Data Processing Agreement (DPA)

Our SCC: Gleemeet SCC

We are GleeMeet Private Limited ('**Company**', '**we**', '**us**', or '**our**') based in India. Any reference herein to **"You or Your"** refers to the **"Users"** whose personal data is being collected for the purpose and objective of the Company. Company and You each a "**Party**" and together the "**Parties**".

This Data Processing Agreement ("**Agreement**") forms a legally binding contract between You and GleeMeet and applies to the extent to which GleeMeet processes Users Personal Data on Your behalf when We are the Data Controller,

WHEREAS

(A) The Company acts as a Data Controller.

(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data 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 wishes to lay down their rights and obligations regarding data protection and compliance with Data Protection Laws, and the Parties (including their representatives) are required to comply with this DPA in connection with the performance of their obligations related to business cooperation between Parties.

The relevant information regarding the Personal Data and the processing activities are described in Schedule 1 to this DPA. This information includes the following:

1. Personal Data to be processed
2. Nature and purpose of the processing of Personal Data,
3. Description of applicable information security measures;
4. Duration, or criteria for the duration of processing of Personal Data

Controller, You and Processor acknowledge that relevant Data Protection Laws must be observed during the business cooperation.

(E) The purpose of this DPA is to ensure the implementation of consistent privacy and data protection practices to be applied in the business cooperation. Furthermore, the Parties recognize and agree that proper data protection is required by Data Protection Laws.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

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

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

1.1.2 "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of the Company pursuant to or in connection with the Principal Agreement;

1.1.3 "**Contracted Processor**" means a Processor, who process the Personal Data on behalf of the Company;

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 outside the EU/EEA with laws considered by the European Commission to provide an adequate level of protection of personal data;

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 the Company 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 online dating platform that the Company provides.

1.1.10 "**Sub-processor**" means any person appointed by or on behalf of a Processor to process Personal Data on behalf of the Company 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 the relevant Company's documented instructions.

2.2 The Company instructs the Processor to process Company Personal Data and the Processor hereby agrees not to process the Company Personal Data other than for the Company's defined purpose.

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 the 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 Principal 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.

To the extent that Processor is processing Personal Data on behalf of Controller, Processor shall, and shall procure that any other sub-processor shall, process Personal Data solely to the extent necessary for fulfilling their obligations under this DPA and General Data Protection Regulation (GDPR) in accordance with the procedures conforming to Controller's requirements and/or instructions expressly provided in this DPA or as otherwise provided by the Controller in writing. Processor shall ensure that its sub-processors comply with the same requirements concerning any Personal Data.

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, the 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. Processor shall implement the following measures as applicable:

(i) the pseudonymisation and encryption of Personal Data

(ii) ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services processing Personal Data;

(iii) restoring the availability and access to Personal Data in a timely manner in the event of an incident;

(iv) regularly testing, assessment and evaluation of the effectiveness of technical and organizational measures for ensuring the security of the processing of Personal Data.

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

4.3 Processor shall keep accurate records of all processing of Personal Data under this DPA and limit access of Personal Data to authorized and properly trained personnel with a well-defined “need-to-know” bases and who are bound by appropriate confidentiality obligations.

5. Sub-processing

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Sub-processor unless authorised by the Company in writing. Company shall not delay in providing such authorization to the Processor.

5.2 Processor shall inform Controller of any intended changes of sub-processor(s). In any event, Processor will remain fully liable for the acts and omissions of its sub-processor(s) towards Controller.

6. Data Subject Rights

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

6.2 Processor shall:

6.2.1 promptly notify Company 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 the Company or as required by Applicable Laws to which the Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

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

7.2 The Data Breach notification shall contain at least the following:

(i) description of the nature of the Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

(ii) the name and contact details of the contact point where more information can be obtained;

(iii) description of the likely consequences of the Data Breach;

(iv) description of the measures taken or proposed to be taken by Processor to address Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

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

8. Data Protection Impact Assessment and Prior Consultation Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Company reasonably considers to be required by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Laws, 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 from the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data. The Processor shall upon request from the Company provide acknowledgment in writing of deletion of all copies of the Personal Data.

10. Audit rights

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

10.2 Information and audit rights of the Company 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. In the event of an audit request directly from a Supervisory Authority regarding processing of Personal Data, Processor must cooperate with Controller in answering the request.

11. Data Transfer

The Processor may not transfer or authorise the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. 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. Liability

Processor shall indemnify, defend and hold harmless Controller against all damages, losses, penalties, compensation and expenses caused by any act, omission, default or negligence of Processor, or its sub-processors, relating to the processing of Personal Data under this DPA, or relating to a Data Breach where the Personal Data is in the possession, custody, or control of Processor or its sub-processors or may be accessed by them, and against all actions, claims, demands and proceedings in respect thereof, or in relation thereto. Controller may, at any time, take over the defense, totally or partly, at Processor's reasonable cost in the event that Controller considers such takeover to be necessary. Breach by Processor, or its sub-processors, as the case may be, of its obligations under this DPA will be deemed a material breach of this DPA.

General Terms

12.1 **Confidentiality**. Each Party must keep this Agreement and 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 delivered personally, sent by post, or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

12.3 **Duration of the obligations under this DPA**. This DPA shall remain in full force for as long as the business cooperation is in force, and for such period thereafter as is necessary for the activities after the termination or expiration of this DPA to be complete, including but not limited to, the return of Personal Data to Controller and/or the deletion of Personal Data), or, if longer, as may be prescribed by any applicable law. To the extent that Personal Data is processed by, or for, Processor, for whatsoever reason, after the termination or expiration of said cooperation, this DPA shall continue to apply to such processing for as long as such processing is carried out.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of India.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Hyderabad.

Schedule- 1

This schedule defines the information regarding (a) the nature and purpose of the processing of Personal Data; (b) the description of security measures; and (c) duration of the processing of Personal Data.

This schedule shall be an integral part of and supplement the DPA, as further agreed below:

(a) Nature and purpose of the processing
Processor processes Personal Data necessary for the business cooperation. Upon written authorization from the Company, the Processor is also transferring such data outside European Economic Area. Controller has also identified the possibility of providing Processor access Controller's data base in the future for the purposes of said cooperation.

(b) Applicable security measures
Processor takes all reasonable measures to protect Personal Data as the data is received from Controller is being processed in connection with business cooperation and during storage and processing in the backend.

These measures include encryption of data and connections wherever applicable, protecting access to Processor infrastructure and databases using industry standard protection methods, including technical and organizational safety procedures, and access control and monitoring of Personal Data.

If the Personal Data will be maintained on external service providers' servers, service providers providing this service will also ensure appropriate safeguards against physical threats against the Personal Data, including access monitoring and control.

(c) Duration of the processing
During the term of this DPA unless otherwise required by applicable Data Protection

Laws.

Schedule- 2

GleeMeet Security Measures