inxmail is a service that can organize and analyze newsletter distribution, among other things. The data you enter for the purpose of receiving the newsletter is stored on Inxmail's servers. We process the following personal data:

• First and last name

• Email address

• Service number

When we send newsletters with Inxmail, we can determine whether and when a newsletter message was opened and which links were clicked, if any. For this purpose, Inxmail stores an anonymized form of the IP address, which serves exclusively as a technical requirement for the counting process. This identifier is not visible in the statistics and does not allow any inference to personal data.

This data processing is based on your consent (Art. 6 Para. 1 lit. a GDPR). You can revoke this consent at any time. The lawfulness of data processing operations already carried out remains unaffected by the revocation. If you do not want analysis by Inxmail, you must therefore unsubscribe from the newsletter. For this purpose, we provide a corresponding link in every newsletter message.

The recipient data stored on the Inxmail server for newsletter subscriptions is retained for audit purposes during the contract term due to the obligation to provide evidence and is deleted 30 days after termination of the contract with Inxmail. The customer data stored in the RIB CRM remains stored until the necessity for processing, including legal retention periods, has expired (see section 10).

We have concluded a data processing agreement with the above mentiond provider in accordance with Art. 28 GDPR.
Insofar your Data is processed outside the EU or the EEA, we rely for that on the standard contractual Clauses ("SCCs") published by the European Commission or an adequacy decision by the European

Commission. When data is transferred to the USA, we rely in particular but on providers that are certified under the data privacy framework. For more information, please consult the following links:
For information about the SCCs: Implementing decision – 2021/914 – EN – EUR-Lex,
For information about the applicable adequacy decisions: Data protection adequacy for non-EU countries
For information about the companies listed under the data privacy framework: https://www.dataprivacyframework.gov/list

For more information, please refer to Inxmail's privacy policy at: https://www.inxmail.de/de/datenschutz/.

13. Google Analytics

13.1 Google Analytics

If you have given your consent, Google Analytics is used on this website, a web analysis service from Google LLC. The responsible entity for users in the EU/EEA and Switzerland is Google Ireland Limited, Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland ("Google").

13.2 Scope of Processing

Google Analytics uses cookies that enable an analysis of your use of our websites. The information collected by the cookies about your use of this website is usually transferred to a Google server in the USA and stored there.

We use the User ID function. Using the User ID, we can assign a unique, permanent ID to one or more sessions (and the activities within these sessions) and analyze user behavior across devices.

We use Google Signals. This allows additional information about users who have enabled personalized ads (interests and demographic data) to be collected in Google Analytics, and ads can be delivered to these users in cross-device remarketing campaigns.

In Google Analytics 4, IP address anonymization is enabled by default. Due to IP anonymization, your IP address is shortened by Google within member states of the European Union or in other contracting states of the Agreement on the European Economic Area. Only in exceptional cases will the full IP address be transmitted to a Google server in the USA and shortened there. The IP address transmitted by your browser as part of Google Analytics will not be merged with other Google data.

• During your website visit, your user behavior is recorded in the form of "events". Events can be: • Page views • First visit to the website • Session start • Your "click path", interaction with the website • Scrolls (whenever a user scrolls to the end of the page (90%)) • Clicks on external links • Internal search queries • Interaction with videos • Seen / clicked advertisements

In addition, the following is recorded: • Your approximate location (region) • Your IP address (in shortened form) • Technical information about your browser and the end devices you use (e.g., language setting, screen resolution) • Your internet provider • The referrer URL (which website/advertising medium you came to this website from)

13.3 Purposes of Processing

On behalf of the operator of this website, Google will use this information to evaluate your use of the website and to compile reports on website activities. The reports provided by Google Analytics serve to analyze the performance of our website.

13.4 Recipients

Recipients of the data are/may be: • Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland (as data processor according to Art. 28 GDPR) • Google LLC, 1600 Amphitheatre Parkway Mountain View, CA 94043, USA • Alphabet Inc., 1600 Amphitheatre Parkway Mountain View, CA 94043, USA

It cannot be ruled out that US authorities may access the data stored by Google.

13.5 Third Country Transfer

Insofar as data is processed outside the EU/EEA and there is no data protection level corresponding to the European standard, we have concluded EU standard contractual clauses with the service provider to establish an adequate level of data protection. The parent company of Google Ireland, Google LLC, is headquartered in California, USA. A transfer of data to the USA and access by US authorities to the data stored by Google cannot be ruled out. The USA is currently considered a third country from a data protection perspective. You do not have the same rights there as within the EU/EEA. You may not have any legal remedies against access by authorities.

13.6 Storage Duration

The data sent by us and linked to cookies will be automatically deleted after 2 OR 14 months. The deletion of data whose retention period has been reached occurs automatically once a month.

13.7 Legal Basis

The legal basis for this data processing is your consent according to Art. 6 Para. 1 S. 1 lit. a) GDPR.

13.8 Revocation

You can revoke your consent at any time with effect for the future by accessing the cookie settings **HERE** and changing your selection there. The lawfulness of processing carried out on the basis of consent until revocation remains unaffected.

Alternatively, you can prevent the storage of cookies from the outset by configuring your browser software accordingly. However, if you configure your browser to reject all cookies, functionality on this and other websites may be limited. You can also prevent the collection of data generated by the cookie and related to your use of the website (including your IP address) to Google and the processing of this data by Google by:

a. not giving your consent to the setting of the cookie, or b. downloading and installing the browser add-on to disable Google Analytics HERE.

For more information on Google Analytics' terms of use and Google's privacy policy, please visit https://marketingplatform.google.com/about/analytics/terms/de/ and https://policies.google.com/?hl=de.

14. Google Ads Conversion Tracking

We use the Google Ads service. Google Ads is an online advertising program from Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland (“Google”).

This means we run Google Ads advertisements and also use Google Remarketing and Conversion Tracking. The ads are displayed after search queries on websites in the Google advertising network. We also use Ads remarketing lists for search ads. This allows us to adapt search ad campaigns for users who have already visited our website. Through these services, we have the option to combine our ads with certain search terms or to display ads for previous visitors, in which, for example, services are advertised that the visitors have viewed on our website. We can therefore show interest-based advertising to users of our website on other websites within the Google advertising network (as “Google ads” in Google search or on other websites).

Interest-related offers require an analysis of online user behavior. Google uses cookies to conduct this analysis. When clicking on an ad or visiting our website, a cookie is set on the user’s computer by Google. These cookies have different durations depending on their type; more information can be found here: https://business.safety.google/adscookies/. The information collected by the respective cookie is used to target the visitor specifically during a later search query. Further information on the cookie technology used can also be found in Google’s information on website statistics and in the privacy policy. With the help of this technology, Google and we as the customer receive information that a user has clicked on an ad and was redirected to our websites. The information obtained in this way is used exclusively for statistical evaluation for ad optimization. We do not receive any information that allows visitors to be personally identified. Your IP address is transferred to Google, but since we use Google’s IP masking on this website as part of Google Analytics, your IP address is anonymized. The statistics provided to us by Google include the total number of users who clicked on one of our ads and, if applicable, whether they were redirected to a page of our website tagged with a conversion tag. Using these statistics, we can track which search terms our ad was clicked on most frequently and which ads lead to the user contacting us via the contact form.

For more information about data protection within Google Ads, please visit: https://policies.google.com/technologies/ads?hl=de.

If you do not want the processing, you can prevent the storing of cookies required for these technologies, e.g., via your browser settings. In this case, your visit will not be included in the user statistics.

You also have the option to select the types of Google ads via the ad settings (https://adssettings.google.com/authenticated?hl=de) or to deactivate interest-based ads on Google. Alternatively, you can deactivate the use of cookies by third-party providers by accessing the Network Advertising Initiative’s opt-out tool.

However, we and Google will continue to receive the statistical information about how many users visited this page and when. If you do not want to be included in this statistic either, you can prevent this with the help of additional programs for your browser (e.g., the Privacy Badger add-on).

The legal basis for this data processing is your consent, Art. 6 Para. 1 lit. a) GDPR. You can revoke your consent at any time with effect for the future by accessing the cookie settings in our Consent Management Platform (“Cookie Settings” at the bottom of the page) and changing your selection there.

15. Meta Conversion Tracking

We use the Custom Audiences service from Meta Platforms, Inc., 1601 S. California Avenue, Palo Alto, CA 94304, USA (hereinafter referred to as “Facebook”) as part of usage-based online advertising. For this purpose, we define target groups of users in the Facebook Ad Manager based on certain characteristics, who then receive advertisements within the Facebook network. The users are selected by Facebook based on the profile information they have provided and other data provided through the use of Facebook. If a user clicks on an advertisement and subsequently reaches our website, Facebook receives information via the Facebook pixel integrated on our website that the user has clicked on the advertising banner.

In principle, a non-reversible and non-personal checksum (hash value) is generated from your usage data, which is transmitted to Facebook for analysis and marketing purposes. A Facebook cookie is set. This collects information about your activities on our website (e.g., browsing behavior, visited subpages, etc.). Your IP address is also stored and used for geographical targeting of advertising.

We do not use Facebook Custom Audiences via the customer list or the “enhanced matching” function.

For more information about the purpose and scope of data collection and the further processing and use of the data by Facebook, as well as your setting options to protect your privacy, please refer to Facebook’s privacy policy. You can make settings about which advertisements are displayed to you on Facebook in your Facebook account settings.

You can prevent data collection by the Facebook pixel by opening the privacy settings below (“Cookie Settings”) and making the corresponding changes there.

An opt-out cookie (persistent HTML5 storage object) is set that prevents the future collection of your data when visiting this website.

You can also prevent the storage of cookies in general by configuring your browser software accordingly. However, we point out that in this case you may not be able to use all functions of our website to their full extent. Further options for deactivating cookies by third-party providers can be found at www.networkadvertising.org/managing/opt_out.asp or on the Digital Advertising Alliance Opt-Out platform at http://optout.aboutads.info/?c=2&lang=en.

16. LinkedIn Conversion Tracking

If you have given your consent, we use the online marketing tool LinkedIn Ads. The responsible service provider in the EU is LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland.

For this purpose, we define target groups of users in the LinkedIn Campaign Manager based on certain characteristics, who subsequently receive advertisements within the LinkedIn network. The users are selected by LinkedIn based on the profile information they have provided, as well as other data provided during the use of LinkedIn. If a user clicks on an advertisement and subsequently arrives on our website, LinkedIn receives information through the Conversion Tag integrated on our website that the user has clicked on the advertising banner.

The LinkedIn Tag thus enables the capture of visited websites, including the URL, referrer ID, IP address, device and browser properties, and timestamp. IP addresses are truncated by LinkedIn or (for cross-device use) hashed.

With the help of the LinkedIn Pixel, we can show personalized ads outside our website without identifying individual members. Data that does not identify you is also used to improve ad relevance and reach LinkedIn members across different devices. LinkedIn members can control the use of their

personal data for advertising purposes through their account settings. LinkedIn refers to the following link to adjust advertising preferences: https://www.linkedin.com/psettings/advertising/actions-that-showed-interest.

We process this data to evaluate our advertising campaigns. Further information about the purpose and scope of data collection and the further processing and use of data by LinkedIn, as well as your settings options to protect your privacy, can also be found in LinkedIn's privacy policy.

Further information on LinkedIn Conversion Tracking can be found at: https://business.linkedin.com/de-de/marketing-solutions/conversion-tracking.

Further information on data processing and storage duration can be found at https://www.linkedin.com/help/linkedin/answer/65521?lang=de.

The legal basis for this data processing is your consent, Art. 6 Para. 1 lit. a) GDPR. You can revoke your consent at any time with effect for the future by opening the privacy settings below ("Cookie Settings") and making the corresponding changes there.

17. Google Tag Manager

For reasons of transparency, we would like to inform you that we use Google Tag Manager. This is a tag management system for managing JavaScript and HTML tags, which is used for implementing tracking and analysis tools. It is a service provided by Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. The controller in the EU/EEA is Google Ireland Limited, Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland.

The Google Tag Manager itself does not collect any personal data. The Tag Manager makes it easier for us to integrate and manage our tags. Tags are small code elements that, among other things, serve to measure traffic and visitor behavior, capture the impact of online advertising and social channels, set up remarketing and targeting audiences, and test and optimize websites. If you have opted out, this opt-out will be respected by the Google Tag Manager.

Recipients of the data are:

Google Ireland Limited, EU,

Google LLC, USA,

Alphabet Inc., USA.

This service may process data outside the European Union and the European Economic Area (EEA) and transfer it to a country that does not offer an adequate level of data protection. If the data is transferred to the USA, there is a risk that your data may be processed by US authorities for control and surveillance purposes without you having legal remedies.

The legal basis for this data processing is your consent, Art. 6 Para. 1 lit. a) GDPR. You can withdraw your consent at any time with effect for the future by accessing the cookie settings in our Consent Management Platform ("Cookie Settings" at the bottom of the page) and changing your selection there. The lawfulness of the data processing until the withdrawal remains unaffected.

For more information about Google Tag Manager, please visit: https://www.google.com/intl/de/tagmanager/use-policy.html.

18. Google Web Fonts (Offline Version)

This page uses web fonts provided by Google for the uniform display of fonts. When you access a page, your browser loads the required web fonts into your browser cache to correctly display texts and fonts. We have decided to use the offline version, where Google Fonts are stored locally on our web server. The management of the fonts is then – via CSS – possible as with any other font family. A transmission of the IP address and other data to Google does not take place.

The use of Google Web Fonts is in the interest of a uniform and appealing presentation of our online offerings with a view to efficiency and cost-saving considerations. This represents a legitimate interest within the meaning of Art. 6 Para. 1 lit. f) GDPR. If your browser does not support web fonts, a standard font from your computer will be used.

For more information about Google Web Fonts, please visit https://developers.google.com/fonts/faq and Google's privacy policy: https://www.google.com/policies/privacy/.

19. Google reCaptcha

We use reCaptcha v2 on our website. reCaptcha is a service offered by Google LLC, 1600 Amphitheatre Parkway Mountain View, CA 94043, USA. The responsible entity for users in the EU/EEA and Switzerland is Google Ireland Limited, Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland.

ReCaptcha serves to prevent abusive automated entries in web forms and thus to protect the technical systems of the host.

When you access one of our websites where reCaptcha is integrated, a connection to Google's servers is established. A reCaptcha cookie is set. Your IP address is transmitted to Google.

In addition, reCaptcha captures the following data via "fingerprinting":

• Browser plugins used

• Cookies set by Google in the last 6 months

• Number of mouse clicks and touches you have made on this screen

• CSS information for the page accessed

• JavaScript objects

• The date

• The browser language

You can prevent the storage of cookies and fingerprinting by selecting appropriate technical settings in your browser software; however, we would like to point out that in this case you may not be able to use all functions of this website to their full extent.

Insofar as data is processed outside the European Economic Area/EU, where there is no data protection level equivalent to the European standard, Google says it uses standard contractual clauses.

Google's privacy policy and terms of use can be found here: https://policies.google.com/privacy and here: https://policies.google.com/terms.

The collection and storage of data only takes place after explicit consent pursuant to Art. 6 Para. 1 S. 1 lit. a) GDPR. This can be revoked at any time with effect for the future.

20. YouTube (without DS mode)

We use services from YouTube, LLC, 901 Cherry Ave., 94066 San Bruno, CA, USA, a subsidiary of Google Inc., Amphitheatre Parkway, Mountain View, CA 94043, USA, on our website. For users who have their habitual residence in the European Economic Area or Switzerland, Google Ireland Limited ("Google"), Gordon House, Barrow Street, Dublin 4, Ireland is the controller responsible for your data.

To protect your personal data, we use a two-click solution. When you access a page with an embedded YouTube video, a connection to YouTube servers is only established when you click the "Confirm" button. In this case, YouTube will set cookies and use your visit data for its own purposes. If you are logged into YouTube at this time, the information about the videos you have viewed will be associated with your YouTube membership account. You can prevent this by logging out of your membership account before visiting our website. Insofar as data is processed outside the European Economic Area/EU, where there is no data protection level equivalent to the European standard, Google says it uses standard contractual clauses.

Further information on YouTube's data protection is provided by Google at the following link: https://www.google.de/intl/de/policies/privacy/

21. Usercentrics

Usercentrics is a Consent Management Platform that enables websites to protect users' privacy and comply with the GDPR when it comes to cookies and tracking. "Usercentrics" is a service offered by Usercentrics GmbH, Rosental 4, 80331 Munich, hereinafter referred to as "Usercentrics".

Through the "Usercentrics" function, we inform our website visitors about the use of cookies on our website and enable them to make a decision about their use.

If the visitor gives their consent to the use of cookies, the following data is automatically logged:

• The user's IP number

• Date and time of consent

• User agent of the end user's browser

• The provider's URL

• An anonymous, random and encrypted key.

The encrypted key and cookie status are stored on the user's device using a cookie to establish the corresponding cookie status for future page visits. This cookie automatically deletes itself after 12 months.

The legal basis for storing the data is Art. 6 Para. 1 lit. c in conjunction with Art. 7 Para. 1 GDPR, as Usercentrics is used to fulfill requirements under the TDDDG. Alternatively: The legal basis for storing the data is Art. 6 Para. 1 lit. f GDPR. Our legitimate interest in using Usercentrics lies in fulfilling the requirements of the TDDDG.

The installation of the cookie as well as its storage, and thus the cookie consent, can be prevented or terminated by the user at any time through browser settings.

Further information about Usercentrics can be found at: https://usercentrics.com/de/datenschutzerklaerung/.

22. Stripe

If you choose Stripe as your payment method, personal data from you will also be transmitted to Stripe (Stripe Payments Europe Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Ireland) and stored there. This includes transaction data, such as the payment method (e.g., credit card, debit card, or account number), bank code, currency, amount, and date of payment. Your name, email address, billing or shipping address, and sometimes your transaction history may also be transmitted. This data is necessary for authentication. Furthermore, to prevent fraud, for financial reporting, and to be able to offer its services fully, Stripe may also collect, in addition to technical data about your device (such as IP address), your name, address, phone number, and country.

Stripe does not sell any of your data to independent third parties, such as marketing agencies or other companies that have nothing to do with the Stripe company. However, the data may be forwarded to internal departments, a limited number of external Stripe partners, or for compliance with legal requirements. Stripe also uses cookies to collect data. You can learn more about the cookies used in the Cookies section. For more information about Stripe's data protection, please visit https://stripe.com/de/privacy.

23. Customer Support on Jira

Should you decide to make a support request on Jira, this is only possible with your own Jira account. Jira is a service offered by Atlassian Pty Ltd, Level 6, 341 George Street, Sydney NSW 2000, Australia, and Atlassian's terms apply to all interaction with Jira. Atlassian is responsible for the processing of your personal data on Jira.

24. Customer Support on Zendesk

Should you decide to make a support request on Zendesk, this is only possible with your own Zendesk account. Zendesk is a service offered by Zendesk, 989 Market St San Francisco, Ca, 94103, USA, and Zendesk's terms apply to all interaction with Zendesk. Zendesk is responsible for the processing of your personal data on Zendesk. For more details, see Zendesk's privacy information https://www.zendesk.com/au/company/agreements-and-terms/privacy-notice/.

25. Salesforce Service Cloud and the RIB Service Portal

We use the Salesforce Service Cloud to provide customer support for the products RIB 4.0, Candy, and Connect. This platform enables us to efficiently process your inquiries, communicate with you, and track the progress of your support case to ensure high-quality support. The data collected through the Salesforce Service Cloud is used exclusively to process your inquiries and is not used for marketing purposes.

The data you provide to us through our customer service channels (e.g., email, online form, or input into the system by our team when you call) is stored in the Salesforce Sales Cloud, which is operated by salesforce.com. The servers of this platform are located within the EU. The European branch of salesforce.com is located at Salesforce Tower Dublin, 60 R801, North Dock, Dublin, Ireland. The parent company of salesforce.com Ireland is salesforce.com Inc, located at One Market Street, Suite 300, San

Francisco, CA 94105, USA. For more information about data processing by Salesforce, please visit: https://www.salesforce.com/eu/company/privacy/.

To support our customers, we operate the “RIB Service Portal”, a web interface through which you can manage your support tickets online. This portal is developed by RIB and hosted on Microsoft Azure servers in the EU. When you log into the portal, your data from the Salesforce Service Cloud is loaded and temporarily cached in Microsoft Azure to ensure fast availability in your web browser. We store error logs and records of certain user actions (such as logins and logouts) for troubleshooting purposes. The processing of this data is based on our legitimate interest pursuant to Art. 6 Para. 1 lit. f GDPR, which consists of the smooth and secure operation of our service portal. Your data is not used for any other purposes and is not shared with third parties. There is no tracking of user activities for marketing purposes.

We have concluded a data processing agreement with the above mentiond provider in accordance with Art. 28 GDPR.
Insofar your Data is processed outside the EU or the EEA, we rely for that on the standard contractual Clauses (“SCCs”) published by the European Commission or an adequacy decision by the European Commission. When data is transferred to the USA, we rely in particular but on providers that are certified under the data privacy framework. For more information, please consult the following links:
For information about the SCCs: Implementing decision – 2021/914 – EN – EUR-Lex,
For information about the applicable adequacy decisions: Data protection adequacy for non-EU countries
For information about the companies listed under the data privacy framework: https://www.dataprivacyframework.gov/list

26. Customer Portal of Omnitracker

Through our customer portal of Omnitracker, you can subscribe to and unsubscribe from newsletters, make support requests, and obtain all software updates. Registration is done using your customer number at https://www.rib-software.com/de/rib-service-login.

Only your email address and customer number are stored in the customer portal. If you provide additional personal data in support requests, we process this data exclusively for the purpose of fulfilling your specific request. The legal basis is Art. 6 Para. 1 S.1 lit. b) GDPR, insofar as the contractual service provision is carried out via or with the help of the Omnitracker customer portal (e.g., regarding contractually owed software updates). Insofar as you make additional requests or, for example, newsletter subscriptions, the legal basis is your consent according to Art. 6 Para. 1 S.1 lit. a) GDPR, which you can revoke at any time. As an existing customer stored in the system, we process your data according to our legitimate interest, Art. 6 Para. 1 S.1 lit. f) GDPR.

The customer portal is provided by OMNINET Software-, System- und Projektmanagementtechnik GmbH, Dr.-Otto-Leich-Straße 3, 90542 Eckental, Germany.

27. Cloudflare

For our website, we use services from CloudFlare Inc., 101 Townsend St, San Francisco, CA 94107 USA.

Cloudflare provides a so-called Content Delivery Network (CDN). This is a network of globally distributed servers that is able to deliver optimized content to website users. This enables, in particular,

large media files to be delivered through a network of locally distributed servers connected via the Internet. This serves the secure and efficient provision of our website and contributes to improving performance and stability.

For this purpose, personal data may be processed in Cloudflare's server log files. Cloudflare also collects statistical data about visits to this website. The collected data includes:

• Name of the accessed website

• Accessed file

• Date and time of access

• Transferred data amount

• Message about successful access

• Browser type and version

• User's operating system

• Referrer URL

• IP address

• Requesting provider

The legal basis for this data processing is our legitimate interest pursuant to Art. 6 Para. 1 lit. f GDPR. Our legitimate interest here lies in the smooth and secure operation of our website. You have the right to object to the processing according to Art. 21 GDPR. Whether the objection is successful must be determined as part of a balancing of interests.

Insofar as data is processed outside the EU/EEA, Cloudflare Inc. has been certified under the Data Privacy Framework (DPF) Program and is listed in the Data Privacy Framework List of the International Trade Administration (ITA). This means that Cloudflare has publicly committed to comply with DPF obligations, and any data transfer to the USA is unobjectionable due to the current adequacy decision of the European Commission of July 10, 2023.

A list of currently certified US companies can be found here: https://www.dataprivacyframework.gov/s/participant-search. For more information about the Data Privacy Framework Program, please visit the official ITA website: https://www.dataprivacyframework.gov/s/.

Cloudflare uses the log data for statistical evaluations for the purpose of operating, securing, and optimizing its own offering. For more information about data processing by Cloudflare, especially regarding data protection and data security, please visit: https://www.cloudflare.com/de-de/privacypolicy/.

28. GoTo Webinar

We use the tool "GoToMeeting or GoToWebinar" to conduct telephone conferences, online meetings, video conferences, and/or webinars (hereinafter: online meetings). "GoToMeeting and GoToWebinar" is a service provided by GoTo Ireland Limited, Bloodstone Building Block C, 70 Sir John Rogersons Quay,

Dublin 2, Ireland. GoTo's parent company is a US company, so data transmissions and processing may also take place outside the EU.

When using GoToWebinar, the following data from you is processed: First name, last name, phone (optional), email address, password, profile picture (optional), department (optional), meeting topic, meeting description (optional), participant IP addresses, device/hardware information.

In the case of recordings, the following data may also be collected: MP4 file of all video, audio, and presentation recordings, M4A file of all audio recordings, text file of the online meeting chat.

There may be the possibility to use the chat, questions, or survey functions in an online meeting. In this respect, the text entries made are processed to display them in the online meeting and, if necessary, to log them.

We use "GoToMeeting or GoToWebinar" to conduct online meetings. If we want to record, this will be announced in advance. The fact of the recording is also displayed in the app.

If it is necessary for the purposes of logging the results of an online meeting, we will log the chat contents.

In the case of online seminars, we may also process the questions asked by online seminar participants for the purposes of recording and follow-up of webinars.

The legal basis for data processing when conducting online meetings is Art. 6 Para. 1 lit. b) GDPR, insofar as the meetings themselves are part of the contract.

If there is no contractual relationship, the legal basis is Art. 6 Para. 1 lit. f) GDPR. Here, too, our interest lies in the effective implementation of "online meetings".

"GoToMeeting and GoToWebinar" is a service provided by a provider from the USA. Processing of personal data thus also takes place in a third country. We have concluded a data processing agreement with the provider that meets the requirements of Art. 28 GDPR.

An adequate level of data protection is guaranteed by the conclusion of the so-called EU standard contractual clauses.

For more information about data protection and data security at GoTo, please visit: https://www.goto.com/de/company/legal/privacy.

29. Microsoft Booking Calendar

For booking appointments with our customer service or support teams, you have the option to use Microsoft Booking Calendar, a tool provided by Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA.

The use of the booking calendar is voluntary. If you do not want to book an appointment via Booking Calendar, you can also reach us in other ways, e.g., via a contact form or by email.

If you choose to use Booking Calendar, we process your name, email address, address, and notes to book the desired appointment. The data is stored on Microsoft servers in the EU and the USA.

The processing is based on Art. 6 Para. 1 lit. f) GDPR in our legitimate interest to organize appointments according to our capacities. In addition, Microsoft processes usage and metadata, which Microsoft uses for security purposes and to optimize the service. As part of the use of the website,

Microsoft may store cookies on users' computers for the purpose of web analysis or to maintain user settings.

For more information, please see Microsoft's privacy policy. You can object to the processing of your data in the Microsoft Cloud in accordance with legal provisions. Insofar as personal data is processed by Microsoft in the USA, we refer to the EU-SCCs concluded with, through, and within the Microsoft Group.

30. Fullstory

With our product line RIB Unify, we use "Fullstory" from Fullstory, Inc. to improve the user experience. This analysis tool provides us with insights into user interactions with our application and supports us in troubleshooting, customer support, and application improvement.

Legal basis for data processing:

Our data processing activities are based on:

Article 6 (1) (a) GDPR

§ 25 (1) TDDDG (Telecommunications Telemedia Data Protection Act)

You can withdraw your consent at any time via our cookie settings.

Processed data:

If you have given your consent, we process the following data:

Master data:

• First name

• Last name

• Email address

• Job title

• Country

Usage patterns:

• Clicks

• Mouse movements

• Scrolling

• Inputs (passwords, payment information, and social security numbers are excluded by default)

Technical specifications:

• Browser

• Device type

• Operating system

• Resolution

• Script errors

• IP address (only recorded during active sessions)

Navigation data:

• Visited pages

• Referrer

• URL parameters

• Session duration

We use this data to:

• Improve the design of RIB Unify

• Identify confusing or little-used areas of the app

• Improve the customer experience and develop better features

• Understand the use of customer end devices

• Fix errors and problems

• Support customers effectively

Data access and storage:

Employees of RIB companies in Australia, Denmark, Hong Kong, India, South Africa, the United Kingdom, and the USA can access the data. The data is stored in the Europe-west3 region of Google (Frankfurt, Germany) and may be processed in the USA under the data protection framework.

Data retention:

Session data: Stored for 1 month Product analysis data: Stored for 12 months

For more detailed information, please visit Fullstory's privacy policy.

By using Fullstory, we commit to improving your experience while protecting your data and handling it responsibly.

31. Microsoft Forms

The creation of this online data query is carried out using Microsoft Forms, an application of Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA.

Type and purpose of data processing:

Microsoft Forms is a type of universal survey tool that can also be used as a tool for designing and evaluating online surveys, queries, and conducting quizzes. The data you provide as part of the survey is sent to us and evaluated through Microsoft Forms.

Recipients of the data:

According to Microsoft, data from Microsoft Forms is stored on servers in Europe, provided the organization is based in Europe.

Accordingly, the data is stored on Microsoft servers in the Netherlands (Evert van de Beekstraat 354, 1118 CZ Schiphol, Netherlands) and Ireland (1, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland). Microsoft Forms data is encrypted both at rest and during transmission.

In addition, Microsoft processes usage and metadata, which Microsoft uses for security purposes and service optimization. When using the website, Microsoft may store cookies on users' computers for web analytics purposes or to maintain user settings.

We use this Microsoft cloud service based on our legitimate interests pursuant to Art. 6 Para. 1 lit. f GDPR. Our legitimate interest consists in standardizing and optimizing the way we collect and organize information so that we can better process, analyze, and store this information and the associated insights.

Further information can be found in Microsoft's privacy policy. In accordance with legal requirements, you can object to the processing of your data in the Microsoft Cloud. We delete the data we receive from Microsoft Forms after 3 years; thereafter, the deletion of data on Microsoft servers is determined by Microsoft.

Insofar as personal data is processed by Microsoft in the USA, we refer to the EU-SCCs concluded with, from, and within the Microsoft Group.

32. Feature Requests via Aha!

Feature requests for the products RIB CostX and RIB Benchmark are processed via the Aha! platform. The "Aha!" tool is provided by Aha! Labs Inc. based at 800 Concar Drive, Suite 100, San Mateo, CA 94402. Aha! is a product management platform that allows us to visualize and plan our product strategy and roadmap. The roadmapping, idea management, and strategy planning functions of Aha! help product teams prioritize features, manage new product releases, and align product development with company goals. Customers must be invited by RIB to use Aha!. To send the invitation, RIB requires the following customer information:

• First name

• Last name

• Email address

• Company

This is done only at your own request. This data is processed solely for the purpose of creating the Aha! account. Once the account is created, Aha! Labs Inc.'s Terms and Conditions apply to all interaction with Aha!.

Data transfer to the USA

Aha! Lab Inc. is headquartered in the USA. Insofar as data is processed outside the EU/EEA, Aha! Lab Inc. has certified itself under the E.U.-U.S. — Data Privacy Framework (DPF) program. This means that Aha! has publicly committed to comply with the DPF obligations and that any data transfer to the USA is

deemed safe on the basis of the current adequacy decision of the European Commission dated July 10, 2023.

A list of currently certified US companies can be found here: https://www.dataprivacyframework.gov/s/participant-search.

In addition, we have concluded a data processing agreement with Aha! Lab Inc. in accordance with the requirements of Art. 28 GDPR.

Further information on data processing by Aha! Lab Inc. can be found at https://www.aha.io/legal/privacy_policy.

Legal basis for data processing

The use of Aha! and the associated processing of personal data is based on Art. 6 Para. 1 lit. f) GDPR. Our legitimate interest consists in improving our product offering based on customer feedback.

Duration of storage

The processed data is stored permanently as long as the account with Aha! exists.

33. Highspot Sales Enablement

Description, purpose, and scope of data processing

We use the Highspot Sales Enablement tool, an application of Highspot Inc., 2211 Elliott Ave Suite 400, Seattle, WA 98121, US. This is a sales promotion platform used to simplify the development of sales strategies for our sales team, provide targeted content, and enable simplified communication with customers and prospects.

To use the platform, the following personal data is processed:

• First and last name

• Email address

• IP address

• Date and time of use

Additional information such as telephone number or location is optional and marked as such by us.

When our salespeople share content from the system with prospects, customers, or clients, Highspot stores certain information for analytical purposes, such as the recipient’s name, email address, and any information we want to use to link the content to records in our CRM, e.g., opportunity, contact, lead, or account name and ID. This information is retrieved from our CRM through a ready-to-use integration.

To optimize our content strategy by analyzing engagement patterns and provide an optimal customer experience through data-driven insights, Highspot also processes the following data:

• Last viewed content (date)

• Number of views (per content)

• Total number of views

• Viewing duration (per content)

• Total viewing duration

• Number of downloads (per content)

• Total number of downloads

Data transfer to the USA

Highspot Inc. is headquartered in the USA. Insofar as data is processed outside the EU/EEA, Highspot Inc. is certified under the E.U.-U.S. — Data Privacy Framework (DPF) program. This means that Highspot has publicly committed to comply with the DPF obligations and any data transfer to the USA is considered safe based on the current adequacy decision of the European Commission dated July 10, 2023.

A list of currently certified US companies can be found here: https://www.dataprivacyframework.gov/s/participant-search.

In addition, we have concluded a Data Processing Agreement with Highspot Inc. in accordance with the requirements of Art. 28 GDPR.

Further information on data processing by Highspot Inc. can be found at https://www.highspot.com/privacy/.

Legal basis for data processing

The use of Highspot and the associated processing of personal data is based on Art. 6 Para. 1 lit. f GDPR. Our legitimate interest consists in providing our sales staff with an efficient and effective sales platform to optimize our sales processes.

When we process data for analytical purposes as described above, this is done only with your consent according to Art. 6 Para. 1 lit. a) GDPR. This is obtained from you via our cookie banner and can be revoked by you at any time.

Storage duration

The processed data is stored permanently as long as the account with Highspot exists.

34. WalkMe

We use the Digital Adoption Platform “WalkMe” provided by WalkMe, Inc., 350 mission St., FL. 26, San Francisco, CA 94105, USA. WalkMe is a digital adoption platform designed to help us streamline and optimize the use of our digital tools, software, and web applications. We use WalkMe to enhance user onboarding and to provide in-app support content. Additionally, WalkMe offers our software development team analytics to track user engagement with product features and overall digital experiences.

Legal basis for data processing

The legal basis for data processing is Article 6 (1) (a) GDPR, Section 25 (1) TDDDG (German Telecommunications-Digital Services Data Protection Act). You can withdraw your consent at any time with effect for the future by accessing the cookie settings in our Consent Management Platform (“Privacy Settings” at the bottom of the page) and changing your selection there.

Description, purpose and scope of data processing

If you have given your consent, the following data may be processed:

User Master Data:

- User Number (UN-Number)
- User Role

User Behavior Data:

- Clicks
- Mouse movements
- Scrolling
- Typing into help content (passwords, payment information, and Social Security numbers are excluded by default from being recorded)

User Device and Environment Data:

- Browser
- Device type
- Operating system
- Screen Resolution
- Script errors
- IP address (the IP address is only recorded while a user's session is active; at the end of the session, the IP address is discarded)

Navigation:

- Pages visited
- Referrers
- URL parameters
- Session duration

All categories of data are used to optimize user experience, tracking adoption, and provide contextual guidance. **User Master data** helps us to personalize the guidance based on user attributes and roles, enabling us to design functionality that better supports their needs. **User Behavior Data** provides to understand how users interact with digital tools and to provide contextual guidance, analyzing these interactions helps identify where users may encounter difficulties or drop off. **User Device and Environment Data** provide to ensure compatibility and optimize the user experience. **Navigation Data** allows us to track individual user sessions for analytical and troubleshooting purposes.

Recipient of the data:

Employees of RIB Affiliates located outside of Europe may have access to the data as part of the support and maintenance processes.

Data Access and Storage

The data is stored in the EU. WalkMe may also process data in the USA. WalkMe, Inc. is certified according under the Data Privacy Framework, so that for data transfers to WalkMe, Inc. an adequacy decision of the European Commission in the sense of Art. 45 GDPR is available. The status of the certification can be accessed via the following website: https://www.dataprivacyframework.gov/list.

Data Retention

The storage period for session data is 1 month. Product analytics data is stored for 12 months.

Further information on data protection at WalkMe can be found at: Privacy Policy – WalkMe™ – Digital Adoption Platform.

35. Hyperlinks to Facebook, Instagram, and YouTube

Some of our internet offerings contain hyperlinks to other websites that are not operated by RIB. We do not monitor these websites and are not responsible for their content or their handling of personal data.

The processing serves to protect a legitimate interest of our company, and the interests, fundamental rights, and freedoms of the data subject do not override the aforementioned interest. The legal basis for the processing of personal data using hyperlinks is Art. 6 Para. 1 lit. f GDPR.

For the Facebook network. These are offered and operated by Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA. The contents of the widget are transmitted directly from Facebook to your browser and displayed accordingly in our environment, without us having any influence on the contents.

For the Instagram network. These are offered and operated by Meta Platforms, Inc., 1601 Willow Road, Menlo Park California 94025, USA. The contents of the widget are transmitted directly from Instagram to your browser and displayed accordingly in our environment, without us having any influence on the contents.

For the YouTube network. These are offered and operated by YouTube LLC, 901 Cherry Ave., San Bruno, CA 94066, USA. The contents of the widget are transmitted directly from YouTube to your browser and displayed accordingly in our environment, without us having any influence on the contents.

For more detailed information on the nature, purpose, and scope as well as the further processing and use of your data by the respective social media provider, please refer to their privacy notices. There you will also find out more about your relevant rights and the setting options to protect your privacy.

Privacy notices at Facebook

Privacy notices at Instagram

Privacy notices at YouTube

36. Data Security

We have taken extensive technical and operational protective measures to protect your data from accidental or deliberate manipulation, loss, destruction, or access by unauthorized persons. Our security procedures are regularly reviewed and adapted to technological advances.

Last updated: March 2025