Brainloop Additional Terms:

The following additional product terms apply (and supersede any terms in the Agreement which cover the same topic to the extent there is a conflict) when the Client purchases access to the Diligent Service identified as **Brainloop Secure Data Room Service (BDRS), MeetingSuite or MeetingSuite$^{\text{CONNECT}}$** (and any references to "Diligent Service" on this page shall be understood to refer only to such Diligent Service). For the avoidance of doubt, the aforementioned Diligent Services will be provided by the Brainloop entity mentioned on the respective Order Form and any mention of "Diligent" in this context shall mean that respective Brainloop entity.

1) <u>Export and Deletion</u>

a) During the Term of the Agreement

During the Term of the Agreement, Client may at any time and in accordance with the applicable Documentation and subject to the technical limitations of the functionalities of the subscribed to Diligent Service:

- export any Client Data stored in the respective Diligent Service on behalf of Client in a standard format defined by Diligent (as further set out in the applicable Documentation), without additional fees; and/or
- request the deletion of the Client Data stored in the respective Diligent Service on behalf of Client, which will then be deleted and/or anonymised in accordance with Diligent's general standard deletion practices.

In the event that Diligent suspends Client's access to the ordered Diligent Service in accordance with Section 6.1 of the Agreement, Client may request Diligent 's assistance, subject to additional fees, in exporting the Client Data stored in the Diligent Service in a standard format defined by Diligent in accordance with the applicable Documentation.

b) Upon termination of the Agreement

Upon termination of this Agreement, Client's access to the Diligent Service and to the Client Data stored in the Diligent Service on behalf of Client ends. For a period of four (4) weeks from the end of the Agreement (the **"Retrieval Period"**), Client will be able to export the Client Data stored in the Diligent Service on behalf of Client in a standard format defined by Diligent (as further described in the applicable Documentation) without additional fees.

After the expiration of the Retrieval Period, Client Data will no longer be available for export. The Client Data will be deleted or anonymised by Diligent according to Diligent's standard deletion procedures as follows:

- seventy-two (72) days after the end of the Retrieval Period for Brainloop Secure Dataroom Service (BDRS); and
- thirty-eight (38) days after the end of the Retrieval Period for MeetingSuite / MeetingSuite$^{\text{CONNECT}}$.

In case of a use of the Diligent Service MeetingSuite$^{\text{CONNECT}}$, the Client Data may – depending on the selected setting and use by Client – be stored in the Diligent Service MeetingSuite$^{\text{CONNECT}}$ and/or – as provided on the basis of a separate license – the Brainloop Secure Dataroom Service (BDRS). For the avoidance of doubt in such event the corresponding product-specific deletion routines and periods listed above as applicable to the respective Diligent Service will apply.

After termination of the Agreement, and to the extent that this Agreement does not otherwise provide for provisions on the deletion of Client Data, Diligent will notify Client of the deletion date for Client Data held by Diligent.

2) Data Protection

The Parties agree that to the extent Diligent, in the context of providing on of the abovementioned Diligent Services, processes personal data on behalf of Client which is entered into or submitted to the Diligent Service by Users as Client Data ("**Client Personal Data**"), Diligent shall be engaged as processor (Auftragsverarbeiter). For this purpose, Diligent and Client agree to conclude a data processing agreement according to Art. 28 GDPR, as attached to these Brainloop Additional Terms and the terms of such data processing agreement are hereby incorporated into the Agreement by reference. Client may separately elect to execute such data processing agreement provided that Client returns a copy of such executed data processing agreement to dataprotection@brainloop.com. . In this respect, Client acts as controller and is responsible for the lawfulness of the processing of Client Personal Data in the context of using the Diligent Service. Each Party undertakes to comply with all Data Protection Law applicable to such Party and shall not knowingly cause the other to breach valid Data Protection Law.

The contractually agreed upon Diligent Service and the related storage and processing of Client Data hosted by Diligent in the respective Diligent Service on behalf of Client shall be carried out exclusively in a member state of the European Union (**"EU"**) or in a contracting state to the agreement on the European Economic Area (**"EEA"**). Any relocation of the Diligent Service or of parts thereof to a third country outside the EU or the EEA requires Client's prior consent.

*   *   *

DATA PROCESSING AGREEMENT

between

each Brainloop Group Entity which is party to an Agreement (as defined below) with Client (each hereinafter referred to as "**Brainloop**")

and

the "**Client**" as identified on the signature page of this DPA or as otherwise identified in an executed Agreement that explicitly incorporates this DPA; and

each a "**party**", together the "**parties**"

PREAMBLE

Brainloop and the Client have entered into a user agreement on the provision of Brainloop Services by Brainloop to the Client ("**Agreement**"). This Data Processing Agreement, including its Attachments, ("**DPA**") stipulates the rights and obligations of the parties to the extent Brainloop, in the context of providing the agreed Brainloop Services under the Agreement, processes any DPA Personal Data (as defined below) on behalf of the Client. This DPA replaces and supersedes any existing prior agreements between the parties with respect to the processing of Personal Data on behalf of the Client in relation to the Brainloop Services ordered pursuant to the Agreement.

For the purposes of this DPA, "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**process**" and "**processing**", "**Processor**" and "**Supervisory Authority**" (including variations thereof) shall have the meaning as defined in the respective current version of the and Regulation (EU) 2016/679 (General Data Protection Regulation – "**GDPR**") and the Swiss Federal Data Protection Act ("**DSG**") (as applicable).

"**Applicable Data Protection Law**" means as applicable, the GDPR, the DSG and any national data protection laws of the EU Member States.

"**Client Personal Data**" means any Personal Data entered into or submitted to the Brainloop Services by Users as Client Data in accordance with the Agreement.

"**DPA Personal Data**" means any Client Personal Data, User Data and Support Data processed by Brainloop on behalf of Client under this DPA.

"**EU**" and "**EEA**" shall have the meaning as defined in Section II(5).

"**Support Data**" means any Personal Data provided to Brainloop, or collected by Brainloop through the Brainloop Services on behalf of the Client, in the context of a support matter request of Client, as further specified in **Attachment 1**. Support Data will not include any Client Personal Data, except if expressly provided to Brainloop by or on behalf of Client in the context of the support matter request or if Brainloop is expressly authorized by or on behalf of Client to obtain access to such data through the Brainloop Services in the context of handling the support matter.

"**User Account Data**" means account information relating to Users of the Brainloop Services (as further specified in **Attachment 1**) which is processed by Brainloop in the role as Controller for technical and administrative account management and other legitimate business purposes. The processing of User Account Data is not subject to this DPA.

"**User Data**" means Personal Data relating to Users processed by Brainloop on behalf of Client to provide the core functional service capabilities of the Brainloop Services. User Data may include the following data categories: service profile data, service usage data and diagnostic and maintenance data, as further specified in **Attachment 1**. For the avoidance of doubt, for purposes of this DPA, the term User Data does not include User Account Data.

For clarity, in cases described under Section I.3(b) below, the definition of 'Brainloop' shall also include Brainloop AG.

Any capitalized terms used in this DPA which are not defined in this DPA shall have the meaning set forth in the Agreement.

I. SUBJECT MATTER OF THE DPA

(1) To the extent Brainloop, in the context of providing the Brainloop Services under the Agreement, processes DPA Personal Data on behalf of the Client (as specified in **Attachment 1** of this DPA), the provisions of this DPA shall apply. To that extent, the Client shall be the Controller and Brainloop shall be the Processor in relation to any such DPA Personal Data processed under this DPA.

(2) For the avoidance of doubt, this DPA does not apply to any Personal Data received by Brainloop in the context of the business relationship with the Client which is not processed as part of providing the core functional service capabilities of the Brainloop Services and which is required by Brainloop, acting in its role as a Controller, for administrative purposes, customer account management, billing purposes or other legitimate business purposes in connection with the performance of the Agreement.

(3) For further clarification and notwithstanding anything to the contrary herein:

(a) If Brainloop AG is the Client's contractual partner, then only Brainloop AG is the autonomous and independent controller in the aforementioned context.

(b) If either Brainloop Austria GmbH or Brainloop Switzerland AG is the Client's contractual partner, then Brainloop AG will act as a joint controller with the Brainloop affiliate which is Client’s contractual partner.

Any related provisions herein shall therefore be interpreted and read accordingly.

(4) The subject matter, nature and purpose of the processing of DPA Personal Data by Brainloop as well as the type of DPA Personal Data and categories of Data Subjects concerned are described in **Attachment 1** of this DPA.

II. Obligations of Brainloop

Brainloop has the following obligations:

(1) Brainloop shall process DPA Personal Data only in accordance with this DPA and the documented instructions of the Client, and only to the extent necessary for the purposes set forth in **Attachment 1**. DPA Personal Data may be processed by Brainloop for another purpose only upon the Client's prior approval in written or electronic form, unless required to do so by applicable laws; in such a case, Brainloop shall inform the Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. In relation to User Data and Support Data solely, the Client hereby agrees, and provides respective authorization and instruction, that Brainloop may process User Data and Support Data also for their own legitimate business purposes specified in **Attachment 1**.

(2) The Client and Brainloop agree that the following person is designated as responsible data protection contacts of Client under this DPA and authorized to issue instructions:

For the Client:

Representative: Last name, first name, position (email address): As communicated separately by the Client.

For Brainloop:

Instructions should be sent to the following email address: dataprotection@brainloop.com

Any changes to the above designated data protection contacts or their corresponding contact details must be communicated to the other party without undue delay in written or electronic form.

(3) In case Brainloop is of the opinion that an instruction of the Client infringes applicable Data Protection Law, Brainloop will inform the Client without undue delay. Brainloop is entitled to suspend the execution of the instruction in question until the Client demonstrates the lawfulness of the instruction in written or electronic form or amends the instruction to comply with Applicable Data Protection Law.

(4) Brainloop shall comply with all Applicable Data Protection Law, as applicable to Brainloop.

(5) The contractually agreed Brainloop Services and the related storage and processing of DPA Personal Data hosted by Brainloop in such Brainloop Services shall be carried out exclusively in a Member State of the European Union ("**EU**"), in Switzerland or in a state that is a party to the Agreement on the European Economic Area ("**EEA**"). Any relocation of any Brainloop Service or of parts thereof to a third country outside the EU, Switzerland or the EEA requires the prior consent of the Client.

(6) Brainloop shall, to the extent legally permitted, inform the Client in case a Supervisory Authority or the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**") shall carry out control and supervision and approach Brainloop in the context of its data protection control and supervision with respect to the processing of DPA Personal Data on behalf of the Client under this DPA. The parties will reasonably support each other in case of any investigation, audit, or any other inquiry from a Supervisory Authority/the FDPIC, insofar as such measure concerns the processing by Brainloop of DPA Personal Data on behalf of the Client within the scope of this DPA.

(7) Where, under Applicable Data Protection Law, the Client is obliged to respond to a Data Subject's rights request related to the processing of the Data Subject's Personal Data by Brainloop on behalf of the Client under this DPA, Brainloop shall, to the extent the Client does not have the ability to address the Data Subject's rights request in its use of the respective Brainloop Service, assist the Client by appropriate technical and organisational measures, insofar as this is possible, in responding to the request, provided that the Client has instructed Brainloop in written or electronic form to do so. The Client shall be solely responsible for communicating directly with Data Subjects in relation to the processing of DPA Personal Data by Brainloop on behalf of the Client and Brainloop shall not respond to a corresponding request itself, unless authorised to do so by the Client. Brainloop shall inform the Client in case a Data Subject directly approaches Brainloop with a Data Subject's rights request.

(8) Brainloop shall assist the Client – within the scope of the legal obligations applicable to Brainloop under Applicable Data Protection Law, and taking into account the nature of the processing and the information available to Brainloop – in ensuring compliance with the obligations pursuant to Applicable Data Protection Law.

(9) Brainloop shall treat DPA Personal Data as strictly confidential, as required under the Agreement. Brainloop shall train all persons authorized by Brainloop to access DPA Personal Data in relation to their

obligations under Applicable Data Protection Law. Brainloop shall provide access to DPA Personal Data only to such employees of Brainloop that have committed themselves to confidentiality (or are under an appropriate statutory obligation of confidentiality) and need to know such DPA Personal Data for the performance of the Brainloop Services and/or the purposes set out in **Attachment 1**. DPA Personal Data may not be disclosed to third parties, except (i) as expressly permitted in the Agreement or this DPA, or (ii) where required by applicable law, in which case, to the extent legally permitted, Brainloop shall provide Client with prior notice of any such compelled disclosure.

(10) Brainloop shall inform the Client (via Client's data protection contact as set out in Section II(2) above) without undue delay after becoming aware of a Personal Data Breach.

III. Technical and Organisational Protection Measures

(1) Brainloop shall implement appropriate technical and organisational protection measures in accordance with the legal provisions applicable to Brainloop under Applicable Data Protection Law. Brainloop shall structure its internal organisation in a manner that ensures compliance with the requirements for the protection of DPA Personal Data and protects the DPA Personal Data against accidental or unlawful destruction or alteration, unauthorised disclosure or access, misuse and loss. The exact measures are set forth in **Attachment 2** to this DPA. Brainloop shall monitor compliance with these measures and review, assess and evaluate the effectiveness of these measures on a regular basis.

(2) Notwithstanding the provisions of Section III (1) above, Brainloop may, as part of ongoing system maintenance and development, change its technical and organisational protection measures. Brainloop shall document any material changes to the measures set forth in **Attachment 2** to this DPA and provide the Client with information on Brainloop's current security measures upon request. Brainloop shall not provide for protection measures that deliver a level of security that is materially lower than that provided at the Effective Date and, in any event, Brainloop shall at all times maintain a level of protection no lower than required under the legal provisions applicable to Brainloop under Applicable Data Protection Law.

IV. Rights and Obligations of the Client

(1) Within the scope of this DPA, the Client is solely responsible for ensuring compliance with applicable Data Protection Law, including the lawfulness of the transmission of DPA Personal Data to Brainloop and the lawfulness of the processing by Brainloop, as well as for fulfilling its obligations to respond to Data Subject's rights requests.

(2) The Client shall, without delay and in a comprehensive fashion, inform Brainloop of any defect the Client may detect in Brainloop's processing of DPA Personal Data and of any irregularities in the implementation of applicable Data Protection Law.

V. SUB-PROCESSORS OF DPA PERSONAL DATA

(1) The Client provides authorisation that Brainloop may engage the sub-processors specified in **Attachment 3** to this DPA, as applicable to the respective Brainloop Services ordered by Client under the Agreement.

(2) The Client further provides general authorisation that Brainloop may engage further sub-processors for the processing of DPA Personal Data under this DPA, subject to the provisions set out below; this also includes the engagement of any further sub-processors by the authorized sub-processors.

(3) To the extent that Brainloop intends to replace or to add further sub-processors, Brainloop shall notify the Client (via the Client's designated data protection contact set out in Section II(2)) thereof in timely manner and reasonably in advance of the replacement or addition. The replacement or addition of sub-processors shall be deemed as approved if the Client does not object within twenty-one (21) calendar days of receipt of the respective notice. The Client may object to the use of a new sub-processor provided that the Client reasonably believes that the use of such sub-processor presents an unreasonable risk to or prevents the Client from complying with applicable law. If the Client so objects, Brainloop shall either (a) not use the new sub-processor to process the DPA Personal Data, or (b) shall find an alternative way of reasonably resolving the Client's objection. If neither (a) nor (b) is reasonably feasible within twenty-one (21) calendar days of receipt of the Client's objection, then the Client shall either rescind its objection or may terminate the Agreement in relation to the respective Brainloop Services for which the new sub-processor would be used.

(4) Brainloop shall choose all sub-processors carefully, in particular taking into account the technical and organisational protection measures they have implemented, and shall, before the engagement and on a regular basis during the contractual term thereafter, verify the sub-processor's compliance with the statutory and contractual data protection provisions. Brainloop shall remain fully responsible to the Client for the performance of the sub-processor's obligations.

(5) Sub-processors shall be engaged by Brainloop on the basis of a written agreement (including in an electronic format) which shall contain provisions regarding confidentiality, data protection and data security providing for, in substance, the same level of data protection obligations as set out in this DPA.

VI. Audit Rights of the Client

(1) The Client is entitled, within the limits and as further specified below, to audit Brainloop's compliance with the technical and organisational protection measures set forth in **Attachment 2**. Brainloop shall allow for and contribute to such audits, including inspections, as set out below, and make available all information necessary for assessing Brainloop’s aforementioned compliance.

(2) The parties agree that Brainloop can demonstrate compliance with the technical and organisational measures regarding the processing of DPA Personal Data by Brainloop on behalf of the Client by providing reasonably reliable documentation, such as current certifications and/or reports (or excerpts of reports) from independent bodies (*e.g.*, external certified auditors), including, as the case may be, in accordance with ISO/IEC 27001:2017 standards, Trusted Cloud (TCDP) standards and/or alternative standards providing for demonstrable assurances of the adequacy of the technical and organizational protection measures implemented at the data processing facilities used by Brainloop to process DPA Personal Data on behalf of the Client. The Client may conduct either by itself or through a qualified third-party independent auditor selected by the Client at the Client's expense an on-site inspection of Brainloop's processing operations. The inspection shall – to the extent reasonable and acceptable considering the severity and urgency of the cause for the inspection – take place after reasonable advance notice. In case of an inspection without a particular reason, the Client shall provide Brainloop with at least sixty (60) calendar days advance notice. An inspection without a particular reason may be carried out once per year.

(3) Any on-site audits shall be carried during regular business hours and be of reasonable duration and shall not unreasonably interfere with Brainloop's day-to-day business operations. Each party shall bear its own costs in relation to such audit. If any audit requires the equivalent of more than one (1) business day of time expended by a Brainloop employee or a Brainloop subcontractor, the Client agrees to reimburse Brainloop for any additional time expended at Brainloop's then current professional service rates.

(4) In the event of an audit through a qualified third-party independent auditor, such third- party independent auditor shall be obliged to observe confidentiality provisions no less restrictive than those set forth in the Agreement to protect Brainloop's confidential information.

(5) Brainloop shall reasonably assist the Client in conducting the audit. In particular, Brainloop agrees to provide the Client with sufficient evidence and information regarding its data processing facilities, upon request in written or electronic form, with all information and documents which are reasonably required for a comprehensive audit of the data processing by Brainloop.

VII. DELETION AND RETURN OF DPA PERSONAL DATA AFTER TERMINATION

(1) Brainloop will store DPA Personal Data processed by Brainloop in its role as Processor on behalf of the Client (as further specified in **Attachment 1**) only for as long as necessary to carry out the data processing set out in the Agreement and this DPA, unless European, Swiss or EU Member State law require Brainloop to further store the DPA Personal Data.

(2) After termination of the Agreement, Brainloop shall, at the choice of the Client (as further instructed and specified in **Attachment 1**), within the technical functionalities and limitations of the agreed Brainloop

Services, (i) return to the Client all Client Personal Data and, as technically feasible, other relevant DPA Personal Data processed on behalf of the Client (as further specified in **Attachment 1**) and/or (ii) delete and/or anonymize the DPA Personal Data in accordance with Brainloop's general deletion routines and Applicable Data Protection Law (as applicable to Brainloop), unless European, Swiss or EU Member State law require Brainloop to further store the DPA Personal Data or any further storage of DPA Personal Data is expressly permitted under this DPA.

VIII. Miscellaneous

(1) The Client shall, in relation to Brainloop, retain all rights in the Client Personal Data and in all copies thereof. If Client Personal Data hosted in a Brainloop Service is endangered by third-party measures affecting Brainloop (e.g., seizure, enforcement, or confiscation), by insolvency, bankruptcy, liquidation, inheritance or settlement proceedings, by the intended or actual discontinuation of business operations, the decision to liquidate, or by other comparable events, Brainloop must inform the Client immediately, unless prohibited from doing so by court or official order. In this context, Brainloop will inform all competent authorities that the Client is the sole owner of all rights to the Client Personal Data and that the Client has sole control over the Client Personal Data.

(2) In the event of a conflict or inconsistency between the Agreement and the DPA, this DPA shall prevail.

(3) Brainloop's liability under this DPA shall be limited in accordance with the limitations on liability agreed between the parties under the Agreement. The provisions on confidentiality as agreed between the parties under the Agreement shall also cover the relationship of the parties under this DPA, including any non-public information exchanged between the parties and the terms of this DPA.

(4) This DPA begins upon the commencement of the Agreement and shall, in relation to each Brainloop Service ordered by the Client under the Agreement, be in force and effect until the Agreement has been terminated or expires in respect of such Brainloop Service. Any cancellation and termination of a Brainloop Service (to the extent possible under the respective Agreement with Brainloop) shall not affect the continued validity of this DPA for any further Brainloop Services ordered by the Client under the Agreement. Where the DPA forms the basis for several Brainloop Services ordered by the Client under multiple Agreements, the DPA shall only terminate in relation to the Brainloop Service ordered under the respective Agreement that has been terminated or expired in respect of such Brainloop Service. The right of either party to terminate this DPA for good cause (*wichtiger Grund*) shall remain unaffected. In the event that after termination or expiry of the Agreement, the processing of DPA Personal Data by Brainloop is provided for by law or necessary for the handling of termination and/or complete fulfilment of the Agreement, e.g., with respect to returning the DPA Personal Data, this DPA shall continue to apply until the Agreement has been completely fulfilled and settled.

(5) This DPA may only be amended or supplemented in writing. This also applies to any waiver of this written form requirement.

(6) Should any provision of this DPA be or become invalid in whole or in part, this shall not affect the validity of the remaining provisions of this DPA.

(7) This DPA shall be governed by the law and the place of jurisdiction of the Agreement

(8) Any obligations of Brainloop under statutory provisions or according to a judicial or regulatory decision shall remain unaffected by this DPA.

On behalf of Client:		On behalf of Brainloop AG:	
Name:	____________________	Name:	Wolfgang Wiesner
Position:	____________________	Position	Board Member
Signature:	____________________	Signature:	Signiert von: Wolfgang Wiesner 9254AB5B562F4F0...
Date:	____________________	Date:	November 18, 2024 | 2:53 AM EST

On behalf of Brainloop Austria GmbH:

Name: Wolfgang Wiesner

Position: Managing Director

Signature: Signiert von: Wolfgang Wiesner 9254AB5B562F4F0...

Date: November 18, 2024 | 2:53 AM EST

On behalf of Brainloop Switzerland AG:

Name: Wolfgang Wiesner

Position: Board Member

Signature: Signiert von: Wolfgang Wiesner 9254AB5B562F4F0...

Date: November 18, 2024 | 2:53 AM EST

Attachment 1: Details of the Processing of DPA Personal Data

I. SUBJECT-MATTER, NATURE AND PURPOSES OF THE DATA PROCESSING

This DPA shall apply to the processing of DPA Personal Data by Brainloop for purposes of providing to Client the core functional service capabilities of the Brainloop Services as ordered by the Client.

Further details of the subject-matter and nature of the data processing are specified in the respective applicable Agreement and the corresponding Specification for the respective Brainloop Services ordered by the Client.

Brainloop shall process DPA Personal Data only to the extent necessary for purposes of providing the Brainloop Services ordered by Client under the Agreement and as further instructed by the Client in its use of the Brainloop Services. This includes any processing of DPA Personal Data for purposes of technical operation and maintenance of the Brainloop Services, including diagnostics, troubleshooting, bug fixing and security, and handling of support matters.

Brainloop will not process any DPA Personal Data for any other purposes, except as expressly instructed or authorized by Client under this DPA or required by Swiss, European or EU Member State law.

In relation to User Data and Support Data solely, the Client acknowledges and agrees that Brainloop will, acting as Controller, carry out limited processing of Personal Data for Brainloop's own legitimate business purposes to the extent necessary for:

- Internal analysis, statistics and reporting;
- General technical operation and maintenance of the Brainloop Services;
- General security of the Brainloop Service, including data security and cybersecurity;
- Product research and development (including optimizing customer support); and
- The establishment, exercise and defense of Brainloop's legal claims and compliance with legal obligations and operational requirements.

To the extent any Personal Data is contained in the relevant data sets, Brainloop, will, to the extent practically technically feasible and sufficient for the related purposes, anonymize such data as early as possible and process such information in aggregated and anonymized form only (except in those cases where processing in personal identifiable form is required).

Any processing of Personal Data by Brainloop as Controller only relates to User Data and Support Data. The processing does not include any Client Personal Data entered into or submitted by the Client to the Brainloop Services (which will be processed by Brainloop solely as Processor as set out in this DPA), with the exception of any Client Personal Data which is expressly included in Support Data by or on behalf of Client in the context of a support matter initiated by Client.

In the context of providing the Brainloop Services, Brainloop may enable the Client – depending on the scope of the instruction and contractual agreement with the Client – to connect and/or otherwise use Third-Party Services, i.e., certain external third-party products, services and/or software. These Third-Party Services do not form part of the Brainloop Services and do not fall under the scope of this DPA. Any Third-Party Services are provided and operated by the respective third party service providers in their own responsibility. Client is responsible for ensuring compliance with applicable legal requirements and the lawfulness of any data processing in connection with the use of any Third-Party Services, including compliance with the requirements for any transfers of DPA Personal Data to the respective providers of the Third-Party Services and the conclusion of appropriate contracts under data protection law for the use of the Third-Party Services. Brainloop has no influence on any data processing by the respective providers of Third-Party Services (and potentially their partners), which is carried out outside of the Brainloop Services, and assumes no responsibility or liability in this regard. To the extent Client uses any Third-Party Services, Client hereby instructs Brainloop to disclose the necessary DPA Personal Data to the respective Third-Party Service on behalf of Client.

II. Categories of Data Subjects and Categories of DPA Personal Data

(1) Categories of Data Subjects

The DPA Personal Data concern the following categories of data subjects:

Client may submit DPA Personal Data to the Brainloop Services, the extent of which is determined and controlled by Client in its sole discretion. DPA Personal Data may include, but is not limited to, the following categories of Data Subjects:

- Users (as defined under the Agreement); and
- Any natural persons whose information is included by or on behalf of Client in Client Data entered into or submitted to the Brainloop Services, including, without limitation, Personal Data relating to corporate directors, officers, employees, agents, advisors, freelancers and other individuals of Client, its Affiliates, its customers, business partners or suppliers, and/or of any third parties included in Client Data.

(2) Categories of Personal Data

The DPA Personal Data concern the following categories of Personal Data:

- Any Client Personal Data contained in the Client Data entered into or submitted to the Brainloop Services by Users of the Client, the extent of which is determined and controlled by Client in its sole discretion.
- User Data, including (as applicable to the respective Brainloop Service):
  - service profile data (*e.g.*, name, title, email address, telephone number, mobile phone number, job title, company, street, postal code, city, country, signature);
  - service usage data (*e.g.*, user ID, IP-address, document ID, usage activity history; and
  - diagnostic and maintenance data (*e.g.*, log files containing service usage data and further diagnostic data, such as document size, format, protection, user device and browser software, technical malfunctions, etc.).
- Support Data, including ticket requestor identification data, requestor data relating to ticket (time/date and form of request), issue description, screenshots, and service usage data and diagnostic and maintenance data (as relevant for handling the support matter request); Support Data may include User Data.

For the avoidance of doubt, Brainloop processes User Account Data relating to Users of the Brainloop Services (including name, title, email address, telephone number, mobile phone number, job title, company, street, postal code, city, country, signature and other Personal Data) in the role as Controller for technical and administrative account management and other legitimate business purposes (such as in particular platform operation, security and general account administration, including User registration and login). Any service profile data (as set out above) processed on behalf of the Client under this DPA is derived from User Account Data. The processing of User Account Data is not subject to this DPA, and Brainloop may retain and otherwise process User Account Data (as required for their legitimate business purposes) in its role as Controller regardless of any processing or deletion of service profile data processed on behalf of the Client as part of DPA Personal Data under this DPA.

III. Return and Deletion of DPA Personal Data

(1) During the term of the Agreement, the Client may at any time, in accordance with the applicable Specification and subject to the technical limitations of the functionalities set out therein in relation to the respective Brainloop Service ordered by the Client,

(a) export any Client Personal Data and relevant User Data (limited to service profile data and relevant service usage data) stored in the Brainloop Services on behalf of the Client in a standard format defined by Brainloop (as further set out in the applicable Specification); and/or

(b) request the deletion of any Client Personal Data and User Data stored in the Brainloop Services on behalf of the Client, which will then be deleted and/or anonymized in accordance with Brainloop's standard deletion routines (subject to the provisions of this DPA and the technical limitations of the functionalities of the ordered Brainloop Service).

(2) Upon termination of the Agreement, the Client's ability to access the Brainloop Services ordered pursuant to the Agreement and the Client Personal Data and relevant User Data stored in the respective Brainloop Services on behalf of the Client ends. For a period of four (4) weeks after the end of the Agreement ("**Retrieval Period**"), the Client will still have the technical possibility of exporting the Client Personal Data and relevant User Data (limited to service profile data and relevant service usage data) stored in the respective Brainloop Services on behalf of the Client in a standard format defined by Brainloop (as further set out in the applicable Specification).

(3) The technical prerequisites and modalities of the data export provided for in Sections III(1) and III(2) of this **Attachment 1** are set out in the applicable Specification of the ordered Brainloop Service. Upon request, Brainloop will assist the Client in creating and providing the data room exports for a separate fee. The amount of the fee due for this support service is set out in the current Professional Services Portfolio Catalogue.

(4) After the end of the Retrieval Period, an export of the Client Personal Data and User Data will no longer be possible. Brainloop will delete and/or anonymize the Client Personal Data and User Data (service profile data, service usage data, and diagnostic and maintenance data) processed on behalf of the Client according to Brainloop's standard deletion routines within the following periods:

- Client Personal Data and service profile data:
  - In case of the use of the product Brainloop Secure Dataroom Service (BDRS): At the latest seventy-two (72) days after the end of the Retrieval Period
  - In case of the use of the product MeetingSuite or MeetingSuite$^{\text{CONNECT}}$: At the latest thirty-eight (38) days after the end of the Retrieval Period
- Service usage data and diagnostic and maintenance data: At the latest two-hundred-and-ten (210) days after the end of the Retrieval Period

(5) In case of a use of the Brainloop Service MeetingSuite$^{\text{CONNECT}}$, the Client Data will – depending on the selected setting and use by Client – be stored in the Brainloop Service MeetingSuite$^{\text{CONNECT}}$ and/or – as provided on the basis of a separate license – the Brainloop Secure Dataroom Service (BDRS); in this respect, the relevant corresponding product-specific deletion routines and periods listed above as applicable to the respective Brainloop Service will apply.

(6) For the avoidance of doubt, Brainloop may store and retain any User Data and Support Data processed separately by Brainloop in its role as Controller (as set out in Section I of this **Attachment 1**) in accordance with the data retention policies and deletion routines of the Brainloop group companies and in accordance with Applicable Data Protection Law, as applicable to Brainloop.

Attachment 2: Technical and organisational data protection measures

Unless specifically stated otherwise in this Attachment, the following description of the technical and organizational protection measures applies to all Brainloop Services ordered by the Client pursuant to the Agreement.

I. Confidentiality

(1) Physical access control

Measures put in place by Brainloop Austria GmbH and Brainloop Switzerland AG:

- Brainloop Austria GmbH and Brainloop Switzerland AG offices are located in a Shared Office Space. Access to the offices provided for Brainloop's use is managed by a central front desk/reception after the Shared Office Space vendor has checked the permissibility of the access.

Measures put in place by Brainloop AG (Munich):

- Access cards are required to enter the Brainloop building and premises. Only Brainloop employees receive access cards. Each card is assigned to an individual person. Card distribution is documented.
- Areas requiring special protection (e.g., HR or network rooms) can only be accessed by authorized personnel. The respective employees use their regular access card to enter these areas.
- Access for visitors is only possible after prior personal registration at the front desk/reception. Visitors are always accompanied by Brainloop staff throughout their stay.
- The loss of an access card must be reported promptly. Lost cards are blocked immediately. Therefore, entry to Brainloop premises cannot be gained with a card which has been reported lost.
- Video surveillance is in place for entry points within the premises.

Measures put in place by the hosting provider:

The data centers in which Brainloop software is hosted are ISO 27001 certified, and respective processes and standards have been implemented. Relating to physical access control, the following measures are in place:

- Access to buildings, premises, and facilities in which personal data are collected, processed, or used is restricted to authorized personnel.

- Secure access to company buildings and premises and the authentication of authorized personnel is ensured by the operator through in-person checks and suitable and effective access controls such as electronic access cards, door locking systems, and technical monitoring equipment. In addition, monitoring systems such as video and alarm systems have been installed.
- Time-restricted access permissions for visitors only grant access to authorized areas.
- Access control measures for visitors, customers, or their representatives are in place.
- The site is fenced; this provides additional protection and security.
- The fences are secured and monitored.
- Entrances, turnstiles, and access roads are guarded. Identity checks and ID cards are used at all access points in order to check access authorizations in accordance with the regulations in place for the respective facility.
- There is an emergency call center (24/7), and security personnel is on site.

(2) System access control

Brainloop ensures that staff who are authorized to use Brainloop's data processing system and carry out the respective tasks only have access to the data covered by their access authorization.

Measures put in place by Brainloop:

- Administrators can access server systems only via a password-protected, encrypted connection. Connections can only be established from the Brainloop VPN.
- Administrators each have their own personal user accounts. Access to the server systems is logged and recorded. Administrator rights are granted by Brainloop management.
- If an incorrect password is repeatedly entered, the respective user account is locked. After a predefined period of inactivity, the session is closed or the user is logged out.
- Only password hashes are stored and hash transmission is encrypted. Special hash algorithms, which are intended to provide protection against brute force attacks, are used for passwords.
- Administrative accounts such as root and DBA are personalized or are protected by privileged access mechanisms.
- Administrative activities are recorded and logged; records are stored for a minimum of 90 days.
- Virus signatures are updated automatically at regular intervals.
- Client documents are stored with encryption on Brainloop's SaaS servers.

- The Brainloop network is protected by firewalls. Access to/communication with the Brainloop SaaS servers takes places securely using transport encryption.

Measures put in place by the hosting provider:

- The unique identification of users is generally personalized.
- Authentication, i.e., verification of the provided identity, requires at least a password.
- The quality (composition, length, etc.) of the passwords and the conditions for their use (storage, transmission, etc.) comply with the current security standards.
- The validity of electronic and internal access authorizations is reviewed regularly, at least once per year.
- Clearly defined workflows are used for setting up, deleting, or changing electronic and internal access authorizations.
- Only password hashes are stored and hash transmission is encrypted. Special hash algorithms, which are intended to provide protection against brute force attacks, are used for passwords.
- Administrative accounts such as root and DBA are personalized or are protected by privileged access mechanisms.
- Administrative activities are recorded and logged; records are stored for a minimum of 90 days.

Network management

- Networks (WLANs in particular) are only set up and operated after prior approval.
- Electronic access control is established at the network and network segment level (IP address or MAC address as well as network services).
- In general, there is a separation between administrative and Client-related network segments. Access to Client-related systems takes place via a dedicated PAM & Jump-Host-Environment.
- A documented procedure is implemented for granting/changing/revoking network access authorizations.
- Access to physical network connections is only granted to authorized persons.
- Network components are securely configured according to defined business processes.
- Network components are monitored in order to ensure operational safety.

Firewall management

- A firewall is used to protect the Internet connection and, where needed, to support network separation/isolation. The following applies:
  - Firewalls are configured to observe the "everything that is not expressly allowed is forbidden" principle.
  - Firewall changes are documented, including defined processes for granting, changing, or deleting firewall rules.
  - Firewall rules are reviewed regularly.
  - Firewall logging is enabled. Firewall logs are sent to a central log management system and specific warnings are defined and evaluated regularly. Log data are stored for minimum of 90 days.
- A system to identify and prevent attacks (IDS/IPS) is being used; warnings are forwarded to the security team.

(3) Data access control

Brainloop puts measures in place to prevent unauthorized access to its data processing systems. In addition, Brainloop also takes measures to prevent the unauthorized reading, copying, or deletion of data as well as the unauthorized storage or modification of stored data.

Measures put in place by Brainloop:

- User rights for the respective Brainloop dataroom are granted by the Client. Brainloop has no access to grant access rights. In detail: The Client's Dataroom Center Administrator (DRC Admin) in BDRS or Organisation Administrator in MeetingSuite / MeetingSuite$^{\text{CONNECT}}$ can set up datarooms and then assign Dataroom Administrators. Each Dataroom Administrator configures the permissions (roles) for their datarooms based on their specific requirements and invites users to the datarooms.
- The permission system of the respective dataroom allows for access rights to be assigned for individual objects within the dataroom based on the confidentiality of the documents and the permissions of the users (groups). Users can be divided into groups and permissions can be assigned to individual users or a group of users. In addition, there are freely definable security categories (e.g., internal, confidential, strictly confidential, etc.) which can be used to determine how a document is presented to the user, i.e., whether the user can view or download a document, make changes to it, etc.

- Brainloop recommends that its Clients secure access to a Brainloop dataroom via multi-factor authentication (access can be configured by the Client accordingly at any time):
    - Personal invitation of users by the Client via email (user invitations by Brainloop are not technically feasible).
    - The Client can define the authentication factor, e.g., a PIN via text message to the user's cell phone, the use of the Brainloop Authenticator (or TOTP-compatible third-party authentication applications), or a user certificate. The cell phone number is provided by the Client (the SMS-PIN is required for registration).
    - When registering for the dataroom, it is necessary to enter a password of at least eight characters (e.g., consisting of upper and lower case letters, numbers, special characters) and, depending on the configuration, a session-based PIN which is sent to the user's cell phone after the password is entered (the cell phone number is provided by the Client). Brainloop strongly recommends its Clients to follow recognized and generally accepted good practices for authentication when configuring their datarooms. After entering an incorrect password and/or PIN three times, the login for the user is temporarily blocked; in addition, the incorrect entries are logged.
- If an incorrect password and/or PIN is repeatedly entered, the user is blocked for a predefined period of time; in addition, the incorrect entries are logged. The user is informed about this via email.
- Brainloop cannot reset passwords for technical reasons. The user can reset their password via the "Forgot password" dialog: To do so, the user must request a PIN on the Brainloop website which will be sent to their email address or cell phone number. After entering this PIN, the user can then choose a new password.
- Client documents are stored with encryption on Brainloop's SaaS servers (AES 256 bit). For the Brainloop Secure Dataroom Services (BDRS) additionally the following applies: Dataroom backups are also encrypted (AES 256 bit) and only allow for the restoration of the entire Dataroom including the existing permission system. Dataroom backups can only be decrypted through the Brainloop system.
- The Client concept of the Brainloop application logically separates the different Dataroom Centers in BDRS or Organisations in MeetingSuite / MeetingSuite^{CONNECT} from each other. Within a Dataroom Center in BDRS or Organisation in MeetingSuite / MeetingSuite^{CONNECT}, the Client can set up any number of datarooms for different purposes. The Client can grant access to the

Datarooms themselves as well as the contents of a Dataroom to certain users (e.g., employees of the Client or third parties).

- Brainloop is assigned certain roles for support and operator purposes which enable it to perform the relevant application administration tasks. Brainloop employees can only view a Client Dataroom Center in BDRS or Organisation in MeetingSuite / MeetingSuite^{CONNECT} or a Client dataroom, e.g., for consulting purposes, if invited to do so by the Client itself; invitations can be revoked at any time.
- The processor does not have access to data stored in the application by the Client. Access must be expressly granted by the Client's Dataroom Administrator or by users who have been authorized to invite additional users.
- All operations within the Dataroom are logged and are therefore traceable. This comprises:
  - Administrative activities
  - Changes to objects

  The log data itself is protected by an authorization and can only be viewed by explicitly authorized users.

Measures put in place by the hosting provider:

- The validity of the access permissions is reviewed regularly, at least once per year.
- Established work processes are used to set up, delete, or change access permissions.
- Administrative rights are granted in accordance with a formal procedure. The granting of administrative rights is kept to the necessary minimum.
- Access meets the following criteria:
  - Person- or computer-based authentication
  - Use of two-factor authentication
  - Role-based granting of access rights
  - Access logs
  - Central user administration
  - Separation of secured networks

II. Integrity

(1) Transfer control

Brainloop provides means that make it possible to verify and determine where a Data Subject's data is processed. Suitable technical and/or organizational measures are used for this purpose.

Measures put in place by Brainloop:

- TLS/SSL encryption of communication channels for all types of information (data and documents) ensures that Personal Data cannot be read, copied, modified, or removed by unauthorized persons during electronic transmission.
- Dataroom operations, i.e., uploads, downloads, access, etc., are logged in the history of the respective object in a traceable manner and can be reviewed by the Client.

Measures put in place by the hosting provider:

- Data transmission channels are encrypted.
- The basis for the implemented encryption technologies are proven and recognized standard procedures and the recommended minimum key lengths.
- In general, there is a separation between administrative and Client-related network segments.
- A boundary firewall is used to protect the Internet connection.
- An attack detection system (IDS/IPS) is being used.
- Security-relevant, system-related incidents and access to the system are logged (system log); log data is stored for a minimum of 90 days.

(2) Input control

It must be possible to verify and determine a posteriori whether and when Personal Data have been entered into data processing systems.

Measures put in place by Brainloop:

- All Dataroom operations, e.g., document creation, document download, document deletion, etc., are logged in the history of the respective object to ensure that it is possible to verify a posteriori whether and by whom Personal Data were entered, modified, or removed in data processing systems. In addition, versioning (manual or automatic) makes it possible to record changes to individual documents.
- Where required, legal and contractual requirements are taken into account when evaluating log data at the system level.

- Log data at system level is backed up as part of the regular backup procedures. Log data can only be restored via the specified revision procedure.

Measures put in place by the hosting provider:

- Security-relevant, system-related incidents and access to the system are logged (system log); log data is stored for a minimum of 90 days.
- Administrative activities are logged and the log data is stored for a minimum of 90 days.

III. Availability and load capacity

(1) Availability control

Measures put in place by Brainloop:

- The Brainloop system has been designed as a fail-safe solution, the components are designed redundantly.
- Application design:
  - Versioning allows users to store, and thus backup, preliminary documents.
  - By default, Brainloop performs a daily data backup. These backups are stored redundantly at two data centers.
  - The permission system restricts read/delete access to authorized users. A deleted document is initially moved to the "recycle bin", from where it can be restored by the Dataroom Administrator or by an appropriately authorized user of the Client.
- Brainloop uses virus scanners in certain areas of the Brainloop systems which are updated automatically on a regular basis.
- A firewall with IDS/IPS functionality is being used.
- A DDOS protection system is in place.

Measures put in place by the hosting provider:

- The operator uses data centers at different locations in an active-passive setup in order to guarantee high availability.
- Suitable measures such as system redundancy, stable power supply, diesel generators to allow for uninterrupted operation during longer power outages, air conditioning, and protection against other harmful environmental and sabotage influences are implemented in the data centers to

ensure system and data availability. The equipment is maintained regularly and tested in line with the manufacturer's specifications.

- Platform data is backed-up daily and retained for 30 days.
- In order to ensure reliable recovery in case of serious disruptions, flow definitions for continuity plans are developed and available when needed. Adopted continuity measures are tested regularly.

(2) Separation of data control

Brainloop must take appropriate measures to ensure that data which were transmitted for different purposes or to which it gains access are processed separately.

Measures put in place by Brainloop:

- Each Clients's datarooms are combined to a Client-specific Dataroom Center in BDRS and a Organisation in MeetingSuite / MeetingSuite$^{\text{CONNECT}}$.
- Only authorized users have access to this Dataroom Center in BDRS and Organisation in MeetingSuite / MeetingSuite$^{\text{CONNECT}}$ and the individual datarooms (i.e., users can only access Datarooms to which they have been invited).
- Documents are encrypted with dataroom- or document-specific keys (i.e., separation into individual Clients not only takes place at Dataroom Center level in BDRS or Organisation level in MeetingSuite / MeetingSuite$^{\text{CONNECT}}$, but also within a Client at the document level).

Measures put in place by the hosting provider:

- Systems and applications are specifically designed for purpose-built and Client-specific processing. There is a separation between production and test systems.

IV. Process for regularly testing, assessing, and evaluating

(1) Order control

The data processed and used by Brainloop may only be processed in accordance with the instructions given by the Client:

- Brainloop employees are subject to corresponding binding organizational guidelines.
- A data processing pursuant to Applicable Data Protection Law without corresponding instructions (in accordance with contract conditions) does not take place; order management is carried out on a formal basis.

- Upon request, responsibility for control of the data processing (*Auftragskontrolle*), in accordance with the provisions of this data processing agreement (DPA), may be transferred to those employees of the Client who are responsible for monitoring the fulfilment of the requirements under this DPA by Brainloop.

Brainloop has implemented an information security management system. The management system comprises security incident management as well as business continuity management.

Attachment 3: Approved Sub-Processors

Brainloop Service	Sub-processor (company, headquarters)	Contractual services
Brainloop Secure Dataroom Services (BDRS) in case of use of the Austrian platform (https:/my.brainloop.at)	Kontron AG (formerly S&T Services GmbH) Lehrbachgasse 11 1120 Vienna, Austria	Hosting provider; data center services
	Brainloop AG Theatinerstraße 12 80333 Munich, Germany (in case Brainloop AG is not the direct contractual partner of Client)	Administration Provision of customer support, platform / application management and service management
Brainloop Secure Dataroom Services (BDRS) in case of use of the Swiss platform (https://my.brainloop.ch) **MeetingSuite** in case of use of the Swiss platform (https://services.brainloop.ch)	Econis AG Neumattstrasse 7 8953 Dietikon, Switzerland	Hosting provider; data center services
	Brainloop AG Theatinerstraße 12 80333 Munich, Germany (in case Brainloop AG is not the direct contractual partner of Client)	Administration Provision of customer support, platform / application management and service management
Brainloop Secure Dataroom Services (BDRS) in case of use of the German platform (https://my.brainloop.net) **MeetingSuite** in case of use of the German platform (https://services.brainloop.net) **MeetingSuite$^{\text{CONNECT}}$** in case of use of the German platform (https://services.brainloop.net)	Telekom Deutschland GmbH, Landgrabenweg 151 53227 Bonn, Germany	Hosting provider; data center services
	Brainloop AG Theatinerstraße 12 80333 Munich, Germany (in case Brainloop AG is not the direct contractual partner of Client)	Administration Provision of customer support, platform / application management and service management