Privacy Policy

according to Art. 13 GDPR

Last updated: 23 October 2026

Bridge ITS GmbH, Dresden

Table of Contents

Name and Address of the Controller 4
Name and Address of the Data Protection Officer 4
General Information on Data Processing 5
Legal Basis for Processing Personal Data 5
Necessity of Providing the Data 5
Data Deletion and Storage Duration 6
Note on Data Transfer to Third Countries 7
Conducting the Online Consultation (Video Conference) 8
Embedded Videos in Consultation Guides 8
Use of AI-Supported Conversation Transcription and Automated Summarization 9
Service Providers Involved and Places of Processing 10
Data Processed 10
Consent and the Scope of This Control 11
Result, Storage and Deletion 12
Marking under the AI Regulation 13
Audio Recording of Consultations and Archiving 13
Customer Master Data and Consultation Documentation 14
Financial and Account Data 15
Account Information Service (Open Banking) 16
Financial Analysis Report according to DIN 77230 17
Health Data and Other Special Categories of Personal Data 17
Electronic Signature 18
Sending of SMS 20
Interfaces to the Service Provider's Systems 20
Checking of Uploaded Files for Malware 21
Processing of Personal Data for Appointments 22
Purpose of Processing 22
Legal Bases under GDPR 23
Integration into Customer Profile 23

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

Sign-in and Calendar Synchronization via Google and Microsoft 23
Google 24
Microsoft 26
Calendar Subscription and Integration of an External Calendar 28
Sign-in Through a Sign-in Service of the Service Provider 29
Registration, User Account and Contract Administration 30
Registered Devices for the Companion App 31
Payment Service Providers and Embedding of Payment Scripts 32
Dispatch of Emails 33
Information and Support for Our Registered Users 33
External Links 34
Rights of the Data Subject 35
Right of Withdrawal 35
Right to Object 35
Right to Lodge a Complaint with a Supervisory Authority 35
Right to Data Portability 36
Right of Access, Rectification and Erasure 36
Right to Restriction of Processing 36
Operation of the bridge Platform (Hosting) 37
Operational and Security Logging, Telemetry 38
Use of Local Storage Items, Session Storage Items and Cookies 39
Use of External Services 41
Web Security 42
Use of AltCha to Prevent Abuse and Spam 42

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

Name and Address of the Controller

The controller within the meaning of the General Data Protection Regulation (GDPR) and other data protection regulations is:

Bridge ITS GmbH
Käthe-Kollwitz-Ufer 76
01309 Dresden
Germany

Contact: info@bridge-systems.com

Scope of this notice. This notice concerns, on the one hand, processing operations for which Bridge ITS GmbH is itself the controller: the registration and administration of user accounts, billing, and the operation and security of the platform. On the other hand, it describes — for your information and without our being the controller in that respect — those processing operations that we carry out as a processor on behalf of the consulting service provider — the contractual partner referred to as the "Service Provider" in our General Terms and Conditions and as the "Client" in the Data Processing Agreement; for these the consulting service provider is the controller, it determines the purposes, the legal bases and the storage periods, and the rights of data subjects are to be asserted against it. The sections concerned indicate this in each case. This notice does **not** apply to our marketing website; a separate privacy policy is available there for it.

Name and Address of the Data Protection Officer

The Data Protection Officer of the controller is:

3 P Datenschutz GmbH
Stefan Leißl
Sanderstraße 47
86161 Augsburg
Phone: 0821 6508 8582
Email: leissl@3-p-datenschutz.de

General Information on Data Processing

Legal Basis for Processing Personal Data

In accordance with Art. 13 GDPR, we inform you about the legal bases of our data processing. Unless the legal basis is specifically mentioned in the privacy policy, the following applies:

The legal basis for obtaining consent is Art. 6(1)(a) in conjunction with Art. 7 GDPR. The legal basis for processing to fulfill our services and implement contractual measures as well as to respond to inquiries is Art. 6(1)(b) GDPR. The legal basis for processing to fulfill our legal obligations is Art. 6(1)(c) GDPR. If the processing of your data is necessary to protect a legitimate interest of our company or a third party and if the interests, fundamental rights and freedoms of the data subject do not override the first-mentioned interest, Art. 6(1)(f) GDPR serves as the legal basis for processing. In cases where vital interests of the data subject or another natural person make the processing of personal data necessary, Art. 6(1)(d) GDPR serves as the legal basis.

Necessity of Providing the Data

Your last name and your email address are required for the conclusion and performance of the usage contract; depending on the installation, your first name and company name may additionally be set up as mandatory entries. For billing, the details necessary for the payment method chosen are added. These details are required under the contract. Without them we cannot set up the user account, cannot conclude the contract and cannot bill for the service. There is no statutory obligation to provide them.

The form of address and the postal address are not mandatory. You may provide them, but you do not have to.

All other details are voluntary. If you do not provide them, you suffer no disadvantage; individual functions building on them — such as the calendar link or sign-in through an external sign-in service — are then unavailable.

For the data collected by the consulting service provider in the course of a consultation, that provider itself determines which details are required and what

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

the consequences of not providing them are; its own information is authoritative in that respect.

Data Deletion and Storage Duration

We adhere to the principles of data minimization according to Art. 5(1)(c) GDPR and storage limitation according to Art. 5(1)(e) GDPR. We store your personal data only for as long as necessary to achieve the purposes mentioned here or as required by statutory retention periods.

A distinction must be drawn between two roles. For **consultation, customer and participant data**, the consulting service provider is the controller; it determines the storage period, and we delete such data on its instruction, upon deletion of the customer record concerned, and upon termination of the user agreement. Conversation transcripts are currently an exception: they are not technically deleted together with the customer record but require a separately triggered deletion; upon termination of the user agreement we initiate that operation (see the section "Use of AI-Supported Conversation Transcription and Automated Summarization"). For **our own data** we determine the storage period ourselves. The following periods apply:

- **Invoices and booking vouchers:** eight years, starting from the end of the calendar year in which the voucher arose (Section 147(3) AO, Section 257(4) HGB).
- **Contract-partner data** (account, company and registration data): until the end of the third calendar year following the end of the contract (Sections 195, 199 BGB).
- **User-account data:** until the user account is deleted.
- **Operational and security logs:** the retention periods are stated in the section "Operational and Security Logging, Telemetry".
- **Audit logs** on account, user and provisioning operations: three years from the time they arise.

The SMS dispatch log is deleted after 90 days. The records of the signature process form part of the consultation documentation and are deleted together with the

associated customer record. Irrespective of this, you can request the deletion of the data concerning you at any time (see "Right of Access, Rectification and Erasure").

To ensure recoverability, the data holdings are backed up regularly. Deleted data may therefore still be contained in backups for the duration of the respective backup cycle; it ceases to exist there too when that cycle expires, and it is not processed further in the meantime.

Note on Data Transfer to Third Countries

Some of the service providers we use are based in a third country, notably the United States of America. This concerns:

- the voluntary linking of your user account with a Google or Microsoft account for sign-in and for calendar synchronization (Google LLC or Microsoft Corporation, USA, depending on the provider used), where those functions are available for your installation;
- the provision of the video conference including speech recognition by Daily.co, Inc., USA, as well as Deepgram, Inc., USA, engaged by it for speech recognition — the media and speech-recognition processing itself takes place in European data centers in accordance with the settings we apply, or via a processing endpoint restricted to the "EU" region;
- the loading of scripts of our payment service provider in your browser (see the section "Payment Service Providers and Embedding of Payment Scripts");
- the playing of an embedded video in a consultation guide, where the consultant uses a slide of the type "online video" and playback is started (YouTube: Google Ireland Limited or Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; Vimeo: Vimeo.com, Inc., 330 West 34th Street, New York, NY 10001, USA);
- the error monitoring of the conferencing software: the program library provided by Daily.co, Inc. and executed in your browser reports technical errors to the Sentry service of Functional Software, Inc., 45 Fremont Street, San Francisco, CA 94105, USA; the data transmitted are error, diagnostic and application-trace data including your IP address.

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

The level of data protection in third countries does not in every case correspond to EU data protection law; there is a risk that data may be disclosed to authorities of those countries and that no effective legal remedies are available against this. We therefore base transfers to third countries on Art. 44 et seqq. GDPR: on an adequacy decision of the European Commission where the recipient is certified under the EU-US Data Privacy Framework, and otherwise on EU Standard Contractual Clauses together with a transfer impact assessment.

Conducting the Online Consultation (Video Conference)

For the online consultation, the video and audio of the participants and — where a participant shares their screen — the screen transmission are transmitted via the conferencing technology of Daily.co, Inc. The data processed in the course of this are the video, audio and screen-sharing data, the IP addresses and device information of the participants, and session and connection metadata (such as duration and room identifier). The conference rooms are set to a processing region within the European Union; as regards the provider's seat in the USA, please note our section "Note on Data Transfer to Third Countries".

The consulting service provider is the controller for the content of the conversation; Bridge ITS GmbH processes such data as a processor acting on its instructions. The legal basis and the storage period are determined by the service provider; as a rule this is the performance of the consultancy agreement (Art. 6(1)(b) GDPR). A transcription or a recording of the conversation takes place only in accordance with the two following sections.

Embedded Videos in Consultation Guides

A consultation guide may contain slides of the type "online video". When such a slide is opened, **no contact is made with YouTube or Vimeo**; what is displayed first is a preview image delivered from our own server. That preview image is generated once when the slide is created: our server retrieves the preview image from the respective provider, adds a source attribution and stores it in our own file store. This retrieval takes place exclusively on the server side and without any involvement of

your device. Only when playback is started — or when you join a consultation in which a video is already running — is the video player of the respective provider loaded into your browser. Playback is usually started by the consultant; it runs synchronously for all participants, so the player is loaded onto the devices of the other participants at that moment as well.

When the player is loaded, your IP address and technical details of your browser and device are transmitted to the provider; this is technically necessary for the video to be delivered. We embed both providers in the most privacy-friendly variant they offer: the YouTube player runs in extended privacy mode via the domain www.youtube-nocookie.com, and for Vimeo the "Do Not Track" mode is activated — Vimeo then sets no tracking cookies and does not evaluate usage. The program library required to operate the YouTube player is, however, obtained from the domain www.youtube.com; in doing so Google sets its own cookies, among them VISITOR_INFO1_LIVE and YSC with a lifetime of several years. This happens only when playback is started, not already when the slide is displayed. Both providers are domiciled in the USA (see the section "Note on Data Transfer to Third Countries").

Whether such a slide is used and whether a video is played is decided by the consulting service provider; it is responsible for that transfer and for the consent required under Section 25(1) TDDDG for the setting of the provider's cookies. If you wish to avoid a transfer to these providers, please tell the consultant before playback is started.

Use of AI-Supported Conversation Transcription and Automated Summarization

The bridge platform offers the possibility to create a transcription and automated summary of the conversation using Artificial Intelligence (AI) during consultation sessions. The aim is to improve the quality of consultation and enable more precise documentation of conversation content.

These functions are not included in every tariff and are enabled separately for each account. Where a consultation is conducted via bridge, the consulting service

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

provider is the controller for the content of the conversation; in this respect Bridge ITS GmbH processes such data as a processor acting on its instructions.

Service Providers Involved and Places of Processing

Depending on the configuration of the installation used, the following processors are involved:

- **Speech recognition (transcription):** Daily.co, Inc., 340 S Lemon Ave #4133, Walnut, CA 91789, USA, which performs speech recognition through a service it engages with a European processing endpoint. Conference rooms and speech recognition are set to European processing regions; the underlying settings can be changed by the operator of the respective installation.
- **Automated summarization:** Mistral AI SAS, 15 rue des Halles, 75001 Paris, France. Processing takes place within the European Union. Under the data processing agreement concluded with the provider and the agreed terms of use, the transmitted content is not used for training AI models and is not stored by the provider (zero data retention).

Where a service provider involved is based outside the European Union, a transfer takes place only on the basis of Art. 44 et seqq. GDPR, in particular on the basis of EU Standard Contractual Clauses together with a transfer impact assessment. Please also note our section "Note on Data Transfer to Third Countries".

Data Processed

For the purpose of speech recognition, the **audio of the conference** is transmitted to the speech-recognition service. The result of speech recognition is a **transcript text** attributed by name to the participant currently speaking. For the automated summary, this transcript text is transmitted to the provider of the summary. Before the transmission, the names of the participants and of the person being advised are replaced by role designations — such as "consultant" and "customer 1" — in the speaker attribution and, where they are detected automatically, within the spoken text. The mapping of these designations to the actual names remains exclusively on our platform, is not transmitted and is not stored; it is resolved again in the summary returned. The transcript text is not truncated: you may still be identifiable

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

from the content of the conversation itself, which is why this is a replacement of names and not anonymization.

Consent and the Scope of This Control

These functions are activated situationally by the respective consultant; an account may also be configured so that transcription starts automatically as soon as at least two participants have joined the conference. The customer is informed about the activation, is pointed to further data protection information and is asked for consent. While transcription is running, the customer can see that the function is active and may change their decision at any time.

If transcription or live captioning is activated in a conference, **only the audio of those participants who have consented** is transmitted to the speech-recognition service. Anyone who has not answered the consent dialog, or who has refused, is excluded from the transmission. If you consent during a running consultation you are included; if you withdraw your consent you are excluded again. If nobody other than the consultant consents, only the consultant's audio is transmitted. Your consent further controls whether

- the transcript text concerning them is **stored** (without consent no storage takes place), and
- **live captions are displayed** to them.

This does not apply to the consultant leading the conference: they are treated as consenting by the system, are not shown the consent dialog, and the transcript text concerning them is stored from the moment the function is activated, with live captions displayed to them. The same applies to the audio recording: where the consultant starts the recording, their own consent is set by that same operation; here too they are not shown a separate consent dialog. The consulting service provider is the controller for the processing of the consultant's data; it determines the legal basis, which in that respect is not the consultant's consent.

The **audio recording** of the conversation is to be distinguished from this and is carried out only for those participants who have consented to it; see the section "Audio Recording of Consultations and Archiving".

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

By consenting, the customer confirms that they have been informed about the purpose, scope and technical functionality and have read and understood the privacy notice regarding the processing.

The legal basis for transmitting your audio to the speech-recognition service, for storing the transcript text, for displaying live captions and for creating the summary is your consent pursuant to Art. 6(1)(a) GDPR. It can be revoked at any time with effect for the future. Refusing or revoking consent has no disadvantages for you; the consultation continues. Please note: after a revocation your contributions are no longer captioned.

If you do not wish your audio to be transmitted to the speech-recognition service, refuse consent in the dialog or withdraw consent already given. Your audio is then not transmitted, or the transmission is ended. The consultation continues; your contributions are then no longer captioned.

Result, Storage and Deletion

The summary is generated by an AI model and contains, in addition to a rendering of the course of the conversation, **model-generated assessments and suggestions** regarding further advisory needs. It is a working result supporting the consultant and not an automated decision: no automated decision-making within the meaning of Art. 22 GDPR takes place on the basis of the data captured.

Transcripts and summaries are stored on the infrastructure of the bridge platform and are used exclusively for consultation purposes. An automatic, deadline-based deletion of this content does not currently take place.

The **summaries** are deleted together with the associated consultation and the customer record. The **conversation transcripts** are likewise deleted together with the associated customer record and on termination of the contract. For them, deletion is not carried out by an automatic run but by a separately triggered operation; we trigger it on the instruction of the responsible service provider, at the request of the data subject and at the end of the contract, provided that no statutory retention obligations conflict with this. The customer may at any time request information about the transcript concerning them and its deletion; please address deletion requests to the consulting service provider or to the contact details given under "Name and Address of the Controller".

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

Marking under the AI Regulation

The usage is in accordance with the transparency requirements of Art. 50 of Regulation (EU) 2024/1689 (AI Regulation). An interaction with Artificial Intelligence exists and is marked accordingly; the summary generated is additionally marked in machine-readable form as artificially generated.

The provider of the AI system within the meaning of Art. 3(3) of the AI Regulation is Bridge ITS GmbH, since it makes the system available under its own name. The deployer within the meaning of Art. 3(4) is the consulting service provider, who decides on its use in the individual conversation.

Audio Recording of Consultations and Archiving

Independently of transcription, a consultation may be recorded as an **audio recording**. The function is not included in every tariff and is enabled separately for each account.

Only the audio of those participants who have **consented** to the recording is recorded; if all participants withdraw their consent, the recording is stopped. The legal basis for the recording is Art. 6(1)(a) GDPR (consent).

The recording is produced by the conferencing technology of Daily.co, Inc. and is buffered until the platform retrieves it. That buffering takes place in storage within the European Union which we ourselves provide and control; the recording is not placed on the provider's own servers. The platform downloads the recording, stores it in encrypted form (AES-256) on its own infrastructure together with a checksum for detecting subsequent alteration and triggers deletion of the buffered copy. If an **external recording archive** is configured for the account concerned — this is the default setting and serves to fulfil any regulatory recording and retention obligations of the consulting service provider (for example Sec. 83(3) of the German Securities Trading Act (WpHG), implementing Art. 16(7) of Directive 2014/65/EU); whether and to what extent such obligations exist is determined by the consulting service provider — the recording is transferred to that archive and subsequently deleted from the platform; a record containing the technical details of the recording (time, duration, format, checksum, archiving status) is retained.

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

In addition to the audio file, the identifiers of the session and of the consultant are transmitted to the archive and — where a customer record is assigned to the conversation — the customer's **name, email address and customer reference number**. The archive is selected by the consulting service provider and operated in its name; it is responsible for the retention and deletion of the recordings stored there. Bridge ITS GmbH does not maintain its own deadline-based retention for the recordings.

If the transfer to the archive fails, the recording remains encrypted on the platform until the consulting service provider decides on its further use; the provider is informed of the failure by email. Bridge ITS GmbH does not warrant that a recording arrives in the consulting service provider's archive; monitoring its arrival is the provider's responsibility.

Customer Master Data and Consultation Documentation

The bridge platform is the central customer relationship management system of the consulting service provider. The master data of the persons advised is therefore **stored in the platform itself** and does not remain exclusively in another system of the service provider.

The data processed includes in particular:

- **Identification and contact data:** form of address, title, first, middle and last name, company name and legal form in the case of legal entities, gender, date of birth, nationality, marital status, number of children, language, customer reference number and status;
- **Means of contact:** email addresses and telephone numbers as well as postal addresses, in each case distinguished as private, business and other;
- **Relationships:** details of spouses and partners as well as children, where these are recorded for the consultation — including where those persons do not themselves use the platform;
- **Consultation data:** consultation histories and protocols, guides and slides used, answers recorded, notes, recommendations, appointments as well as

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

documents uploaded and downloaded, including identity and contract documents;

- **Participation data:** name and email address of the participants of an online consultation, time of joining and leaving, the browser and device identifier used (user agent), any rating given and a free-text comment. Where the account is configured to require the data protection information and the initial information provided by the service provider to be displayed and confirmed before joining, the confirmation that they were displayed and acknowledged is added, in each case with the time and the reference of the document displayed. That prompt is optional; the consulting service provider decides whether it is required for its account.

The consulting service provider is the controller for this processing; Bridge ITS GmbH processes the data as a processor acting on its instructions. The legal basis and the storage period are determined by the service provider; as a rule these are the performance of the consultancy agreement (Art. 6(1)(b) GDPR) and its statutory documentation and retention obligations (Art. 6(1)(c) GDPR, in particular under the German Insurance Contract Act and Sec. 34d of the German Trade Regulation Act).

Financial and Account Data

In order to produce financial analyses and needs assessments, the platform processes **financial data** of the person advised. This includes in particular income and other earnings, expenditure and running costs, assets and investments, liabilities and loans, real estate, retirement provision, existing insurance contracts, occupational details as well as goals and wishes.

The controller for this processing is the consulting service provider; Bridge ITS GmbH processes the data as a processor acting on its instructions. The legal basis and the storage period are determined by that provider; as a rule these are the performance of the consultancy contract or the taking of steps prior to entering into it (Art. 6(1)(b) GDPR).

In addition, **bank account details** may be stored: account holder, bank name, IBAN and BIC. These details are recorded via the programming interface of the platform

and from within the consultation flow and are assigned to the customer record; they are deleted together with the customer record.

Account Information Service (Open Banking)

At the consultant's initiative, the person advised may be sent a personalized link to an **account information service** of fino digital GmbH, Universitätsplatz 12, 34127 Kassel, Germany, through which they may voluntarily have their bank accounts read out. The link is valid for a limited period (default: seven days).

For this purpose, the name of the person advised, the name of the consultant and technical identifiers of the consultant and the customer are transmitted to the service provider. The connection to the bank and the authentication take place directly between the person advised and the account information service; Bridge ITS GmbH does not receive any bank account access credentials.

Transmitted back to the platform are a structured evaluation and a summarizing PDF document. The evaluation also contains **individual account transactions**. From it, the platform adopts into the customer record only the monthly net income and pension income, aggregated expenditure and a list of the insurance and retirement-provision contracts identified; individual account transactions are not adopted into the customer record and are not displayed to the consultant. The unaltered response of the account information service is deleted as soon as the evaluation has been adopted and the PDF document has been stored, and at the latest seven days after it was retrieved. The values adopted and the PDF document are stored assigned to the customer record and are deleted together with it. If the corresponding account setting is active — which is the default — the PDF document is additionally sent by email to the person advised.

Both the individual account transactions contained in the response and the contract categories identified may permit conclusions about special categories of personal data, in particular about health, long-term care and occupational disability insurance, and may therefore concern health data within the meaning of Art. 9 GDPR; see the following section. The legal basis for the use of the account information service is the consent of the person advised (Art. 6(1)(a) GDPR, and additionally Art. 9(2)(a) GDPR where health data are concerned).

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

Financial Analysis Report according to DIN 77230

Where the function is enabled for the installation used, a financial analysis report according to DIN 77230 can be produced from the household and financial data recorded. For this purpose we transmit the first and last name and the date of birth of the person advised and of the further persons included in the analysis, together with the complete household and financial data set including the health insurance status, to **VorFina GmbH**, Aidenbachstraße 30, 81379 Munich, Germany. Transmitted back to the platform is the report, as a PDF document. The processing takes place within Germany; no transfer to third countries takes place. The consulting service provider is the controller for this processing; Bridge ITS GmbH processes the data as a processor acting on its instructions. Where health data are concerned in the process, the following section applies in addition.

Health Data and Other Special Categories of Personal Data

Where the function is enabled for the installation in use, the platform provides input forms for certain advisory situations — such as cover against illness, the need for long-term care or occupational disability — in which **health data** may be recorded. The data that may be recorded includes pre-existing conditions and complaints by organ group — comprising mental illness and addiction disorders, benign as well as malignant tumours, a suicide attempt, and infectious, sexually transmitted and tropical diseases including HIV infection —, treatments and medication, height and weight, dioptre values, smoking behaviour, the degree of a disability and any reduction in earning capacity, a long-term care level, operations, hospital and rehabilitation stays as well as accidents, injuries and poisonings, details of the attending physicians including their name, address and medical specialty, declined insurance applications including the stated reason for refusal and the insurer concerned, health insurance status including any civil-service healthcare assistance entitlements, existing supplementary cover, and whether an advance healthcare directive or a healthcare power of attorney is in place. Details of occupational activity may likewise be recorded — occupation, job description, vocational training and the share of office-based and physical work — as well as occupational and leisure risks, such as motorcycling or stays in crisis areas. For

many of these entries, free-text fields are additionally available in which further health details may be recorded. Details of the attending physicians concern third parties who do not themselves use the platform.

Such details may also be recorded about **family members** of the person advised who do not themselves use the platform — in particular spouses and partners, children, parents and grandchildren.

In the course of recording occupational and tax details, it may additionally be recorded whether the person advised and, where applicable, their partner are **liable to church tax**. That detail permits inferences about religious beliefs and is therefore likewise a special category of personal data. Its recording is voluntary; it takes place exclusively on the basis of the data subject's explicit consent pursuant to Art. 9(2)(a) GDPR, which the consulting service provider obtains as the controller. The following paragraph on withdrawal and erasure applies to it accordingly.

Health data are special categories of personal data. Their collection and processing takes place exclusively on the basis of the **explicit consent** of the data subject pursuant to Art. 9(2)(a) GDPR in conjunction with Art. 6(1)(a) GDPR. If consent is withdrawn, the data are deleted unless they continue to be necessary for the establishment, exercise or defense of legal claims (Art. 9(2)(f) GDPR) or statutory retention obligations exist. Consent is obtained by the consulting service provider; it is the controller for this processing and determines the scope and the storage period. Recording such data is not a precondition for using the platform and is voluntary for the data subject.

Electronic Signature

Where the function is activated for the installation used, the consulting service provider can make a document available to the person advised for electronic signature. This happens in one of two ways: either the document is signed directly during the consultation appointment on a device of the consulting service provider, or the person advised receives a request by e-mail or SMS containing a link to the signature process and signs on their own device.

The data processed are the name of the person advised and, from their customer record, their e-mail address and, where available, their mobile number; both are

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

passed to the signature server for a possible delivery, even where only one channel is used in the individual case or the signature is given on site. If no mobile number is stored, the general telephone number is used. Also processed are the document to be signed and the result of the signature process, the signature itself, and the process history — time of creation, status changes, the number of documents involved and the service provider's user who triggered it. The process is assigned to the consulting service provider's account and to the associated customer record; the process history is kept as an audit log and is deleted together with the associated customer record.

Where signing takes place on a touch-sensitive screen, dynamic writing characteristics are captured in addition to the image of the signature — such as the timing, the speed and the pressure of the writing process. These characteristics are embedded in the signed document and stored with it; the document is held exclusively in this version. The characteristics serve solely as evidence that the signature originates from the signing person. Their capture may be objected to; in that case the signature cannot be given electronically by this route.

The controller for this processing is the consulting service provider that makes the document available; Bridge ITS GmbH processes the data as a processor acting on its instructions. The legal basis and the storage period are determined by that provider; as a rule these are the performance or initiation of the contract being signed (Art. 6(1)(b) GDPR) and, for the retention of the signed document, its evidentiary purpose (Art. 6(1)(c) and (f) GDPR).

The signature server used for this is operated by Bridge ITS GmbH itself on the infrastructure described in the section "Operation of the bridge Platform (Hosting)". No transmission to an external signature service provider takes place in this case. Where the consulting service provider has instead set up a connection from its account to its own signature and document system, which it uses with its own access credentials, the data is transmitted to that system; the section "Interfaces to the Service Provider's Systems" applies to this.

Sending of SMS

For invitations to consultation appointments and for notifications, the platform may send **SMS messages**. Dispatch takes place via seven communications GmbH & Co. KG ("seven.io"), Willestraße 4–6, 24103 Kiel, engaged by us.

The recipient's **mobile number** and the **message text** are transmitted to the SMS service provider. The message text may contain the names of the customer and the consultant as well as the date, time and access link of the appointment. The number and the message text are additionally stored in a dispatch log of the platform and are deleted there after 90 days. In the billing record, the number is stored in abbreviated form.

Where these are messages sent in the course of a consultation, the consulting service provider is the controller for this processing; Bridge ITS GmbH and the SMS service provider process the data in that respect as processors. The legal basis is Art. 6(1)(b) GDPR where dispatch is necessary in order to carry out the consultation appointment, and otherwise Art. 6(1)(f) GDPR.

Interfaces to the Service Provider's Systems

The consulting service provider may set up **interfaces to its own systems or to systems selected by it** for its account, for example to a broker management program, a comparison calculator, a document archive or a signature service. Where such an interface is set up, the platform transmits the data required for this purpose on its instruction — depending on the interface, for example the name, customer reference number and contact details of the person advised, details of the transaction, and either a retrieval reference to the document produced or the document itself. Interfaces can operate in both directions: where the consultant opens bridge from a connected system, the platform takes over the master and contact data of the person advised supplied from there — first, last and company name, title, form of address, date of birth, telephone numbers, email addresses, postal addresses and customer reference number — and uses them to create or update the customer record in bridge; where contract synchronisation is activated for the installation, the insurance and retirement provision contracts held there are taken over as well. The consulting service provider is the controller for this too.

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

Where a document is handed over to a document archive, the file is transferred in full; in the case of signed documents including the signature embedded in them and its dynamic writing characteristics.

Two cases deserve particular mention. Where the consultant triggers the **pre-population of an insurer's application or tariff calculator**, the master, contact and bank details of the person being advised, including the IBAN, are transmitted to that insurer, with whom the consulting service provider maintains its own broker or agency relationship and its own access. Where the consulting service provider has configured a **callback address (webhook)**, the platform reports events from its account — such as the completion of a consultation or the creation of a document — together with the associated case and customer references to the address it has specified. Where an audio recording is created, it may be handed over to a recording archive determined by the consulting service provider (see the section "Audio Recording of Consultations and Archiving").

The consulting service provider is responsible for the selection, set-up and operation of these recipients; the recipients do not act as sub-processors of Bridge ITS GmbH. The consulting service provider provides information about the interfaces set up in the individual case and the processing carried out there in its own privacy notice.

Checking of Uploaded Files for Malware

Uploaded files may be checked for malware before they are stored. For this purpose we use a scanning service operated by ourselves, to which the uploaded file is transmitted for checking; no transmission to third parties takes place. The check is a technical and organizational measure pursuant to Art. 32 GDPR. Where consultation and customer data are concerned in the process, we carry it out as a processor on behalf of the consulting service provider; for our own processing operations we base it on Art. 6(1)(f) GDPR, our legitimate interest lying in the security of the platform and of the data of all users.

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

Processing of Personal Data for Appointments

The bridge platform enables end users to independently book consultation appointments with their personal consultant. The controller for this processing is the consulting service provider with whom the appointment is made; Bridge ITS GmbH provides the technical platform for this and processes the data as a processor acting on its instructions.

The booking form links to this privacy notice because the form is part of the platform provided by Bridge ITS GmbH and concerns the technical processing described here. The consulting service provider is the controller for the processing of your booking data itself; its own privacy information takes precedence in that respect.

Specifically, we process first name and last name, email address, optionally a phone number, for appointments at the customer's premises additionally the address (street, house number, postcode, town and an optional address supplement) as a mandatory entry, contents of the free text field such as concerns or appointment type, the details of which website the appointment request was submitted from, as well as the calendar entry with associated metadata like timestamp and status.

> **Note:** Please do not provide any sensitive information according to Art. 9 GDPR in the free text field, such as health data or information about religious beliefs. The content of this field is adopted into the appointment description and, where the consultant uses calendar synchronization, thereby transferred to Microsoft or Google (see the section "Sign-in and Calendar Synchronization via Google and Microsoft"). This happens as soon as the appointment is requested and not only upon its acceptance, so that the consultant can also handle the request from within their calendar. For the recording of health data in the course of a consultation, the platform provides separate input forms (see the section "Health Data and Other Special Categories of Personal Data").

Purpose of Processing

The data collected during appointment booking is used exclusively for the appointment arrangement and its performance. This includes sending you

appointment confirmations and reminders, contacting you for questions or changes, maintaining the consultant's calendar and avoiding double bookings.

An appointment can be scheduled maximum 120 days in advance. The retention period is determined by the consulting service provider; the appointment details are deleted together with the associated customer record.

Legal Bases under GDPR

The legal basis is determined by the consulting service provider as the controller. As a rule this is Art. 6(1)(b) GDPR, as the processing is necessary for the implementation of pre-contractual measures as well as for the fulfillment of a contract.

The information in the consulting service provider's own privacy notice is authoritative; data subject rights are to be asserted against it.

Integration into Customer Profile

The information collected during appointment scheduling – i.e. name, email address, if applicable phone number and if applicable address – is assigned to the customer record in the customer management system of the bridge platform. This system serves the structured management of the consulting service provider's customer interactions.

The consulting service provider is the controller for this assignment as well; the section "Customer Master Data and Consultation Documentation" applies in addition. Bridge ITS GmbH does not use the data for its own purposes. If there is a technical interface to a system of the consulting service provider, the data can additionally be transferred there once an appointment is accepted.

Sign-in and Calendar Synchronization via Google and Microsoft

The bridge platform offers the option to link your user account with a Google or Microsoft account. The link can be used for registration and sign-in (single sign-on) and – independently of that – for the synchronization of appointments with the calendar of the respective provider.

Both functions are voluntary, optional additional features and not a mandatory part of using the platform. bridge can be used entirely with your own email address and your own password and without any calendar link. If you choose not to create a link, there is no limitation other than the calendar synchronization itself.

Whether these functions are available at all depends on the functional scope of the installation you use. There are installations in which neither Google nor Microsoft is integrated, and others in which only one of the two providers is available. The section below describes, in each case, the situation where the function concerned is available and you use it.

The legal basis for the link and the associated processing is your consent pursuant to Art. 6 para. 1 lit. a GDPR, which you give by actively creating the link and confirming the permission dialog at the respective provider. The link is established using the standard OAuth 2.0 / OpenID Connect procedure; bridge never receives your password for the respective provider, only time-limited access tokens.

Since the processing technically takes place at Google LLC or Microsoft Corporation, both based in the USA, data is transferred to a third country in the process. Both providers are certified under the EU-US Data Privacy Framework, for which the European Commission has issued an adequacy decision. Please also note our section "Note on Data Transfer to Third Countries".

Google

Which data is accessed: For registration and sign-in, bridge requests only the permissions (scopes) openid, email and profile. This provides us with a pseudonymous account identifier, your email address and basic profile data such as your name and, where applicable, profile picture and language setting.

For calendar synchronization, the permissions https://www.googleapis.com/auth/calendar.readonly (reading your calendar list and your appointments) and https://www.googleapis.com/auth/calendar.events.owned (creating, modifying and deleting only those appointments that you created yourself or for which you are the organizer) are added. This involves reading the calendar name and identifier as well as, for each appointment, the title, start and end, description, location, availability status (free/busy) and the markers for all-day and cancelled

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

appointments. So that synchronization can also run without an open session, a refresh token is additionally issued and stored.

There is no access to your phone number, your postal address, your contacts, your email mailbox, your files or any other content of your Google account.

What the data is used for: Account identifier, email address and name are used exclusively for authentication, i.e. signing in securely without a separate bridge password, and for creating and matching your bridge user account. The calendar data is used exclusively to display and reconcile your appointments in bridge, to avoid double bookings, to correctly represent your availability and to write bridge appointments back to your calendar.

Write access: When a bridge appointment is written back to your Google calendar, the title, start and end, availability status, description and location of the appointment are transferred. The title and the description thereby contain **personal data of the person advised** as well as details of the consultation: as the title the name of the consultation guide used, failing that the appointment designation, and further the name of the person advised, depending on the appointment type their telephone number or postal address, a management link to the appointment in bridge, the free-text notes stored, and a list of the participants which, for each participant, contains their name and email address — or, where no email address is stored, their telephone number — as well as their response status; the name and email address of the consultant are likewise transferred. Please note that the designation of a consultation guide may allow conclusions to be drawn about the subject of the consultation, for instance cover against illness or occupational disability. The service provider conducting the consultation is responsible for this transfer. If you wish to avoid a transfer of customer data to Google, do not use calendar synchronization.

Sharing, transfer and disclosure: Data received from Google APIs is not shared with or sold to third parties, is not used for advertising or profiling and is not used to train generalized AI or machine learning models. It is processed exclusively by Bridge ITS GmbH and by the processors and hosting providers named in this privacy policy. Humans do not read this data – except with your explicit consent, for security and abuse purposes, to comply with applicable law, or in aggregated and anonymized form.

bridge's use and transfer of information received from Google APIs to any other app will adhere to the Google API Services User Data Policy, including the Limited Use requirements.

Storage duration and withdrawal: We store access and refresh tokens as well as the assignment of the linked calendar for as long as the link exists; they are deleted once the link is removed. Imported calendar data is stored only for as long as it is required for synchronization. You can remove the link at any time in bridge in your profile or calendar settings and additionally withdraw your consent directly at Google at myaccount.google.com/permissions. After withdrawal, bridge no longer accesses your Google account. Please note the scope of the withdrawal: appointments already written to your Google calendar remain there and may have to be deleted there; the lawfulness of the processing carried out up to the withdrawal remains unaffected; removing a link used for sign-in does not delete your bridge user account – in that case you subsequently sign in with your email address and password.

Microsoft

Which data is accessed: For registration and sign-in, bridge requests only the permissions (scopes) openid, email and profile. This provides us with a pseudonymous account identifier, your email address and basic profile data such as your name.

For calendar synchronization, bridge requests the permissions openid, offline_access, Calendars.Read and Calendars.ReadWrite. This access deliberately takes place without profile and email permission, so only the account identifier and the calendar data are processed. We read your calendar list as well as, for each appointment, the identifier, title, start and end, description, location, availability status (free/tentative/busy) and the markers for all-day and cancelled appointments. For ongoing synchronization, bridge registers a subscription for change notifications for the linked calendar with Microsoft so that changes can be applied promptly. The permission offline_access enables synchronization even without an open session.

There is no access to your phone number, your postal address, your contacts, your email mailbox, your files or any other content of your Microsoft account.

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

What the data is used for: Account identifier, email address and name are used exclusively for authentication and for creating and matching your bridge user account. The calendar data is used exclusively to display and reconcile your appointments in bridge, to avoid double bookings and to correctly represent your availability.

Write access: bridge writes appointments exclusively to those calendars that you explicitly marked as target calendars when creating the link. The title, start and end, availability status, description and location of the appointment are transferred, plus two technical markers by which bridge recognizes its own entries.

Please note that the title and the description of the appointment **contain personal data of the person advised**: the title is composed of the name of the consultation guide used — failing that the appointment designation — and the **name of the person advised**; the designation of a consultation guide may allow conclusions to be drawn about the subject of the consultation, for instance cover against illness or occupational disability. The description contains the appointment type, the name of the person advised, depending on the appointment type their **telephone number** (telephone appointment) or **postal address** (on-site appointment), a management link to the appointment in bridge, the free-text notes stored for the appointment, and a list of the participants which, for each participant, contains their name and email address — or, where no email address is stored, their telephone number — as well as their response status; the name and email address of the consultant are likewise transferred. No meeting invitations are sent to third parties via this interface.

If you use calendar synchronization, this data is thereby transferred to Microsoft. The service provider conducting the consultation is responsible for this; it must ensure that this transfer is permissible. If you wish to avoid a transfer of customer data to Microsoft, do not use calendar synchronization — bridge is fully usable without it.

Sharing, transfer and disclosure: Data received from the Microsoft interfaces is not shared with or sold to third parties, is not used for advertising or profiling and is not used to train generalized AI or machine learning models. It is processed exclusively by Bridge ITS GmbH and by the processors and hosting providers named in this privacy policy.

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

Storage duration and withdrawal: We store access and refresh tokens as well as the assignment of the linked calendar for as long as the link exists; they are deleted once the link is removed, and the subscription for change notifications is terminated. Imported calendar data is stored only for as long as it is required for synchronization. You can remove the link at any time in bridge in your profile or calendar settings and additionally withdraw the granted permission directly in the permission settings of your Microsoft account. After withdrawal, bridge no longer accesses your Microsoft account. Please note the scope of the withdrawal: appointments already written to your Microsoft calendar remain there and may have to be deleted there; the lawfulness of the processing carried out up to the withdrawal remains unaffected; removing a link used for sign-in does not delete your bridge user account.

Calendar Subscription and Integration of an External Calendar

Besides the link with Google and Microsoft, the platform offers two further ways of reconciling appointments. In each case the consultant alone decides on the set-up; here too the consulting service provider is the controller.

Subscription to one's own bridge appointments. In the settings, the consultant can have a permanent subscription address generated and enter it into any calendar application or with any calendar service. Whoever calls up that address receives the consultant's appointments created in bridge, going back one year from the time of retrieval, in iCalendar format; appointments taken over from a linked external calendar are not delivered. Transmitted are the title, start and end, description and location of the appointment as well as the name and email address of the consultant as the organiser and the email addresses of all invited participants. As with calendar synchronisation, the title and description may contain the **name of the person being advised**, and for on-site appointments their **address** may appear as the location. The address contains a random credential of 60 characters and can be retrieved without signing in; whoever knows it can retrieve the appointments. The consultant alone determines which service it is passed to and therefore also to whom this data is transmitted; the consultant must ensure that this transmission is permissible.

Integrating an external calendar through its address. Conversely, the consultant can store the address of an external calendar. bridge then retrieves that calendar

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

regularly and takes from the appointments it contains the title, start and end, description, location, availability status as well as all-day and cancellation markers, in order to avoid double bookings. Where the integrated calendar contains personal data of third parties, that data thereby enters the platform; the consultant must ensure that they are entitled to do so. The appointments taken over are deleted as soon as the integration is removed.

Sign-in Through a Sign-in Service of the Service Provider

Where the consulting service provider uses its own sign-in service for its installation (single sign-on via OpenID Connect), signing in to bridge takes place through that service. In that case no password is stored with us. Where the installation is operated for a group of service providers — for example for a broker pool — that sign-in service may also be provided by the operator of the group; signing in then takes place through that operator's service, and Bridge ITS GmbH is registered there as the requesting party.

What is taken over is the user's identifier together with the details about the person supplied by the sign-in service, in particular name and e-mail address. Where **role mapping** is additionally set up for the installation, bridge evaluates the role and group memberships supplied by the sign-in service and derives the user's permissions within bridge from them. This assignment is stored with the user account and updated on every sign-in; while role mapping is active, the permissions concerned cannot be edited manually in bridge.

Where the consulting service provider has additionally set up **automated user provisioning** (SCIM), its identity management system transmits the user data directly to bridge and keeps it up to date there. What is stored in that case is an external identifier, the user name, first and last name, a title or function designation, e-mail addresses, gender, telephone numbers and addresses, the user's active status and the group memberships.

The persons affected by this are the employees and agents of the consulting service provider, not the persons being advised. The controller for this processing is the consulting service provider as employer or principal; it decides on the use of

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

the sign-in service, on the scope of the details transmitted and on the legal basis. Bridge ITS GmbH processes this data as a processor acting on its instructions, for the purpose of setting up and administering the user accounts and controlling permissions. For the technical creation and continued existence of the user account as a means of access — sign-in data, account status and the associated security logs — we are, by contrast, the controller ourselves; the section "Registration, User Account and Contract Administration" provides information on this.

Registration, User Account and Contract Administration

For the initiation, conclusion and performance of the usage contract for the bridge platform, and for the creation and administration of the user accounts, Bridge ITS GmbH is itself the controller.

Data processed. On registration and in the further course of the contractual relationship we process the form of address, first and last name, company name and legal form, address, email address, phone number, language setting, commercial register and VAT identification number details, the service package and payment model chosen, an identifier for the payment method stored, as well as the account status and the times of registration, of the last sign-in and of the last activity. We store your password exclusively as a check value from which the password cannot be recomputed.

Purposes. The processing serves the initiation and conclusion of the usage contract, the creation and administration of your user account including the granting and verification of permissions, the provision of the contractually owed service, billing, and compliance with our obligations under commercial and tax law.

Legal bases. Art. 6(1)(b) GDPR for the initiation and performance of the contract, Art. 6(1)(c) GDPR for the statutory retention and accounting obligations, and Art. 6(1)(f) GDPR for the security of the account and the prevention of misuse.

Recipients. Payment service providers (see the section "Payment Service Providers and Embedding of Payment Scripts"), the email platform we use (see the sections "Email Dispatch" and "Information and Support of Our Registered Users") and the

hosting service provider (see the section "Operation of the bridge Platform (Hosting)"). Beyond this we do not pass on this data.

Storage duration. The periods stated in the section "Data Deletion and Storage Duration" for contract-partner data, user account data and invoices and booking vouchers apply.

Where you did not create the account yourself. Where your user account is created not by you but by an account administrator of your organisation, we receive your details — form of address, first and last name, gender, email address and, if applicable, address — from that source and not from you. We use them to set up the account and, in accordance with the section "Information and Support of Our Registered Users", for support and information about our own product; in doing so they are transferred to the email platform named there. We inform you about this origin with the invitation email, at the latest within one month of receiving the data (Art. 14(3)(a) GDPR). Your rights under Art. 15 to 21 GDPR are unaffected; in particular you may object to receiving information at any time and free of charge. Where your organisation sets up the account through its own sign-in service or through automated user provisioning, it is itself responsible for the selection and scope of the details transmitted (see the section "Sign-in Through a Sign-in Service of the Service Provider").

Registered Devices for the Companion App

Users can register a device for the companion app in order to sign it in to a consultation in progress. Stored in the process are a device identifier supplied by the device, the device designation assigned by the user, the assignment to the user account, an access credential — this too only as a check value, not in clear text — and the time of last access. The purpose is to sign the device in to a consultation; the legal basis is Art. 6(1)(b) GDPR. The registration persists until the user removes it in the settings; when the user account is deleted, the associated device entries are deleted.

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

Payment Service Providers and Embedding of Payment Scripts

For the billing of usage charges we use the payment service providers **Stripe Payments Europe, Limited**, The One Building, 1 Grand Canal Street Lower, Dublin 2, Ireland, and **PayPal (Europe) S.à r.l. et Cie, S.C.A.**, 22-24 Boulevard Royal, L-2449 Luxembourg. The technical handling of PayPal payments takes place via the "Braintree" interface, a service of the PayPal group of companies.

We transmit to the payment service provider the details of our contractual partner required for billing, i.e. the name and email address of the account, the language setting and technical identifiers of the account. Payment-instrument data such as card numbers or bank account details are collected directly in the browser by the payment service provider; of these we store only an abbreviated detail in order to identify the payment instrument.

In order to collect the payment-instrument data, a **script of the payment service provider is loaded from its servers**. In doing so, your IP address is transmitted to the payment service provider and technical details of your browser may be processed. This script is loaded on the registration, billing and payment-instrument management pages and — for technical reasons — on the consultant's view of the consultation room where SMS dispatch or transcription is available for the consultation concerned. It is not loaded on the pages displayed to the persons advised.

Where PayPal is offered as a payment method, the program library used for this purpose loads further scripts from servers of the PayPal group of companies at runtime. These include a fraud-prevention component which collects technical details of your device and browser. Transmitted in the process are your IP address as well as device and browser details.

The legal basis is Art. 6(1)(b) GDPR for the performance of the contract, Art. 6(1)(f) GDPR for the technical provision of the payment function and — as regards fraud prevention — the legitimate interest of the payment service provider together with our own interest in preventing abusive payment transactions (Art. 6(1)(f) GDPR).

Dispatch of Emails

All emails generated by the platform — in particular invitations to consultation appointments, appointment confirmations and reminders, the dispatch of consultation documents and evaluations, requests for an electronic signature, and system and account notifications — are sent via the email platform of **Brevo GmbH**, Köpenicker Straße 126, 10179 Berlin, Germany (parent company: Sendinblue SAS, Paris).

Transmitted in the process are the email address and name of the recipient, the subject and content of the message including the personal data contained therein, any file attachments, and dispatch and delivery metadata.

Where these are messages sent in the course of a consultation, the consulting service provider is the controller for this processing; Bridge ITS GmbH and Brevo process the data in that respect as processors. The legal basis is Art. 6(1)(b) GDPR where dispatch is necessary in order to carry out the consultation, and otherwise Art. 6(1)(f) GDPR.

Information and Support for Our Registered Users

We use the same email platform of **Brevo GmbH** for the support and information of the users registered with us — that is, the users of the bridge platform, not the end customers advised by them. Bridge ITS GmbH is itself the controller for this processing.

Transmitted are the email address, first and last name, a technical user identifier, the name and identifier of the associated account, the account status including an indication of a termination given, the address of the installation used, the registration date and the time of the last sign-in, as well as whether the receipt of onboarding information or of the newsletter is deactivated for the account. The purposes are support during set-up ("onboarding") and the dispatch of product information about the platform you use.

We inform you exclusively about our own product and comparable services of our own; we do not send advertising for third-party offerings. The legal basis is Art.

6(1)(b) GDPR to the extent that the information serves the performance of the user agreement, and otherwise Art. 6(1)(f) GDPR. Our legitimate interest lies in informing the users registered with us about changes, new features and comparable services of our own relating to the platform they use; the admissibility of contacting you by email is governed by Sec. 7(3) of the German Act against Unfair Competition (UWG).

This information concerns the users registered with us. Where we receive contact details by another route — for example through a form on our marketing website or at an event — we inform you of this at the point of collection; the privacy policy published there applies to the marketing website.

You may object to receiving these messages at any time and free of charge — via the unsubscribe link in every email or informally to datenschutz@bridge-systems.com; dispatch will then be discontinued. If your user account is deleted, the corresponding contact at Brevo is deleted. If you change your email address, the corresponding contact is moved to the new address; an objection declared earlier remains in effect.

External Links

The platform may contain links to third-party websites or to other websites under our responsibility. If you follow a link to any websites outside our responsibility, please note that these websites have their own privacy policies. We do not accept any responsibility or liability for these external websites and their privacy notices. Therefore, please check before using these websites whether you agree with their privacy policies.

You can recognize external links either by being slightly offset in color from the rest of the text or by being underlined. Your cursor will indicate external links when you hover over such a link. Only when you click on an external link will your personal data be transmitted to the link destination. The operator of the other website receives in particular your IP address, the time at which you clicked the link, the page on which you clicked the link, as well as other information that you can find in the privacy policy of the respective provider.

Please also note that individual links may lead to data transmission outside the European Economic Area. This could allow foreign authorities to access your data. You may not have any legal remedies against such data access. If you do not want your personal data to be transferred to the link destination or even unintentionally exposed to access by foreign authorities, please do not click on any links.

Rights of the Data Subject

As a data subject within the meaning of the GDPR, you have various rights that you can exercise. The data subject rights under the GDPR include the right of access (Art. 15), the right to rectification (Art. 16), the right to erasure (Art. 17), the right to restriction of processing (Art. 18), the right to object (Art. 21), the right to lodge a complaint with a supervisory authority, and the right to data portability (Art. 20).

Right of Withdrawal

Some data processing operations can only be carried out with your express consent. You have the right to withdraw your consent at any time. The lawfulness of data processing, up until the withdrawal, remains unaffected.

Right to Object

If processing is based on Art. 6(1)(e) or (f) GDPR, you as a data subject have the right to object at any time to the processing of personal data concerning you on grounds relating to your particular situation. This right also applies to profiling based on these provisions within the meaning of Art. 4(4) GDPR. Following an objection we will no longer process the personal data concerning you, 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.

If personal data is processed for direct marketing purposes, you also have the right to object at any time. The same applies to profiling related to direct marketing. Here too, we will no longer process personal data once you raise an objection.

Right to Lodge a Complaint with a Supervisory Authority

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

If you believe that the processing of your personal data violates the GDPR, you have the right to lodge a complaint with a supervisory authority, particularly in the Member State of your residence, place of work or place of the alleged violation, without prejudice to any other administrative or judicial remedy.

The supervisory authority responsible for us is the Sächsische Datenschutz- und Transparenzbeauftragte, Postfach 11 01 32, 01330 Dresden, Germany (visitor address: Maternistraße 17, 01067 Dresden), telephone +49 351 85471-101, post@sdtb.sachsen.de.

Right to Data Portability

If your data is processed based on consent or contract performance in an automated manner, you have the right to receive this data in a structured, commonly used and machine-readable format. Furthermore, you have the right to request the transfer and provision of the data to another controller, insofar as this is technically feasible.

Right of Access, Rectification and Erasure

You have the right to obtain information about your processed personal data regarding the purpose of data processing, the categories, recipients and duration of storage. For questions on this topic or other topics regarding personal data, you can of course contact us via the contact details provided in the imprint.

Right to Restriction of Processing

You can request restriction of the processing of your personal data at any time. To do so, you must meet one of the following requirements:

- You contest the accuracy of the personal data. For the duration of verifying the accuracy, you have the right to request restriction of processing.
- If processing is unlawful, you can request restriction of data use instead of erasure.
- If we no longer need your personal data for processing purposes but you need the data for the establishment, exercise or defense of legal claims, you can request restriction of processing instead of erasure.

- If you object to processing pursuant to Art. 21(1) GDPR, a balancing of interests between your and our interests will be carried out. Until this balancing is completed, you have the right to request restriction of processing.

A restriction of processing means that personal data may only be stored and not processed in any other way, except with your consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

Operation of the bridge Platform (Hosting)

The bridge platform itself — that is, the application, the database and the file storage in which consultation, customer and account data are processed — is operated separately from the marketing website. It runs on Microsoft Azure cloud infrastructure, which we procure through the Cloud Solution Provider

dotSource SE
Goethestraße 1
07743 Jena
Germany

namely on the services Azure Kubernetes Service (application), Azure Database for MySQL Flexible Server (database) and Azure File Storage (file storage). The operator of the infrastructure is Microsoft; processing takes place in data centers in the "Germany West Central" region, that is, in Germany. A data processing agreement is in place with dotSource SE; in addition, the Microsoft Data Protection Addendum applies to the Microsoft services.

For individual, separately agreed installations, operation takes place instead on cloud servers of

1&1 IONOS SE
Elgendorfer Straße 57
56410 Montabaur
Germany

Here too, processing takes place in data centres in Germany; no transfer to a third country takes place. A data processing agreement is likewise in place with 1&1

IONOS SE. Which hosting provider is used for the respective installation is set out in Annex 1 of the data processing agreement of the contractual relationship concerned.

Where consultation, customer and participant data is stored on this infrastructure, the consulting service provider is the controller for it; we process that data as a processor acting on its instructions. For our own processing activities — the provision, operation and security of the platform as well as the account and billing data — we are the controller; the legal basis in that respect is Art. 6(1)(b) GDPR for the provision of the contractually owed service and Art. 6(1)(f) GDPR for secure and uninterrupted operation.

Operational and Security Logging, Telemetry

Technical log data arise for the operation, troubleshooting, billing and security of the platform.

Server-side logs. Web server access logs contain, among other things, the IP address of the accessing device, the time, the resource requested, the status code and the volume of data transferred; they are deleted after 60 days. The application log is deleted after 30 days. Event logs within the application (session log, log of interface calls) are deleted by an automatic cleanup run after a configured period; the default setting for production systems is 90 days. In the dispatch log for emails, the recipient address, subject, sender name and time of dispatch are stored for 90 days; message content and file attachments are removed after 30 days. On our production systems, the interface call log also records the complete content of the request and the response: method, address and query parameters, the headers transmitted, the request payload, the calling user, the status code and the response data. Headers containing access credentials are masked before storage. As customer and consultation data is also transmitted through these interfaces, these log entries may contain personal data; they are deleted after 90 days.

Telemetry. In installations operated in containers, the application monitoring **Azure Application Insights / Azure Monitor** of Microsoft is additionally integrated. Technical telemetry data on calls, run times, dependencies and errors of the application are captured; depending on the configuration of the monitoring service, these may also include the address called, the IP address of the accessing

device and messages from the application log. The purposes are ensuring operation, error analysis, capacity and billing determination, and the detection of security incidents. The retention period depends on the configuration of the service; under the default setting of the service it is 90 days and may be extended in an individual case in order to investigate an incident.

On the installations operated on cloud servers of 1&1 IONOS SE, this application monitoring is **not** integrated. We do not integrate any additional monitoring service there; only the monitoring and logging that the hosting provider carries out as standard for the operation of its infrastructure applies. The server-side logs named above and the application's event and audit logs arise there unchanged.

Audit logs. For evidentiary purposes, the platform maintains separate audit logs (concerning, among other things, account, user, user-data, signature and provisioning operations). They are deleted after three years; records of signature processes are deleted, by way of exception, together with the associated customer record.

The legal basis for logging and telemetry is Art. 6(1)(f) GDPR. Our legitimate interest lies in the secure, traceable and uninterrupted operation of the platform and in preventing misuse; where logging serves to comply with statutory obligations, the legal basis is Art. 6(1)(c) GDPR. These legal bases concern our own processing activities. Where the logs contain consultation, customer or participant data, we maintain them as a processor on behalf of the consulting service provider; it is the controller in that respect, determines the storage duration, and the rights of data subjects are to be asserted against it.

Use of Local Storage Items, Session Storage Items and Cookies

Our platform uses local storage items, session storage items and/or cookies. Cookies are small records that are stored on your device through your browser and are automatically sent back with every request to the web server that set them. They serve, for instance, to maintain a sign-in or to store settings. Local and session storage likewise store data in the browser, but are not automatically transmitted to the server.

These objects can also be stored on your device by third-party companies when you enter our site (third-party requests). This enables us as operators and you as visitors of this website to use certain services from third parties that are installed on this website. Examples include the processing of payment services or the display of videos.

These mechanisms have various applications. They can ensure the functionality of a website, increase the security and convenience of website usage, and enable analyses regarding visitor flows and behavior. Under data protection law, what matters is whether the access to your device is strictly necessary. Where it is strictly necessary in order to provide a service you have expressly requested — for instance to maintain your sign-in — it is permitted without consent under Section 25(2) no. 2 TDDDG; we base the subsequent processing of the data on Art. 6(1)(f) GDPR, our legitimate interest being the technically error-free provision of our services. Any storage of information on your device, or access to information already stored there, going beyond this — in particular for analysis, audience measurement or advertising purposes — is permitted under Section 25(1) TDDDG only with your consent; the legal basis for the subsequent processing is then Art. 6(1)(a) GDPR.

We currently use exclusively strictly necessary cookies. No consent is required for these, and we therefore do not use a consent banner. Should we use cookies or third-party services requiring consent in the future, we will inform you separately in this privacy notice and obtain your consent beforehand; it can be withdrawn at any time with effect for the future.

Cookies set by us. We set exclusively technically necessary cookies of our own domain: the session cookie for maintaining your sign-in (`BRIDGE_SESSION`), which expires at the end of the session; a cookie for the optional persistent sign-in ("stay signed in"; `BRIDGE_LOGIN`) with a lifetime of 30 days by default, which can be configured differently per installation and which ends on sign-out; and the `BRIDGE_AUTH` cookie where you sign in through an external sign-in service, with a lifetime of one year. The `BRIDGE_AUTH` cookie is set only where you sign in through an external sign-in service (single sign-on) — this may be an existing account with Google or Microsoft, equally your own organisation's sign-in service or another service set up for your installation. It contains nothing but the designation of the service used — no identifier and no sign-in credentials. It ensures that once a

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

session has ended you are taken straight back to that provider instead of having to go through the sign-in page again; it is not set where you sign in with a password. You can remove it by signing out. **We do not set any cookies for analysis, audience measurement or advertising purposes.** No web analytics or tracking service is embedded in our pages; audience measurement via an analytics service has been discontinued. The protection against automated access that we use (see the section "Use of AltCha to Prevent Abuse and Spam") operates without cookies and without any transmission to third parties.

Local storage and session storage entries set by us. In your browser's local storage we place: a security credential protecting against cross-site request forgery (CSRF-Token); where the online consultation is used, your selection of camera and microphone including the clear-text designation of the devices as well as the resolution and mirroring chosen (bridge.camera-id, bridge.camera-label, bridge.camera-resolution, bridge.camera-image-mirrored, bridge.microphone-id, bridge.microphone-label); the display name last used by the participating person (participantName); and your settings for the drawing tool (Sii_drawingColor, Sii_drawingLineWidth, Sii_drawingFontSizeScale). These entries remain stored until you delete your browser's data. In session storage — that is, only for the duration of the browser tab — we place the email address of an invited participating person (newEmail) and the logging level set (logLevel). All of the entries named are necessary for the application to function; they are not evaluated for analysis or advertising purposes.

Use of External Services

The only third-party service embedded in the platform is our payment service provider's script; see the section "Payment Service Providers and Embedding of Payment Scripts". No web analytics or tracking service is integrated. Within the platform, third-party content may additionally be loaded where the consulting service provider uses it — this concerns embedded videos in consultation guides and the error monitoring of the conferencing software; see the sections "Embedded Videos in Consultation Guides" and "Note on Data Transfer to Third Countries". Should further external services be used in future, we will provide information about

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107

this in this privacy notice and, where necessary, obtain your consent, which may be revoked at any time (Art. 6(1)(a) GDPR).

Web Security

In the platform, we use tools that protect against unauthorized access, spam or other attacks. This increases the security of the platform.

We base this processing on a legitimate interest (Art. 6(1)(f) GDPR).

Our legitimate interest is to ensure the security of the platform and protect ourselves against unauthorized access, spam and other attacks.

Use of AltCha to Prevent Abuse and Spam

We use the AltCha service to protect the platform and our online services from automated attacks, bots and spam.

AltCha is a so-called Captcha service that ensures that the interactions carried out in the platform are with human users. Unlike other providers, AltCha is not based on the analysis of personal data or the creation of user profiles. Instead, AltCha uses a process called proof-of-work, in which the end device used solves small computing tasks in the background to rule out automated bots. No personal data is collected, processed or stored in the process.

In particular, there is no tracking, no transfer of data to third parties and no evaluation of user behavior. No cookies are set, no IP addresses are stored and no data is transmitted to AltCha servers, as the captcha service is hosted entirely by bridge.

The legal basis for the processing is our legitimate interest pursuant to Art. 6 para. 1 lit. f GDPR to ensure the security of the platform and the trouble-free operation of our online services and to protect us against misuse and attacks.

You can find more information about AltCha at: https://altcha.org

Bridge ITS GmbH — Käthe-Kollwitz-Ufer 76 — 01309 Dresden, Germany — www.bridge-beraten.de
Managing Director: Holm Hallbauer — Registered office: Dresden — Commercial register: Dresden HRB 18730 — Commerzbank AG
IBAN: DE59 8508 0000 0553 1135 00 — BIC: DRESDEFF — VAT ID: DE210242365 — Tax number: 203/106/14107