ASORA DATA PROCESSING AGREEMENT

Last Modified: 4 October 2022

We update these terms from time to time. If you have an active Asora subscription, we will let you know when we do via email.

The term of this DPA will follow the term of the Agreement.

BETWEEN

(1) **Customer** (as defined in the Master Terms and hereafter referred to as the "**Controller**", "**you**" or "**your**"); and

(2) **Asora Technologies Limited** t/a Asora, company number 706300 with its registered office at 20 Hatch Street Lower, Dublin, DUBLIN, D02 XH02, Ireland (hereafter referred to as the "**Processor**", "**our**", "**us**" or "**we**").

(each a "**Party**" and together the "**Parties**")

A. The Processor is engaged to carry out services on behalf of the Controller pursuant to the Agreement.

B. The Processor's provision of these services to the Controller necessitates the processing of personal data on behalf of the Controller by the Processor. This data processing agreement which is intended to be read in conjunction with the Agreement sets out the terms upon which the Processor must process Customer Data for and on behalf of the Controller.

IN CONSIDERATION of the mutual benefit to the Parties of the arrangements referred to in this Data Processing Agreement and for other valuable consideration pursuant to the Agreement **IT IS AGREED** as follows:

1 DEFINITIONS

1.1 In this DPA the following expressions, shall, unless the context otherwise requires have the following meanings:

Agreement	means the agreement between the Parties which governs the Controller's use of the Processor's services. It consists of the following documents: Master Terms; Product Specific Terms; this DPA; and any Order Form(s) entered into between the Parties.

Customer Data	means personal data processed by the Processor on behalf of the Controller in connection with the performance by the Processor of its obligations under the Agreement, as more particularly set out in Appendix 1;
Data Protection Laws	means applicable data protection and privacy laws including the Data Protection Acts 1988 to 2018, the General Data Protection Regulation ((EU) 2016/679) ("GDPR") and the European Communities (Electronic Communications Networks and Services)(Privacy and Electronic Communications) Regulations 2011;
DPA	means this data processing agreement;
Effective Date	means the date you enter into the Agreement with Processor;
Instructions	means the written, documented instructions of the Controller contained in the Agreement;
Sub-Processor	means any processor engaged by us or our Affiliates to assist in fulfilling our obligations with respect to the provision of the services under the Agreement. Sub-Processors may include third parties or our Affiliates but will exclude any of our employees or consultants.

1.2 In this Agreement unless the context requires: (a) the terms "**controller**"; "**data subject**"; "**personal data**"; "**personal data breach**", "**processor**", "**processing**" (and derivatives of this term) and "**supervisory authority**" each have the meaning given under the GDPR; (b) headings will not affect the interpretation of this Agreement; (c) any reference to any statute, statutory provision, order, decision or regulation shall be construed as a reference to that statute, statutory provision, order, decision or regulation as extended, modified, replaced or re-enacted from time to time and all statutory instruments, regulations and orders from time to time made thereunder or deriving validity therefrom; (d) phrases introduced by the terms "including", "include" or any similar expression will not limit the sense of the words preceding those terms; and (e) words in the singular include the plural and words in the plural include the singular.

1.3 In the event of a conflict or inconsistency between any provision in this DPA and any provision in the Master Terms, Product Specific Terms or any Order Form entered into between the Parties, this DPA will take precedence to the extent of such conflict or inconsistency.

1.4 In this DPA all terms that are capitalised and not defined here shall have the meaning given to them in the Master Terms.

2 DATA PROCESSING PROVISIONS

2.1 The Parties acknowledge and agree that:

2.1.1 for the purposes of the Data Protection Laws and the Agreement, Controller is the controller and Processor is a processor of Customer Data; and

2.1.2 Appendix 1 sets out the scope, nature and purpose of the processing by Processor of Customer Data, the duration of the processing and the types of personal data and categories of data subject involved.

3 CONTROLLER RESPONSIBILITIES

3.1 Compliance with Laws. Within the scope of the Agreement and in its use of the Subscription Services provided by Processor under the Agreement, the Controller will be responsible for complying with all requirements that apply to it under Data Protection Laws with respect to its processing of Customer Data and the Instructions it issues to the Processor.

3.2 In particular but without prejudice to the generality of the foregoing, the Controller acknowledges and agrees that it will be solely responsible for: (i) the accuracy of, quality of, and legal basis used to process Customer Data and the means by which the Controller acquired Customer Data; (ii) complying with all necessary transparency and lawfulness requirements under Data Protection Laws for the collection and use of the Customer Data, including obtaining any necessary consents and authorisations (particularly for use by the Controller for marketing purposes); (iii) ensuring the Controller has the right to transfer, or provide access to, the Customer Data to the Processor for processing in accordance with the terms of the Agreement (including this DPA); and (iv) ensuring that its Instructions to the Processor regarding the Processing of Customer Data comply with applicable laws, including the Data Protection Laws. The Controller will inform the Processor without undue delay if the Controller is not able to comply with its responsibilities under clauses 3.1 and 3.2 or the Data Protection Laws.

3.3 Controller Instructions. The Parties agree that the Agreement (including this DPA), together with the Controller's use of the Subscription Service in accordance with the Agreement, constitute the Controller's complete Instructions to the Processor in relation to the processing of Customer Data, so long as the Controller may provide additional instructions during the Subscription Term that are consistent with the Agreement. The Controller shall authorise the Processor to process the Customer Data in any manner that may reasonably be required in order to provide the Subscription Services.

3.4 Security. The Controller is responsible for independently determining whether the data security provided for in the Subscription Service adequately meets the Controller's obligations under applicable Data Protection Laws. The Controller is also responsible for ensuring secure use of the Subscription Service, including protecting the security of Customer Data in transit to and from the Subscription Service (including to securely backup or encrypt any such Customer Data).

3.5 Warranties. The Controller warrants that:

3.5.1 its current Instructions to the Processor for the processing of Customer Data are contained in this Agreement;

3.5.2 any Instructions that it issues to the Processor shall comply with Data Protection Laws; and

3.5.3 it is entitled to transfer the Customer Data to the Processor and has complied with its obligations under Data Protection Laws to enable it to do so.

4 PROCESSOR OBLIGATIONS

4.1 Compliance with Instructions. The Processor will only process Customer Data for the purposes described in the Agreement or as otherwise agreed within the scope of the Controller's lawful Instructions, except where and to the extent otherwise required by applicable law. The Processor is not responsible for compliance with any Data Protection Laws applicable to the Controller or to the Controller's industry that are not generally applicable to the Processor. The Processor will inform the Controller if in its opinion an instruction issued by the Controller infringes Data Protection Laws.

4.2 Conflict of Laws. If the Processor becomes aware that it cannot process Customer Data in accordance with the Controller's Instructions due to a legal requirement under any applicable law, the Processor will (i) promptly notify the Controller of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all processing (other than merely storing and maintaining the security of the affected Customer Data) until such time as the Controller issues new Instructions with which the Processor is able to comply. If this provision is invoked, the Processor will not be liable to the Controller under the Agreement for any failure to perform the applicable Subscription Services until such time as the Controller issues new lawful Instructions with regard to the processing.

4.3 Security. The Processor will implement and maintain appropriate technical and organisational measures to protect Customer Data from personal data breaches, as described under Appendix 2 to this DPA ("**Security Measures**"). Notwithstanding any provision to the contrary, the Processor may modify or update the Security Measures at its discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

4.4 Confidentiality. The Processor will ensure that any personnel whom it authorises to process Customer Data on its behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Customer Data.

4.5 Personal Data Breaches. The Processor will notify the Controller without undue delay after Processor becomes aware of any verified personal data breach and will provide timely information relating to the personal data breach as it becomes known or reasonably requested by the Controller. At the Controller's request, Processor will

promptly provide the Controller with such reasonable assistance as necessary to enable the Controller to notify relevant personal data breaches to competent supervisory authorities and/or affected data subjects, if the Controller is required to do so under Data Protection Laws.

4.6 Deletion or Return of Customer Data. Processor will delete or return all Customer Data (including copies thereof) processed pursuant to this DPA, on termination or expiration of the Controller's Subscription Service in accordance with the procedures set out in our Product Specific Terms. This term shall apply except where the Processor is required by applicable law to retain some or all of the Customer Data. The Controller may request the deletion of the Controller Asora account after expiration or termination of the Subscription Service. The Controller may also cancel their account in accordance with the 'Early Cancellation' section of the Master Terms and request permanent deletion of Customer Data. The Controller may retrieve its Customer Data from its account in accordance with the 'Retrieval of Customer Data' section of our Product Specific Terms.

4.7 The Processor, taking into account the nature of processing of Customer Data and the information available, will provide assistance to the Controller at the Controller's cost in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR.

4.8 The Processor will make available to the Controller on request (acting reasonably) all information necessary to demonstrate compliance by the Processor as processor of Customer Data with the obligations laid down in Article 28 of the GDPR and allow for audits of the processing of Customer Data, including inspections, conducted by Customer or another auditor mandated by the Controller. These audits or inspections must be carried out during Processor's normal working hours, and may occur only once in any 12-month period and in accordance with the following conditions:

(a) The Controller must inform the Processor of its intention to carry out the audit or the inspection at least thirty (30) calendar days before the audit or inspection takes place;

(b) The Controller shall ensure that

(i) no damage of any nature whatsoever (to property or persons),

(ii) no disturbance or discontinuity of the Processor's activities,

will take place during the audit or inspection;

(c) Controller shall ensure that the persons carrying out the audit or inspection or having access to information relating to this audit or inspection are subject to an appropriate confidentiality obligation regarding this audit or inspection;

(d) only the systems, premises and equipment used by the Processor during its processing of the Customer Data to fulfil its obligations under the Agreement may be subject to audit or inspection; and

(e) the costs and charges incurred by the audit or inspection shall be the sole responsibility of the Controller.

5 DATA SUBJECT REQUESTS

5.1 To the extent that the Controller is unable to independently address a request from a data subject to exercise their rights under Data Protection Laws ("**Data Subject Request**") through the Subscription Service, then upon the Controller's written request the Processor will provide reasonable assistance to the Controller to respond to any Data Subject Requests or requests from supervisory authorities relating to the processing of Customer Data under the Agreement. The Controller shall reimburse the Processor for the commercially reasonable costs arising from this assistance.

5.2 If a Data Subject Request or other communication regarding the processing of Customer Data under the Agreement is made directly to the Processor it will promptly inform you and will advise the data subject to submit their request to the Controller. You will be solely responsible for responding substantively to any such Data Subject Requests or communications involving Customer Data.

6 SUB-PROCESSORS

6.1 The Controller agrees that the Processor may engage Sub-Processors to process Customer Data on the Controller's behalf. The Processor has appointed, as Sub-Processors, the Asora Affiliates and third parties listed in Appendix 3 to this DPA.

6.1.1 Where the Processor proposes to appoint a new Sub-Processor the Processor will notify the Controller of its intention to make such an appointment.

6.1.2 The Processor will give the Controller the opportunity to object to the engagement of new Sub-Processors on reasonable grounds relating to the protection of Customer Data, such objection to be made to the Processor within thirty (30) days of the notification pursuant to Clause 6.1.1.

6.1.3 Where such an objection is made, the Parties will discuss the Controller's concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, the Processor will, at its sole discretion, either:

(a) not appoint the new Sub-Processor; or

(b) permit the Controller to suspend or terminate the affected Subscription Service in accordance with the termination provisions of the Agreement without liability to either Party.

6.2 Where the Processor engages Sub-Processors, the Processor will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Customer Data as those in this DPA (including, where appropriate, the

Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors. The Processor will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of our obligations under this DPA.

7 DATA TRANSFERS

7.1 The Processor shall not transfer or otherwise process Customer Data outside of the European Economic Area unless the prior written consent of the Customer has been obtained, such consent not to be unreasonably withheld, conditioned or delayed.

8 LIABILITY

8.1 Nothing in this Agreement shall operate to exclude or limit either Party's liability for:

(a) death or personal injury caused by its negligence;

(b) fraud; and/or

(c) any other liability which cannot be excluded or limited under applicable law.

8.2 The Controller shall remain solely and fully liable for any damage which a data subject may suffer as a result of the processing of their Customer Data which is under the Customer's control and which does not result from a breach by the Processor of its obligations under this DPA and/or Data Protection Laws. The Controller acknowledges and agrees that the Processor shall not be liable in the event that any failure to comply with its obligations is caused by or results from the acts or omissions of the Controller (or its Affiliates, officers, employees, agents or contractors) in which case the Controller shall be fully liable.

8.3 Each Party acknowledges and agrees that in respect of a Party's liability under this Agreement and/or under Data Protection Laws:

(a) neither Party shall be liable to the other Party for any indirect or consequential loss or damage;

(b) nothing in this Agreement relieves the Parties of their own direct responsibilities and liabilities as controller or processor (as applicable) under Data Protection Laws.

8.4 Subject to clauses 8.1, 8.2 and 8.3, the Processor's aggregate liability in respect of claims based on events in any calendar year arising out of or in connection with this DPA in contract or tort (including negligence) or otherwise, shall in no circumstances exceed the total fees paid by Controller to Processor under the Agreement during the twelve (12) month period immediately preceding the earliest act or omission giving rise to such liability.

8.5 Subject to clauses 8.1, 8.2 and 8.3 the Controller agrees to indemnify and keep indemnified and hold harmless the Processor fully and effectively against all losses, costs, claims, demands, actions, proceedings, fines, penalties, awards, liabilities, damages, compensation, settlements, expenses and/or professional costs including legal fees and/or charges which the Processor may sustain or incur as a result of any breach of the provisions of the DPA.

9 GENERAL PROVISIONS

9.1 Amendments. Notwithstanding anything else to the contrary in the Agreement and without prejudice to the Clauses 3.3 or 4.3 of this DPA, Processor reserves the right to make any updates or changes to this DPA and the terms that apply in the 'Amendment; No Waiver' section of the Master Terms will apply.

9.2 Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

9.3 Governing Law. This DPA shall be governed by and construed in accordance with the laws of Ireland and the Parties hereby agree that the Courts of Ireland are to have exclusive jurisdiction to settle any disputes, which may arise out of or in connection with this DPA provided that nothing in this DPA shall operate to prevent a Party from seeking interim, protective or provisional relief in the courts of any state.

APPENDIX 1

DETAILS OF PROCESSING

This Appendix describes the subject-matter and the duration of the processing of Customer Data to be carried out by Processor on behalf of Controller, the nature and purpose of such processing, the type of personal data and the categories of data subject involved.

Subject matter of processing	The provision of the Subscription Service, including all services included in your chosen subscription plan and any other services made available by us to you through our website or otherwise.
Duration of processing	The duration during which Processor is to provide the Subscription Services.
Nature and purpose of the processing	Asora will process Customer Data as necessary to perform the Subscription Services and to perform its other obligations under the Agreement and to comply with the Controller's Instructions.
Categories of data subject	Customer Data may relate to the following categories of data subjects: Controller's Clients and their Affiliates, Contacts and other end users including Controller's employees, contractors, collaborators, customers, Clients, prospects, suppliers and subcontractors. Data subjects may also include individuals attempting to communicate with or transfer personal data to Controller's end users.
Types of personal data	Customer Data shall typically include: name, email address, phone number, online user name(s), financial information to the extent that such information includes personal data, similar information uploaded by the Controller and any other personal data submitted by, sent to, or received by the Controller, or the Controller's end users, via the Subscription Service.
Special categories of personal data	The Parties do not anticipate the transfer of special category data.
Period of Retention	Subject to the 'Deletion or Return of Personal Data' section of this DPA, we will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

APPENDIX 2

SECURITY MEASURES

We currently observe the Security Measures described in this Annex 2. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Master Terms.

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: We host our product infrastructure with multi- tenant, outsourced infrastructure providers. The physical and environmental security controls are audited ISO 27001 compliance, among other certifications.

Authentication: We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data. We require multi-factor authentication unless otherwise agreed in writing.

Authorization: Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure.

The authorization model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorization.

ii) Preventing Unauthorized Product Use

We implement industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: We implement a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in our source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: We maintain relationships with industry recognized penetration testing service providers for our annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through “just in time” requests for access; all such requests are logged.

Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

Background checks: All Asora employees undergo a third-party background check prior to being extended an employment offer, in accordance with and as permitted by the applicable laws. All Asora employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control

In-transit: We make HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and on our website, www.asora.com. Our HTTPS implementation uses industry standard algorithms and certificates.

At-rest: We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control

Detection: We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we

will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to you will be in accordance with the terms of the Agreement.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.5% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime.

APPENDIX 3

LIST OF SUB-PROCESSORS[1]

Third Party Sub- Processor	Purpose	Applicable Service	US Data Center Sub- Processor Location: United States	EU Data Center Sub-Processor Location: EU or Other
MS Azure	Hosting & Infrastructure	Used as a on-demand cloud computing platforms and APIs	n/a	Ireland with Netherlands backup
Twilio, Inc.	2 Factor Authentication	Used as an authentication service	US	None

Asora Sub-Processor	Purpose	Location
Asora Dataconnect Ltd	Services & Support	Ireland