Plivo Data Processing Addendum Incorporating: GDPR and Standard Contractual Clauses

This Data Processing Addendum ("DPA") forms part of the Plivo Master Services Agreement or Terms of Use available at https://www.plivo.com/tos/ or other electronic agreement or mutually executed written agreement between Plivo and Customer applicable to Customer's use of Plivo Service (the "**Agreement**") and reflects the Parties' agreement with regard to the Processing of Customer Personal Data. For good and valuable consideration, the receipt and sufficiency of which are hereby acknowledge, the Parties hereby agree as follows:

I. Introduction

In the course of providing the Plivo Service to Customer pursuant to the Agreement, Plivo may Process Customer Personal Data on behalf of Customer and the Parties agree to comply with the following provisions and instructions with respect to any Customer Personal Data. By signing this DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Legislation, in the name and on behalf of its Data Controller Affiliates, if and to the extent Plivo Processes Customer Personal Data for which such Data Controller Affiliates qualify as the Controller. For the purposes of this DPA only, and except where otherwise indicated herein, the term "**Customer**" shall include Customer and Data Controller Affiliates. Subject to the terms set forth below, this DPA will be effective and replace any previously applicable data processing and security terms related to Processing as of the DPA Effective Date.

II. Parties to the DPA

If the Customer entity signing this DPA is a party to the Agreement, this DPA will be an addendum to and forms part of the Agreement. In such case, the Plivo entity which is party to the Agreement is party to this DPA. If the Customer entity signing this DPA has executed an Order with Plivo pursuant to the Agreement, but is not itself a party to the Agreement, this DPA is an addendum to that Order and applicable renewal Orders, and the Plivo entity that is party to such Order is party to this DPA.

If, however, the Customer entity signing this DPA is neither a party to the Agreement or an Order, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA. The Plivo entity that is the party to the Agreement and applicable Order is the Plivo entity to this DPA and is set forth in the signature block below.

III. Definitions

Definitions for capitalized terms used in this DPA shall apply to this DPA only and have the meaning ascribed to such terms in this section, regardless of whether the Agreement is governed by different definitions for the same terms. Capitalized terms not defined herein shall have the meaning set forth in the Agreement.

"Adequacy" means where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question, ensures an adequate level of protection.

"Affiliate" means, unless otherwise defined in the Agreement, any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Plivo" means the Plivo entity (either Plivo, Inc., a company incorporated in Delaware) that is the named party to the Customer's Order.

"Plivo Service" means the cloud-based communication platform and related services provided by Plivo (including the Plivo Cloud) and subscribed to under an Order or Agreement.

"Controller" means the entity that determines the purposes and means of Processing of Customer Personal Data.

"**Customer Account Data**" means mean personal data that relates to the relationship between the Customer and Plivo, such as contact information/names of authorized users of the access Customer's Plivo account, billing information, data collected, if any, for the purpose of identity verification, or to comply with legal obligations to collect identify or address proof.

"Customer Personal Data" means Content (as defined in the Agreement) which contains Personal Data.

"**Customer Usage Data**" means data processed by Plivo for the purposes of transmitting or exchanging Customer Content, including data collected and processed when the Customer uses Plivo services, such as when customer makes a call, the length of the call, and whether Customer is using voice or text services, activity logs, details of text messages or voice calls or voice call audio.

"Data Controller Affiliates" means any of Customer's Affiliates (a) (i) that are subject to applicable Data Protection Legislations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (ii) permitted to use the Services

pursuant to the Agreement between Customer and Plivo, but have not signed their own Order and are not a "Customer" as defined under the Agreement, (b) if and to the extent Plivo processes Personal Data for which such Affiliate(s) qualify as the Controller.

"Data Protection Legislation" means the laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, as applicable to the Processing of Customer Personal Data under this DPA.

"Data Subject" means the identified or identifiable person to whom Customer Personal Data relates.

"DPA Effective Date" means the date of Customer's signature date below.

"GDPR" means General Data Protection Regulation and is 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 of Directive 95/46/EC.

"Order" means the separately executed document(s) under which Customer subscribes to the Plivo Service, products or services pursuant to the Agreement and has been agreed to in writing by the Parties or as agreed to between Customer and Plivo.

"Personal Data" means data relating to: (i) an identified or identifiable natural person; and (ii) an identified or identifiable legal entity that has standing under the applicable Data Protection Legislation.

"Processor" means the entity which is Processing Customer Personal Data on behalf of the Controller.

"Processing" means any operation or set of operations which is performed upon Customer Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Standard Contractual Clauses" means the standard contractual clauses herein set out as Appendix 2 for the transfer of any personal data to processors in third countries in accordance to the terms set out European Commission Decision 2021/914/EU

"Subprocessor" means any Processor engaged by Plivo, for the sake of clarification the telecommunication provider are not Subprocessor

"Supervisory Authority" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

"Users" means, collectively, the any users of the Customer including but not limited to any administrator, managed user or external user.

IV. Processing of Customer Personal Data.

A. Roles and Responsibilities.

i. Plivo as a Processor: The Parties acknowledge and agree that with regard to the Processing of Customer Personal Data under the Data Protection Legislation and this DPA, Customer is the Controller and Plivo is the Processor and that Plivo or its Affiliates will engage Sub-processors pursuant to the requirements set forth in Section VII "Sub-processors" below.

ii. Each Party will comply with the obligations applicable to it under the Data Protection Legislation with respect to the Processing of Customer Personal Data.

iii. Customer's Processing of Personal Data. Customer shall, in its use of the Services and provision of instructions, Process Personal Data in accordance with the requirements of applicable Data Protection Legislation. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

B. Customer's Instructions and Authorization to Process Customer Personal Data. By entering into this DPA, Customer instructs Plivo, subject to Customer's compliance with Data Protection Legislation, to Process Customer Personal Data: (a) to provide the Plivo Service (in accordance with the features and functionality of the Plivo Service); (b) to enable User initiated actions on the Plivo Service; (c) as set forth in the Agreement or applicable Order; and (d) as further documented by a mutually agreed upon written instruction given by Customer and accepted by Plivo, unless required to do so otherwise by law to which Plivo is subject; in such a case, Plivo shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Taking into account the nature of the processing, Customer agrees that it is unlikely Plivo can form an opinion on whether instructions infringe the GDPR. If Plivo forms such an opinion, it will immediately inform Customer, in which case, Customer is entitled to withdraw or modify its instructions. If Customer is processing personal data of a child, Customer acknowledges it has made reasonable efforts to verify that consent has been given or authorised by the holder of parental responsibility over the child. Customer further acknowledges that Plivo is not responsible for collecting consent or authorization for the processing of child's data.

C. Scope of Processing. Plivo will Process Customer Personal Data as necessary to perform the Plivo Service pursuant to the Agreement and in accordance with this DPA. Plivo will Process Customer Personal Data for the period of the Agreement or applicable Order, unless otherwise agreed to by the Parties in writing. The types of Customer Personal Data and categories of Data Subjects that may Processed under this DPA are set forth in Appendix 1 ("Processing Scope"). Customer understands and acknowledges that Plivo main processing facilities are in the United States of America.

D. Data Protection Impact Assessment and Prior Consultation Assistance. Plivo will provide reasonable assistance to Customer, as required by law and applicable to Plivo's role as a Processor, for Customer to comply with Customer's obligations to perform a data protection impact assessment. Further, in such situations where Customer's processing of Customer Personal Data results in a high risk to the rights and freedoms of natural persons, Plivo will provide reasonable assistance to Customer as it seeks prior consultation from a supervisory authority.

E. Confidentiality of Customer Personal Data. Plivo will not access or use, or disclose to any third party, any Customer Personal Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends Plivo a demand for Customer Personal Data, Plivo will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, Plivo may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Personal Data to a governmental body, then Plivo will use reasonable efforts to give Customer a notice of the demand unless Plivo is legally prohibited from doing so.

F. Notwithstanding any other provision in the DPA or Agreement or applicable Order, Customer agrees that, for Plivo to provide the Services, Customer Personal Data may be: (i) used, managed, accessed, transferred or held on a variety of systems, networks and facilities (including databases) worldwide; (ii) provided or transferred by us to any Plivo Affiliate, subcontractor or supplier worldwide to the extent necessary to allow that Plivo Affiliate, subcontractor or supplier to perform its obligations in respect of the Service. Customer appoints Plivo to perform any such transfer in order to provide the Services, provided that Plivo takes appropriate steps and enters into appropriate agreements with Plivo Affiliates, subcontractors or suppliers, as required, for such transfer to be adequately protected. If relevant, Customer will ensure that the Customer obtains and/or submits promptly any relevant regulatory approvals and/or notifications that Customer may be subject to under the Data Protection Legislation. Customer agrees that, to the extent permitted by applicable law, Plivo will not be liable for any claim arising out of or in connection with any action or omission by Plivo, to the extent that such action or omission results from any failure by Customer to comply with this DPA.,

V. Data Security

A. Security Controls. Plivo will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access as described in Appendix 2 (the "Security Controls") to the Standard Contractual Clauses. As described in Appendix 2, the Security Controls include measures to encrypt Customer Personal Data; to help ensure ongoing confidentiality, integrity, availability and resilience of Plivo's systems and services; to help restore timely access to Customer Personal Data following an incident; and for regular testing of effectiveness.

B. Security Compliance of Plivo Personnel. Plivo will take appropriate steps to ensure compliance with the Security Controls by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorised to process Customer Personal Data have agreed to an appropriate obligation of confidentiality.

VI. Data Incident Notification

After becoming aware of an accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to Customer Personal Data transmitted, stored or otherwise Processed by Plivo or its Subprocessors ("**Data Incident**"), Plivo will notify Customer without undue delay ("**Data Incident Notification**"). Plivo will take reasonable steps to: (i) identify the cause of such Data Incident; and (ii) take the steps necessary and reasonable to remediate the cause of such Data Incident to the extent such remediation is within Plivo's reasonable control. Data Incident Notification will be delivered to the Administrator(s) of Customer's Plivo Service account ("**Notification Email Address**"). Customer is solely responsible for ensuring that the Notification Email Address associated with Customer's account is current and valid.

To enable Customer to notify a Data Incident to supervisory authorities or Data Subjects (as applicable), Plivo will cooperate with and assist Customer by including in the notification under Section VI such information about the Data Incident as Plivo is able to disclose to Customer, taking into account the nature of the processing, the information available to Plivo, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Data Incident.

VIII. Deletion and Return of Customer Data

The Plivo Service provides Customer with controls to enable Customer to retrieve, rectify, delete or block Customer Personal Data as described in the Agreement. For purposes of this provision, Plivo will provide reasonable assistance to Customer where necessary to assist with such obligations.

VII. Subprocessors

A. Consent to Subprocessors. Customer hereby explicitly consents to the use of Subprocessors by Plivo in order to allow Plivo to fulfil its contractual obligations under the Agreement and this DPA and to provide certain services on Plivo's behalf such as support services. For clarification, Subprocessors are third party Subprocessors that may be engaged by Plivo and Plivo Affiliates.

B. Subprocessor Commitments. Plivo undertakes to enter into a written agreement with any applicable Subprocessors in accordance with such obligations that will in no event be less protective than this DPA. Plivo will restrict the Sub processor's access to only what is necessary to maintain the Plivo Service or to provide the Plivo Service to Customer and any of its Users. Customer hereby consents to Plivo's use of Subprocessors as described in this Section IX (Subprocessors) and those listed on the Plivo Subprocessor website list referred to below. Plivo will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Subprocessors.

C. Current Subprocessors. Information regarding current Subprocessors including their location and services can be found on the Plivo Subprocessor website found here: https://www.plivo.com/subprocessors/. This Subprocessor list may be updated from time to time by Plivo in accordance with this Section IX (Subprocessors).

D. Changes to Subprocessors. Plivo will provide Customer with notice at least 30 days in advance before a new Subprocessor Processes any Customer Personal Data. Such notice may be provided either by sending an email to the Notification Email Address or via the Plivo Console within the Plivo Service. Customer may object to any new Subprocessor by terminating the applicable Order(s) with respect only to those services which cannot be provided by Plivo without the use of the objected-to new Subprocessor. Such termination will be made by providing written notice to Plivo, on the condition that Customer provides such notice within 20 days of being informed of the engagement of the new Subprocessor as described herein. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Subprocessor.

VIII. Data Subject Rights

A. Access and Rectification. Plivo will, in a manner consistent with the functionality of the Plivo Service, enable Customer to access, rectify and restrict processing of Customer Personal Data, including via the deletion functionality provided by the Plivo Service.

B. Data Subject Requests. Plivo shall, to the extent legally permitted, promptly notify Customer if Plivo receives any requests from a Data Subject to exercise Data Subject rights afforded to the Data Subject under applicable Data Protection Legislation in relation to Personal Data, including, as

applicable, the following: access, rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, or to not be subject to an automated individual decision making (each, a "**Data Subject Request**"). Taking into account the nature of the Processing, Plivo shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request as required by applicable Data Protection Legislations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Plivo shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Plivo is legally permitted to do so and the response to such Data Subject Request is required under applicable Data Protection Legislations. To the extent legally permitted, Customer shall be responsible for any costs arising from Plivo's provision of such assistance, including any fees associated with provision of additional functionality.

IX. Data Controller Affiliates

A. Relationship and Communication. By signing this DPA, Customer acknowledges and agrees that it is entering into this DPA on behalf of itself and, as applicable in accordance with Section I (Introduction), in the name and on behalf of its Data Controller Affiliates, thereby establishing a DPA between Plivo and each Data Controller Affiliate, subject to the provisions of the Agreement and this DPA. Each Data Controller Affiliate agrees to be bound by the obligations of this DPA. However, a Data Controller Affiliate is not and does not become a party to the Agreement and is only a party to this DPA. All access and use of the Plivo Service by the Data Controller Affiliate must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by a Data Controller Affiliate shall be deemed a violation by Customer. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communications with Plivo under this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Data Controller Affiliate.

B. Rights of Data Controller Affiliates. In the event a Data Controller Affiliate becomes a party to the DPA with Plivo, it shall do so only to the extent required under applicable Data Protection Legislation. Except as expressly required by Data Protection Legislation for a Data Controller Affiliate to exercise a right or seek a remedy under this DPA from Plivo by itself directly, the Parties agree that: (i) the Customer that is the contracting party to the Agreement shall have the sole right to exercise any such right or seek any such remedy on behalf of the Data Controller Affiliate and (ii) the Customer that is the contracting party to the Agreement shall, to the extent not prohibited by Data Protection Legislation, exercise any such rights under this DPA in a combined manner for all of its Data Controller Affiliates together.

X. Limitation of Liability

Each Party's and of its Affiliate's liability taken together in the aggregate, arising out of or related to this DPA whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability provisions of the Agreement. Any reference in such limitation of liability provisions to the liability of a Party means the aggregate liability of that Party and all of its Affiliates (including Data Controller Affiliates) under the Agreement and all DPAs taken together. For the avoidance of doubt, Plivo and its Affiliates' total liability for all claims from the Customer and all of its Data Controller Affiliates arising or related the Agreement or any DPA shall apply in aggregate for all claims under both the Agreement and all DPAs and shall not be understood to apply individually and severally to Customer or to any Data Controller Affiliate that is a contractual party to any such DPA.

XI. Audit

In compliance with obligations under Applicable Data Protection Legislation and this Addendum, at the reasonable request of Customer or any Regulator, Plivo can demonstrate compliance with its obligations set out under this Addendum and pursuant to Article 28(5) of the GDPR or the Standard Contractual Clauses by providing Customer with an audit report issued by an independent third-party auditor (subject to appropriate confidentiality obligations and not use this audit report for any other purpose). To the extent that Plivo's provision of an audit report does not provide sufficient information or to the extent that Customer must respond to a regulatory authority audit, at the request of Customer or any Regulator, submit its data processing facilities and/or any other location from which Relevant Personal Data can be accessed by Plivo or a relevant Sub-Contractor for audit or inspection in order for Customer or the relevant Regulator to ascertain and/or monitor compliance with these Data Processing Terms and Data Protection Legislation. Unless otherwise required by applicable law, such audit shall be carried out by (a) an independent third party; (b) during regular business hours; (c) upon reasonable prior notice of at least 30 days; (d) at the sole cost of the Customer; (e) occurs once annually; (f) do not disrupt Plivo's business or interfere with Plivo's legal obligations or the interests of Plivo's other customers and (g) under a duty of confidentiality by Customer and/or by a third party appointed by Customer.

XII. GDPR and Data Transfers

A. GDPR. Plivo will Process Customer Personal Data in accordance with the GDPR requirements applicable to Plivo's provision of the Plivo Service.

B. Transfer mechanisms for data transfers. Subject to the terms and conditions of the Agreement and Data Protection Legislation, Plivo makes available the transfer mechanisms listed below. Such transfer mechanisms shall apply to the Plivo Service in the order of precedence set forth herein with respect to any transfer of Customer Personal Data under this DPA from the European Union, the European Economic Area (including its member states), Switzerland and the United Kingdom to countries which are not deemed to have Adequacy (to the extent that such transfers are

subject to such Data Protection Legislation): (i) the Standard Contractual Clauses set forth in Appendix 2 to this DPA, subject to the additional terms set forth in Section XIII(D) (GDPR and Data Transfers)).

C. Additional Terms applicable to the Standard Contractual Clauses.

1. Customers covered by the Standard Contractual Clauses. The Standard Contractual Clauses and the additional terms specified herein apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Controller Affiliates and, (ii) all Affiliates of Customer established within the European Economic Area, Switzerland and the United Kingdom, which have signed Orders for the Services. For the purpose of the Standard Contractual Clauses and this Section 1, the aforementioned entities shall be deemed "data exporters".
2. Instructions. This DPA and the Agreement are Customer's complete and final instructions at the time of execution of the DPA for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the processing described in Section IV of the DPA ("Plivo's Processing of Personal Data") is deemed an instruction by the Customer to process Personal Data."
3. Appointment of new Sub-processors and List of current Sub-processors. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Plivo will appoint Sub-processors in accordance with Section VII ("Sub-processors") of the DPA. Plivo shall make available to Customer the current list of Sub-processors in accordance with Section VII of the DPA.
4. Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Plivo may engage new Sub-processors as described in Sections VII of the DPA.
5. Copies of Sub-processor Agreements. The parties agree that the copies of the Sub-processor agreements that must be provided by Plivo to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Plivo beforehand; and, that such copies will be provided by Plivo, in a manner to be determined in its discretion, only upon request by Customer.
6. Audits and Certifications. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with Section ("Audits") of the DPA.
7. Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Plivo to Customer only upon Customer's request.

8. Conflict. In the event of any conflict or inconsistency between the body of the DPA, this Exhibit, and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Exhibit C, the Standard Contractual Clauses shall prevail.

XIII. LEGAL EFFECT

This DPA shall only become legally binding between Customer and Plivo when both parties have fully executed the DPA and the formalities for execution are duly completed. If Customer has previously executed a "data processing addendum" with Plivo, this DPA supersedes and replaces such prior Data Processing Addendum.

XIV. GOVERNING LAW

This DPA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by, and construed in accordance with, the laws of Ireland.

The Parties authorized signatories have duly executed this Agreement.

On behalf of the data exporter:	On behalf of the data importer:
	Plivo, Inc.
Signature:	Signature:
Name:	Name: Venkatesh Balasubramanian
Title:	Title: Co-founder & CEO
Date Signed :	Date Signed :
Address :	

Appendix 1
Processing Scope

Details of the Data Processing

Plivo will process information to provide the Services pursuant to the Agreement. Plivo will process information sent by Customer's end users identified through Customer's implementation of the Services.

Types of Personal Data (may include)

- **Customer Account Data**
  - Personal data that relates to customer's relationship with Plivo, including contact names, individual names authorized by customer for account access and billing information, username, password, email address, IP address, Location, Country, Credit card information.

- **Customer Usage Data**
  - Interactions with end users via the communication platform, including phone number, date, time, duration and type of communication

Additional detail regarding what information Customer may send to Plivo can be found in the terms of the Agreement.

Categories of Data Subjects

Customer may submit personal data to Plivo through the Services, the extent of which is determined and controlled by the Customer in compliance with applicable Data Protection Legislation and which may include, but is not limited to, personal data relating to the following categories of Data Subject:

- Users;
- employees of the Customer;
- vendors/consultants of the Customer;
- contractors of the Customer;
- agents of the Customer; and/or
- third parties with which the Customer conducts business.

Sensitive Data

Sensitive Data may be processed from time to time through the Services, where Customer or its end users choose to include Sensitive Data within the communications that are transmitted using the Services ,the extent of which is determined and controlled by the Customer in compliance with Applicable Data Protection Legislation and Customer is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing, or prior to permitting Customer's end users to transmit or process, any Sensitive Data via the Service.

Processing Activities

The personal data transferred will be processed in accordance with the Agreement and any Order and may be subject to the following processing activities:

- Personal data will be transferred from the Customer to Plivo for Plivo to provide a communication platform to facilitate interaction between the Customer and User.
- Storage and other processing necessary to provide, maintain and update the Services provided to the Customer
- The Services will consist of providing a communication platform for the Customer to use in order to onboard, analyse and retain Users/end-users and their use of Customer's services.
- to provide customer and technical support to the Customer; and
- disclosures in accordance with the Agreement, as compelled by law
- Full details about the Plivo Services can be found at https://www.plivo.com

Appendix 2
Standard Contractual Clauses

This attachment is attached to and forms part of the Plivo Data Processing Agreement available or other agreement between Customer and Plivo governing the processing of Customer Data (the "DPA"). Unless otherwise defined in this attachment, capitalised terms used in this attachment have the meanings given to them in the DPA.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices andagencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC(OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legalact between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8: Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9: Clause 9(a), (c), (d) and (e);

(iv) Clause 12: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18: Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Not Used

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1. Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3. Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4. Accuracy and data minimisation

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5. Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6. Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful

destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7. Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter

'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9. Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required:

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([4]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([5]);

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1. Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2. Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679

becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Belgium.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Belgium.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: The entity identified as "Customer" in the DPA.

Address: The address for Customer associated with its Plivo account or as otherwise specified in the DPA or the Agreement or applicable Order.

Contact person's name, position and contact details: The contact details associated with Customer's account, or as otherwise specified in the DPA or the Agreement or applicable Order.

Activities relevant to the data transferred under these Clauses: The activities specified in Section VI - Processing of Customer Personal Data of the DPA.

Signature:

Date:

Role: Controller

Data importer(s):

1. Name: **Plivo Inc.**

Address: 6001 W Parmer Ln, Ste 370 PMB 2774, Austin, TX 78727.

Contact person's name, position and contact details: The contact details for Plivo specified in the Addendum or the Agreement – Privacy@plivo.com

Activities relevant to the data transferred under these Clauses: The activities specified in Section VI - Processing of Customer Personal Data of the DPA

Signature:

Date:

Role: Processor

B. DESCRIPTION OF TRANSFER

Data Exporter

The Data Exporter is a customer of the Data Importer's cloud based communication services, systems and/or technologies, and the Data Exporter is established in the territory of an EU Member State.

Data Importer

The Data Importer is a provider of cloud based communication services and systems and/or technologies. Data Importer will process information to provide the Services pursuant to the Agreement. Data Importer will process information sent by Customer's end users identified through Customer's implementation of the Services.

Categories of data subjects whose personal data is transferred:

Data Exporter may submit personal data to the Data Importer through the Services, the extent of which is determined and controlled by the Data Exporter in compliance with applicable Data Protection Legislation and which may include, but is not limited to, personal data relating to the following categories of data subject:

- Users;
- employees of the Data Exporter;
- vendors/consultants of the Data Exporter;
- contractors of the Data Exporter;
- agents of the Data Exporter; and/or
- third parties with which the Data Exporter conducts business.

Categories of personal data transferred:

Types of Personal Data (may include)

- **Customer Account Data**
    - Personal data that relates to Data Exporter's relationship with Data Importer, including contact names, individual names authorized by customer for account access and billing information, username, password, email address, IP address, Location, Country, Credit card information.
- **Customer Usage Data**
    - Interactions with end users via the communication platform, including phone number, date, time, duration and type of communication.

Additional detail regarding what information Data Exporter may send to Data Importer can be found in the terms of the Agreement.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Data Exporter may from time to time submit personal data to the Data Importer through the Services, where Data Exporter or its end users choose to include Sensitive Data within the communications that are transmitted using the Services ,the extent of which is determined and controlled by the Data Exporter in compliance with applicable Data Protection Legislation and which may concern the following special categories of data, if any:

- passport details and other identifiers;
- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade-union membership;
- genetic or biometric data;
- health; and
- Sex Life

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Personal data is transferred in accordance with Data Exporter's instructions as described in Section IV of the DPA

Nature of the processing:

The personal data transferred will be processed in accordance with the Agreement and any Order and may be subject to the following processing activities:

- Personal data will be transferred from the Data Exporter to Data Importer for Data Importer to provide a communication platform to facilitate interaction between the Data Exporter and User.
- Storage and other processing necessary to provide, maintain and update the Services provided to the Data Exporter
- The Services will consist of providing a communication platform for the Data Exporter to use in order to onboard, analyse and retain Users/end-users and their use of Data Exporter's services.
- to provide customer and technical support to the Data Exporter; and
- disclosures in accordance with the Agreement, as compelled by law
- Full details about the Data Importer Services can be found at https://www.plivo.com

Purpose(s) of the data transfer and further processing:

The provision of Services by Data Importer to the Data Exporter

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data Importer will store the data for the duration of the Agreement and/or Services. After the Agreement and/or Services are terminated, Data Importer may retain certain data for as long as required for Data Importer's legitimate business needs or as required by applicable law, provided the data remains protected in accordance with the Data Protection Legislation and the terms of the Agreement. Upon termination of the Agreement and/or Services, Data Importer shall, upon Data Exporter's request, and subject to the limitations described in the Agreement, return all Personal Data in Data Importer's possession to Data Exporter or securely destroy such Personal Data and demonstrate to the satisfaction of Data Exporter that it has taken such measures, unless applicable law prevents it from returning or destroying all or part of Personal Data.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter, nature and duration of the processing are described in Nature of Processing above.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the data importer

Data importer has implemented stringent data privacy structures within the company. These structures ensure adequate data privacy with the measures implemented by data importer:

- Organization
- Entry
- Admission
- Access
- Transmission of data
- Input of data
- Commissioned data processing
- Data availability
- Data separation

The specific details regarding the technical and organizational measures are explained in the following text.

A. Organizational Control

Measures, which comply with the specific requests of Data Protection, regarding the internal organization:

- Instalment of an external Data Protection Officer with expertise
- Commitment of employees to data secrecy
- IT-Emergency concept
- Data back-up concept (for production data)
- Regulations regarding the correct and secure processing of duties done by data processing
- Regular instruction of relevant regulations
- Control of compliance with the regulations

- Regulations and instructions for entry control
- Regulations and instructions for admission control
- Regulations and instructions for access control
- Regular information and instruction of the employees
- Documentation of IT-procedures, software, IT-configuration

B. Entry Control

Measures to limit entrance of unauthorized persons to areas where personal data is used or processed with electronic data processing devices.

- Entry control
- Regulations and instructions of entry control
- Gate control
- Identification badges / code cards
- Entry regulations organization for employees
- Entry regulations for external service providers (cleaning and maintenance personal, craftsmen, customers, visitors
- Classification of security areas
- Identification of admission authorized persons
- Safeguarding by alarm system, intrusion detector, police emergency call
- Security locks with centralized key administration and master key plan
- Revision secure organization of admission rights
- Revision secure grant and revocation of admission rights

C. Access Control (Electronic data processing)

Measures to limit access of unauthorized persons to systems where personal data is used or processed with electronic data processing devices.

- Regulations and instructions for access control
- Processes for file organization
- Rights- and role-concept
- Assignment of rights for data-input as well as for information, modification and deletion of stored data
- Regulated procedure for granting, changing and revocation of access rights

- Selective access regulations for procedures, operation control tickets
- User adaptive access protection
- Selective access for files and functions
- Automatic screensaver protection in case of inactivity
- Requirement of user identifiers (Passwords) for files, system data, application data
- Machine control of authorizations
- Logging access to specific data (e.g.: Console log, machine Log)
- Functional and/or timely limited use of terminals
- Password policy at the level of configuration of IT-systems
- Identification and authentication of users
- Control of administrator activities
- Limitation of free style queries in databases
- Specific written directives for the restart-procedure
- Safeguards for access by self-acting institutions
- Use of encryption

D. Access Control (Data media)

Measures to limit access of unauthorized persons to data and/or applications being stored on storage devices outside of an electronic data processing system.

- Write-protection for data media
- Identification of authorized personnel
- Rules regarding the production of copies
- Labelling obligation for data media with classification
- Guidelines for the organization of data storage
- Data privacy conform elimination of out of use data media with protocol
- Controlled storage of in use and swapped out data media in a secure area (Archive, secure cabinets)

E. Transmission Control:

Measures to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

Measures to ensure and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.

Measures to ensure, that an automated procedure for the retrieval of personal data is running a log procedure in order to have retrospect information which data has been retrieved by whom.

- Determination of authorized person for transmission and transport
- Documentation of the retrieval and transmission programs
- Determination and documentation of the transmission procedure and the data receivers
- Regulations and instructions for data media transport and transmission control
- Secured data lines

F. Input Control

Measures to ensure that it is possible to check and establish whether and by whom personal data / social data have been entered, modified or removed into/from data processing systems.

- Automatic protocol of input, modification and deletion of personal data
- Protocol of system generation and modification of system parameters
- Definition of deletion and retention periods for the protocols

G. Job Control

Measures to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal.

The following measures are relevant in case of sub-order for the subcontractor as well.

- Careful selection of the contractor (processor)
- Written agreement with definition of the decisional authority based on statutory mandatory law
- Outline of the rights and duties of principal and contractor in regard to:
- Data security measures
- Transmission directives
- Retention and deletion periods
- Breach of contract
- Insurance

- Definition of safety measures
- Right of access to subcontractor premises
- Control of security measures at the subcontractor
- Control of the correct execution of the contract
- Sanctions in case of contract violations

H. Availability Control

Measures to ensure that personal data is protected from accidental destruction or loss (e.g.: loss of power, lightning, protection from water damage)

- Ordinance of work instructions and safety directives
- Fire preventions
- Definition and control of fire precautions and fire/water early warning system
- Risk- and weak-point-analysis for relevant IT-division
- Regular and intense instruction of all employees
- Disaster recovery plan, emergency handbook, security-infrastructure
- Recovery-Procedures for production data
- Data mirroring
- Regular stringent data back up
- Formalized approval process for new IT-applications and in case of relevant changes of running applications
- Used software is checked and released in a formalized procedure
- Centralized procurement for hard- and software
- Database-Logging

I. Separation Control

Measures to ensure that data collected for different purposes can be processed separately.

- Stringent company internal directives for data collection, data processing and use of data
- Grant of specific access rights
- Use of separate user roles to ensure separation control
- Documentation of data bases

- Documentation of application programs
- Documentation of the specific purposes of the collection, processing and use of data
- Logical separation of data

ANNEX III

LIST OF SUB-PROCESSORS

This Appendix forms part of the Clauses and must be completed and signed by the parties. Sub-processors of Plivo, Inc. shall be updated or removed periodically and may be reviewed by the Data Exporter by visiting https://www.plivo.com/subprocessors/. The list of Sub-processors approved by the data importer as of the effective date of the DPA is as set forth below:
