Version: 21 July 2021

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("Agreement") is a Schedule of and forms part of the BBB On Demand Terms and Conditions having the same version date:

1. Definitions and interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning or, if not defined here, the meaning set out in section 1.1 of the Terms and Conditions:

"**Agreement**" means this Data Processing Agreement and all Schedules;

"**Customer Personal Data**" means Customer Data which is Personal Data processed by the Provider on behalf of Customer pursuant to or in connection with the Agreement, including Personal Data of Third Party Users;

"**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

"**EEA**" means the European Economic Area;

"**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR including United Kingdom's Data Protection Act 2018;

"**GDPR**" means EU General Data Protection Regulation 2016/679;

"**Data Transfer**" means a transfer of Customer Personal Data from the Customer to the Provider; or an onward transfer of Customer Personal Data from the Provider to a Sub Processor, or between two establishments of the Provider, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

"**Sub Processor**" means any person appointed by or on behalf of Provider to process Personal Data on behalf of the Customer in connection with the Agreement.

The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Preamble

2.1 The Parties seek to implement a data processing agreement that complies with the requirements of the current legal frameworks in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). The Parties wish to lay down their rights and obligations.

2.2 The Customer:

(a) Shall act as Data Controller.

(b) Confirms that they wish to subcontract certain Services, which imply the processing of personal data, to the Provider.

2.3 The Provider:

(a) Shall comply with all applicable Data Protection Laws in the Processing of Customer Personal Data; and

(b) Shall not Process Customer Personal Data other than on the relevant Customer's documented instructions.

3. Provider Personnel

3.1 The Provider shall take reasonable steps to ensure the reliability of any employee, agent or contractor or Sub Processor who may have access to the Customer Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Provider, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Provider shall in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, the Provider shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Sub Processing

5.1 The Customer agrees that the Provider shall appoint Google inc. as a Sub Processor for the following purposes:

(a) Some Customer Personal Information – specifically the name, address and email used for the Customer account - will be stored on the Google Compute Firestore cloud database system. This data may be stored outside of the EEA.

(b) Some Customer Personal Data – specifically, data entered into BigBlueButton meetings - may be processed on Google Compute Instances in countries selected by the Customer. At the option of the customer this can be within and remain within the EEA.

(b) Customer Personal Data – specifically, data within meeting recordings created at the request of the Customer - may be stored on Google Compute Storage. This storage is within the EEA; specifically, the Netherlands.

5.3 The Customer agrees that the appointment of Google inc. as a Sub Processor includes the Sub Processors declared by Google Inc. in their data processing agreement (including those listed on the web page: https://cloud.google.com/terms/subprocessors)

5.4 The Customer agrees that the Provider shall appoint Stripe inc. as a Sub Processor for the following purposes:

(a) PSD2 / SCA and GDPR compliant payment processing.

5.5 The Customer agrees that the Provider shall appoint Amazon inc. as a Sub Processor for the following purposes:

(a) Sending of emails.

5.6 The Provider shall not appoint (or disclose any Customer Personal Data to) any other Sub Processor unless required or authorized by the Customer.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, the Provider shall assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Provider shall:

(a) Promptly notify the Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

(b) Ensure that it does not respond to that request except on the documented instructions of Customer or as required by Applicable Laws to which the Provider is subject, in which case Provider shall to the extent permitted by Applicable Laws inform the Customer of that legal requirement before the Provider responds to the request.

7. Personal Data Breach

7.1 The Provider shall notify the Customer without undue delay upon the Provider becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow the Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 The Provider shall co-operate with the Customer and take reasonable commercial steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment

8.1 The Provider shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to the Provider.

9. Deletion or return of Customer Personal Data

9.1 Subject to this section 9 the Provider shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Customer Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Customer Personal Data.

10. Audit rights

10.1 Subject to this section 10, the Provider shall make available to the Customer on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by the Providers.

10.2 Information and audit rights of the Customer only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Provider may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Customer. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. Confirmation

12.1 This agreement forms part of the Terms and Conditions and does not need to be signed to become binding on the parties. If required for regulatory compliance the Customer and Provider may, at the request of the Customer, sign and date this Agreement.

Signed for the Customer	Signed for the Provider
Date	Date