Vivun Inc. - Data Processing Addendum

This Data Processing Agreement ("DPA") represents the Parties' agreement regarding the processing of Customer Personal Data (defined below by Vivun on behalf of Customer in order to carry out the Services and it is incorporated into and forms part of the Vivun's Master Services Agreement (the "Agreement"), as updated from time to time. Defined terms used in the DPA but not defined in this DPA shall have the same meaning in this DPA as are given to them in the Agreement.

1. Definitions

"Affiliate " means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity. Control " means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term " Controlled " will be construed accordingly.

"Customer Personal Data" means any Customer's Proprietary Information that is personal data and that is processed by Vivun on behalf of Customer in the course of providing the Services under the Agreement, as more particularly described in Schedule A of this DPA.

"Customer's Proprietary Information" or "Customer Data" means the proprietary content provided by Customer to Vivun or other Information belonging to Customer, that is provided to and processed by Vivun on behalf of Customer in the course of providing the Services under the Agreement, including personal data, that is not public knowledge and that is viewed as the property of the holder.

"Data Protection Laws" means all data protection and privacy laws and regulations applicable to the Customer Personal Data in question, including, where applicable, EU/UK Data Protection Laws.

“Data Systems” means information systems including, but not limited to, cloud-based systems, net-services, networks, computers, computer systems, communication systems and other information systems which may or may not be part of the Vivun software.

"EU/UK Data Protection Law" means: (i) the GDPR; (ii) the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "UK GDPR"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time.

“Vivun Affiliate” means the Affiliates of Vivun that may assist in the performance of the Services in accordance with this DPA.

“EEA” means the European Economic Area.

“GDPR” means the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (European Union General Data Protection Regulation).

“Vivun Software” or the “Software” is the software provided by Vivun as part of the Services.

"Permitted Affiliate" means any Affiliate of Customer which: (i) is the controller of Customer Personal Data; and (ii) is permitted to use the Service pursuant to the Agreement, but has not signed its own service agreement or Order Form with Vivun and is not a "Customer" as defined under the Agreement.

“Process”, “Processing” or “Processed” means any operation or set of operations which is performed upon Customer Proprietary Information including Personal Data, whether or not by automated means, according to the definitions given to such terms in the GDPR.

"Restricted Transfer" means: (i) where the GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

"Standard Contractual Clauses" means: (i) where the GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("UK SCCs").

“Security Breach” means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data transmitted, stored or otherwise processed by Vivun and/or its Sub-processors in connection with the provision of the Service.

"Security Breach" shall not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

“Services” means all services provided by Vivun in accordance with, and as defined in, the Agreement.

“Sub-processor” means any third party engaged by Vivun or Vivun Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA.

The terms “controller”, "data subject", “processor”, “processing”, “personal data” and "supervisory authority" shall have the meanings given to them in Data Protection Laws

or if not defined therein, the GDPR.

2. Roles and Scope of Processing

2.1 This DPA applies where and only to the extent that Vivun processes Customer Personal Data as a processor or sub-processor on behalf of the Customer in the course of providing Services pursuant to the Agreement.

2.2 Customer is the controller of the Customer Personal Data and is solely responsible for providing all required notices and obtaining all the necessary authorizations and approvals to enter, use, provide, store and process Customer Personal Data to enable Vivun to provide lawfully the Services. Customer shall, in its use of the Service and provision of instructions to Vivun, process Customer Personal Data in accordance with all laws and regulations.

Customer shall not disclose (and shall not permit any data subject to disclose) any special categories of personal data to Vivun for processing [except where and to the extent expressly disclosed in Schedule A of this DPA].

2.3 Customer, as the controller, hereby appoints Vivun as the processor in respect of all processing operations required to be carried out by Vivun on Customer Personal Data in order to provide the Services in accordance with the terms of the Agreement.

2.4 Vivun shall collect, retain, use, disclose, and otherwise process the Customer Personal Data only in accordance with documented instructions given by Customer for the for the following purposes: (i) processing in accordance with the Agreement; (ii) processing initiated by software users in their use of the Services; and (iii) processing to comply with other documented reasonable and lawful instructions provided by Customer (unless required by law to act without such instructions, in which case Vivun shall, except where prohibited by law from doing so, inform the Customer of that legal requirement before Processing). For these purposes, Customer instructs Vivun to process Customer Personal Data for the purposes described in Schedule A. The DPA and Main Agreement are Customer's complete and final instructions.

3. Sub-Processing

3.1. Customer acknowledges and agrees that Vivun and Vivun Affiliates may engage third-party Sub-processors to process Customer Personal Data on behalf of Vivun in connection with the provision of the Services.

3.2 A list of Vivun's current Sub-processors, their functions and locations, is available at https://static.vivun.com/privacy/Vivun_DPA_Subprocessors_EN.pdf ("Sub-processor List").

3.3 Customer may opt into notifications regarding any additions to the Sub-processor List by notifying Vivun at Legal@vivun.com. If Customer has elected to receiving these notifications, Vivun shall notify Customer of any proposed amendments to the Sub-processor List (including the addition or any replacement to the list) at least fifteen days prior to any such change.

3.4 Vivun will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of all Sub-processors it engages to provide the Services, that cause Vivun to breach any of Vivun’s obligations under this DPA.

4. Compliance with Laws

4.1 Each Party will comply with all applicable laws, including the Data Protection Laws applicable to it and binding on it in the performance of the Service, including all statutory requirements relating to data protection.

4.2 Customer acknowledges that Vivun is not responsible for determining the requirements of laws applicable to Customer’s business, clientele, or choice of markets, or that Vivun’s provision of the Services meet the requirements of such laws.

5. Security Responsibilities of Vivun

5.1 Vivun shall implement and maintain appropriate technical and organizational measures for ensuring the security of, and protecting the confidentiality and integrity of, Customer Personal Data and to ensure that Vivun’s processing of Customer Personal Data is in accordance with the requirements of the Data Protection Laws and protects the rights of Data Subjects. These measures ensure a level of security appropriate to

the risks presented by the nature of the processing activities having regard to the state of the art and the cost of their implementation.

5.2 Information relevant to how Vivun security measures are implemented and maintained is provided in the “Information Protection and Security Standard” document, attached hereto as Schedule B. Vivun reserves the right to make changes to the document to reflect technological developments provided, that such changes to not result in any degradation to the security of Customer Personal Data or the manner in which the Services is provided.

5.3 The technical and organizational measures implemented by Vivun include the following:

i. Vivun has implemented and will maintain appropriate procedures to ensure that unauthorized persons will not have access to Customer Personal Data and to the Data Systems used to process Customer Personal Data, and that any persons authorized to have access to Customer Personal Data will protect and maintain its confidentiality and security.

ii. Vivun has implemented and will maintain appropriate measures to ensure that all employees and contractors involved in the processing of Customer Personal Data are authorized personnel with a need to access the data, are bound by appropriate confidentiality obligations and have undergone appropriate training in the protection and handling of Personal Data.

5.4 Customer declares and confirms to have evaluated the security measures implemented by Vivun as providing an appropriate level of protection for the Customer Proprietary Information, taking into account the risk associated with the processing of such information.

6. Security Breach

6.1 If Vivun becomes aware of a Security Breach affecting Customer Personal Data, Vivun shall, without undue delay: (I) notify Customer of the Security Breach; and (II) take reasonable steps to mitigate the effects and to minimize any damage resulting

from the Security Breach.

6.2 In the event of a Security Breach, Vivun shall provide Customer with a reasonable assistance in dealing with the Security Breach, in particular in relation to making any notification to a supervisory authority or any communication to data subject, as required under Data Protection laws. In order to provide such assistance and taking into account the nature of the Services and the information available to Vivun, Vivun shall provide all such timely information as it becomes known or as is reasonably requested by Customer.

6.3 Customer agrees that Vivun's obligation to report or respond to a Security Breach under this Section is not and will not be construed as an acknowledgement by Vivun of any fault or liability of Vivun with respect to the Security Breach.

7. Subject Access Requests & Other Communications

Taking into account the nature of the Services, Vivun shall provide reasonable assistance to Customer, to allow the Customer to respond to (i) any request from a data subject to exercise any of its rights under applicable Data Protection Laws; and (ii) any other correspondence, inquiry or complaint received from a data subject, regulator or other third party in connection with the processing of Customer Personal Data.,. To the extent permitted by law, Vivun shall forward to Customer any such request, correspondence, enquiry or complaint it receives. Any cost arising from the provision of assistance by Vivun under this Section 7 shall be borne by Customer. Vivun shall provide an estimate of any such costs which shall be to be agreed in writing by the Parties.

8. Data, Retrieval & Destruction

8.1 Subject to Section 8.2, on termination of this DPA, Customer will uninstall, remove, or otherwise fully cease all interactions with all instances of the Services contemplated by this Agreement and the applicable Order Forms. Within One Hundred and Twenty days (120) following the termination of this agreement, the Receiving Party shall destroy all Disclosing Party Confidential Information (including all data contained within

the Services), provided that, no fewer than Forty Five (45) days prior to the termination of this agreement, the Disclosing Party elects to make a request of the Receiving Party to return, as directed by the Disclosing Party, all copies of Confidential Information (including all data contained within the Services) received pursuant to this Agreement, in which case, such destruction or return shall be completed within One Hundred and Twenty Days of the notified Party's receipt of the same. Notwithstanding the foregoing, neither party shall be obligated to erase or destroy Confidential Information that such party is required to retain under any applicable law, regulation or order (only during such required period of retention), or that is contained in an archived computer system backup made in accordance with such party's records retention, security and/or disaster recovery procedures, provided that such archived copy will (i) eventually be erased or destroyed in the ordinary course of such party's data processing procedures, and (ii) shall remain fully subject to the obligations of confidentiality stated herein until the earlier of the erasure or destruction of such copy, or the expiration of the confidentiality obligations set forth in this Agreement.

8.2 Customer acknowledges that the Services rely on Amazon Web Services (AWS), and that Vivun can only logically delete terminated Customer Proprietary Information stored in the Platform. Vivun will carry out the logical deletion within One Hundred and Twenty (120) days from the termination of the Agreement and will refrain from using Customer Personal Data for any other purpose during that period.

9. Information Security Assessment

9.1 Customer acknowledges that Vivun is regularly audited against ISO 27001 and SSAE 18 SOC1 and 2 standards by independent third auditors. Upon request, Vivun shall supply a summary copy of its audit report(s) to Customer, which reports shall be subject to the confidentiality provisions of the Agreement. In addition, upon Customer's request and on a confidential basis, Vivun will provide, no more than once per calendar year to Customer and its designees, all reasonably requested information necessary to demonstrate Vivun's compliance with Data Protection Laws.

9.2 Customer is responsible for reviewing the information made available by Vivun

relating to data security and making an independent determination as to the provisions of the DPA in relation to the provision of the Services meets Customer’s requirements and legal obligations, as well as the obligations under this DPA.

10. Processing locations

Customer acknowledges and agrees that Vivun may transfer and process Customer Personal Data to and in the United States and other locations in which Vivun, Vivun Affiliates or Vivun's Sub-processors maintain data processing operations. Vivun shall at all times ensure such transfers are made in compliance with the requirements of this DPA.

11. Europe

11.1 The terms in this Section 11 apply only if and to the extent Customer Personal Data is subject to EU/UK Data Protection Law.

11.2 Vivun shall notify Customer in writing, unless prohibited from doing so under EU/UK Data Protection Law if it becomes aware or believes that any data processing instruction from Customer violates applicable EU/UK Data Protection Law.

11.3 Vivun will enter into a written agreement with each Sub-processor imposing data protection obligations no less protective of Customer Personal Data as this DPA and to the extent applicable to the nature of the services provided by such Sub-processor.

11.4 Customer may object in writing to Vivun’s appointment of a new Sub-processor on reasonable grounds relating to data protection by notifying Vivun promptly in writing within 30 calendar days of receipt of any notice provided by Vivun in accordance with Section 3.3 and the parties shall discuss Customer's concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Vivun will, at its sole discretion, either (i) not appoint Sub-processor; or (ii) permit Customer to suspend or terminate the affected Service(s) in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination). In such

case, Vivun shall refund Customer for any prepaid unused portion of the affected Service(s).

11.5 To the extent Vivun is required under EU/UK Data Protection Law and Customer does not already have access to the relevant information, Vivun shall provide reasonably requested information regarding Vivun's processing of Customer Personal Data under the Agreement to enable Customer to carry out data protection impact assessments or prior consultations with supervisory authorities as required by EU/UK Data Protection Law. Any costs arising from the provision of assistance by Vivun under this Section 11.5 shall be borne by Customer. Vivun shall provide an estimate of any such costs which shall be agreed in writing by the Parties.

11.6 To the extent the transfer of Customer Personal Data from Customer to Vivun is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

11.6.1 In relation to Customer Personal Data that is protected by the GDPR, the EU SCCs will apply as follows:

(i) Vivun will be the "data importer" and Customer will be the "data exporter";

(ii) Module Two (Controller to Processor Clauses) will apply;

(iii) in Clause 7, the optional docking clause will apply;

(iv) in Clause 9, Option 2 will apply and the time period for prior notice of Sub-processor changes is identified in Section 3.3 of this DPA;

(v) in Clause 11, the optional language will not apply;

(vi) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
(vii) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(viii) Annex I shall be deemed completed with the information set out in Schedule A of this DPA; and

(ix) Annex II shall be deemed completed with the information set out in Schedule B of

this DPA.

11.6.2 in relation to Customer Personal Data that is protected by the UK GDPR or Swiss DPA, the EU SCCs as implemented under Clause 11.6.1 above will apply with the following modifications:

(i) references to "Directive 95/46/EC" or "Regulation (EU) 2016/679" are interpreted as references to the UK GDPR or the Swiss DPA (as applicable);

(ii) references to specific Articles of "Regulation (EU) 2016/679" are replaced with the equivalent article or section of the UK GDPR or Swiss DPA (as applicable);

(iii) references to "EU", "Union" and "Member State," are replaced with "UK" and "Switzerland" (as applicable);

(iv) Clause 13(a) and Part C of Annex II are not used and references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the "Information Commissioner" and the "courts of England and Wales" or the "Swiss Federal Data Protection and Information Commissioner" and the "relevant courts of Switzerland" (as applicable);

(v) in Clause 17, the EU SCCs are governed by the laws of England and Wales or Switzerland (as applicable); and

(vi) in Clause 18(b), disputes will be resolved before the courts of England and Wales or Switzerland (as applicable).

11.6.3 to the extent that and for so long as the EU SCCs as implemented in accordance with Clause 11.6.2 above cannot be used to lawfully transfer Customer Personal Data in accordance with the UK GDPR to Vivun, the UK SCCs shall be incorporated into and form an integral part of this DPA and shall apply to transfers governed by the UK GDPR. For the purposes of the UK SCCs, the relevant annexes, appendices or tables of the UK SCCs shall be deemed populated with the information set out in Schedule A and Schedule B (as applicable) of this DPA.

11.7 The rights and obligations afforded by Standard Contractual Clauses will be

exercised in accordance with this DPA, unless stated otherwise. It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict.

11.8 For the purposes of Clause 15(1)(a) of EU SCCs, Vivun shall notify Customer and not the data subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the data subject, as necessary.

11.9 To the extent Vivun adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses adopted pursuant to Data Protection Laws) for the transfer of Customer Personal Data ("Alternative Transfer Mechanism"), the Alternative Transfer Mechanism shall automatically apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with EU/UK Data Protection Law and extends to territories to which Customer Personal Data is transferred).

12. Nondisclosure

Customer agrees that the details of this DPA are not publicly known and constitute Vivun's Confidential Information under the confidentiality provisions of the Agreement. If the Agreement does not include a confidentiality provision protecting Vivun Confidential Information and Customer and Vivun or its Affiliates do not have a non-disclosure agreement in place covering this DPA, then Customer will not disclose the contents of this DPA to any third party except as required by law.

13. Permitted Affiliates

When a Permitted Affiliate becomes a party to the DPA, then such Permitted Affiliate shall be entitled to exercise its rights and remedies available under this DPA to the extent required under Data Protection Laws. However, if Data Protection Laws requires the Permitted Affiliate to directly exercise a right or remedy against Vivun directly by itself, the parties agree that to the extent permitted under law: (i) only the Customer

that is the contracting entity to the Agreement shall exercise any such right or seek any such remedy on behalf of the Permitted Affiliate; and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA in a combined manner for all of its Permitted Affiliates together, instead of doing so separately for each Permitted Affiliate. The Customer that is the contracting entity is responsible for coordinating all communication with Vivun under the DPA and be entitled to make and receive any communication related to this DPA on behalf of its Permitted Affiliates.

14. Liability

14.1 Vivun's and all of Vivun Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA (including the Standard Contractual Clauses) and all data processing agreements between Customer, Permitted Affiliates and Vivun, whether in contract, tort, or under any other theory of liability, is subject to the limitations and exclusions of liability under the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement, this DPA and the Standard Contractual Clauses.

14.2 Vivun's and Vivun Affiliates' total liability for all claims from Customer and all Permitted Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all data processing agreements established under this DPA or the Agreement, including by Customer and all Permitted Affiliates, and shall not be understood to apply individually and severally to Customer and/or to any Permitted Affiliate that is a contractual party to any such DPA. Each reference to the DPA herein means this DPA including its schedules, attachments, or terms incorporated by reference.

15. California Consumer Privacy Act

15.1 The terms in this Section 15 apply only if and to the extent Customer Personal Data is subject to the California Consumer Privacy Act, California Civil Code §

1798.100 et seq. (as may be amended, modified, or supplemented from time to time, and together with any implementing regulations, “CCPA”.

15.2 Customer and Vivun are are referred to within this section collectively as the “Parties”, and each, individually, as a “Party”. All terms used but not defined in this CCPA Addendum shall have the meaning set forth in the CCPA.

a. “California resident” has the meaning given to such term under Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017
b. “Personal Information” has the meaning given to such term under the CCPA.
c. “Collection” has the meaning given to such term under the CCPA
d. “Sensitive personal information” has the meaning given to such term under the CCPA.
e. “Service Provider” has the meaning given to such term under the CCPA.
f. “Sell” has the meaning given to such term under the CCPA. “Share” has the meaning given to such term under the CCPA.

15.3 Vivun acknowledges and agrees that it is required to assist Customer through appropriate technical and organizational measures in complying with certain requirements under subdivisions (d) through (f) of Section 1798.100 of the CCPA, which include: (1) acknowledging that the California PI is being disclosed by Customer only for limited and specified purposes set forth in this CCPA Addendum or the Agreement; (2) Vivun agreeing to comply with the applicable obligations of the CCPA and provide at least the level of privacy protections as are required by the CCPA; (3) acknowledging and agreeing that Customer has the right to take reasonable and appropriate steps to help to ensure that Vivun uses the California PI in a manner consistent with Customer’s obligations under the CCPA; (4) Vivun agreeing to notify Customer if Vivun makes a determination that it can no longer meet its obligations under this Section; and (5) acknowledging and agreeing that Customer has the right, upon notice, including under this Section 2(3) above, to take reasonable and appropriate steps to stop and remediate unauthorized use of California PI.

15.4. Vivun will reasonably assist Customer with any data subject access, erasure or opt-out requests and objections. If Vivun receives any request from data subjects, authorities, or others relating to its data processing, Vivun will without undue delay inform Customer and reasonably assist Customer with developing a response (but Vivun will not itself respond other than to confirm receipt of the request, to inform the data subject, authority or other third party that their request has been forwarded to Customer, and/or to refer them to Customer, except per reasonable instructions from Customer). Vivun will also reasonably assist Customer with the resolution of any request or inquiries that Customer receives from data protection authorities relating to Vivun, unless Vivun elects to object such requests directly with such authorities.

15.5 Unless otherwise indicated, any reference herein to the CCPA or provisions thereof shall be construed as a reference thereto as amended, modified, varied, restated, supplemented or re-enacted from time to time or as a reference to any successor thereto and all rules and regulations promulgated thereunder.

16. Miscellaneous

16.1 Notwithstanding the foregoing and anything to the contrary in the Agreement (including this DPA), Customer acknowledges that Vivun shall have a right to process Customer Personal Data or data related to Customer's use of the Service for the purposes of creating anonymized, aggregate and/or de-identified information for its own legitimate business purposes, including but not limited to improve and develop the Service.

16.2 This DPA supersedes and replaces all prior representation, understanding, communications and agreements between the Parties in relation to the matter of this DPA.

16.3 As between Customer and Vivun, this DPA is incorporated into and subject to the terms of the Agreement and shall be effective and remain in force for the term of the Agreement or the duration of the Service. Except for the changes made by this DPA,

the Agreement remains unchanged and in full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Customer Personal Data.

16.4 In no event shall this DPA benefit or create any right or cause of action on behalf of a third party, but without prejudice to the rights or remedies available to data subjects under Data Protection Laws or this DPA (including the Standard Contractual Clauses).

16.5 Each party acknowledges that the other party may disclose the Standard Contractual Clauses, this DPA, and any privacy related provisions in the Agreement to any regulator or supervisory authority upon request.

16.6 Notwithstanding anything to the contrary in the Agreement, Vivun may periodically make modifications to this DPA as may be required to comply with Data Protection Laws.

16.7 Other than as required by applicable Data Protection Laws or the Standard Contractual Clauses, the dispute mechanisms, including those related to venue and jurisdiction, set forth in the Agreement govern any dispute pertaining to this DPA.

Schedule A to the DPA

Description of the Processing Activities / Transfer

List of Parties	
Data Exporter	Data Importer
Name: The party identified as the "Customer" in the Agreement	Name: Vivun, Inc. ("Vivun")
Address: The address associated with the Vivun account or as otherwise specified in the Agreement.	Address: 1954 Mountain Blvd #13246, Oakland, CA 94611)

Contact Person's Name, position and contact details: The contact details associated with the Customer's account, or as otherwise specified in the DPA or Agreement.	Contact Person's Name, position and contact details: The contact details associated with the Customer's account, or as otherwise specified in the DPA or Agreement.
Activities relevant to the transfer: See Annex 1(B) below	Activities relevant to the transfer: See Annex 1(B) below
Signature and date: See front end of Agreement	Signature and date: See front end of Agreement
Role: Controller	Role: Processor

Description of Transfer	
Categories data subjects	Customer may submit Customer Personal Data to Vivun, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to: (i) clients, customers and prospects of Customer (each a "Client"); (ii) business partners, (iii) vendors and (iv) end-users.
Purposes of the transfer(s)	Processing: (i) to provide the Service in accordance with the Agreement; (ii) to perform any steps necessary for the performance of the Agreement; (iii) initiated by Customer and its end-users in its use of the Service; and (iv) to comply with other reasonable instructions provided by Customer (e.g., via email or support tickets) that are consistent with the terms of the Agreement (individually and collectively, the "Purpose").
Categories of personal data	Customer may submit Customer Personal Data to Vivun, the extent of which is determined and controlled by Customer in its sole discretion [and may vary depending on the Service] but which may include, but is not limited to identification and contact data (name, address, title, contact details); employment details (employer, job title, geographic location, area of responsibility, employer financial information); or any other personal data elements contained within Customer Data that Customer chooses to input into or otherwise provide to the Service.
Frequency of the transfer.	The Customer Personal Data will be transferred in accordance with the Customer's instructions as described in this DPA.
Sensitive data (if appropriate)	N/A. Customer is prohibited under the Agreement from submitting special category data to the Service.
Duration of processing:	Term of the Agreement plus the period from the expiry of the Agreement until deletion of Customer Personal Data in accordance with the terms of the Agreement (including the DPA or as otherwise instructed by Customer.
Subject matter of the processing:	The subject matter of the processing is the Customer Personal Data processed by Vivun to provide the Service.

Nature of the Processing:	[Customer Personal Data transferred will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities: (i) storage and other processing necessary to provide, maintain and improve the Service (as applicable) provided to Customer as instructed by Customers or its end-users; and/or (ii) disclosures in accordance with the Agreement and/or as compelled by applicable laws.]
Retention period (or, if not possible to determine, the criteria used to determine that period):	[Vivun will retain Customer Personal Data for the term of the Agreement and any period after the termination of expiry of the Agreement during which Vivun processes Customer Personal Data.]

Competent supervisory authority
The Data Exporter's competent supervisory authority will be determined in accordance with the GDPR. With respect to Personal Data protected by UK GDPR, the competent supervisory authority is the Information Commissioners Office (the "ICO").

Schedule B

Technical and Organizational Security Measures

Description of the technical and organizational measures implemented by the processor(s) / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Measure	Description
Measures of pseudonymization and encryption of personal data	Data is encrypted in transit with TLS 1.2+. As applicable, data is encrypted at rest with native AWS solutions such as Key Management Service (KMS).
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Vivun uses vulnerability assessment, patch management, threat prevention and on-going monitoring procedures, processes and policies to identify, detect and mitigate against identified security threats, risks and malicious code.
Measures for ensuring the	A resilient Platform architecture is deployed by leveraging AWS features. Critical Platform

ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	components are replicated across multiple AWS Availability Zones, each of them designed as an independent failure zone. This capability is leveraged by balancing the architecture components between two AWS Availability Zones to keep the system operational, even if one Availability Zone stops working. Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Vivun performs external, independent penetration testing at least annually with a firm that has a strong reputation within the security industry and internally, as a significant change has been made to applications or infrastructure services. Additionally, we perform continuous vulnerability scans and assessments on production assets.
Measures for user identification and authorisation	Vivun uses logical access controls to manage access to data and systems based on access levels, job roles and data classification.
Measures for the protection of data during transmission	All communication between Vivun Servers and Connected Applications is encrypted in transit. Vivun uses secure TLS protocols (1.2 and above) and strong cipher suites to ensure your organization’s data is protected as it moves in and out of Vivun.
Measures for the protection of data during storage	Data is encrypted at rest, secured by FIPS 140-2 certified hardware security modules (HSMs) via Amazon Key Management Service (KMS).
Measures for ensuring physical security of locations at which personal data are processed	Vivun relies on Amazon AWS and Salesforce, both of whom are responsible for implementing controls for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.
Measures for ensuring events logging	Vivun production servers and systems are configured to log access related events and send logs to a centralized logging repository, and monitoring tools are in place in order to analyze the systems for possible or actual security breaches. The logging and monitoring tools used are configured to provide e-mail alerts to appointed personnel when suspicious activity is detected.
Measures for ensuring system configuration, including default configuration	Vivun uses configuration management processes and tools to deploy, enforce and monitor configurations to systems.
Measures for internal IT and IT security governance and management	Vivun Inc. maintains an information security management system (“ISMS”), which is aligned to and self-assessed against NIST 800-53. Within this framework, Vivun has defined an information security program implementing, in accordance with NIST 800-53, policies, procedures, administrative and technical safeguards to minimize security risks, through risk assessment, and to

	protect its customers' data against accidental or unlawful loss, access or disclosure or other misuse. The information security program includes the following measures.
Measures for certification/assurance of processes and products	Vivun Security and Compliance team regularly reviews its processes on an annual / as-needed basis. Vivun undergoes a SOC2 Type 2 audit annually to ensure effectiveness of Vivun security controls, operations and policies.
Measures for ensuring data minimisation	Vivun data classification, data handling, and data destruction policies and procedures describe the relevant controls to ensure data privacy and protections. Customer data is protected with least privilege access and handled with appropriate operational controls.
Measures for ensuring data quality	Vivun uses change management procedures and auditing mechanisms to test, approve, and monitor changes to Vivun services and infrastructure.
Measures for ensuring limited data retention	We will retain your information for the period necessary to fulfill the purposes outlined in this Policy unless a longer retention period is required or permitted by law. When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize it, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.
Measures for ensuring accountability	Vivun has a dedicated Security department, where the CISO reports directly to the CEO to ensure unfiltered visibility and analysis of risks. The Security department is charged with holding the company, departments and services to achieve the security policies, processes and compliance goals. The security department shall accomplish these objectives by the following mechanisms: Security Operations and Engineering team is responsible for threat detection, incident response and cloud, network and host security. Governance Compliance and Risk Management team is responsible for customer assurance, governance, risk and compliance across our internal, SOC 2 and ISO requirements. Product and Application Security team is responsible for ensuring Vivun's products are secure.
Measures for allowing data portability and ensuring erasure	Data (privacy) request processes are in place to handle termination, erasure or removal of data.

Schedule C

Transfer Impact Assessment

Description of the technical and organizational measures implemented by the processor(s) / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Relevant Laws			
Law	Description	Data importer's experience from prior five years.	Industry experience from prior five years.
Section 702 of the Foreign Intelligence Surveillance Act ("S702 FISA")	S702 FISA is a federal law that allows US government agencies to conduct targeted surveillance of foreign persons located outside the US with the compelled assistance of electronic communications service providers ("ECSPs") within the meaning of 50 U.S.C § 1881(b)(4). This includes "electronic communication service providers" and "remote computing service providers" as defined under 18 U.S.C. § 2510 and 18 U.S.C. § 2711, telecommunications carriers as defined under 47 U.S.C. §153, other communication service providers that have access to wire or electronic communications, and other relevant entities that are officers, employees or agents of the foregoing.	To date, Vivun has never received any government agency requests for access to personal data from Europe under S702 FISA.	Like most US-based cloud computing providers, sales intelligence platforms such as Vivun may technically qualify as "electronic communications service providers" within the scope of S702 FISA and therefore US government authorities could (at least theoretically) compel access to personal data that we process. However, sales intelligence platforms such as Vivun do not generally deal in the type of data that is of interest to US intelligence agencies. As detailed in the US Department of Commerce's white paper titled "Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II", companies whose European operations involve data transfers limited to commercial information (such as employee, customer, prospect, or sales records) are not the target of US intelligence and counter-terrorism agencies.
Executive Order 12333 ("EO 12333")	EO 12333 authorizes and governs the circumstances in which US intelligence agencies can engage in foreign intelligence surveillance outside the US. It authorizes collection of the content of communications of foreign communications that occur outside the US in the course of a lawful foreign intelligence investigation.	Vivun is not aware of any direct access to personal data	As noted above, sales-intelligence platforms such as Vivun do not process data that is the target of US intelligence and counter-terrorism agencies

	Unlike S702 FISA, EO 12333 does not rely on the compelled assistance of electronic communications service providers but appears to rely on exploiting vulnerabilities in telecommunications infrastructure.	originating from Europe under EO 12333	

Factors Potentially Impacting Disclosure to Public Authorities		
Circumstances	Description	Impact on government access risk
Services Offered by Data Importer	*See Schedule 1 EU SCC, Annex I.B*	N/A: As outlined above, sales intelligence platforms such as Vivun are unlikely to be the targets of US intelligence and counter-terrorism agencies
Personal Data Transferred	*See Schedule 1 EU SCC, Annex I.B*	N/A: As noted above, the personal data processed by Vivun is unlikely to be the target of US intelligence and counter-terrorism agencies
Length of Processing Chain (is there another entity involved before it gets to data importer)	Transfers are affected from Salesforce to AWS, with any sub-processing outlined per https://static.vivun.com/privacy/Vivun_DPA_Subprocessors_EN.pdf	Low
Onward Transfers by Data Importer	The sub-processors used by data importer as part of its normal and ordinary course of business are identified at https://static.vivun.com/privacy/Vivun_DPA_Subprocessors_EN.pdf.	Low
Transmission Channel of Data	Personal data may be transmitted through a variety of industry standard channels, including HTTPS/TLS	(Presumed Low – see supplied security framework and documentation)
Format of Transferred Data	Encrypted (see above)	Low
Purpose of Processing	*See Schedule 1 EU SCC, Annex I.B*	Low
Economic Sector Involved	Contingent on Client Activities	N/A

Storage Location	Amazon Web Services US-WEST REGION	Low

Additional Factors that May Be Relevant		
Circumstances	Description	Impact on Government Access Risk (increase, decrease, neutral)
Does the Destination Country Have Comprehensive Data Protection Law?	The USA does not have comprehensive data protection law that applies to government authorities. However, there are various laws that govern the collection, use and disclosure of personal information by US federal and state governments. For example, the Privacy Act establishes a code of fair information practices regarding the use of personal information by federal agencies. In the context of USG surveillance activities, there are a number of protections and safeguards that apply to USG collection and use of data in connection with security and surveillance. Some of these are found in the laws that authorize such activities, others in other legislation or directives. For example, PPD-28 is a presidential directive that imposes restrictions on signals intelligence activities by US intelligence agencies, including those conducted under FISA 702 and EO 12333. However, in the Schrems II judgment the CJEU held that the protections afforded by PPD-28 are not sufficient to ensure an adequate level of protection for personal data under the GDPR. As regards, transfers, the USA does not have a generally applicable law (equivalent to Chapter V of the GDPR) that restricts the transfer of personal data to third countries. Generally speaking, while the United States do not have a comprehensive privacy law similar to the GDPR, many states have enacted or are in the process of enacting comprehensive privacy laws that provide similar protections and privacy rights to individuals (e.g., CCPA/CPRA in California)	Low
Does the Destination Country Have an Independent Data Protection Authority?	The US does not have a single independent supervisory authority responsible for ensuring and enforcing compliance with data protection rules or with assisting and advising individuals in the exercise of their data protection rights. However, a variety of authorities at the state and federal level are responsible for rulemaking and enforcing compliance with sectoral data protection rules.	Low
Is the Destination County a Party to Any Relevant International	The United States adheres to international instruments on data protection standards, such as the Universal Declaration of Human Rights, and participates in the APEC Cross-Border Privacy Rules (CBPR) privacy certification program.	Low

Instruments / Treaties?		
Can Data Subjects Seek Judicial Redress for Violation of Their Privacy Rights?	Generally, yes to the extent the information is sought to be used against the individual in a criminal proceeding, although in some cases a defendant may lack standing or sufficient information to effectively seek redress. Note that the CJEU held in the Schrems II judgement that European data subjects lack an adequate right of redress in connection with data that is accessed by the U.S. government under FISA 702 and EO 12333, as the latter do not confer rights which are enforceable against the US authorities (and, in particular, data subjects may lack standing under US law to challenge activities authorized under FISA 702 and EO 12333).	Low
Will the Data Importer Document Requests for Access to the Data Processed in Providing the Services?	Yes, and will notify and cooperate with customer per DPA terms.	Low
Does the Data Importer Publish Transparency Reports? If so, how often?	No – however, as mentioned above, to this date, Vivun has not received any access request from a public authority	Low
Does the Data Importer Have a Policy for Processing Law Enforcement Requests?	Yes – Policy is for Vivun to review all incoming request with council, notify and cooperate with information security teams and customer per DPA terms	Low