PLAYipp Data Processing Agreement

This Data Processing Agreement (this “DPA”) is entered into between PLAYipp AB with company registration number 556712-3012 (the "Supplier") and the Customer (as defined in PLAYipp’s Terms of Service). The Customer is hereinafter referred to as the “Controller” and the Supplier as the “Processor”. The Controller and Processor are hereinafter collectively referred to as the “Parties”.

1. INTRODUCTION

1.1. The Parties have entered into an agreement regarding the Processor’s provision of its services (the “Agreement“). This DPA is incorporated into the Agreement by reference in PLAYipp Terms of Service.

1.2. This DPA governs the Controller’s rights and obligations as a Personal Data Controller and the Processor’s rights and obligations as a Personal Data Processor when the Processor Processes Personal data on behalf of the Controller and according to the written instructions included in this DPA.

1.3. Both Parties shall each act in accordance and comply with their respective obligations under all applicable national regulations, legal requirements and laws relating to the Processing of Personal data. With regard to EU Personal Data, the Parties will comply with each of their respective obligations under the GDPR and any subordinate legislation and regulation implementing the GDPR and/or SCC which may apply (collectively referred to as the “Applicable Data Protection Legislation”).

2. DEFINITIONS

2.1. **GDPR**: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

2.2. Unless otherwise stated, all references to "**Personal data**", "**Processing**", "**Data subject**", "**Personal data breach**" and "**Supervisory authority**" shall have the same meaning in this DPA as stated in article 4 of the GDPR.

2.3. **SCC**: Commission implementing decision (EU) 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, or other updated version.

2.4. **Third party**: A Third party means someone other than the Controller (and the persons who are authorised to Process the Personal Data), the Data subject or the Processor (and the persons who are authorised to Process the Personal Data). A Third party may be a legal person or a natural person, institution, authority or other body.

2.5 Terms and expressions used in this DPA, but not defined herein, shall be defined in accordance with the definitions stated in **PLAYipp's Terms of Use** and **PLAYipp's Terms of Service**.

3. APPENDICES TO THIS DPA

3.1. Appendix 1: Instructions for the Processing of Personal data.

3.2. Appendix 2: Pre-approved Sub-processors.

3.3. Appendix 3: Technical and organisational security measures.

4. PROCESSING OF PERSONAL DATA

4.1. Obligations of the Processor

4.1.1. The Processor undertakes to Process Personal data only in accordance with documented instructions from the Controller (the "Instructions" stated in Appendix 1) and Applicable Data Protection Legislation, unless otherwise provided by Applicable Data Protection Legislation. If Processing deviating from the Instructions, is required under Applicable Data Protection Legislation, the Processor shall inform the Controller of the legal requirement before Personal Data is Processed for that purpose, unless such information is prohibited with reference to an important public interest under Applicable Data Protection Legislation. This DPA and Appendix 1 sets out the Controller's instructions to the Processor about the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal data and categories of Data subjects.

4.1.2. The Controller confirms that the Processor's obligations under this DPA, including Appendix 1, constitute the complete instructions to be followed by the Processor. Any changes to the Controller's instructions shall be negotiated separately and shall be made in writing and signed by both Parties.

4.1.3. The Processor shall without undue delay inform the Controller if the Processor believes that the Controller's instructions regarding the Processing of Personal data are in violation of Applicable Data Protection Legislation.

4.1.4. The Processor shall assist the Controller with appropriate technical and organisational measures, taking into account, as far as possible, the nature of the processing and the information available to the Processor, in order for the Controller to comply with the requirements of Article 28 of the GDPR, and for the Controller to comply its obligations regarding: security in connection with the Processing, notification of a Personal data breach to the Supervisory authority, information to the Data subject about a Personal data breach, impact assessment regarding data protection and prior consultation (Articles 32-36 of the GDPR). The Processor shall also provide assistance to the Controller through appropriate technical and organisational measures so that the Controller can fulfil its duty regarding the rights of Data subjects in accordance with Chapter 3 of the GDPR.

4.1.5. The Processor shall, at the Controllers request, correct or delete incorrect, incomplete or outdated Personal data without undue delay.

4.2. Obligations of the Controller

4.2.1. The Controller is obliged to comply with the provisions of the Applicable Data Protection Legislation with regard to the Processing of Personal data.

4.2.2. The Controller is solely responsible for the accuracy, integrity, content, reliability and legality of the Personal data provided to the Processor by the Controller.

4.2.3. The Controller shall not transmit any sensitive Personal data, such as information on ethnic origin, health, sexual orientation, political opinions, religious beliefs and others.

5. SUB-PROCESSORS AND TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES

5.1. The Processor shall ensure that sub-processors are bound by written agreements which impose on them corresponding data Processing obligations as the obligations under this DPA in respect of data protection. If the sub-processor does not fulfil its obligations in accordance with the agreement between the Processor and the sub-processor, the Processor shall be fully liable to the Controller for the performance of the sub-procesor's obligations. Appendix 2 contains a list of sub-processors that from the date of entry into force of this DPA have been pre-approved by the Customer.

5.2. If the Processor intends to hire a new sub-processor or replace an existing sub-processor to Process Personal data covered by this DPA, the Processor shall inform the Controller of this in advance and give the Controller the opportunity to object to such changes. Such objections by the Controller shall be made in writing without undue delay from receipt of the information by the Controller. The Processor shall provide the Controller with all information that the Controller may reasonably request to assess whether the appointment of the proposed sub-processor complies with the obligations under this DPA and Applicable Data

Protection Legislation. If, in accordance with the Controller's justifiable opinion, compliance with these obligations is not possible through the proposed sub-processor and the Processor despite the Controllers objection wants to hire the proposed sub-processor, the Controller is entitled to terminate the Subscription including this DPA, at no extra cost.

5.3. If Personal data is transferred to or made available from outside EU/EEA, the Processor shall ensure that the transfer is subject to an appropriate safeguard under Applicable Data Protection Legislation.

5.4 Should the Processor consider appointing a sub-processor outside the EU/EEA, the Controller has the right to take part in the Transfer Impact Assessment (TIA) in connection with third country transfers and to demand additional protection measures if the existing ones are deemed to be insufficient. If the Processor does not approve the proposed protection measures, the Controller is entitled to terminate the Subscription including this DPA, at no extra cost.

6. DATA PROTECTION AND CONFIDENTIALITY

6.1. The Processor is obliged to fulfil its legal obligations regarding data protection under Applicable Data Protection Legislation and shall in all cases take appropriate technical and organisational measures to protect the Personal data being Processed.

6.2. The Processor shall implement systematic, organisational and technical measures to ensure an appropriate level of security, taking into account the latest technology and implementation costs in relation to the risk involved in the Processing and the type of Personal data to be protected. When assessing the appropriate level of security, special consideration shall be given to the risk of accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to Personal data. The measures implemented are described in Appendix 3.

6.3. The Processor shall Process Personal data subject to this Agreement with confidentiality and ensure that persons authorised to Process Personal data have undertaken to observe confidentiality and that they are informed of how Personal data may be Processed in accordance with instructions from the Controller. The confidentiality obligation shall continue to apply even after this agreement has expired.

6.4. The Processor certifies that its activities are conducted in a manner that ensures compliance with the provisions and requirements of the Applicable Data Protection Legislation regarding adequate protection of Personal data Processing.

7. DISCLOSURE OF PERSONAL DATA AND CONTACTS WITH COMPETENT AUTHORITIES

7.1. If a Data subject requests information from the Processor regarding the Processing of the Data subject's Personal data, the Processor shall without undue delay refer such request to the Controller.

7.2. If a competent authority requests information from the Processor regarding the Processing of Personal data, the Processor shall inform the Controller thereof without undue delay. The Processor may not act in any way on behalf of the Controller or as its agent and may not transfer or otherwise disclose Personal data or other information relating to the Processing of Personal data to Third parties without the prior consent of the Controller, unless otherwise required by Swedish or European law or pursuant to a non-appealable decision by a competent court or authority.

7.3. If, in accordance with applicable Swedish or European laws and regulations, the Processor is requested to disclose Personal data Processed by the Processor on behalf of the Controller, the Processor shall promptly notify the Controller thereof, unless otherwise provided by applicable law or pursuant to a decision by a competent court or authority, and in connection with the disclosure request that the Personal data be given confidential treatment.

8. PERSONAL DATA BREACH

8.1. The Processor shall notify the Controller without undue delay after having become aware of a Personal data breach concerning the Personal data regulated by this DPA.

8.2. The Processor shall enable the Controller to comply with all legal obligations regarding information to be provided to relevant data protection authorities and Data subjects in Personal data breaches.

8.3. The Processor shall provide the Controller with a description of the Personal data breach. The description must contain at least the following:

a) Description of the nature of the Personal data breach, including, if possible, the categories and approximate number of Data subjects affected, and the categories and approximate number of Personal data items concerned.

b) Name of the person who can provide more information about the breach or answer questions.

c) Description of the likely consequences of the Personal data breach.

d) Description of the measures taken or proposed by the Processor to address the Personal data breach, including, where appropriate, measures to mitigate its potential adverse effects.

9. RIGHT TO AUDIT

9.1. The Controller in its capacity as Personal Data Controller, or other examiner appointed by the Controller, has the right to conduct a review of the Processor's compliance with this DPA regarding the Processing of Personal data, provided that the persons performing the review enter into customary confidentiality agreements.

9.2. The Processor undertakes to provide the information required to prove compliance with the obligations under this DPA and to participate in any review, and to provide the Controller, or the appointed examiner, with the assistance necessary for conducting such review. The Processor shall also allow the Supervisory authority to carry out the audits required by law regarding the Processing of Personal data.

9.3. The audit shall be subject to the following conditions:

a) it may only cover the Personal data that the Processor Processes on behalf of the Controller in accordance with this DPA;

b) it may only be carried out during office hours on weekdays between 08: 00-17: 00 and shall be performed as smoothly and efficiently as possible to minimise disruption to operations;

c) the audit must not reveal any business secrets protected by law;

d) no more than one (1) audit per year shall be performed, unless it takes place after a significant breach of the Processing of Personal data has been identified or if it is required by applicable law, government decision or similar;

e) information on the intention to conduct an audit shall be communicated in writing to the Processor at least 14 working days before the date of conducting the audit.

10. REMUNERATION

10.1. The Processor is entitled to compensation in accordance with the Processor’s applicable hourly rates for work performed or assistance provided pursuant to the obligations in sections 7 and 9 of this DPA.

11. LIMITATIONS OF LIABILITY

11.1. If the Controller or the Processor has been held liable for damages against a third party or has suffered administrative penalty fees due to its actions in violation of the Applicable Data Protection Legislation or this DPA, each Party shall be liable for the consequences of its actions in accordance with a court or other competent authority decision.

11.2. With exception for situations when article 82 in GDPR are applicable, the limitations of liability set out in section 7 of "**PLAYipp's Terms of Service**" shall apply to the Processor's liability under this DPA as if set out herein.

12. TERM OF AGREEMENT

12.1. The provisions of this DPA shall apply as long as the Processor Processes Personal data for which the Controller is the controller.

12.2. This DPA supersedes previously entered data Processing agreement between the Parties and this DPA applies from the signing date below.

13. MEASURES AFTER TERMINATION OF THIS DPA

13.1. The Processor shall at the choice of the Controller, delete or return all the Personal data to the Controller after the end of the provision of services relating to Processing, and delete existing copies unless Union or Member State law requires storage of the Personal data;.

13.2. If the Processor does not receive a response from the Controller regarding the above measures within fourteen (14) days after the termination of the agreement, the Controller is deemed to demand that the Personal data in question shall be deleted. Deleted data may be contained up to 180 days after erasure in the Processors backup storage, and in sub-processors backup storage during the periods stated in Appendix 2.

13.3. If the Processor retains Personal data after the termination of the agreement to the extent required by law, the Processor shall apply the same type of technical and organisational security measures as described in this DPA.

14. CHANGES TO THIS DPA

14.1. Changes and additions to this DPA shall be made in writing and be accepted by the Parties.

15. GOVERNING LAW AND DISPUTE RESOLUTION

15.1. This Agreement shall be governed by the substantive law of Sweden.

15.2. Any dispute, controversy or claim arising out of or in connection with this Agreement, or the breach, termination or invalidity thereof, shall be finally settled by arbitration in accordance with the Rules for Expedited Arbitrations of the Arbitration Institute of the Stockholm Chamber of Commerce. The seat of

arbitration shall be Stockholm, Sweden. The arbitral proceedings shall be confidential.

16. SIGNATURES

16.1. This Data Processing Agreement has been signed in two (2) copies by authorised representatives of the Parties.

Processor:	Controller:
PLAYipp AB	
_____	_____
Date and location	Date and location
_____	_____
Signature	Signature
_____	_____
Legal name	Legal name

APPENDIX 1

Instructions for the Processing of Personal data

PURPOSES

The purposes for which Personal data will be Processed by the Processor:

- For the performance of the Services to the Customer,
- To fulfil other obligations by the Processor under this DPA.

CATEGORIES OF PERSONAL DATA

The Processor shall Process all categories of Personal data that are transferred by the Controller or the User to the Processor, such as:

- Users' name, e-mail, phone number, login-information,
- Images and videos, documents and other content,
- Other Personal data that is shown on the screens that are part of the Service,
- Other Personal data that are registered in the Service by the Customer or User.

CATEGORIES OF DATA SUBJECTS

The Processor shall Process all categories of Data subjects that are transferred by the Controller or the User to the Processor, such as for example:

- Employees and consultants of the Controller, including Users of the Service,
- Other Data subjects that are shown on the screens that are part of the Service,
- Other Data subjects that are registered in the Service by the Customer or User.

PROCESSING ACTIVITIES

The Processor may use such type of Processing activity that is necessary to provide the Service to the Customer, fulfil the terms of this DPA and Applicable Data Protection Legislation, such as:

- any Processing activity or set of Processing which is performed on Personal data or on sets of Personal data, whether or not by automated means, in order to for example: create a User account, handle support

cases, comply with the obligations stated in this DPA, the Terms of Service, the Terms of Use and to provide the Service.

LOCATION FOR PROCESSING OF PERSONAL DATA

Locations where Personal data will be Processed by the Processor:

- Within EU/EEA and through Sub-processors located within or outside of the EU/EEA, as approved by the Controller (see Appendix 2).

Appendix 2

Pre-approved sub-processors

The Controller has approved the use of the following sub-processors:

Sub-Processor and description	Headquarters & Data location	Types of information	Storage time	Transfer mechanisms
Glesys AB The hosting provider for the Service. They provide the virtual and physical servers where the Service is hosted.	Sweden, Sweden	Any information stored within the Service, such as: - Firstname - Surname - Email - Phone number - IP address - Anonymous analytics data - Crash reports - Any information manually stored in text fields, media, posts etc.	As long as the Controller is a Customer of the Processor, or until the data is removed by the User, and up to 180 days thereafter (backup storage).	DPA

Google Cloud EMEA Ltd Hosting provider for external integrations to the Service	Ireland, EU	Integrations set up in PLAYipp Digital Signage are cached through Google Cloud	As long as you are a customer, or until the data is removed by the user and up to 180 days thereafter (backup storage)	DPA (and if applicable, SCC)

Comment regarding Google Cloud EMEA Ltd:
Google's sub-processors for Workspace and Cloud Identity, who provide support, do not have access to customer data stored or processed by the services. This is also explicitly stated in Google's appendix specifying their sub-processors. PLAYipp's internal policy is to never share customer data with Google support or accept that they have access to customer data. Google's appendix specifying their subprocessors is available at the following link: https://workspace.google.com/intl/en/terms/subprocessors.html

Where applicable in accordance with clause 10 of Google's DPA (https://admin.google.com/terms/apps/7/2/en/dpa_terms.html), the relevant SCC is entered into between PLAYipp and Google. Links to the SCC are set out in the definition list in Google's DPA, clause 2.1:

- SCCs (EU Controller-to-Processor) means the terms at: https://cloud.google.com/terms/sccs/eu-c2p
- SCCs (EU Processor-to-Controller) means the terms at: https://cloud.google.com/terms/sccs/eu-p2c
- SCCs (EU Processor-to-Processor) means the terms at: https://cloud.google.com/terms/sccs/eu-p2p
- SCCs (EU Processor-to-Processor, Google Exporter) means the terms at: https://cloud.google.com/terms/sccs/eu-p2p-google-exporter
- SCCs (UK Controller-to-Processor) means the terms at: https://cloud.google.com/terms/sccs/uk-c2p

General Comment, Derogations for specific situations (such as for example support and service)
In the absence of an adequacy decision pursuant to Article 45(3) GDPR, or of appropriate safeguards pursuant to Article 46 GDPR, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation may take place on for instance the following conditions:

- **Article 49.c) GDPR:** the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the

data subject between the controller and another natural or legal person.

- **Article 49.e) GDPR:** the transfer is necessary for the establishment, exercise or defence of legal claims.

Appendix 3

Description of the Technical and Organisational measures taken by the Processor

Information security	- Access to Personal data is limited both physically and virtually, and all data transfer and cold backup data is encrypted. - Internal routines have been established with instructions regarding the Processing of Personal data. Among other things, internal routine for erasure of Personal data and documentation of Personal data breaches. - Internal routines, policies and instructions are reviewed regularly, at least annually and when necessary. - Staff members have knowledge of the provisions of the GDPR regarding the Processing of Personal data and the instructions in this Agreement.
Distribution of roles and tasks	- Specifically named persons have been appointed as responsible for ensuring compliance with internal routines and policies and assigned roles and tasks with regard to security management processes. - A contact person for Personal data matters has been appointed, who also responds directly to the company's top management. - The contact person for Personal data matters has been included in all Processes connected to Personal data Processing and has been given sufficient access to all information and all documentation connected to the Processing of Personal data.

Access rights	- Processes have been established to assign, monitor and control access rights regarding access to databases, IT systems and parts of the IT infrastructure and network. - Natural persons who are authorised to Process Personal data are granted the minimum access rights, unless additional authorizations are necessary for the performance of the work. - There are internal Processes for granting/revoking access rights to Personal data, especially IT systems. - An internal routine for password management has been introduced, which all staff members must follow. The internal routine contains instructions for creating secure passwords for IT system users.
Security of service	- Any staff-member of the Processor that requires access to the Controller's PLAYipp Manager account to fulfil the Controller's instructions requires the use of two factor authentication. - External security testing of the vulnerability of IT systems that Process Personal data is performed. - The suppliers and sub-processors hired guarantee an adequate level of technical and organisational security for the services provided and the tasks performed.
Handling of breaches etc.	- Internal routines for handling and responding to breaches involving Personal data or other security breaches have been introduced, so that staff members are aware of handling and reporting in the event of a suspected breach or breaches. - The routines are in writing and are reviewed at least annually and if necessary.
Confidentiality	- All the Processors staff-member have undertaken a written confidentiality agreement to not disclose any Personal data to unauthorised persons. - All staff members who are authorised to Process Personal data have been included in the internal training program for Personal data security and have access to internal control documents and policies.

Premises	- The buildings and rooms used for Personal data Processing are secured against unauthorised access through the application of access control systems, burglar alarm systems and mechanical or code locks.
Storage spaces	- Personal data stored in data storage devices is secured against loss of availability and integrity through mechanisms for backing up data at predetermined time intervals (data backup). - Secure access authentication methods are applied for access to computers, servers, network equipment used for Personal data Processing.