Data Processing Agreement

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services under the BlueCall Terms and Conditions (the "**Supplier Agreement**"). This Agreement is an amendment to the Supplier Agreement and is effective upon its incorporation to the Supplier Agreement, which incorporation may be specified in the Supplier Agreement or an executed amendment to the Supplier Agreement. Upon its incorporation into the Supplier Agreement, this Agreement will form a part of the Supplier Agreement.
We periodically update this Agreement. If you have an active BlueCall account, you will be informed of any modification by email. You can find archived versions of the terms here (https://www.bluecallapp.com/dpa).
The term of this Agreement shall follow the term of the Supplier Agreement. Terms not defined herein shall have the meaning as set forth in the Supplier Agreement.

Whereas

(A) Your company act as a Data Controller (the "Controller").

(B) Your company wishes to subcontract certain Services (as defined in Supplier Agreement), which imply the subprocessing of personal data, to BlueCall, acting as a Data Processor (the "Processor").

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework 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).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1
Unless otherwise defined herein, capitalized terms and expressions used in this DPA shall have the following meaning:

1.1.2
"Company Personal Data" means any Personal Data Processed by a Contracted Processor on Controller's behalf pursuant to or in connection with the Supplier Agreement;

1.1.3
"Contracted Processor" means a Subprocessor;

1.1.4
"Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5
"EEA" means the European Economic Area;

1.1.6
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means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7
"GDPR" means EU General Data Protection Regulation 2016/679;

1.1.8
"Data Transfer" means:

1.1.8.1
a transfer of Company Personal Data from Controller to a Contracted Processor; or

1.1.8.2
an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, 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);

1.1.9
"Services" means the services determined by the Supplier Agreement

1.1.10
"Subprocessor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of Controller in connection with the Agreement.

1.2
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. Processing of Company Personal Data

2.1
Processor shall:

2.1.1
comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2
not process Company Personal Data other than on Controller's documented instructions.

2.2
Controller instructs Processor to process Company Personal Data to provide the Services and related technical support.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Supplier Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, 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, Processor shall in relation to the Company

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, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing

5.1
Controller agrees that Processor may engage Subprocessors to Process Personal Data on Controller's behalf. Processor has currently appointed, as Subprocessors, third parties listed in Annex 1 to this DPA. Processor will notify Controller if Subprocessors are added or replaced in the list in Annex 1 at least 30 days prior to any such changes, this notification will be received to the Controller's appointed email address.

Where Processor engages Subprocessors, it will impose data protection terms on the Subprocessor that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Subprocessors. Processor will remain responsible for each Subprocessor's compliance with the obligations of this DPA and for any acts or omissions of such Subprocessor that cause Processor to breach any of its obligations under this DPA.

5.2
List of approved Subprocessors can be found in Annex 1

6. Data Subject Rights

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

6.2
Processor shall:

6.2.1
promptly notify Controller if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2
ensure that it does not respond to that request except on the documented instructions of Controller or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Controller of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

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

7.2
Processor shall cooperate with Controller and take reasonable commercial steps as are directed by Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

8.1
Processor shall provide reasonable assistance to Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Controller 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 Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

9.1
Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete/irreversible anonymize and procure the deletion/irreversible anonymization of all copies of those Company Personal Data, unless the Data Processor is required under Applicable Laws to continue to store the Personal Data.

9.2
Processor shall provide written certification to Controller that it has fully complied with this section 9 within 10 business days of the Cessation Date.

10. Audit rights

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

10.2
Information and audit rights of Controller 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.

10.3
Further, at Controller's written request, Processor shall provide written responses (on a confidential basis) to all reasonable requests for information made by Controller necessary to confirm Processor's compliance with this DPA, provided that Controller will not exercise this right more than once per calendar year unless Controller has reasonable grounds to suspect non-compliance with the DPA.

11. Data Transfer

11.1
The Processor 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 Controller. 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 General Terms

12.1
Confidentiality. Each Party must keep any information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must

not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a)
disclosure is required by law;

(b)
the relevant information is already in the public domain.

12.2
Notices. All notices and communications given under this Agreement must be in writing and will be sent by email. Controller shall be notified by email sent to the address related to its use of the Service under the Supplier Agreement. Processor shall be notified by email sent to the address: gdpr@bluecallapp.com

13. Governing Law and Jurisdiction

13.1
This Agreement is governed by Swedish law.

13.2
Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be finally settled by arbitration in accordance with the Arbitration Rules of the Arbitration Institute of the Stockholm Chamber of Commerce. The arbitral tribunal shall be composed of three (3) arbitrators. The arbitration shall take place in Stockholm and the language shall be English. Any dispute, arbitral proceeding, decision and award shall be kept strictly confidential.