



Data Processing Agreement

Agreement on the Processing of Personal Data on behalf of a Controller
pursuant to Art. 28 GDPR

Last updated: 23 October 2026

Bridge ITS GmbH, Dresden

Table of Contents

1. Subject Matter of the Agreement.....	3
2. Scope of Contract.....	3
3. Right of the Client to Issue Instructions.....	6
4. Client Responsibilities	7
5. Personnel Requirements	8
6. Security of Processing.....	8
7. Engagement of Sub-Processors	9
8. Rights of Data Subjects	10
9. Contractor Obligations to Provide Notification and Support	11
10. Deletion of Data	12
11. Proof of Verification	12
12. Duration and Termination of Contract	14
13. Liability	14
14. Final Clauses	15
Annex 1: Sub-Processors	16
dotSource SE – provision and operation of the cloud infrastructure (Microsoft Azure)	16
Mistral AI SAS – AI-supported summarization of consultations.....	17
Daily.co, Inc. – video conferencing, recording and speech-recognition service ..	18
Amazon Web Services EMEA SARL – Buffer Storage for Audio Recordings.....	20
1&1 IONOS SE – hosting provider for separately agreed installations.....	20
fino digital GmbH – account information service (retrieval and evaluation of bank account data)	21
Brevo GmbH – dispatch of emails.....	22
seven communications GmbH & Co. KG – dispatch of SMS messages.....	22
VorFina GmbH – service provider for financial analysis reports according to DIN 77230.....	23
Recipients and components not listed as Sub-Processors.....	24

Agreement on the Processing of Personal Data on behalf of a Controller pursuant
to Art. 28 GDPR

between

the user of the bridge Software

– hereinafter referred to as the "Client" –

and

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

– hereinafter referred to as the "Contractor" –

1. Subject Matter of the Agreement

In the course of performing the services, the Contractor is required to handle personal data (hereinafter referred to as "Client Data") for which the Client acts as the controller within the meaning of data protection law. This Agreement sets out in detail the data protection rights and obligations of the parties in connection with the Contractor's handling of Client Data for the performance of the Main Contract.

The Main Contract within the meaning of this Agreement is the usage agreement for the bridge platform concluded between the parties on the basis of the General Terms and Conditions of Bridge ITS GmbH, including the service options selected during online registration. This Agreement is concluded together with the Main Contract and forms part of it; no separate signature is required.

2. Scope of Contract

2.1 The Contractor shall process Client Data on behalf of and in accordance with the Client's instructions within the meaning of Art. 28 GDPR (processing on behalf of the controller). The Client remains the controller within the meaning of data protection law. The Client within the meaning of this Agreement is the contractual partner referred to as the "Service Provider" in the General Terms and Conditions and as the "consulting service provider" in the privacy notice; the Contractor is Bridge ITS GmbH.

2.2 Contractor processing of Client Data is performed in the manner, to the extent, and for the purpose specified in the Main Contract. The duration of data processing corresponds to the duration of the Main Contract.

The subject matter and purpose of the processing is the provision and operation of the bridge platform for the preparation, conduct and documentation of consultations in accordance with the Main Contract. Unless the Main Contract provides otherwise, the following applies:

Categories of data subjects: persons advised by the Client as well as their family members recorded in the course of the consultation; where the Client advises a business, its authorised representatives, named contacts and the employees referred to in the course of the consultation; participants in online consultations, employees and agents of the Client (consultants and other users), persons submitting an appointment request, other third parties named in the course of the consultation, in particular attending physicians, and – where the Client uses calendar synchronisation – persons appearing as the organiser or a participant of an appointment in a calendar released by it for that purpose.

Types of personal data:

- master and identification data (including form of address, title, name, company name and legal form, gender, date of birth, nationality, marital status, number of children, customer reference number, status)
- contact data (email addresses, telephone and mobile numbers, postal addresses)
- relationship and contract data (details of spouses and partners as well as children, existing insurance and retirement-provision contracts)
- financial and account data (income and other earnings, expenditure, assets, liabilities, real estate, retirement provision, occupational details as well as account holder, bank name, IBAN and BIC)
- consultation and documentation data (consultation histories and protocols, guides and slides used, answers recorded, notes, recommendations, appointments, documents uploaded and downloaded including identity and contract documents)

- communication content (video, audio and screen transmission during an online consultation and – depending on the functional scope used – audio recordings, conversation transcripts and the summaries generated from them, email and SMS content)
- calendar data (name and identifier of the calendars released for synchronisation and, for the appointments they contain, title, start and end, description, location, availability status, all-day and cancellation markers), where the Client uses calendar synchronisation or the integration of an external calendar
- usage and connection data (IP addresses, device and browser identifiers, timestamps, session and connection metadata, log data)
- evidentiary data (ratings and free-text comments as well as – where the Client requires the confirmation for its account – confirmations that data protection information and initial information were displayed, in each case with the time and reference). Consents given during an online consultation to recording, transcription and live captioning are held in memory only for the duration of the session and are not stored as a separate evidentiary record; they are recorded as an event in the session log and – where a consultation protocol is generated – in that protocol
- **special categories of personal data pursuant to Art. 9 GDPR**, where the Client uses the corresponding recording functions: health data (including 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, diopetre values, smoking behaviour, details of occupational activity as well as occupational and leisure risks, degree of a disability and any reduction in earning capacity, 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, whether an advance healthcare directive or a healthcare power of attorney is in place, and free-text details on

the state of health), also concerning family members of the person advised; furthermore — where the Client uses the recording of occupational and tax details — the indication of whether the person advised and their partner are liable to church tax, which permits inferences about religious beliefs

The Client shall ensure that the conditions of Art. 9(2) GDPR are met for the processing of special categories of personal data and shall inform the Contractor of any heightened protection requirement.

2.3 The Contractor reserves the right to anonymize or aggregate any Client Data so that it is no longer possible to identify individual persons concerned, and to process it in this form for the purpose of demand-oriented design, further development and optimization, and to provide the service agreed upon in accordance with the Main Contract. The parties agree that anonymized Client Data or Client Data aggregated in accordance with the above provision shall no longer be considered Client Data within the context of this Agreement.

2.4 Processing of Client Data through the Contractor generally takes place within the European Union or in another contracting state of the Agreement on the European Economic Area (EEA). The Contractor is nevertheless permitted to process Client Data outside the EEA in compliance with the terms of this Agreement if the Contractor informs the Client in advance of the location of data processing and the requirements of Articles 44–48 of the GDPR are met or an exception pursuant to Article 49 of the GDPR applies.

3. Right of the Client to Issue Instructions

3.1 The Contractor processes Client Data in accordance with the Client's instructions, unless the Contractor is required by law to do otherwise. In the latter case, the Contractor must notify the Client of such legal requirements prior to processing, unless the relevant law prohibits such notification due to an important public interest.

3.2 Client instructions are generally and conclusively defined and documented in the terms and conditions of this Contract. The Client issues individual instructions that deviate from the terms of this Agreement, or that impose additional

requirements, in text form to the contact address designated by the Contractor. The Contractor confirms receipt in text form and documents the instruction.

Instructions that are necessary to comply with data protection law — in particular instructions to erase, rectify or restrict processing, and to implement orders of a supervisory authority — are implemented by the Contractor without undue delay and irrespective of any cost arrangement.

Where any other individual instruction causes the Contractor effort going beyond the service owed under this Agreement, the Contractor informs the Client without undue delay and the parties agree on how the additional costs are to be borne. No further requirement of consent exists.

3.3 The Contractor guarantees to handle Client Data in accordance with the Client's instructions. If the Contractor is of the opinion that an instruction of the Client violates this Agreement or the applicable data protection law, the Contractor shall inform the Client thereof without undue delay; the Contractor is then entitled to suspend the execution of the instruction until the Client confirms it. The parties agree that responsibility for the lawfulness of the instruction lies with the Client; the Contractor's own obligations under Articles 28 and 32 GDPR remain unaffected.

4. Client Responsibilities

4.1 In the relationship between the parties, the Client is solely responsible for the lawfulness of the processing of Client Data and for safeguarding the rights of data subjects. The indemnification of the Contractor against claims of third parties is governed by Section 13.1.

4.2 The Client is responsible for providing the Contractor with the Client Data in a timely manner for the rendering of services under the Main Contract and is responsible for the quality of the Client Data. The Client must inform the Contractor without undue delay and in full if errors or irregularities regarding data protection regulations or its own instructions are discovered during the testing of the Contractor's work order output.

4.3 If requested, the Client must provide the Contractor with the information referred to in Article 30(2) of the GDPR, provided that the Contractor does not already have this information.

4.4 If the Contractor should be obligated to provide information about the processing of Client Data to a government agency or person, or to otherwise cooperate with such agencies, the Client is obligated to provide the Contractor with assistance in supplying such information without undue delay, and/or in fulfilling other commitments to cooperate.

4.5 Where the Client processes personal data of its employees via the platform – in particular sign-in, usage and session data as well as evaluations of the consultations they conduct – the Client shall ensure that a legal basis exists for this and that any participation rights of an employee representative body are observed. The Contractor shall provide the Client, on request, with the information it needs for this purpose.

5. Personnel Requirements

The Contractor shall bind all persons who process Client Data to confidentiality.

The Contractor ensures that the persons involved in operating the AI-supported functions have the AI literacy required under Article 4 of Regulation (EU) 2024/1689.

6. Security of Processing

6.1 The Contractor will take the necessary and appropriate technical and organizational measures in accordance with Article 32 of the GDPR, to ensure a level of protection for Client Data appropriate to the risk. This takes into account the state of technology, the implementation costs and the nature, scope, circumstances and purposes of the processing of Client Data, as well as the varying likelihood and severity of the risk to the rights and freedoms of the data subjects. The measures taken are described in **Annex 2**. Annex 2 forms part of this Agreement. Because it describes security measures in detail, it is not published; it is made available at any time – including before the contract is concluded – on request to info@bridge-systems.com in its current version.

6.2 The Contractor is permitted to change or adapt technical and organizational measures during the term of the contract as long as the level of protection described in Annex 2 is not thereby reduced. The Contractor updates Annex 2 accordingly and makes it available to the Client in its current version on request.

6.3 Client Data is transmitted between the users' devices and the publicly reachable endpoints of the platform exclusively over transport-encrypted connections. A minimum standard of TLS 1.2 is enforced; TLS 1.3 is supported. The exclusive use of encrypted connections is declared to the browser in binding form (HTTP Strict Transport Security). The Contractor will evidence the protocol versions in use on request.

6.4 For the connection between the application and the database, a distinction must be drawn according to the mode of operation. Where the application and the database run on the same server, the database traffic does not leave that server; transport encryption of this connection is therefore not necessary and does not take place. Where the database is operated as a separate service, the connection is transport-encrypted using TLS 1.2.

7. Engagement of Sub-Processors

7.1 The Client hereby grants the Contractor general authorisation to engage sub-processors with regard to the processing of Client Data. The sub-processors engaged at the time of entering into the contract are listed in Annex 1. Contractual agreements with service providers whose subject matter is the testing or maintenance of data processing procedures or systems, or other ancillary services, are not subject to approval provided that the processing of Client Data is not the subject matter of the service and access merely cannot be ruled out. This requires that the Contractor binds such service providers to confidentiality and to the Contractor's instructions, contractually excludes any processing of Client Data for their own purposes, and makes appropriate arrangements to protect the confidentiality of Client Data. The Contractor will name these service providers to the Client on request.

7.2 The Contractor agrees to inform the Client about any intended changes with regard to the engagement or replacement of sub-processors. In individual cases, the Client has the right to object to the engagement of a potential sub-processor. An objection may only be raised by the Client for just cause, which must be proven to the Contractor. If the Client does not raise an objection within 14 days of receipt of the notification, the right to object with regard to the corresponding

commissioning expires. If the Client raises an objection, the Contractor is entitled to terminate the Main Contract and this Contract with a notice period of 3 months.

7.3 The agreement between the Contractor and any sub-processor must impose on the sub-processor the same obligations as are incumbent on the Contractor under this Agreement. The parties agree that this requirement is met if the contract has a level of protection corresponding to this contract, or if the obligations set out in Article 28(3) of the GDPR are placed on the sub-processor.

7.4 Subject to compliance with the requirements of Section 2.4 of this Agreement, the stipulations in this clause 7 shall also apply where a sub-processor established in a third country is engaged. The Client authorizes and instructs the Contractor to conclude, in its own name as data exporter, a contract with any such sub-processor incorporating the Standard Contractual Clauses pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, Module Three (transfer processor to processor), as amended from time to time. The Client agrees to cooperate to the extent necessary in fulfilling the requirements pursuant to Art. 46 GDPR.

8. Rights of Data Subjects

8.1 The Contractor will support the Client with technical and organizational measures within the scope of what is reasonable, so the Client can meet their obligation to respond to requests for the protection of the legal rights of Data Subjects to which they are entitled. The Contractor answers the Client's requests under this clause within ten working days of receipt.

8.2 If a Data Subject submits a request to exercise the rights to which it is entitled directly to the Contractor, the Contractor shall forward this request to the Client in a timely manner.

8.3 The Contractor will provide the Client with information about stored Client Data, the recipients of Client Data to whom the Contractor passes it on according to the Contract, as well as the purpose of the storage, unless the Client is in possession of this information already, or is able to procure it.

8.4 The Contractor shall enable the Client, to the extent reasonable and necessary, to rectify or erase Client Data or to restrict its further processing, or shall at the

Client's request carry out the rectification, erasure or restriction of further processing itself, if and to the extent this is impossible for the Client itself.

8.5 If the Data Subject has a right to data portability with respect to the Client Data pursuant to Art. 20 GDPR, the Contractor will support the Client within the scope of what is reasonable and necessary in providing that Client Data in a common and machine-readable format, if the Client is unable to procure the data otherwise.

9. Contractor Obligations to Provide Notification and Support

9.1 If the Client has a legal obligation to report or notify a breach of protection of Client data (in particular pursuant to Art. 33, 34 GDPR), the Contractor is obliged to inform the Client without undue delay, and at the latest within 24 hours of becoming aware of it, about any reportable occurrences in the Contractor's scope of responsibility. The notification contains the information set out in Article 33(3) GDPR to the extent available to the Contractor at that time; the Contractor supplies any missing information without undue delay. The Contractor will support the Client in fulfilling the reporting and notification obligations at the Client's request and within the scope of what is reasonable and necessary.

9.2 The Contractor agrees to support the Client, to the extent reasonable and necessary, in connection with any data protection impact assessments to be carried out by the Client and any subsequent consultations with the supervisory authorities pursuant to Art. 35, 36 GDPR.

Support under Sections 8.4, 8.5, 9.1 and 9.2 is provided irrespective of any cost arrangement. Where the effort goes beyond what the Contractor owes under Art. 28(3)(e) and (f) GDPR, taking into account the nature of the processing and the information available to it, the Contractor may claim reimbursement of the demonstrated additional effort; it may not make the support itself conditional on this.

10. Deletion of Data

10.1 The Contractor agrees to delete the Client Data after termination of this Agreement, unless the Contractor is required by law to continue storing the Client Data. Deletion takes place after expiry of the retrieval period governed by the Main Contract (Section 8.3 of the Main Contract); until then the Contractor retains the Client Data exclusively for the purpose of retrieval and porting by the Client and processes it for no other purpose. The deletion also covers existing copies; Client Data contained in backups is deleted as the respective backup cycle expires. For individual categories of data, in particular conversation transcripts, deletion is not effected by an automatic run but by a separately triggered operation, which the Contractor initiates after termination of this Agreement.

10.2 Prior to deletion, the Contractor returns the Client Data, at the Client's choice, in a commonly used, structured and machine-readable format. The Client may exercise this choice until expiry of the retrieval period under Section 8.3 of the Main Contract; deletion does not take place before that period expires. The return of the exportable Client Data is free of charge; in all other respects Section 8.4 of the Main Contract applies.

10.3 Where the Client, on termination, chooses continued retention of the Client Data or a later deletion (Section 8.5 of the Main Contract), the provisions of this Agreement continue to apply for the duration of that retention; Section 12.1 does not preclude this. The Client may request deletion at any time.

10.4 Documentation serving as evidence of the proper processing of Client Data in accordance with the Contract may be retained by the Contractor even after the Contract has ended.

11. Proof of Verification

11.1 The Contractor agrees to provide the Client, at the Client's request, with all information required and available to the Contractor, in order to prove compliance with its obligations under this Agreement.

11.2 The Client is entitled to check the Contractor with regard to compliance with the terms of this Agreement, in particular the implementation of the technical and organizational measures; this includes conducting inspections.

11.3 In order to carry out inspections in accordance with clause 11.2, the Client is entitled to enter the Contractor's business premises from which Client Data is accessed (Dresden location, Annex 2 Part B), during normal business hours (Monday to Friday from 10 a.m. to 6 p.m.), after giving prior notice in accordance with clause 11.5, at its own expense, without disrupting the course of business and subject to strict confidentiality regarding the Contractor's trade and business secrets. The data centres of the hosting providers named in Annex 1 are accessible to neither the Contractor nor the Client; to that extent, evidence is provided under clause 11.7 through those providers' certifications and attestations.

11.4 The Contractor is entitled not to disclose information to the extent that statutory or contractual confidentiality obligations or overriding legitimate interests of third parties preclude disclosure; this concerns sensitive information with regard to the Contractor's business, and information whose disclosure would cause the Contractor to violate legal or other contractual regulations. The Client is not entitled to have access to data or information relating to other Contractor's clients. Clients also do not have access to information relating to costs, to quality review and contract management reports and to any other confidential Contractor data which is not directly relevant to the agreed upon inspection purposes.

11.5 The Client is required to inform the Contractor in advance (as a rule at least two weeks in advance) about all matters related to the inspection. The Client may perform one inspection per calendar year. Additional inspections are carried out against reimbursement of costs and after coordinating with the Contractor. Inspections for a specific cause, in particular following a breach of the protection of Client Data or where there is reasonable suspicion of such a breach, are exempt from the limit of one inspection per calendar year.

11.6 If the Client commissions a third party to perform the inspection, the Client is required to commit the third party in writing just as the Client is committed to the Contractor on the basis of this Clause 11 of this Agreement. The Client must also commit the third party to confidentiality, unless the third party is already bound by a professional confidentiality agreement. Should the Contractor request to see or

have copies of the Agreements, the Client is required to submit them to the Contractor without undue delay. The Contractor may reject an auditor designated by the Client for good cause, in particular where that auditor is in direct competition with the Contractor for the same services. The Contractor notifies the rejection within ten working days of the designation, stating the reason; the Client then designates another auditor.

11.7 Evidence of compliance with the obligations under this Agreement may also be provided by submitting a suitable, up-to-date attestation or report from an independent body (e.g., an external auditor, internal audit, the data protection officer, the IT security department, data protection auditors or quality auditors) or a suitable certification by IT security or data protection audit – e.g., in accordance with BSI-Grundschutz – ("audit report"), if the audit report allows the Client to verify compliance with the contractual obligations. The Client's right to an inspection under Section 11.2 remains in place to the extent that an audit report submitted does not answer the Client's specific question or that a specific cause within the meaning of Section 11.5 exists.

12. Duration and Termination of Contract

12.1 The duration and termination of this Agreement are governed by the terms and conditions pertaining to the duration and termination of the Main Contract. Termination of the Main Contract automatically results in termination of this Contract. An isolated termination of this contract is excluded.

13. Liability

13.1 The exclusions and limitations of liability under the Main Contract apply to the liability of the Contractor under this Contract; the statutory apportionment between the parties under Art. 82(5) GDPR remains unaffected. If third parties assert claims against the Contractor arising from a culpable breach by the Client of this Agreement or of one of the Client's obligations as controller under data protection law, the Client shall indemnify the Contractor against such claims to the extent that the Client is responsible for the breach. The Contractor notifies the Client of such a claim without undue delay, leaves the defence to it and makes no admission and no settlement without its consent.

13.2 Where a party pays damages under Art. 82 GDPR, it may claim from the other party the share attributable to that party's responsibility in accordance with Art. 82(5) GDPR. Where a fine is imposed on a party, that party bears it itself; it is not reimbursed by the other party. Compensation for other damage caused to a party by a culpable breach of this Agreement by the other party remains unaffected.

14. Final Clauses

14.1 Should individual clauses of this contract be or become ineffective, or should this contract contain a gap (an unregulated matter), the remaining clauses shall remain unaffected. The parties undertake to replace the invalid clause with a legally permissible clause that comes as close as possible to the intent of the invalid clause, and meets the requirements of Article 28 of the GDPR.

14.2 In the event of contradictions between this Agreement and other agreements between the Parties, in particular the Main Contract, the provisions of this Agreement take precedence. This does not apply to the provisions of the Main Contract on switching to another provider and on the retrieval period (Section 8.3 of the Main Contract); those take precedence over the deletion provisions of this Agreement. Nor does it apply to a data processing agreement individually agreed between the parties and signed by both parties; such an agreement takes precedence over this Agreement.

14.3 This Agreement is made available in German and in English. The German version prevails; the English version is provided for information.

Annex 1: Sub-Processors

For the processing of data on behalf of the Client, the Contractor makes use of services of third parties which process data on its behalf ("Sub-Processors"). These are the following companies; Section 7.1, third sentence, of this Agreement applies in addition.

dotSource SE – provision and operation of the cloud infrastructure (Microsoft Azure)

Address: Goethestraße 1, 07743 Jena, Germany

Role: Cloud Solution Provider; the Microsoft Azure services named below are procured and administered through dotSource SE.

Purpose of Processing:

1. Operation and hosting of the application, the database and the file storage of the platform via the services Microsoft Azure Kubernetes Service, Azure Database for MySQL Flexible Server and Azure File Storage, including data backup.
2. Technical monitoring and error analysis of the application via Azure Application Insights / Azure Monitor, including safeguarding operations, capacity and billing determination and the detection of security incidents.

Categories of Processed Data:

- re 1.: all Client Data processed in the platform (master, consultation, financial, health, appointment and document data as well as recordings and transcripts)
- re 2.: technical telemetry data on calls, run times, dependencies and errors of the application; depending on the configuration of the monitoring service, this may also include the address called, the IP address of the accessing device and messages from the application log

Location of Data Processing:

Microsoft data centers in the "Germany West Central" region (Germany).

Sub-Processor:

Microsoft (Microsoft Azure)

Role: Operation of the cloud infrastructure and of the Azure services named above

Location of data processing: Microsoft data centers in the "Germany West Central" region (Germany)

Legal basis: Microsoft Products and Services Data Protection Addendum (DPA) pursuant to Art. 28 GDPR

Contractual Basis:

- Data processing agreement pursuant to Art. 28 GDPR with dotSource SE
- Microsoft Products and Services Data Protection Addendum (DPA) pursuant to Art. 28 GDPR

Mistral AI SAS – AI-supported summarization of consultations

Address: 15 rue des Halles, 75001 Paris, France

Website: <https://mistral.ai>

Purpose of Processing:

Creation of an automated summary of the course of the conversation from the transcript text of a consultation by means of an AI model.

Categories of Processed Data:

- transcript text of the consultation. Names of the conversation participants and of the person being advised are replaced by role designations in the speaker attribution and, where they are detected automatically, within the conversation text; the mapping remains with the Contractor. The transcript text may nevertheless contain personal data, including special categories under Article 9 GDPR.
- the instruction (prompt) used to generate the summary

Location of Data Processing:

Processing in data centers within the European Union in accordance with the data processing agreement concluded with the provider; the provider is domiciled in the European Union.

Specific Arrangements:

Under the data processing agreement concluded with the provider and the agreed terms of use, any use of the transmitted content for training AI models is excluded, as is storage of the transmitted content by the provider (Zero Data Retention).

Contractual Basis:

Data Processing Addendum (DPA) of Mistral AI pursuant to Art. 28 GDPR: <https://legal.mistral.ai/terms/data-processing-addendum>

Daily.co, Inc. – video conferencing, recording and speech-recognition service

Address: 340 S Lemon Ave #4133, Walnut, CA 91789, USA

Website: <https://www.daily.co>

Purpose of Processing:

Provision and operation of video conferencing infrastructure (signaling, media routing, real-time communication), production of audio recordings of the conversation, and speech recognition for the creation of conversation transcripts and live captions.

Categories of Processed Data:

- video, audio and, where applicable, screen sharing data
- IP addresses and device information of participants
- session and connection metadata (e.g., duration, room ID)
- transcript text generated from the conversation audio

Location of Data Processing:

The conference rooms are set to a processing region within the European Union (default: AWS region "eu-central-1"); speech recognition is set to the processing region "EU". Audio recordings are buffered until retrieval by the platform in storage within the European Union which the Contractor itself provides and controls; they are not placed on servers of Daily.co, Inc. Daily.co, Inc. is domiciled in the USA; access from the third country is accordingly not excluded.

Sub-Processors:

Amazon Web Services EMEA SARL

Address: 38 Avenue John F. Kennedy, L-1855 Luxembourg

Role: Infrastructure and cloud service provider (hosting, network, storage)

Location of data processing: Data centers within the EU

Legal basis: Processing under Art. 28 GDPR

Deepgram, Inc.

Address: 548 Market St, Suite 25104, San Francisco, CA 94104-5401, USA

Role: Speech recognition on behalf of Daily.co, Inc.; the selection and engagement is carried out by Daily.co, Inc.

Location of data processing: European processing endpoint in accordance with the configured processing region "EU"

Legal basis: Processing under Art. 28 GDPR in relation to Daily.co, Inc.; the safeguarding of any transfers to the United States is in this respect the responsibility of Daily.co, Inc.

Daily.co, Inc. engages further sub-processors for the operation of its service, among others for network traversal, logging and error monitoring. Error monitoring is carried out in part by a program library loaded into the participants' browsers, which transmits technical error, diagnostic and application-trace data including the IP address to the Sentry service of Functional Software, Inc., USA. Daily.co, Inc. publishes the current, complete list at <https://www.daily.co/legal/sub-processors/> (reviewed as of 1 September 2026); it forms part of the agreement concluded with Daily.co, Inc.

Contractual Basis:

- Data Processing Addendum (DPA) by Daily: <https://www.daily.co/legal/data-processing-addendum>
- AWS Data Processing Addendum: <https://aws.amazon.com/compliance/gdpr-center/>
- EU Standard Contractual Clauses together with a transfer impact assessment for the transfer to Daily.co, Inc.
- Safeguarding the transfer to Functional Software, Inc. is the responsibility of Daily.co, Inc. as the entity commissioning it; according to Daily.co, Inc. it is likewise based on the EU Standard Contractual Clauses.

Amazon Web Services EMEA SARL – Buffer Storage for Audio Recordings

Address: 38 Avenue John F. Kennedy, L-1855 Luxembourg

Website: <https://aws.amazon.com>

Purpose of Processing:

Provision of the object storage in which the audio recordings produced by the conferencing technology are buffered until the platform retrieves them. The storage is operated and controlled by the Contractor; Daily.co, Inc. writes the recording directly into it. Once the platform has retrieved it, the buffered file is deleted. This entry concerns only that storage operated by the Contractor; the role of Amazon Web Services EMEA SARL as a sub-processor of Daily.co, Inc. is set out separately there.

Types of Data Processed:

- audio recording of the consultation including the conversation content it contains
- technical identifiers of the session and of the recording

Place of Data Processing:

Data centres within the European Union.

Contractual Basis:

AWS Data Processing Addendum pursuant to Article 28 GDPR:
<https://aws.amazon.com/compliance/gdpr-center/>

1&1 IONOS SE – hosting provider for separately agreed installations

Address: Elgendorfer Straße 57, 56410 Montabaur, Germany

Purpose of Processing:

Where separately agreed for a contractual relationship: operation and hosting of the application and database servers of individual installations, including system administration and data backup. The platform operated on the Microsoft Azure cloud infrastructure is **not** hosted with 1&1 IONOS SE. The Contractor's marketing

website is likewise operated with 1&1 IONOS SE; it processes no Client Data and is not the subject of this Annex.

Categories of Processed Data:

- all Client Data processed on the installation concerned (master, consultation, financial, health, appointment and document data as well as recordings and transcripts)
- technical log data of server operation arising at the hosting provider in the course of system administration and its standard monitoring; no additional application monitoring is integrated on these installations

Location of Data Processing:

Data centers of 1&1 IONOS SE in Germany. No transfer of personal data to third countries outside the EU.

Contractual Basis:

Data processing agreement pursuant to Art. 28 GDPR with 1&1 IONOS SE.

fino digital GmbH – account information service (retrieval and evaluation of bank account data)

Address: Universitätsplatz 12, 34127 Kassel, Germany

Purpose of Processing:

Provision of an account information service through which the person advised may voluntarily have their bank accounts read out, and creation of a structured evaluation and a summarizing PDF document for use in the financial analysis.

Categories of Processed Data:

- name of the person advised, name of the consultant as well as technical identifiers of the consultant and the person advised
- the account information released by the person advised at their bank
- transmitted back to the platform: income and pension details, aggregated expenditure, a list of the insurance and retirement-provision contracts identified, and a PDF document

Location of Data Processing:

Data centers within the European Union.

Contractual Basis:

Data processing agreement pursuant to Art. 28 GDPR.

Brevo GmbH – dispatch of emails

Address: Köpenicker Straße 126, 10179 Berlin, Germany

Register court: Amtsgericht Charlottenburg, HRB 133191

Parent company: Sendinblue SAS, 17 rue de Salneuve, 75017 Paris, France

Purpose of Processing:

Technical dispatch of all emails generated by the platform, in particular invitations to consultation appointments, appointment confirmations and reminders, dispatch of consultation documents and evaluations, requests for an electronic signature, and system and account notifications.

Categories of Processed Data:

- email address and name of the recipient
- subject and content of the message, including the personal data contained therein
- file attachments, such as consultation documents or evaluations
- dispatch and delivery metadata

Location of Data Processing:

Processing within the European Union in accordance with the data processing agreement concluded with the provider.

Contractual Basis:

Data processing agreement pursuant to Art. 28 GDPR.

seven communications GmbH & Co. KG – dispatch of SMS messages

Address: Willestraße 4–6, 24103 Kiel, Germany

Register court: Amtsgericht Kiel, HRA 11707 KI

Purpose of Processing:

Dispatch of all SMS messages generated by the platform, in particular invitations to online consultations, appointment reminders and requests for an electronic

signature. Used only where SMS dispatch is enabled for the respective installation and activated for the account.

Categories of Processed Data:

- mobile number of the recipient
- message text, which may contain the names of the person advised and of the consultant as well as the date, time and access link of the appointment

Location of Data Processing:

Data centers within the European Union.

Contractual Basis:

Data processing agreement pursuant to Art. 28 GDPR.

VorFina GmbH – service provider for financial analysis reports according to DIN 77230

Address: Aidenbachstraße 30, 81379 Munich, Germany

Purpose of Processing:

Preparation of financial analyses and reports in accordance with DIN 77230 on the basis of the data recorded by the Client. Used only where the function is enabled for the respective installation.

Categories of Processed Data:

- first and last name as well as date of birth of the person advised and of the further persons included in the analysis
- the complete household and financial data set according to DIN 77230 (income, expenditure, liquidity, assets, liabilities, insurance cover, goals, life situation)
- special categories of personal data pursuant to Art. 9 GDPR: details of health insurance status (type of health insurance, including any entitlement to civil-service healthcare assistance or free medical care, and the premium) and of existing supplementary cover (inpatient, outpatient, dental prosthetics, foreign travel, daily sickness allowance) of the person advised and of the further persons included in the analysis
- transmitted back to the platform: the report produced, as a PDF document

Location of Data Processing:

Processing of personal data within Germany. No transfer of personal data to third countries outside the EU.

Contractual Basis:

- Cooperation agreement for the preparation of financial analyses according to DIN 77230 (November 2020)
- Data processing agreement pursuant to Art. 28 GDPR with VorFina GmbH.

Recipients and components not listed as Sub-Processors

For the avoidance of doubt as to the scope of this Annex:

Systems of the Client and recipients selected by it. Where the Client sets up an interface for its account or for an installation operated for it, to a system of its own or to a system selected by it – for example to a broker management program, a comparison calculator, a document archive, a recording archive for the fulfilment of regulatory retention obligations, a signature service or a callback address determined by it (webhook) – the Contractor transmits the data concerned to that recipient on the Client's instruction. In this respect the Contractor is not the principal of that recipient; this constitutes a transmission to the Client itself or to a third party determined by it. The Client is responsible for the selection of these recipients, for the legal basis of the transmission and for the processing carried out there. The same applies to the linking of a user account with an account of the Client at a sign-in or calendar service (in particular Google and Microsoft) as well as to specialist applications which the Client uses with its own access credentials. The same further applies to a sign-in service operated or commissioned by the Client and to its identity management, where the Client handles sign-in to the platform, the adoption of role and group memberships or automated user provisioning (SCIM) through it; the Contractor receives the details concerned but does not commission those systems. Where an installation is operated for a group of Clients – for example for a broker pool – the sign-in service may be operated by the operator of that group rather than by the individual Client; in that case the Contractor is registered with the sign-in service as the requesting party. Here too the Contractor does not commission the sign-in service but merely receives the sign-in and profile details transmitted by the group operator; the group operator is

responsible towards the Client for the use of that sign-in service and for the legal basis of the transmission. The same applies to interfaces which the Contractor provides server-side for all installations but whose use is triggered by the consultant in the individual case, and whose recipient stands in its own brokerage or agency relationship with the Client to which the Client holds its own access – in particular the pre-population of an insurer's application or tariff calculator, in which master, contact and bank account data of the person advised are transmitted to the insurer. In this respect the Contractor merely conveys the data to the access the Client already uses.

The Contractor's own processing activities. Processing activities for which the Contractor is itself the controller – in particular the administration of contract-partner and billing data including the engagement of payment service providers, the creation and continued existence of the user account as a means of access (sign-in data, account status, security logs), and the information and support of the users registered with it (onboarding, newsletter) – do not concern Client Data and are not the subject of this Annex. The Contractor provides information about these in its own privacy notice. This does not cover the selection, content and scope of the employee data transmitted by the Client or the assignment of roles and groups within its account; the Client is the controller for these, and the Contractor implements them as a processor in accordance with this contract. Section 2.2 accordingly lists the Client's employees and agents as a category of data subjects of the processing on behalf.

Embedded video content. Where the Client uses a slide of the online video type in a consultation guide and playback is started, the player of the respective provider – Google Ireland Limited or Google LLC for YouTube, or Vimeo.com, Inc. for Vimeo – is loaded into the browsers of all participants. Their devices thereby transmit the IP address and browser and device details directly to the provider, including to the United States; no transmission of these details is made by the Contractor. The Client decides whether to use a video slide and which video is embedded; the technical form of integration is prescribed by the platform. The Contractor does not engage these providers; they are not sub-processors. The Client is responsible for the legal basis of this transmission. Details are described in the Contractor's privacy notice.

Testing and maintenance service providers. Contractual relationships with service providers whose subject matter is the testing or maintenance of data processing procedures or systems, or other ancillary services, are not subject to approval under Section 7.1, third sentence, and are not set out separately in this Annex, even where access to Client Data cannot be ruled out in the process. The Contractor makes appropriate arrangements to protect confidentiality in this respect and will name these service providers to the Client on request.

Components operated by the Contractor itself. Components which the Contractor operates itself on the infrastructure named in this Annex are not separate Sub-Processors. This concerns in particular the signature server, the protection against automated access, the service for checking uploaded files for malware, and the service for generating preview images; the latter is provided exclusively with synthetic sample data instead of real customer data; the only data transmitted are the name of the user triggering the preview and the design settings of the account. Where a third party's scanning service is used to check uploaded files for malware, that service will be listed separately in this Annex.