Data Processing Agreement

Playable ApS | Version 2.0 | May 2026

Annex 1 to the Subscription Agreement

All references in the Agreement to "EU GDPR", to "GDPR" and to "General Data Protection Regulation" shall also mean to include UK 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 (General Data Protection Regulation) OJ L 119/1, 4.5.2016. as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018).

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR) between Playable ApS (Data Processor) and the Customer (Data Controller);

Each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. **Table of Contents**

2. Preamble

2.1. These Contractual Clauses (the Clauses) set out the rights and obligations of the Customer (Data Controller) and the Playable (Data Processor), when processing personal data on behalf of the Data Controller.

2.2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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).

2.3. In the context of the provision of services specified in Agreement signed by both parties. The Data Processor will process personal data on behalf of the Data Controller in accordance with the Clauses.

2.4. The Clauses shall take priority over any similar provisions contained in other agreements between the

parties.

2.5. Three appendices are attached to the Clauses and form an integral part of the Clauses.

a) Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of Data Subject and duration of the processing.

b) Appendix B contains the Data Controller's conditions for the Data Processor's use of Sub-Processors and a list of Sub-Processors authorised by the Data Controller.

c) Appendix C contains the Data Controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the Data Processor and how audits of the Data Processor and any Sub-Processors are to be performed.

2.6. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

2.7. The Clauses shall not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the Data Controller

3.1. The Data Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

3.2. The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3.3. The Data Controller shall be responsible, among other, for ensuring that the processing of personal data, which the Data Processor is instructed to perform, has a legal basis.

4. The Data processor acts according to instructions

4.1. The Data Processor shall process personal data only on documented instructions from the Data Controller, unless required to do so by Union or Member State law or other national law (including but not limited to the laws in the UK) to which the processor is subject.

4.2. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

4.3. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

5.1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

5.2. The data processor shall at the request of the data controller demonstrate that the concerned persons

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

6.1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

6.2. The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

a) Pseudonymisation and encryption of personal data;

b) the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.3. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

6.4. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.
If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of Sub-Processors

7.1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

7.2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

7.3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least three months in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

7.4. Where the Data Processor engages a Sub-Processor for carrying out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in the Clauses shall be

imposed on that Sub-Processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.
The Data Processor shall therefore be responsible for requiring that the Sub-Processor at least complies with the obligations to which the Data Processor is subject pursuant to the Clauses and the GDPR.

7.5. A copy of such a Sub-Processor Agreement and subsequent amendments shall – at the Data Controller's request – be submitted to the Data Controller, thereby giving the Data Controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the Sub-Processor. Clauses on business related issues that do not affect the legal data protection content of the Sub-Processor agreement, shall not require submission to the Data Controller.

7.6. If the Sub-Processor does not fulfil his data protection obligations, the Data Processor shall remain fully liable to the Data Controller as regards the fulfilment of the obligations of the Sub-Processor. This does not affect the rights of the Data Subject's under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the Data Controller and the Data Processor, including the Sub- Processor.

8. Transfer of data to third countries or international organisations

8.1. Any transfer of personal data to third countries or international organisations by the Data Processor shall only occur on the basis of documented instructions from the Data Controller and shall always take place in compliance with Chapter V GDPR.

8.2. In case transfers to third countries or international organisations, which the Data Processor has not been instructed to perform by the Data Controller, is required under EU or Member State law or other national law (including but not limited to laws in the UK) to which the Data Processor is subject, the Data Processor shall inform the Data Controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

8.3. Without documented instructions from the Data Controller, the Data Processor therefore cannot within the framework of the Clauses:

a) transfer personal data to a Data Controller or a Data Processor in a third country or in an international organization

b) transfer the processing of personal data to a Sub-Processor in a third country

c) have the personal data processed by the Data Processor in a third country

8.4. The Data Controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

8.5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the Data Controller

9.1. Taking into account the nature of the processing, the Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the Data Controller's obligations to respond to requests for exercising the Data Subjects rights laid down in Chapter III GDPR.
This entails that the Data Processor shall, insofar as this is possible, assist the Data Controller in the Data Controller's compliance with:

a) the right to be informed when collecting personal data from the Data Subject

b) the right to be informed when personal data have not been obtained from the Data Subject

c) the right of access by the Data Subject

d) the right to rectification

e) the right to erasure ('the right to be forgotten')

f) the right to restriction of processing

g) notification obligation regarding rectification or erasure of personal data or restriction of processing

h) the right to data portability

i) the right to object

j) the right not to be subject to a decision based solely on automated processing, including profiling

9.2. In addition to the Data Processor's obligation to assist the Data Controller pursuant to Clause 6.3., the Data Processor shall furthermore, taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller in ensuring compliance with:

a) the Data Controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b) the Data Controller's obligation to without undue delay communicate the personal data breach to the Data Subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c) the Data Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

d) the Data Controller's obligation to consult the competent supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk.

9.3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the Data Processor is required to assist the Data Controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

10.1. In case of any personal data breach, the Data Processor shall, without undue delay after having become aware of it, notify the Data Controller of the personal data breach.

10.2. The Data Processor's notification to the Data Controller shall, if possible, take place within 24 hours after the Data Processor has become aware of the personal data breach to enable the Data Controller to comply with the data Data Controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

10.3. In accordance with Clause 9(2)(a), the Data Processor shall assist the Data Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Data Processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the Data Controller's notification to the competent supervisory authority:

a) The nature of the personal data including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned;

b) the likely consequences of the personal data breach;

c) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

11. Erasure and return of data

11.1. On termination of the provision of personal data processing services, the Data Processor shall be under obligation to return all the personal data to the Data Controller and delete existing copies unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

12.1. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller.

12.2. Procedures applicable to the Data Controller's audits, including inspections, of the Data Processor and Sub- Processor are specified in appendices C.7. and C.8.

12.3. The Data Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Data Controller's and Data Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the Data Processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

13.1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the Data Subject and the protection afforded by the GDPR.

14. Commencement and termination

14.1. The Clauses shall become effective on the date of both parties' signature.

14.2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

14.3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

14.4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the Data Controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

15. Data Processor contacts/contact points

- Name: Playable Legal Team
- Email: legal@playable.com

Appendix A Information about the processing

A.1. The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

The purpose of the collaboration is that the Data Controller may use Playable's Platform to create campaigns to engage participants in the campaigns.

A.2. The Data Processor's processing of personal data on behalf of the Data Controller shall mainly pertain to (the nature of the processing):

The Data Processor makes the Playable Platform available for the Data Controller for setting up and launching campaigns to collect personal data via the campaign, to host the collected personal data and make the personal data available to the Data Controller.

A.3. The processing includes the following types of personal data about Data Subjects:

Directly Collected Data

The following data is collected directly from participants or the Data Controller:

- Any information provided by the participant as requested by the Data Controller. This usually consists of general data such as name and email address.
- Any data directly provided to Playable in order to deliver services. This usually consists of a pseudomized ID.

Indirectly Collected Data

The following data is collected automatically as part of the platform's operation and security:

- **IP Address** – Required for security and fraud prevention.
- **Device Information:** Device type, browser information, screen resolution – Helps ensure compatibility and enhance user experience.
- **Game Data, as applicable** – Game won, game lost, number of correct answers, prize information, etc.

Analytics and event data

Event data is aggregated on session level. Event and session data are used to create statistics for the Data Controller. Analytics and event data can be disabled. If analytics and event data is disabled, Playable will not be able to show certain types of statistics to the Data Controller.

Analytic and event type:

- UTM source and referral data, to understand from which link the participant has entered the campaign.
- Page-view events (triggered when you move from one flow page to the next)
- External link click (triggered when an external link is clicked, if the Data Controller has added an external link to the campaign)

Processing of sensitive personal data

The Data Controller may not request or process any sensitive personal data via the Playable Platform, unless separately agreed between the parties.

A.4. Processing includes the following categories of Data Subject:

Data Subjects is categorized as individuals that engage in the Data Controllers campaign via the Playable Platform. This can be, but not limited to, subscribers, participants in online draws, games, contests and quizzes.

A.5. The Data Processor's processing of personal data on behalf of the Data Controller may be

performed when the Clauses commence. Processing has the following duration:

Processing shall not be time-limited and shall be performed until this Data Processing Agreement is terminated or cancelled by one of the Parties.

Appendix B Authorised Sub-Processors

B.1. Approved Sub-Processors

On commencement of the Clauses, the Data Controller authorises the engagement of the following Sub-Processors:

NAME	COMPANY NO.	ADDRESS	DESCRIPTION OF PROCESSING
Amazon Web Services EMEA Sarl	IE3493067RH	Burlington Plaza, Burlington Rd, Dublin 4, Ireland	All data and infrastructure are hosted at Amazon Web Services in Ireland.
Heysender ApS	DK31282322	Jens Baggesens Vej 47, 8200 Aarhus N, Denmark	Sending emails via the Playable Platform. The Sub-Processor is used only if emails are sent via the Platform. Hosting in Denmark.
inMobile ApS	DK31426472	Axel Kiers Vej 18L, 8270 Højbjerg, Denmark	Sending SMS messages via the Playable Platform. The Sub- Processor is used only if SMS messages are sent via the Platform. Hosting in Denmark.

The Data Controller shall on the commencement of the Clauses authorise the use of the abovementioned Sub-Processors for the processing described for that party. The Data Processor shall not be entitled – without the Data Controller's prior general written authorisation – to engage a Sub-Processor for a 'different' processing than the one which has been agreed upon or have another Sub-Processor perform the described processing.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The Data Processor's processing of personal data on behalf of the Data Controller shall be carried out by the Data Processor performing the following:

The Data Processor makes the Playable Platform available for the Data Controller for setting up and launching campaigns to collect personal data via the campaign, to host the collected personal data and make the personal data available to the Data Controller.

C.2. Security of processing

The level of security shall take into account:

In general, the Data Processor has a control environment, which is largely based on established technical procedures, supplemented by manual guidelines and procedures.

The Data Processor's technical control environment in Playable's Platform builds, among other things on:

a) Only authorized hardware and software are used on networks that store or access data.
b) Access controls with 2-factor log-in.
c) Access restriction to those parts of the platform where personal data is stored.
d) Possibility of systematic obtaining of consent for legal basis of treatment.
e) Advanced malware and virus detection software is used.
f) Use secure configuration for devices and no default passwords are used.
g) A neutral test environment with "dummy data".
h) Automatic password and password replacement. Passwords are assigned on an individual basis.
i) Encryption of data is done by hardware encryption of server data. (AES-256 at rest on the AWS RDS).
j) Encryption in transit via https (minimum TLS 1.2)
k) Annual penetration test by third party providers. Vulnerability scan twice a year by third party providers.
l) Event logging, access logging and data export logging.
m) Automatic deletion of data in accordance with retention policy.
n) GDPR interface in the Playable Platform that allows the Data Controller to easily comply with the request and rights of the data subject (data portability, right to be forgotten).

The technical system-based control environment is supported by a number of manual procedures and access controls to the physical work environment, including:

o) Information Security Management System (ISMS) based on the ISO27001:2022 framework.
p) IT security policy and IT security guidelines
q) Data breach procedure.
r) Information transfer policies.
s) Updating the operating software, applications and program libraries at Data Processor is only done by domain administrators.
t) The principle of the fewest possible rights to handle access control and rights.
u) Awareness training of employees.
v) Disaster recovery plan and business continuity plan.
w) Yearly GDPR audit by external auditors (ISAE3000 report)
x) ISO27001 audit (internal and external)
y) Data retention policy in accordance with data minimization.

C.3. Assistance to the Data Controller

The Data Processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the Data Controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

The Data Processor has implemented measures in order to detect any data breaches and act promptly in order to assist the Data Controller.

The Data Processor has implemented procedures to assist the Data Controller in fulfilling Data Subjects rights in accordance with GDPR legislation, such as:

- Assist the Data Controller if Data Subjects has inquiries.
- The Data Subject can be directly searched for in the Platform in the GDPR-interface
- There are procedures if Data Subjects contacts the Data Processor

An ISAE-3000 report is each year prepared by a third party which can be shared upon the Data Controllers request.

C.4. Storage period/erasure procedures

Personal data are stored with the Data Processor in 30 (default), 60 or 90 days after end live campaign or 7 or 14 days after registration or until the Data Controller requests that the data are erased or returned whichever is earlier. "Always on"-campaigns will delete data 30 days after registration as default, but can be shortened to 7 or 14 days after registration via settings.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the Data Controller's prior written authorisation:

- EU/EEA

Access to the personal data under the Clauses cannot be from other locations than the following without the Data Controller's prior written authorisation:

- EU/EEA
- United Kingdom, when an adequacy decision by the EU commission is valid and in force

C.6. Instruction on the transfer of personal data to third countries

The Data Processor may only transfer personal data to third countries or international organizations to the extent that this is stated in the instructions of the Data Controller.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

The transfer of personal data may in all cases only be done to the extent permitted by the regulation currently in force.

If The Data Processor acts on behalf of a Data Controller located outside of the EEA the data processing and the transferring of data outside of the EEA will follow the regulations stated in "MODULE FOUR: Transfer processor to controller" in "ANNEX to the COMMISION IMPLEMENTATION DECISION 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 (Brussels, 4.6.2021 C (2021) 3972 final).

C.7. Procedures for the Data Controller's audits, including inspections, of the processing of personal data being performed by the Data Processor

The Data Controller or the Data Controller's representative has access to inspecting, including physically inspecting, the processing at the Data Processor's facilities when the Data Controller deems that this is required.

The Data Controller's costs, if applicable, relating to physical inspection shall be defrayed by the Data Controller. The Data Processor shall, however, be under obligation to set aside the resources (mainly time) required for the Data Controller to be able to perform the inspection. The Data Processor will invoice the Data Controller a fee of 150 EUR pr. hour excl. VAT for time spent on these physical inspections.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by Sub-Processors

The Data Processor or the Data Processor's representative shall in addition have access to inspecting compliance materials. Data are hosted at Amazon in Ireland. Amazon does not allow physical inspections, but the Data Processor have access to all compliance documents - i.e. audit reports. The Data Processor has access to all data at the servers.