PlayPlay

DATA PROCESSING AGREEMENT

Update: October 2024

This Data Processing Agreement (“DPA”) applies in relation to the services provided by PlayPlay (also the “Service Provider”) to the Customer under the current service agreement between the parties (the “Service Agreement”).

1. DEFINITIONS

The terms capitalized herein are defined by 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 (the "GDPR"), unless otherwise defined within the Service Agreement.

Within the scope of this DPA:

"Applicable rules" refer to all national, European, and international laws, regulations, and other standards applicable to the processing of personal data implemented under the Service Agreement, including, in particular, the GDPR and all national laws of the European Union Member States adopted in addition to or in implementation of the provisions of the GDPR, as well as, where applicable, laws, regulations, and other national, European, and international standards applicable to the processing of electronic communications data, the use of tracking technologies such as cookies, and direct marketing (commonly referred to as "e-Privacy" rules).

"**Personal data**" refers to all personal data to which the Service Provider is granted access or of which the Service Provider takes or receives a copy in accordance with the DPA.

2. DESCRIPTION AND TERMS OF AUTHORIZED PROCESSING

For the purposes of executing the Service Agreement, the Customer authorizes the Service Provider to carry out the following Personal Data processing activities (the "Assigned Processing").

For all Assigned Processing, the Parties expressly acknowledge that the Customer is the Data Controller and the Service Provider is a Data Processor.

Purpose and objective of the Assigned Processing: to perform the Service Agreement, which enables the Users to create and download videos that may include Personal data (Service provider as a data processor).

For clarification purposes, it is being specified that the processing activities related to the Customer and User accounts (managing the account, communications to the

Customers/Users and product updates) and the analysis of their use of the Platform for the purpose of improving services, are carried out by the Service Provider as the data controller.

Nature of the Assigned Processing: all necessary processing operations for the performance of the Service Agreement, including but not limited to collection, recording, organization, storage, adaptation, modification, extraction, consultation, use, deletion, or destruction.

Types of personal data processed:

- any Video-related data, such as personal data in any Customer Content uploaded by the Users through the Platform, in the Videos, in Users' inputs
- any User Account-related data for support purpose, which may include Identification data (first name, last name, ID, email address, password), Video-related data, Access logs (authentication attempts, error reports, session recordings), Technical information (IP address, web browser version, information system), Usage/statistical data (number of created videos, video settings, media type used, etc.).

Categories of data subjects: Customer, all individuals whose personal data needs to be processed in order to ensure the performance of the Service Agreement, including personal data provided by the Customer/Users through the Platform for Video-creation purpose.

The Service Provider informs the Customer of the following implementation details of the Assigned Processing:

Server location of the Service Provider: Personal data is hosted by the Service Provider and/or its authorized subprocessors: European Union (in Belgium and Finland, and possibly elsewhere in Europe for high availability and data replication needs).

Service Provider's certification: The Service Provider guarantees to have SOC 2 Type I, SOC 2 Type II and ISO 27001 certifications as of the effective date of the Service Agreement.

List of Service Provider's subprocessors: see Appendix A.

Data Protection Officer: The Service Provider has appointed a Data Protection Officer who can be contacted at the following coordinates: privacy@playplay.com, attention to Adélaïde Briffod.

The processing terms described in this Article 2 can only be specified or modified by the Customer's documented instruction and/or, if applicable, with the Customer's prior written consent.

3. PARTIES' OBLIGATIONS

The Parties undertake to execute the DPA in compliance with the Applicable Rules and to fulfill their respective obligations under these Applicable Rules.

3.1 SERVICE PROVIDER'S OBLIGATIONS

3.1.1 Processing based on documented instruction from the Customer

The Service Provider agrees to process Personal Data only based on documented instructions from the Customer, including regarding transfers of data outside the EU, unless the Service Provider is required to process the Personal Data under the law of the European Union or a European Union Member State to which it is subject. In such a case, the Service Provider undertakes to inform the Customer of this obligation to process the Personal Data before carrying out such Assigned Processing, unless the relevant law prohibits such information for important reasons of public interest.

The Customer's instructions are constituted by this DPA and may be supplemented in writing during the execution of the DPA.

3.1.2 Assistance provided to the Customer

The Service Provider undertakes to take all necessary or useful measures to assist the Customer in fulfilling its obligations under the GDPR, including its obligation to respond to requests from Data Subjects and comply with such requests, obligations related to the security of the Assigned Processing and the notification of Personal Data Breaches, its obligation to maintain records of its processing activities as a Data Controller and/or Data Processor, as well as its obligations to carry out prior impact assessments (PIA) and consult Supervisory Authorities prior to the implementation of an Assigned Processing, where applicable.

These measures shall include, but are not limited to, the Service Provider maintaining comprehensive documentation of the conditions for the implementation of the Assigned Processing and any incidents related to these Assigned Processing, and timely communicating to the Customer the relevant elements of this documentation upon the Customer's first request. The Service Provider also undertakes, at the Customer's request, to provide loyal advice to the Customer, to the extent of each Party's means and respective competencies, regarding the choice of available technical means for the implementation of the Assigned Processing.

The Service Provider undertakes to promptly transfer Data Subject’s requests to the Customer or redirect Data Subjects to the Customer for any request of the Data Subjects to exercise their rights and not to respond to such a request on its own, unless specifically documented instructions are given by the Customer to do so. The Service Provider also undertakes, in accordance with the Applicable Rules, to comply with documented instructions from the Customer in order to fulfill a request from a Data Subject, such as rectification or erasure of certain Personal Data.

3.1.3 Security of Processing

The Service Provider undertakes to implement and maintain all necessary or useful technical, logical, and organizational measures to ensure an adequate level of security for the Assigned Processing, considering (i) the state of known techniques, (ii) the modalities of the Assigned Processing and/or in the documented instructions from the Customer

(especially if these modalities include the processing of sensitive data or data subject to specific regulations under the Applicable Rules), and in any case (iii) the security requirements provided or arising from the Applicable Rules, the practice and documentation of Supervisory Authorities, as well as any laws, regulations, and national, European, or international standards that provide obligations or applicable benchmarks for the security of Personal Data or information systems.

These measures implemented as of the date of signature of this DPA are listed in Appendix B. The Service Provider undertakes to maintain and update these measures throughout the execution of this DPA, in order to ensure at all times an adequate level of security in accordance with the aforementioned criteria and not to diminish this level of security.

3.1.4 Confidentiality of Personal Data

The Service Provider undertakes to restrict access to Personal Data to only those individuals among its employees and Subprocessors who need access for the performance of their duties in the context of the implementation of the Assigned Processing (**"Authorized Recipients"**).

The Service Provider vouches for the compliance of the Authorized Recipients with the provisions of this DPA as well as the provisions of the Applicable Rules and undertakes to provide, or ensure that adequate information is provided to the Authorized Recipients, to ensure their proper awareness of the resulting obligations.

The Service Provider undertakes to ensure that the Authorized Recipients are all bound by appropriate obligations of confidentiality regarding the entrusted Personal Data, whether through commitments or confidentiality agreements or by applying confidentiality or secrecy obligations imposed by applicable laws or regulations on these Authorized Recipients.

In the event that the Service Provider is ordered by any court, administrative authority, or representative of public authority (**"Authority"**) to allow access to the entrusted Personal Data or to transmit or produce a copy of the entrusted Personal Data, the Service Provider undertakes to take all necessary precautions and measures to ensure the protection of the confidentiality of the entrusted Personal Data, including at least the following measures:

- Promptly inform the Customer of the received order (if and to the extent that this information is not expressly prohibited by the order in question or by applicable law or regulations) and strictly comply with the documented instructions from the Customer to respond to this order.
- Use all reasonable means at its disposal to (i) redirect the Authority to the Customer to obtain a response to the received order, and/or (ii) challenge the prohibition on informing the Customer of the received order, and/or (iii) challenge the validity of the received order.
- In any case, only communicate the Personal Data or provide access to the Personal Data upon presentation of a judicial decision, and do so in the most limited manner possible.

In the event that the communication of Personal Data to an Authority requires a transfer of data outside the EU, the Service Provider undertakes to immediately inform the Customer in

order to conclude appropriate Standard Contractual Clauses, if such clauses have not already been concluded.

3.1.5 Information and Right to Audit

The Service Provider undertakes to make available to the Customer, and to provide upon first request, any necessary or useful document or evidence to demonstrate compliance with its obligations under this DPA, including its obligations regarding the security of the Assigned Processing and the confidentiality of Personal data. These elements may include certificates or attestations from professional third parties, or audit reports conducted by the Service Provider. The Service Provider agrees that these elements may be communicated to any competent authority or jurisdiction to demonstrate compliance with the applicable Rules for the Assigned Processing.

The Customer may exercise its right to audit by sending a written request to the Service Provider. The audit request must contain a clear and detailed justification for the need for the audit, as well as proposed dates and times for the audit. The Service Provider must respond to the audit request as soon as possible and in any case within 15 days.

The audit must be limited to the verification of specific processing activities carried out by the Service Provider on behalf of the Customer and mentioned in this DPA. The audit must be conducted in a manner that does not disrupt the normal business activities of the subprocessors and complies with the subprocessor's security measures.

The Customer may use the results of the audit only to verify the Service Provider's compliance with the obligations arising from this DPA and to perform similar verifications. The audit results must be treated confidentially and must not be disclosed to third parties unless required by law or authorized by the Service Provider.

The Customer shall bear all costs related to the audit, including reasonable expenses incurred by the Service Provider to enable the conduct of the audit.

It is specified that the Customer has the right to have the Service Provider audited by any third party of its choice under the conditions described above. The Customer undertakes to ensure that the chosen third party provides sufficient confidentiality guarantees in relation to the nature of the information to which it may have access during the audit. The Service Provider shall have the right to object to the appointment of a specific third-party auditor if the performance of the audit by that third-party auditor poses a risk of harm to the Service Provider.

Personal Data Breaches

The Service Provider undertakes to inform the Customer in writing, as soon as possible, of any personal data breach affecting or concerning the personal data, from the moment the Service Provider becomes aware of the personal data breach. The Service Provider also undertakes to take and/or propose to the Customer, as soon as possible, all necessary and useful measures to (i) identify the origin, nature, scope, and consequences of the personal

data breach, (ii) remedy the personal data breach, and (iii) mitigate or neutralize its consequences.

The information provided to the Customer shall include, at a minimum, the following details:
- A description of the personal data breach, specifying at least the nature and origin of the personal data breach, the categories of affected or concerned personal data entrusted, and an estimate of the number of affected individuals.
- The name and contact details of the Data Protection Officer or any other person from whom the Customer can obtain further information and follow-up on the examination and handling of the personal data breach.
- A description of the possible and foreseeable consequences of the personal data breach to the extent of the subprocessor's capabilities and knowledge of the processing.
- A description of the measures taken and/or proposed by the Service Provider to remedy the personal data breach and mitigate or neutralize its consequences.

When all of the above details are not immediately known or accessible, the Service Provider undertakes to inform the Customer of the occurrence of the personal data breach as soon as possible, and then provide additional information as it becomes available.

The Service Provider also undertakes to assist the Customer in fulfilling its obligations to notify Personal Data Breaches to the supervisory authorities and to communicate such Personal Data Breaches to the data subjects, if applicable.

3.1.6 Subcontracting

The Service Provider is authorized to subcontract all or part of the Assigned Processing, provided that such subcontracting complies with the provisions of the Applicable Rules.

In the event of subsequent subcontracting, the Service Provider must ensure that the subcontractor provides sufficient guarantees regarding the implementation of appropriate technical and organizational measures to ensure that the processing meets the requirements of the GDPR and protects the rights of data subjects. The Service Provider remains responsible for the entire Assigned Processing, including any breaches committed by the subsequent subcontractor.

The subsequent subcontractor must comply with the same obligations as those incumbent upon the Service Provider under this DPA. The Service Provider is responsible for ensuring that the subsequent subcontractor complies with these obligations.

The Service Provider must inform the Data Controller in advance and in writing of any changes regarding the addition or replacement of other subsequent subcontractors. This information clearly indicates the subcontracted processing activities and the identity of the subsequent subcontractor. The Data Controller has one month from the date of receipt of this information to raise any objections.

3.1.7 Data transfers outside the EU, EEA, and to a country without an adequacy decision

The Service Provider is authorized to transfer personal data to countries outside the European Union (EU) or the European Economic Area (EEA), including countries that do not benefit from an adequacy decision from the European Commission, subject to compliance with the GDPR provisions relating to the transfer of personal data to third countries.
Before carrying out such transfers, the Service Provider must implement appropriate measures to ensure an adequate level of protection for personal data, in accordance with the requirements of the GDPR. These measures may include the use of standard contractual clauses adopted by the European Commission or any other mechanism approved by the competent supervisory authorities.

The Service Provider undertakes to inform the Customer of any transfer of personal data to a third country, providing details of the protection measures implemented to ensure an adequate level of protection for personal data. This information is presented to the Customer in Appendix A.

The Customer reserves the right to object to any transfer of personal data to a third country if the protection measures implemented by the subprocessor are not deemed adequate to ensure the protection of personal data in accordance with the requirements of the GDPR.

In the event of a transfer of personal data to a third country, the Service Provider remains responsible for complying with the obligations of the GDPR regarding such transfers, including the obligation to ensure an adequate level of protection for personal data.

3.1.8 Deletion of Personal Data

At the end of the Assigned Processing period, the Service Provider shall default to the permanent and irreversible deletion of all personal data still in its possession and shall instruct all its subprocessors to carry out this deletion.

Deletion means the removal of all files, documents, media, or any other materials containing personal data within the scope of the DPA.

The Service Provider undertakes to retain all necessary and useful evidence of the proper completion of this deletion, in any useful form, including certificates or attestations from professional third parties, and to provide such evidence to the Customer upon first request.

3.1.9 Customer's Notice

In the event that the Service Provider considers that a documented instruction from the Customer regarding the Assigned Processing may be deemed unlawful under the applicable rules or may result in a breach or violation of such rules, the Service Provider undertakes to immediately inform the Customer, with the latter being the sole judge of the validity of the instructions given regarding the Assigned Processing.

3.2 CUSTOMER'S OBLIGATIONS

3.2.1 Lawfulness of Assigned Processing

The Customer, as the Data Controller, remains solely responsible for the lawfulness of the Assigned Processing, particularly regarding the legal basis of the Assigned Processing and the information provided to the data subjects in cases where the Service Provider is the data processor. In cases where the Service Provider is also the data controller, both Parties must comply with their obligations under the GDPR as data controllers.

3.2.2 Communication with data subjects and supervisory authorities

Unless otherwise expressly documented and instructed, and except for cases mandated by applicable regulations, the Customer remains solely responsible and in charge of communicating with the data subjects and supervisory authorities regarding the Assigned Processing.

4. ENTRY INTO FORCE AND DURATION

This DPA enters into force on the same date as the Service Agreement and will remain in effect until the deletion of all Personal Data in accordance with Article 3.1.8 above.

5. LIABILITY

In the event of a breach of this DPA, the liability of each Party is limited as described in the Service Agreement.

Each Party is responsible towards the other for the performance of its obligations under the DPA and undertakes, therefore, to compensate for any direct damages caused to the other Party in case of non-compliance with its obligations.

If either Party is sued by a data subject in accordance with Article 82(4) of the GDPR, it may bring in the other Party as a third-party defendant. If either Party is held fully liable for damages suffered by a person in accordance with Article 82(4) of the GDPR, it may claim from the other Party the portion of the compensation corresponding to its share of responsibility in the repaired damage in accordance with Article 82(5) of the GDPR, without the other Party being able to invoke any limitation or exclusion of liability provided for in the Service Agreement and/or in this DPA.

6. FINAL PROVISIONS

In the event of a conflict between the provisions of this DPA and those of the Service Agreement, the provisions of this DPA shall prevail.

This DPA may only be amended by a written agreement signed by all Parties.

APPENDIX A

SERVICE PROVIDER'S SUBPROCESSORS

PlayPlay's Subprocessors are listed here: https://playplay.com/docs/subprocessors.pdf

APPENDIX B

SECURITY MEASURES TAKEN BY THE SERVICE PROVIDER

The security measures applied by the Service Provider are described here: https://security.playplay.com/ and more specifically under the "Security Whitepaper" section.