DATA PROCESSING AGREEMENT

This **Data Processing Agreement** ("DPA") is entered into between Locl Interactive Inc. ("Meya.ai") and **Customer** (jointly "the Parties"), and forms a part of the **Terms and Conditions** ("T&C") between the Parties, and reflects the Parties' agreement with regard to the processing of **Personal Data** in accordance with the requirements of the **Data Protection Laws**.

By signing this DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates, if and to the extent Meya.ai processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates.

This DPA is effective on the date that it has been duly executed by both Parties ("Effective Date"), and amends, supersedes and replaces any prior data processing agreements that the Parties may have been entered into. Any modifications to the terms of this DPA (whether handwritten or otherwise) will render this DPA ineffective unless Meya.ai has separately agreed to those modifications in writing.

1. Introduction

This DPA sets out terms that apply to Meya.ai's Processing of Customer Data (including without limitation Personal Data) under the T&C.

2. Definitions

a. "Adequate Country" means a country which is deemed adequate by the European Commission under Article 25(6) of Directive 95/46/EC or Article 45 of GDPR.
b. "Alternative Transfer Mechanism" means an alternative data export solution for the lawful transfer of Customer Data (as recognized under EU Data Protection Law) outside the EEA.
c. "Data Controller" means the party that determines the purposes and means of the Processing of Personal Data.
d. "Data Processor" means the party that Processes Personal Data on behalf of, or under the instruction of, the Data Controller.
e. "Data Protection Authority" means the competent body in the jurisdiction charged with enforcement of applicable Data Protection Law.
f. "Data Protection Laws" means with respect to a party, all privacy, data protection, information security related and other laws and regulations applicable to such party, including, where applicable, EU Data Protection Law.
g. "Data Subject" means the identified or identifiable person who is the subject of Personal Data.
h. "EEA" means the European Economic Area, United Kingdom and Switzerland.
i. "EU Data Protection Law" means (i) prior to 25th May 2018, European Union Directive 95/46/EC; and (ii) on and after 25th May 2018, European Union Regulation 2016/679 ("GDPR").

j. References to "instructions" or "written instructions" and related terms mean Data Controller's instructions for Processing of Customer Data, which consist of (1) the terms of the T&C and this DPA, (2) Processing enabled by Data Controller through the Service, and (3) other reasonable written instructions of Data Controller consistent with the terms of the DPA.
k. "Model Contracts" means the Standard Contractual Clauses for Processors as approved by the European Commission under Decision 2010/87/EU in the form made accessible in the Meya.ai Platform Services.
l. "Processing" has the meaning given to it in the applicable EU Data Protection Law and "process", "processes" and "processed" will be interpreted accordingly.
m. "Personal Data" means any information included in the Customer Data relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.
n. "Security Incident" means any unauthorized or unlawful confirmed breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data in Data Processor's control.
o. "Subprocessor" means any Third Party engaged by Data Processor or its affiliates to process any Customer Data pursuant to the T&C or this DPA.
p. "Third Party" shall mean any natural or legal person, public authority, agency or any other body other than the Data Subject, Data Controller, Data Processor, or Subprocessors or other persons who, under the direct authority of the Data Controller or Data Processor, are authorized to Process the data.
q. Other capitalized terms not defined herein have the meanings given in the T&C.

3. General Termination

a. This DPA forms part of the T&C and except as expressly set forth in this DPA, the T&C remains unchanged and in full force and effect. If there is any conflict between this DPA and the T&C, this DPA shall prevail to the extent of that conflict in connection with the Processing of Customer Data.
b. All activities under this DPA (including without limitation Processing of Customer Data) remain subject to the applicable limitations of liability set forth in the T&C.
c. Data Controller agrees that any regulatory fines or penalties incurred by Data Processor in relation to the Customer Data that arise as a result of, or in connection with, Data Controller's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce Data Processor's liability under the T&C as if it were liability to Data Controller under the T&C.
d. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the T&C, unless required otherwise by applicable Data Protection Laws.
e. This DPA will automatically terminate upon expiration or termination of the T&C.

4. Scope and Applicability of this DPA

a. This DPA applies where and to the extent that Meya.ai processes Customer Data that is subject to EU Data Protection Law on behalf of Customer in the course of providing the Service pursuant to the T&C, as detailed at Appendix A.
b. Part A (being Sections 5-11 (inclusive) as well as Appendices A and B of this DPA) shall apply to the processing of Customer Data within the scope of this DPA from the Effective Date.
c. Part B (being Sections 12-14 (inclusive) of this DPA) shall apply to the processing of Customer Data within the scope of this DPA from and including 25th May 2018. For the avoidance of doubt, Part B shall apply in addition to, and not in substitution for, the terms in Part A.

Part A: General Data Processing Obligations

5. Role and Scope of the Processing

a. Customer will act as the Data Controller and Meya.ai will act as the Data Processor under this DPA. Both Customer and Meya.ai shall be subject to applicable Data Protection Laws in the carrying out of their responsibilities as set forth in this DPA.
b. Customer retains all ownership rights in the Customer Data, as set forth in the T&C. Except as expressly authorized by Customer in writing or as instructed by Customer, Meya.ai shall have no right directly or indirectly to sell, rent, lease, combine, display, perform, modify, transfer or disclose the Customer Data or any derivative work thereof. Meya.ai shall act only in accordance with Customer's instructions regarding the Processing of the Customer Data except to the extent prohibited by applicable Data Protection Laws.
c. Additional instructions not consistent with the scope of the T&C require prior written agreement of the parties, including agreement on any additional fees payable by Customer.
d. Notwithstanding the above, Customer acknowledges that Meya.ai shall have a right to use Aggregated Anonymous Data as detailed in the T&C.
e. Meya.ai shall not disclose the Customer Data to any Third Party in any circumstances other than in compliance with Customer's instructions or in compliance with a legal obligation to disclose. Meya.ai shall inform Customer in writing prior to making any such legally required disclosure, to the extent permitted by Data Protection Laws.
f. For clarity, nothing in this DPA limits Meya.ai from transmitting Customer Data (including without limitation Personal Data) among Sources and Destinations as instructed by Customer through the Service. The parties agree that Destinations are not considered Subprocessors of Meya.ai.

6. Subprocessing

a. Customer agrees that Meya.ai is authorized to use Subprocessors (including without limitation cloud infrastructure providers) to Process the Personal Data, provided that Meya.ai: (i) enters into a written agreement with any Subprocessor, imposing data protection obligations substantially similar to this DPA; and (ii) remains liable for compliance with the obligations of this DPA and for any acts or omissions of the Subprocessor that cause Meya.ai to breach any of its obligations under this DPA.

b. Information about Subprocessors, including their functions and locations, is available at: https://www.meya.ai/gdpr (as may be updated by Meya.ai from time to time in accordance with this DPA).

7. Security

a. Meya.ai shall implement and maintain appropriate technical and organizational security measures to protect Personal Data from Security Incidents and to preserve the security and confidentiality of the Personal Data, in accordance with Meya.ai's security standards described in Appendix B ("Security Measures").
b. Customer is responsible for reviewing the information made available by Meya.ai relating to data security and making an independent determination as to whether the Service meets the Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and that Meya.ai may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Service purchased by Customer.

8. Onward Transfer

a. Meya.ai may, subject to complying with this Section 8, store and process Customer Data anywhere in the world where Meya.ai, its affiliates or Subprocessors maintain data processing operations.
b. To the extent that Meya.ai processes any Personal Data protected by GDPR and/or originating from the EEA in the United States or another country outside the EEA that is not designated as an Adequate Country, then the parties shall sign additional Model Contracts.
c. The parties agree that Meya.ai is the "data importer" and Customer is the "data exporter" under such Model Contracts (notwithstanding that Customer may be an entity located outside of the EEA).
d. The parties agree that the data export solution identified in Section 8.b shall not apply if, and to the extent that, Meya.ai adopts an Alternative Transfer Mechanism. In which event, the Alternative Transfer Mechanism shall apply instead (but only to the extent such Alternative Transfer Mechanism extends to the territories to which Personal Data is transferred).

9. Regulatory Compliance

a. At Customer's request and expense, Meya.ai shall reasonably assist Customer as necessary to meet its obligations to Data Protection Authorities.
b. Meya.ai shall (at Customer's expense) reasonably assist Customer to respond to requests from individuals in relation to their rights of data access, rectification, erasure, restriction, portability and objection. In the event that any such request is made directly to Meya.ai, Meya.ai shall not respond to such communication directly without Customer's prior authorization unless required by Data Protection Laws. Information on how to initiate a request is available here: https://www.meya.ai/gdpr

10. Reviews of Data Processing

a. At Customer's request, Meya.ai shall provide Customer with written responses to all reasonable requests for information made by Customer relevant to the Processing of Personal Data under this DPA, including responses to security and audit questionnaires, in each case solely to the extent necessary to confirm Meya.ai's compliance with this DPA.
b. Except as expressly required by Data Protection Laws, any review under this Section will: (i) be conducted no more often than once per year during Meya.ai's normal business hours, in a manner so as not to interfere with standard business operations; (ii) be subject to Meya.ai's reasonable confidentiality and security constraints; (iii) be conducted at Customer's expense; and (iv) not extend to any information, systems or facilities of Meya.ai's other customers or its Third Party infrastructure providers.
c. Any information provided by Meya.ai under this Section 10 constitutes Meya.ai's Confidential Information under the T&C.

11. Return or deletion of data

a. Meya.ai shall, within one hundred and eighty (180) days after request by Customer at the termination or expiration of the T&C, delete or return, at Customer's choice, all of the Personal Data from Meya.ai's systems. Within a reasonable period following deletion, at Customer's request, Meya.ai will provide written confirmation that Meya.ai's obligations of data deletion or destruction have been fulfilled.
b. Notwithstanding the foregoing, Customer understands that Meya.ai may retain Customer Data as required by Data Protection Laws, which data will remain subject to the requirements of this DPA.

Part B: GDPR Obligations after May 25th 2018

12. Additional Security

a. Upon becoming aware of a confirmed Security Incident, Meya.ai shall notify Customer as set out in the Security Measures.

13. Changes to Subprocessors

a. When any new Subprocessor is engaged, Meya.ai will, at least ten (10) calendar days before the new Subprocessor processes any Customer Data, inform Customer of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform) either by sending an email to the Platform Services Billing Email Address or via the Platform Services directly.
b. Customer may object in writing to Meya.ai's appointment of a new Subprocessor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If Meya.ai cannot provide an alternative Subprocessor, or the parties are not otherwise able to achieve resolution as provided in the preceding sentence, Customer, as its sole and exclusive remedy, may terminate the T&C for

convenience, on condition that Customer provides written notice to Meya.ai within five (5) calendar days of being informed of the engagement of the Subprocessor.

14. Further cooperation

a. Where and when required by Data Protection Laws, Meya.ai will provide the relevant Data Protection Authorities with information related to Meya.ai's Processing of Personal Data. Meya.ai further agrees that it will maintain such required registrations and where necessary renew them during the term of this DPA. Any changes to Meya.ai's status in this respect shall be notified to Customer immediately.
b. To the extent Meya.ai is required under Data Protection Laws, Meya.ai shall (at Customer's expense) provide reasonably requested information regarding the Service or prior consultations with Data Protection Authorities to enable Customer to carry out data protection impact assessments.

SIGNED
for and on behalf of the Customer

x _____

Name: _____

Email: _____

Company: _____

Account ID: _____

Title: _____

Date: _____

SIGNED
for and on behalf of Meya.ai

x _____

Name: _____

Email: _____

Title: _____

Date: _____

Appendix A - Details of Processing

Subject Matter: The subject matter of the data processing under this DPA is the Customer Data.

Duration of the Processing: The duration of the data processing under this DPA is until the termination of the T&C plus the period from the expiry of the T&C until deletion of all Customer Data by Meya.ai in accordance with the terms of the T&C.

Nature and Purpose of the Processing: The purpose of the Processing under this DPA is the provision of the Service to Customer and the performance of Meya.ai's obligations under the T&C (including this DPA) or as otherwise agreed by the parties.

Categories of Data: Data relating to individuals provided to Meya.ai via the Service by (or at the direction of) Customer.

Data Subjects: Data subjects include the individuals about whom data is provided to Meya.ai via the Platform Services by (or at the direction of) Customer.

Appendix B – Security Measures

Introduction

Meya.ai considers protection of Customer Data a top priority. As further described in these Security Measures, Meya.ai uses commercially reasonable organizational and technical measures designed to prevent unauthorized access, use, alteration or disclosure of Customer Data stored on systems under Meya.ai's control.

1. **Access to Customer Data:** Meya.ai limits its personnel's access to Customer Data as follows:
    a. Requires unique user access authorization through secure logins and passwords, including multi-factor authentication for Cloud Hosting administrator access and individually-assigned Secure Socket Shell (SSH) keys for external engineer access;
    b. Limits the Customer Data available to Meya.ai personnel on a "need to know" basis;
    c. Restricts access to Meya.ai's production environment by Meya.ai personnel on the basis of business need; and
    d. Encrypts user security credentials for production access.

2. **Data Encryption:** Meya.ai provides industry-standard encryption for Customer Data as follows:
    a. Customer Data is encrypted over the internet; and
    b. Uses strong encryption methodologies to protect Customer Data, including AES 256-bit encryption for Customer Data stored in Meya.ai's production environment.

3. **Data Management**
    a. Meya.ai logically separates each of its customers' data and maintains measures designed to prevent Customer Data from being exposed to or accessed by other customers.

4. **Network Security, Physical Security and Environmental Controls**
    a. Meya.ai uses a variety of techniques designed to detect and/or prevent unauthorized access to systems processing Customer Data, including firewalls and network access controls.
    b. Meya.ai maintains measures designed to assess, test and apply security patches to all relevant systems and applications used to provide the Service.
    c. Meya.ai monitors privileged access to applications that process Customer Data, including cloud services.
    d. The Service operates on Amazon Web Services ("AWS") and is protected by Amazon's security and environmental controls. Detailed information about AWS security is available at:
        i. https://aws.amazon.com/security/
        ii. http://aws.amazon.com/security/sharing-the-securityresponsibility/
        iii. https://aws.amazon.com/compliance/soc-faqs/

5. **Independent Security Assessments.** Meya.ai periodically assesses the security of its systems and the Service as follows:
    a. Ongoing detailed security and vulnerability assessments of the Service conducted by independent third-party security and compliance professionals. Meya.ai shall attest

to Customer the date of the most recent security and vulnerability assessment at Customer's reasonable request.

b. Automated weekly vulnerability scanning, including automated static code analysis of any new code added to the Platform Services.

6. **Incident Response.** If Meya.ai becomes aware of a Security Incident, Meya.ai will:
   a. Take reasonable measures to mitigate the harmful effects of the Security Incident and prevent further unauthorized access or disclosure.
   b. Upon confirmation of the Security Incident, notify Customer in writing of the Security Incident without undue delay. Notwithstanding the foregoing, Meya.ai is not required to make such notice to the extent prohibited by Laws, and Meya.ai may delay such notice as requested by law enforcement and/or in light of Meya.ai's legitimate needs to investigate or remediate the matter before providing notice.
   c. Each notice of a Security Incident will include:
      i. The extent to which Customer Data has been, or is reasonably believed to have been, used, accessed, acquired or disclosed during the Security Incident;
      ii. A description of what happened, including the date of the Breach and the date of discovery of the Security Incident, if known;
      iii. The scope of the Security Incident, to the extent known; and
      iv. A description of Meya.ai's response to the Security Incident, including steps Meya.ai has taken to mitigate the harm caused by the Security Incident.

7. **Business Continuity Management**
   a. Meya.ai maintains processes to ensure failover redundancy with its systems, networks and data storage.

8. **Personnel Management**
   a. Meya.ai performs employment verification, including proof of identity validation and criminal background checks for all new hires.
   b. Meya.ai provides training for its personnel who are involved in the processing of the Customer Data to ensure they do not collect, process or use Customer Data without authorization and that they keep Customer Data confidential.
   c. Meya.ai conducts routine and random monitoring of employee systems activity.
   d. Upon employee termination, whether voluntary or involuntary, Meya.ai immediately disables all access to critical and noncritical systems, including Meya.ai's physical facilities.