

Partner Data Processing Agreement

This Partner Data Processing Agreement (this “**Agreement**”) effective as of the last date signed below (“**Effective Date**”) entered into by and between **Vyzz Global Contracting Entity/Entities** listed in the Partner Agreement (“**Vyzz Global**”) and **Partner Contracting Entity/Entities** listed in the Partner Agreement (“**Partner**”), is incorporated into and made a part of the Partner Agreement, reseller agreement, channel partner agreement, or other agreement in effect between the parties allowing Partner to resell Vyzz Global Services to its own customers (“**Channel Agreement**”), as the same may be or have been amended by the parties from time to time. If the provisions of this Agreement and the Channel Agreement conflict, including any previously executed or incorporated data protection agreement or privacy terms and conditions, then the provisions of this Agreement shall control. Except for any changes made by this Agreement, the Channel Agreement remains unchanged and in full force and effect.

For clarity, if there are more than one Vyzz Global contracting entity or Partner contracting entity listed above, then each such entity shall be referred to separately as “Vyzz Global” or “Partner”, as appropriate.

1. Definitions. Unless otherwise defined herein, all capitalized terms used in this Agreement shall have the meanings assigned to such terms in the Channel Agreement.

“Agreement Personal Data”	means all Personal Data that Vyzz Global processes on behalf of Partner as a data processor, as specified in Schedule 1.
“Authorized Sub-Processor”	means any third party appointed by Vyzz Global in accordance with this Agreement to process Agreement Personal Data on behalf of and as instructed by the Partner. For the avoidance of doubt, suppliers to Vyzz Global that provide bandwidth connectivity and/or colocation services for Vyzz Global owned and controlled servers globally, where such providers have no access to communications or any data located on Vyzz Global servers (i.e., such suppliers acting as “mere conduits”), shall not be considered Authorized Sub-Processors.
“Cross-Border Transfer Mechanism”	means applicable legal mechanisms required for the transfer of Personal Data from a Data Controller or Data Processor in a given jurisdiction to another Data Controller or Data Processor operating in a separate jurisdiction where applicable Data Protection Laws require a legal mechanism for cross-border transfer. Such mechanisms include, by way of example and without limitation, adequacy decisions, binding corporate rules, the EU 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 pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as may be updated or replaced from time to time.
“Data Protection Laws”	means all applicable laws (including decisions and guidance by relevant Supervisory Authorities) relating to data protection, the processing of personal data, and privacy applicable to Vyzz Global and the Partner in respect of the processing of Agreement Personal Data to provide the Services, including such laws, by way of example and without limitation, the General Data Protection Regulation, the California Consumer Privacy Act, and the Personal Information Protection and Electronic Documents Act.

<p>“Data Controller”, “Data Exporter”, “Data Importer”, “Data Processor” “Data Subject”, “Personal Data”, and “Personal Data Breach”</p>	<p>shall each have the definitions and meanings ascribed to them by the applicable Data Protection Laws and shall include any equivalent or corresponding terms applied by such applicable Data Protection Laws (e.g., “Business” instead of “Data Controller” and “Service Provider” instead of “Data Processor” under the California Consumer Privacy Act, or “organization” or “agency” under the Australian Privacy Principles).</p>
<p>“Supervisory Authority”</p>	<p>means the government agency, department or other competent organization given authority over the processing of Personal Data relevant to this Agreement.</p>

2. Data Processing

2.1 **Roles and Compliance with Law.** For the purpose of this Agreement, it is assumed that the Partner acts as a data controller and Vyzzze Global as a data processor or in the respective role under applicable Data Protection Laws (e.g., a business and a service provider under CCPA). As there is no data processing agreement template in place to cover a data processor – data sub-processor relationship and the parties nevertheless desire to cover their data processing responsibilities by an agreement, the above mentioned roles (Vyzzze Global as data processor and Partner as data controller) apply for the purpose of this Agreement also where the Partner considers itself to act on behalf of its Client as a data processor and the Partner’s Client to act as the ultimate data controller.

Partner and Vyzzze Global each shall comply with their respective obligations as Data Controller and Data Processor, as applicable, under the Data Protection Laws.

2.2 **Data Processor Terms.** The parties agree and acknowledge that:

2.2.1 Partner hereby authorizes Vyzzze Global to process Agreement Personal Data as a Data Processor for the purposes of providing the Services only. Vyzzze Global is authorised to engage, use or permit an Authorized Sub-Processor for the Processing of Agreement Personal Data provided that:

- (a) Vyzzze Global undertakes reasonable due diligence on them in advance to ensure appropriate safeguards for Agreement Personal Data and respective individual rights in accordance with applicable Data Protection Laws;
- (b) Vyzzze Global shall provide the Partner with advance written notice of any intended changes to any Authorized Sub-Processor, allowing the Partner sufficient opportunity to object; and
- (c) The Authorized Sub-Processor’s activities must be specified in accordance with the obligations set out in this Section 2.2.

Without prejudice to this Section 2.2.1, Vyzzze Global shall remain responsible for all acts or omissions of the Authorized Sub-Processor as if they were its own. The Partner hereby approves the Authorized Sub-Processors that Vyzzze Global uses to provide the Services, listed at <https://vyzzze.com/legal/pdpa/> Further, to the extent that any Data Protection Laws would deem an Vyzzze Global Affiliate, by sole virtue of its ownership of Vyzzze Global servers used to provide the Services, to be a sub-processor for purposes of this Agreement, the Partner hereby authorizes Vyzzze Global’s use of such Vyzzze Global Affiliates as Authorized Sub-Processors.

2.2.2 Vyzzze Global shall (and procure that any Authorized Sub-Processor shall):

- (a) process Agreement Personal Data only on documented instructions from the Partner, including those set forth in the Channel Agreement, this Agreement, technical specifications provided for administration of the Services, and configuration settings set in any of Vyzzze Global’s customer portals provided for administration of the Services;

- (b) without prejudice to Section 2.2.2(a), ensure that Agreement Personal Data will only be used by Vyzz Global as set forth in this Agreement or the Channel Agreement;
- (c) ensure that any persons authorized to process Agreement Personal Data:
 - (i) have committed themselves to appropriate confidentiality obligations in relation to Agreement Personal Data or are under an appropriate statutory obligation of confidentiality;
 - (ii) access and process Agreement Personal Data solely on written documented instructions from the Partner; and
 - (iii) are appropriately reliable, qualified and trained in relation to their processing of Agreement Personal Data;
- (d) implement technical and organizational measures at a minimum to the standard set out in Schedule 2 to ensure a level of security appropriate to the risk presented by processing Agreement Personal Data, including as appropriate:
 - (i) the pseudonymisation and encryption of Personal Data;
 - (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
 - (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- (e) notify the Partner without undue delay (and in any event no later than 48 hours) after becoming aware of a Personal Data Breach as set forth in Section 4; (f) assist the Partner in:
 - (i) responding to requests for exercising the Data Subject's rights under the Data Protection Laws, by appropriate technical and organizational measures, insofar as this is reasonably possible, provided that Vyzz Global shall not be required to store or process any data for the purpose of reidentifying an individual when such information is not normally processed or stored by Vyzz Global;
 - (ii) responding to any requests or other communications from the Partner or Partner's Clients as Data Controller relating to the processing of Agreement Personal Data under this Agreement;
 - (iii) reporting any Personal Data Breach to any Supervisory Authority or Data Subjects and documenting any Personal Data Breach;
 - (iv) taking measures to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects; and
 - (v) conducting mandatory privacy impact assessments of any processing operations and consulting with any applicable Supervisory Authority or appropriate persons accordingly;
- (g) at the choice of the Partner and where appropriate, to the extent that Agreement Personal Data is stored by Vyzz Global, securely delete or return all Agreement Personal Data to the Partner after the end of the provision of relevant Services relating to processing, and securely delete any remaining copies and certify when this exercise has been completed;
- (h) make available to the Partner all information necessary to comply with its obligations to do so under Data Protection Laws;
- (i) immediately inform the Partner if Vyzz Global is of the opinion that an instruction of the Partner or Partner's Client regarding the processing of Agreement Personal Data violates applicable Data Protection Laws; and

- (j) not sell, rent, disclose, release, transfer, make available or otherwise communicate, Agreement Personal Data to a third party for monetary or other valuable consideration.

2.3 Cross-Border Transfers.

2.3.1 The Partner hereby acknowledges and accepts that Vyzz Global transfers Agreement Personal Data for service operation purposes to countries outside the jurisdiction the Partner operates in to Authorized Sub-Processors. Where Agreement Personal Data is transferred to a country that is not considered to have an adequate data protection level under Data Protection Laws, Vyzz Global ensures that the data transfers comply with Data Protection Laws, e.g., by having in place effective Cross-Border Transfer Mechanism(s) and having performed data transfer risk assessments. Details of Vyzz Global's data transfers, the data transfer mechanism(s) in place and assessments performed are available in Vyzz Global's Privacy Trust Center in the Cross-Border Data Transfer section, at: <https://vyzze.com/legal/>.

2.3.2 Where Partner is acting on behalf a customer and such customer is acting as the data exporter and Vyzz Global Technologies, Inc. and its Authorized Sub-Processors act as data importers for the Agreement Personal Data transferred by Vyzz Global as part of its service operation, Vyzz Global offers to agree on EU Standard Contractual Clauses with the Partner on behalf of the data exporting customer. The respective EU Standard Contractual Clauses are available for Partner to download in the Cross-Border Data Transfer Section in Vyzz Global's Legal Center: <https://vyzze.com/legal/>.

3. Audits

Vyzz Global shall conduct periodic audits of its processing of Agreement Personal Data to ensure compliance with Data Protection Law.

In addition, in the event that Partner reasonably believes that the relevant documentation provided by Vyzz Global warrants further examination to demonstrate compliance with Data Protection Laws and this Agreement, upon Partner's request not less than thirty (30) days in advance, one (1) on-site audit per annual period during the term of the Channel Agreement may be conducted at a representative Vyzz Global facility involved in the delivery of Services, at reasonable times during business hours and at Vyzz Global's then-current rates. The scope of such audit, including conditions of confidentiality, shall be mutually agreed prior to initiation of the audit.

4. Personal Data Breach

4.1 Vyzz Global shall notify Partner without undue delay (and in any event within 48 hours), after becoming aware of a Personal Data Breach via e-mail to the 24/7 security contacts provided by Partner from time to time in the Vyzz Global Control Center. Such notice shall include a description of the nature of the Personal Data Breach and, where possible, other information as is required by applicable Data Protection Law(s); provided, that, where, and insofar as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

4.2 Vyzz Global shall take all commercially reasonable measures and actions as are appropriate to remedy or mitigate the effects of the Personal Data Breach and shall keep Partner (and where applicable the Supervisory Authority) up-to-date about developments in connection with the Personal Data Breach.

5. Express Third-Party Beneficiaries

The parties hereby agree that Partner's Clients are intended and express third party beneficiaries of all of the provisions of this Agreement and shall have the right, exercisable in their discretion, to enforce the terms and conditions of this Agreement against the parties, as applicable, or prevent the breach thereof, or to exercise any other right, or seek any other remedy, which may be available to it as a third-party beneficiary of this Agreement. For the avoidance of doubt, the terms of this Agreement shall be enforceable by Partner's Clients as though executed directly by such parties.

For avoidance of doubt Partner's Clients shall be third party beneficiaries in the meaning of this section in relation to their own data that is part of the Agreement Personal Data only.

6. Service Operation Personal Data

During its service operation, Vyzz Global logs every access made to one of its servers. The logging ensures the application of security rules, the ability to block non-legitimate access attempts, creation, and improvement of Vyzz Global's knowledge about cyberthreats and attacks and its knowledge about the state of its server network, as well as improvement of Vyzz Global Services. Further it enables Vyzz Global to collect the data required to troubleshoot, bill partners in accordance with their traffic, plan future capacity and deployment needs and create reports on the traffic on its server network.

7. Miscellaneous

7.1 This Agreement may be executed in two or more counterparts, each of which shall be deemed an original and all of which taken together shall be deemed to constitute one and the same document. The parties may sign and deliver this Agreement by facsimile or email transmission.

7.2 This Agreement may not be modified except by a subsequent written instrument signed by both parties.

7.3 If any part of this Agreement is held unenforceable, the validity of all remaining parts will not be affected.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be duly executed and delivered by their respective authorized representatives as of the Effective Date.

Vyzz Global Contracting Entity/Entities

By: _____
Name: _____
Title: _____
Date: _____

Partner Contracting Entity/Entities

By: _____
Name: _____
Title: _____
Date: _____

Schedule 1 of the Data Processing Agreement: Details of Vyze Global's Processing Activities

1. Data Processor

Vyze Global is a provider of compute, performance and security services.

2. Data Subjects

Vyze Global processes Personal Data of individuals accessing Customer Content and/or using Partner's or Partner's Clients' services or accessing Customer's corporate systems ("End Users") when performing its services.

"Customer Content" means all content and applications, including any third-party content or applications, provided to Vyze Global in connection with Partner's or Partner's Clients' access to or use of the Services.

3. Categories of data processed

Vyze Global processes the following categories of Personal Data when performing Vyze Global Services:

a) Compute Services

Vyze Global processes Personal Data embedded in Customer Content ("**End User Personal Data**") when providing Compute Services to Customer. Upon the Customer's or End User's choice, End User Personal Data may include data such as:

- a. Login credentials
- b. Subscriber name and contact information
- c. Financial or other transaction information
- d. Other Personal Data relating to the end user embedded in Customer Content

Special categories of personal data or sensitive data as defined under Data Protection Laws or any other applicable law or regulation, may be part of End User Personal Data, as determined by the Customer.

b) Performance Services

Vyze Global processes **End User Personal Data** as defined above when providing Performance Services to Customer.

For the Service **mPulse** Vyze Global solely processes Personal Data associated with End User activity and interaction with web and internet protocol sessions transiting Vyze Global's servers as part of an End User's session with the Customer's Content ("**Site Personal Data**"). Site Personal Data include data such as:

- a. End User IP address
 - b. URLs visited with time stamps
 - c. geographic location based on the IP address and location of Vyze Global server
 - d. browser and device information (type, version, OS version, chosen language)
- End User Personal Data is not processed for the Service mPulse.

c) Security Services

(i) Enterprise Security Services:

Vyze Global processes Personal Data as provided by Customer or collected during the provision of Vyze Global's Enterprise Security Services in order to protect users of the Customer's enterprise network and the network itself from Internet security and policy abuse risks ("**Enterprise Security Personal Data**"). The Enterprise Security Personal Data includes such data as:

- a. Login and user authentication data

- b. Contents of communications, including attachments
- c. End User IP address
- d. Browser and device information, including location information, browser type, version, OS version, chosen language, device name, MSIN, device type and OS, other information shared by the device as chosen by the end user)
- e. URLs visited

(ii) Application Security Services:

Vyzze Global processes Personal Data to determine whether access to Customer Content in form of applications or via API is made in a legitimate manner or not and to then apply rules set by Customer to allow or block the access request ("**Application Security Personal Data**"). The Application Security Personal Data includes such data as:

- a. End User IP address
- b. URLs of sites visited with time stamps (with an associated IP address)
- c. Geographic location based upon IP address and location of Vyzze Global server
- d. Browser data (type, version, language, OS version)

d) Support Services

Vyzze Global processes personal data embedded in access logs relating to end user access made to an Vyzze Global servers to provide support services ("**Support Log Personal Data**"). The Support Log Personal Data includes such data as:

- a. End User IP address
- b. URLs of sites visited with time stamps (with an associated IP address)
- c. Geographic location based upon IP address and location of Vyzze Global server
- d. Browser data (type, version, language, OS version)

4. Description of Vyzze Global's Personal Data processing activities:

The above listed processing activities are performed when providing the following Services:

a) Compute Services

For Compute, End User Data is uploaded by Customer and/or End User, stored on Vyzze Global servers, and deleted in accordance with the retention period set by the Customer.

The storage location is chosen by the Customer.

Where the location of data center(s) chosen includes countries that are not recognized to have an adequate data protection level under Data Protection Laws, data transfers may take place (e.g., where the End User Personal Data relates to an EU end user and the storage location chosen is the USA).

b) Performance Services

For Performance, End User Personal Data is transmitted via Vyzze Global's server network (without being stored) to ensure Customer Content can be accessed by End Users in a fast reliable and secure manner. Depending on the location of the End User and the Customer origin server, End User Personal Data may be transferred to a country recognized to have a non-adequate data protection level under Data Protection Laws (e.g., where an EU End User is accessing Customer Content on a Customer origin server located in the USA)

For mPulse, Site Personal Data is collected, transferred, analyzed, stored and deleted, to enable Customer to understand the nature of End User traffic to their Customer Content, as well as to monitor the performance of Customer Content.

Vyzze Global offers a service configuration, where, if chosen, the end user IP address embedded in the Site Personal Data is anonymized within in an instance after having been collected at the Vyzze Global

server and the data further processed for website performance purposes, does not consist of Personal Data anymore. For this configuration Site Personal Data is only collected and anonymized.

c) Security Services (i) Enterprise Security Services

For Enterprise Security Services, Enterprise Security Personal Data is collected, transferred, analyzed, stored and deleted, to monitor Customer network activity, provide secure access to Customer's enterprise applications, and establish and enforce access policies.

(ii) Application Security Services

For Application Security Services, Application Security Personal Data is collected, transferred, analyzed, stored and deleted to protect application and APIs that are part of Customer Content from malicious activities. Where malicious activities are recognized, access to Customer Content is blocked and further analyzed in accordance with Customer's instructions.

d) Support Services

The Support Log Personal Data is collected, transferred, analyzed, stored, shared with Customer and deleted to determine the course for service incidents and to resolve such incidents.