Data Processing Addendum to
The Training Arcade® Agreement

This Data Processing Addendum ("**DPA**") is an addendum to The Training Arcade® Agreement ("**Agreement**") and is entered into by and between the entity you represent ("**Customer**") and The Game Agency, LLC ("**TGA**").

Customer and TGA shall be referred to jointly as the "**Parties**" and individually as a "**Party**".

Content

1. DEFINITIONS....1
2. BACKGROUND, SCOPE, AND ORDER OF PRECEDENCE....3
3. JURISDICTION-SPECIFIC OBLIGATIONS AND INTERNATIONAL DATA TRANSFER....4
4. OBLIGATIONS....5
5. SUB-PROCESSING....7
6. AUTHORIZED PROVIDER OF SERVICE....7
7. ONWARD TRANSFER OF DATA....8
8. LIABILITY....8
9. TERMINATION....8
10. GENERAL....8

SCHEDULE A - PERSONAL DATA PROCESSING PURPOSES AND DETAILS....11

SCHEDULE B - TECHNICAL AND ORGANIZATIONAL MEASURES....13

SCHEDULE C – JURISDICTION-SPECIFIC OBLIGATIONS AND INFORMATION FOR INTERNATIONAL TRANSFERS....21

IT IS AGREED:

1. DEFINITIONS

1.1 The following expressions bear the following meanings unless the context otherwise requires. All capitalized terms not defined in this DPA will have the meaning set forth in the Agreement.

"**Business**," "**Business Purpose**", "**Commercial Purpose**", "**Contractor**," "**Consumer,**" "**Sell**," "**Share**," "**Service Provider**" and "**Third Party**" shall have the same meanings set out in the CCPA.

"**Controller**" means the entity that determines the purposes and means of the processing of Personal Data. "Controller" includes equivalent terms in Data Protection Laws, such as the CCPA-defined terms "Business" or "Third Party," as context requires.

"**Data Exporter**" means the party that (1) has a corporate presence or other stable arrangement in a jurisdiction that requires an International Data Transfer Mechanism and (2) Transfers Personal Data, or makes Personal Data available to,

the Data Importer. This term also describes a party that receives Personal Data from a third party and further discloses that Personal Data to the Data Importer.

"**Data Importer**" means the party that is (1) located in a jurisdiction that is not the same as the Data Exporter's jurisdiction and (2) receives Personal Data from the Data Exporter or is able to access Personal Data made available by the Data Exporter. This term includes a party that receives Personal Data from the Data Exporter in an onward transfer.

"**Data Protection Authority**" means, in relation to each of the Parties, the relevant data protection authority or enforcement body in the respective jurisdiction.

"**Data Protection Laws**" means all applicable legislation and regulations governing the processing and protection of Personal Data under this DPA, including but not limited to EU General Data Protection Regulation No 2016/679 ("**GDPR**"), the GDPR as implemented by the United Kingdom Data Protection Act 2018 ("**UK GDPR**"), and Cal. Civ. Code 1798.100 *et seq.* (California Consumer Privacy Act) ("**CCPA**").

"**Data Subject**" means an identified or identifiable natural person.

"**EEA**" means the European Economic Area.

"**International Data Transfer Mechanism**" means the special protections that some jurisdictions require two or more parties that transfer information across international borders to adopt to make the transfer lawful, e.g., standard contractual clauses, binding corporate Rules, or statutory obligations that require the parties to adopt certain technical, organizational, or contractual measures. "**Transfer**," in the context of an International Data Transfer Mechanism, means to disclose or move Personal Data from a storage location in one jurisdiction to another, or to permit a party in one jurisdiction to access Personal Data that the other party stores in another jurisdiction that requires an International Data Transfer Mechanism.

"**Personal Data**" means any information or set of information that identifies, relates to, describes, is reasonably capable or being associated with, or could reasonably be linked to, directly or indirectly, a Data Subject. "Personal Data" includes equivalent terms in Data Protection Laws, such as the CCPA-defined term "personal information," as context requires.

"**Process**" or "**Processing**" means any operation or set of operations that a party performs on data, including collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"**Processor**" means an entity that processes Personal Data on behalf of another entity.

"Processor" includes equivalent terms in Data Protection Laws, such as the CCPA-defined terms "Service Provider" or "Contractor," as context requires.

"**Prohibited Data**" means any: (1) special categories of data enumerated in Article 9(1) of the GDPR, any successor legislation, and any applicable United Kingdom laws including the UK GDPR; (2) patient, medical, or other protected health information regulated by the Health Insurance Portability and Accountability Act (as amended and supplemented) ("**HIPAA**"); (3) credit, debit, or other payment card data or financial account information, including bank account numbers; (4) credentials granting access to an online account (e.g. username plus password); (5) social security numbers, driver's license numbers, or other government identification numbers; (6) other information subject to regulation or protection under specific laws such as the Children's Online Privacy Protection Act or Gramm-Leach-Bliley Act (or related rules or regulations); or (7) any data similar to the above protected under foreign or domestic laws.

"**Purposes**" are the provision of the Service to Customer and Users as set out in the Subscription Agreement.

"**EEA Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, Commission Implementing Decision (EU) 2021/917 of 4 June 2021.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data that Processor or its subprocessors use in connection with this DPA, or an event that qualifies as a reportable data breach under applicable Data Protection Laws.

"**Sub-processor**" means a Processor engaged by a party who is acting as a Processor.

1.2 In this DPA, unless the contrary intention appears:

(a) references to a person include an individual, a body corporate and an unincorporated association of persons; and
(b) references to a Party to this DPA include references to the successors or assigns (immediate or otherwise) of that Party.

1.3 Any reference to this DPA includes any Schedules hereto, all of which are hereby incorporated by reference into this DPA.

2. BACKGROUND, SCOPE, AND ORDER OF PRECEDENCE

2.1 Pursuant to the Agreement, TGA provides to Customer a cloud-based

customizable training game service and related technical support to Customer and its authorized end users ("**Users**") called The Training Arcade® (**"Subscription Service**" or "**Service**").

2.2 This DPA only applies to the extent that TGA Processes Personal Data in connection with the Service.

2.3 The Parties agree that the Processing of the Personal Data described in **Schedule A** will be governed by this DPA.

2.4 Customer is the Controller of Personal Data Processed on behalf of Customer by TGA, and all references to Controller in this DPA shall be considered a reference to Customer as context requires and unless otherwise indicated. TGA is the Processor of Personal Data that it receives from Customer and Users, and all references to Processor in this DPA shall be considered a reference to TGA as context requires and unless otherwise indicated.

2.5 In the event of a conflict between this DPA and the Agreement, this DPA will control to the extent necessary to resolve the conflict. In the event the Parties use an International Data Transfer Mechanism and there is a conflict between the obligations in the International Data Transfer Mechanism and this DPA, the International Data Transfer Mechanism will control.

3. JURISDICTION-SPECIFIC OBLIGATIONS AND INTERNATIONAL DATA TRANSFER

3.1 The Parties acknowledge that Controller is responsible for verifying the applicability of foreign Data Protection Laws to Customer's use of the Service, and thus also for verifying whether an International Data Transfer Mechanism is necessary for the Processing of Personal Data pursuant to this DPA.

3.2 The Parties shall comply with any International Data Transfer Mechanism that may be required by applicable Data Protection Laws. Before Controller Transfers Personal Data to Processor, or permits Processor to access Personal Data located in a jurisdiction that requires an International Data Transfer Mechanism, Controller shall notify Processor of the relevant requirement and the Parties will work together in good faith to fulfill the requirements of the International Data Transfer Mechanism.

3.3 The Parties agree to abide by the additional terms, conditions, and provisions set forth in **Schedule C**, which also describes the International Data Transfer Mechanisms that the Parties anticipate using at the outset of this DPA.

3.4 For any jurisdiction not listed in Schedule C that requires an International Data Transfer Mechanism, the Parties hereby agree to negotiate an update to this DPA to incorporate such International Data Transfer Mechanism.

3.5 If the International Data Transfer Mechanism on which the Parties rely is invalidated

or superseded, the Parties will work together in good faith to find an alternative. If the Parties are unable to find an alternative within 60 days, or another period as agreed in writing, either of them may terminate this DPA.

4. OBLIGATIONS

4.1 Controller will ensure that it has all necessary appropriate consents and notices in place to enable Processor to Process the Personal Data pursuant to this DPA.

4.2 With respect to the CCPA:

(a) Except where TGA is acting as a Controller (e.g., to enforce its rights under the Agreement), TGA as Processor shall (i) comply with the obligations of a Service Provider required by the CCPA, (ii) provide the level of privacy protections for Personal Data of Consumers required of a Business by the CCPA, and (iii) notify Customer if it makes a determination that it can no longer meet its obligations under the CCPA; and shall not (i) retain, use or disclose Personal Data of any Consumer for any purpose other than for the specific purpose of providing the Services under the Agreement, including for a Commercial Purpose other than the Business Purposes specified in Schedule A, or as otherwise permitted by the CCPA, (ii) Sell or Share Personal Data of any Consumer, (iii) retain, use, or disclose Personal Data of any Consumer outside of its direct business relationship with Customer; or (iv) combine Personal Data of any Consumer received from or on behalf of SUBCRIBER with Personal Data received from or on behalf any other person or entity, or with Personal Data TGA collects from its own interaction with the Consumer, provided that TGA may combine Personal Data to perform any Business Purpose in accordance with the CCPA.

(b) SUBSRIBER as a Business shall (i) have the right to take reasonable and appropriate steps to ensure that Processor uses Personal Data of Consumers received from or on behalf of Customer consistent with Customer's obligations under the CCPA; and (ii) have the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data of any Consumer received from or on behalf of Customer.

(c) The Parties acknowledge that any disclosure of Personal Data pursuant to the Agreement does not confer any value under the Agreement. The provision of Personal Data from Controller to Processor does not constitute a Sale under the CCPA.

(d) Processor shall promptly (and, in any case within fifteen (15) business days of receipt) comply with Controller's written instructions

associated with responding to a Consumer's request to access, correct, or delete Personal Data obtained as a result of providing the Services under the Agreement or otherwise exercise their CCPA rights with respect to such Personal Data, or enable Controller to do so, in accordance with the CCPA. In the event that a Consumer makes a request to access, correct, or delete Personal Data or otherwise exercise CCPA rights directly to Processor, Processor shall, to the extent permitted under applicable law, forward the request to Controller within fifteen (15) business days and not respond to the Consumer, other than to advise the individual that the request has been sent to Controller, without Controller's written consent.

(e) If Processor authorizes any subcontractor or other party to Process Personal Data subject to this DPA that is covered by CCPA, such engagement shall (i) be pursuant to a binding and written contract that contains provisions so that such person or entity meets the definition of a Service Provider or Contractor and is not a Third Party, and requires such person or entity to observe all the requirements set forth under subsection (a) of Clause 4.2; and (ii) otherwise in accordance with the terms set forth in Clauses 5.1 and 5.2.

(f) Controller and Processor recognize that future modifications to this DPA may be required to address CCPA amendments and implementing regulations that may be adopted or become operative at a later date.

4.3 Processor will ensure that each of its employees, consultants, and agents are made aware of its obligations under this DPA with regard to the security and protection of the Personal Data and shall require that they enter into binding obligations with Processor to respect and maintain the confidentiality and security of the Personal Data to the levels of security and protection provided for in this DPA.

4.4 Processor will not keep the Personal Data longer than is necessary for the Purposes and will, at the choice of Controller, delete, return, or irreversibly anonymize all the Personal Data once the Purposes have been fulfilled (save to the extent that there is a lawful obligation on Processor to store the Personal Data).

4.5 Processor will provide reasonable assistance to Controller to facilitate the provision to Data Subjects of rights provided under applicable Data Protection Laws to the extent required by such Data Protection Laws.

4.6 Processor shall implement and maintain reasonable security measures appropriate to the nature of the Personal Data, in order to protect the Personal Data from a Security Incident and at least those measures set out in **Schedule**

B. If Processor becomes aware of such a Security Incident, Processor will promptly: (a) notify Controller of the Security Incident but no later than 36 hours of Processor becoming aware; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

4.7 Notwithstanding anything to the contrary, Processor undertakes to take commercially reasonable steps to repair any harm any person may suffer due to Processing performed in breach of Data Protection Laws or this DPA, except if Processor proves that it is not liable for such harm.

4.8 To the extent that Controller transfers Personal Data to Processor, Controller shall be solely responsible for the lawfulness of the transfer under Data Protection Laws and is obligated to ensure that Controller's instructions for the Processing by Processor are lawful under applicable data protection law. Controller's instructions to Processor include but are not limited to communications sent via email by Controller to Processor, the actions undertaken by Controller's Authorized Users in the Portal, and/or Controller's usage of single sign on in concert with the Service.

4.9 Processor is obliged to establish the Technical and Organizational Measures according to Schedule B before the start of the Processing and to maintain them for the duration of the contractual relationship. Controller hereby confirms that the Technical and Organizational Measures are suitable and appropriate for its purposes.

5. SUB-PROCESSING

5.1 The Processor shall not sub-contract to any third party any of its obligations to Process Personal Data (each, a Sub-processor) unless all of the following provisions of this Clause 5 have first been complied with:

(a) Processor has provided reasonable prior notice (at least thirty (30) days') to Controller and Controller has not objected to such Sub-processor on reasonable grounds; and

(b) the proposed Sub-processor has agreed to adhere to standards that are substantially the same and no less robust than those that apply to Processor under this DPA.

5.2 For the purpose of Clause 5.1(a), Controller authorizes the use of the Sub-processors in Schedule A.

6. AUTHORIZED PROVIDER OF SERVICE

6.1 Subject to Section 10(b) of the Agreement, TGA uses aggregated or anonymized Personal Data for operating and improving the experience on the Service. To the extent TGA Processes Personal Data for the purposes of creating aggregated or anonymized data, it does so as a Controller pursuant to Data Protection Laws (including, without limitation, GDPR) and the terms of

the Privacy Policy for the Service (https://thetrainingarcade.com/privacy-policy/).

7. ONWARD TRANSFER OF DATA

7.1 Processor shall not onward transfer any Personal Data received from the Controller within or outside the United States of America without prior written consent of Controller.

7.2 Any such onward transfer of Personal Data shall comply with Data Protection Laws and be subject to an agreement the terms of which are no less robust than the terms included in this DPA.

7.3 Processor and its Sub-processors shall put in place appropriate safeguards for such onward transfers where necessary pursuant to Data Protection Laws.

8. LIABILITY

8.1 To the extent permitted by applicable laws, the aggregate liability of TGA for a breach of this DPA shall be subject to the limitation on the liability provisions under the Agreement. For the avoidance of doubt, to the extent permitted by applicable laws, any liability arising under this DPA shall be deemed to be included under the cap on liability under the Agreement and the cap under the Agreement shall not apply as a separate liability cap for this DPA.

9. TERMINATION

9.1 This DPA may be terminated, with immediate effect, on the agreement of the Parties.

9.2 The termination of this DPA does not exempt either Party from its obligations under this DPA as regard to the Processing of the Personal Data. In the event of termination, Processor shall return all Personal Data to Controller or, at the Controller's request, erase, destroy, or irreversibly anonymize all copies of the same unless prevented from doing so by law in which case it will keep such Personal Data confidential and not process it for any purpose other than as directed by Controller or required by law.

10. GENERAL

10.1 To the extent required to comply with Data Protection Laws, or the requirements of a competent supervisory authority, (a) TGA may update this DPA at this URL from time to time by posting an updated DPA on this URL, and Customer's continued use of the Services constitutes Customer's acceptance of the updated Agreement, or (b) TGA may require Customer to execute a new data processing addendum or comparable terms to this DPA with TGA.

10.2 Failure or neglect by a Party to enforce at any time any of the provisions hereof shall not be construed nor shall be deemed to be a waiver of that Party's rights hereunder nor in any way affect the validity of the whole or any part of this DPA nor prejudice that Party's rights to take subsequent action.

10.3 This DPA and the Agreement supersede and replace any arrangements, representations (excluding fraudulent representations) understandings, promises or agreements made or existing between the Parties prior to the signing of this DPA, and this DPA constitutes the entire understanding between the Parties hereto regarding the subject matter hereof.

10.4 In the event that any or any part of the terms, conditions or provisions contained in this DPA, or any Schedule attached or adopted as relative hereto shall be determined by any competent authority to be invalid, unlawful or unenforceable to any extent such term, condition or provision shall to that extent be severed from the remaining terms and conditions which shall continue to be valid and enforceable to the fullest extent permitted by law.

10.5 If and to the extent that either Party (the "**Affected Party**") is hindered or prevented by circumstances not within its reasonable ability or control, including, but not limited to, acts of God, severe weather, flood, lightning, fire, acts or omissions of Governments or other competent authority, acts of terrorism, war, military operations, acts or omissions of third parties for whom the Affected Party is not responsible ("**Force Majeure**") from performing any of its obligations under this DPA, the Affected Party shall be relieved of liability for failure to perform such obligations for the duration of such Force Majeure event.

10.6 This DPA shall inure to the benefit of and be binding upon the Parties and their respective successors and assigns.

10.7 The headings preceding the text of the clauses of this DPA are for purposes of reference only and will not limit or otherwise affect the meaning hereof.

10.8 This DPA may be executed in any number of counterparts, each of which, when executed, shall be an original and all of which together shall constitute one and the same agreement. The Parties each further consent to and acknowledge that a copy of the executed version of this DPA which is retained in electronic form shall constitute an original of this DPA, and that such original shall be relied on by the Parties for subsequent reference and as evidence of this DPA.

10.9 This DPA and any dispute or claim arising out of it or in connection with its subject matter or formation shall be governed by and construed in accordance with the Agreement.

This DPA has been signed and entered into by duly authorized representatives of the Parties to be effective as of the Effective Date of the Agreement, incorporating this DPA by reference.

SCHEDULE A - PERSONAL DATA PROCESSING PURPOSES AND DETAILS

1. SUBJECT MATTER OF PROCESSING

   TGA's provision of a cloud-based customizable training game service and any related technical or customer support to Customer and its authorized end users.

2. DURATION OF PROCESSING

   The Personal Data is retained for the term of the Agreement and a three-month period after the term expires ("**Post Expiration Period**"). During the Post Expiration Period, Users can access and play the games. The Personal Data is needed during the Post Expiration Period for the following reasons: (i) gate access to the Service to only the Authorized Users intended by Controller, (ii) deliver the results of the User activity on their local device to the database hosted in the cloud which resides in the United States for Controller to view, (iii) send Service-related emails to Authorized User, and (iv) provide customer and technical support to Controller.

3. NATURE OF PROCESSING

   The first name and last name of the Controller Authorized User is used two ways: (i) on game leaderboards (the Authorized User decides what identifying data will appear on a leaderboard) and (ii) to identify the Authorized User in the Service analytics. The data is transferred when a User starts a game and then again when they finish playing, as well as when the Authorized User accesses the Service analytics.

   Email address is used to send Authorized Users (as applicable) password resets, invitations to participate in certain Service activities, and information on their performance in the Service activities. The frequency of the data transfer of email data is dependent on (i) whether the email address is used as the unique identifier for Controller Authorized User, if so, the frequency of transfer is each time a game is started and then finished by an Authorized User, (ii) how often an Authorized User needs to be reminded of their password, (iii) whether the Controller invites Authorized Users to gamification activities, and (iv) the cadence of communication designated by a particular Authorized User for transmittal to another Authorized User (none, weekly, or monthly).

   A unique identifier (such as employee ID #) is used to confirm authorized access to the Service when the Controller uses single sign on for the Service and can be used to associate Service activity to a particular Authorized User in the Service analytics and to Service-related permissions for Authorized Users in the Service Portal. The frequency of the unique ID data transfer is directly proportional to the Service usage as indicated in the "frequency of the transfer" section.

   The IP Address is used solely when fraudulent use of the Service requires identifying a specific user such as an Authorized User who is cheating in a game. The IP Address is transferred each time a user accesses the Service, and the frequency of its transfer is tied to the Service usage as indicated in the "frequency of the transfer" section.

   Processor will process Personal Data for the following Business Purposes under the CCPA:

(a) Helping to ensure security and integrity to the extent the use of the information is reasonably necessary and proportionate for these purposes.

(b) Debugging to identify and repair errors that impair existing intended functionality.

(c) Performing services on behalf of the business, such as maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

(d) Undertaking internal research for technological development and demonstration.

(e) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance such a service or device.

4. PERSONAL DATA CATEGORIES

Customer Data, as defined in the Agreement, less Prohibited Data.

For purposes of clarity, such Customer Data includes the following: (i) first name, (ii) last name, (iii) email address, (iv) unique identifier such as employee ID # (if the email address is not used as the unique identifier), (v) internet protocol address ("IP Address") and (vi) the data associated with the game ranking/leaderboard and game analytics.

Customer is strictly forbidden from requesting Prohibited Data from its Authorized Users or otherwise submit Prohibited Data to the service and is entirely responsible for all consequences of doing so, including but not limited to indemnifying TGA from such submission.

5. DATA SUBJECT TYPES

Authorized Users (as defined by the Agreement)

6. SUB-PROCESSORS

Name of Sub-Processor	**Location of Processing**	**Processing Activities**
Amazon Web Services (AWS)	North America	Database and application hosting. Authorized User can log-in to the Service to create training games, publish games for their Authorized Users to play, and review analytics for their user activity. In addition, AWS is used to send service-related emails to Authorized Users such as password resets, invitations to participate in certain Service activities, and overviews of their performance in those activities as compared to their peers.

SCHEDULE B - TECHNICAL AND ORGANIZATIONAL MEASURES

This Schedule describes the technical and organizational measures of the provider ("The Game Agency, LLC", "TGA", or "organization") at the time of the conclusion of the contract ("Agreement"). If the provider makes material changes during the contract period, the customer will be informed about them.

The scope of the referenced documents extends over TGA's policies and controls as they apply to the services being offered through The Training Arcade®. In addition, the documents also apply to the portions of customer environments that are contractually in the provider's operational responsibility.

Guidelines, standards, process descriptions and the documentation of the implementation of the procedures are internal documents of the provider, which are generally not made available to customers or third parties subject to the parties execution of appropriate non-disclosure agreements.

1. Procedures for regular monitoring, analysis and evaluation

a. Data protection management

Data protection management	Requirement	Status	References
Data protection management system for the protection of Personal Data	Data protection officer	The organization has appointed a Security Manager who reports directly to executive management. The Security Manager's role includes responsibility for data protection.	• Information Security Policy
	Data protection policies	The organization maintains appropriate information security policies that include provisions for data protection. Employees are required to review the policies on an annual basis as part of the organization's security program.	• Information Security Policy • Access Control Policy • Data Retention and Disposal Policy • Internal Privacy Policy • Privacy Policy for Websites • Risk Assessment Policy • Server Security Policy • Vulnerability and Penetration Testing Management Policy
	Continual improvement process for data protection and information security	The organization maintains an effective information security management system. Policies and controls are reviewed on a regular basis. This ensures the technical and organizational measures will be checked on a regular basis and improvements will be tracked and documented.	• Information Security Policy
	Auditing of data protection measures	Control implementation status and effectiveness is reviewed during internal audits. Executive management reviews policies on a regular basis. Risk assessments are conducted on a regular basis.	• Information Security Policy

b. Organizational controls

Organisation	Requirement	Status	References

General organizational measures	The organization maintains an effective Information Security Management System (ISMS).	The ISMS includes a set of policies and supporting controls.	• Information Security Policy
	Security Manager	The organization has appointed a Security Manager who is responsible for overseeing the organization's security program. The roles and responsibilities of the Security Manager are set forth in the Information Security Policy.	• Information Security Policy
	Information security policy	The organization has a complete set of information security policies.	• Information Security Policy
	Password policy	The organization has a password policy that meets current best practices and government guidance.	• Password Policy
	Internal control system	The organization has an appropriate set of security controls to support the security policy objectives.	• Information Security Policy • Supporting policies and all controls.
	Risk management	The organization's security policies require an annual risk assessment and are supported by appropriate controls.	• Information Security Policy • Risk Assessment Policy
	Employee compliance and training	Employees are required to review and comply with all policies and are provided with annual security awareness training.	• Information Security Policy

c. Incident-Response Management

Incident-Response Management	Requirement	Status	References
Handling of Security Incidents in with relation to Personal Data	Process for security incidents	The organization has an Incident Response Plan supported by appropriate security policies and controls. Issues related to personal data are included in the plan.	• Information Security Policy • Incident Management Policy • Incident Response Plan • GDPR Breach Notification Procedure
	Security incidents will be noticed and handled. The incidents will be documented and reported and if needed also reported according to Art. 33 GDPR.	Intrusion detection and proactive monitoring are in place. A security incident reporting procedure is in place.	• Information Security Policy • Network Security Policy • Incident Management Policy • Incident Response Plan • GDPR Breach Notification Procedure

d. Data protection-friendly defaults

Data protection friendly defaults	Requirement	Status	References
Privacy and security by design.	Data protection is considered during design, development, and operation of systems and services.	Appropriate policies and procedures are in place to ensure that data protection is considered.	• Information Security Policy • Change Management Policy • Privacy Impact Assessment Policy and Procedure • Risk Assessment Policy

e. Order control

Order	Requirement	Status	References
Measures to ensure competence and compliance with customer and contractual requirements.	Criteria for choosing the contractor	The organization has policies in place that require assessing the competence and performance of contractors.	• Vendor Management Policy
	Checks of potential contractors	The organization performs background checks on contractors commensurate with their role.	• Vendor Management Policy
	Evaluation of IT security before order decision	The organization considers IT security prior to accepting a new contract.	• Information Security Policy • Risk Assessment Policy • Customer Support and SLA Policy
	Clear contract design	The organization has a standard subscription agreement in place for the customer to review prior to accepting.	• Customer Support and SLA Policy
	Contract execution prior to onboarding.	The organization verifies that the contract is signed by the customer and organization prior to customer onboarding.	• Customer Support and SLA Policy

2. Confidentiality

a. Physical Access Control

Personal Access control	Requirement	Status	References
General regulation for access control	Regulation of access to data processing equipment	Physical security, including physical access control, is provided by the datacenter owner, Amazon Web Services. The organization regularly reviews the performance and compliance of all vendors.	• Vendor Management Policy
Protection of rooms with data processing systems from unauthorized access	Fenced premises	Physical security, including physical access control, is provided by the datacenter owner, Amazon Web Services. The organization regularly reviews the performance and compliance of all vendors.	• Vendor Management Policy
	Alarm system and video monitoring	Physical security, including physical access control, is provided by the datacenter owner, Amazon Web Services. The organization regularly reviews the performance and compliance of all vendors.	• Vendor Management Policy
	Identity check at building access	Physical security, including physical access control, is provided by the datacenter owner, Amazon Web Services. The organization regularly reviews the performance and compliance of all vendors.	• Vendor Management Policy
	Access control system	Physical security, including physical access control, is provided by the datacenter owner, Amazon Web Services. The organization regularly reviews the performance and compliance of all vendors.	• Vendor Management Policy

	Key Policy	Physical security, including physical access control, is provided by the datacenter owner, Amazon Web Services. The organization regularly reviews the performance and compliance of all vendors.	• Vendor Management Policy
	Additional policies	Physical security, including physical access control, is provided by the datacenter owner, Amazon Web Services. The organization regularly reviews the performance and compliance of all vendors.	• Vendor Management Policy

b. IT System Access Control

IT System Access Control	Requirement	Status	References
Protection of computer systems against access for unauthorized persons	Access to systems only via access permissions	The organization has an access control policy in place that is supported by appropriate controls. Access to all production systems is restricted to authorized individuals.	• Information Security Policy • Access Control Policy • Password Policy
	Authorizations only after approval	The organization's policies requires that access be requested and approved prior to being granted.	• Access Control Policy
	Restricted Authorization	The organization has an access control policy in place that is supported by appropriate controls. Access is restricted to authorized personnel only. Access is revoked when no longer required.	• Access Control Policy
	Password procedures	The organization has a password policy that is supported by appropriate controls.	• Password Policy
	Logging and control of unauthorized login attempts	Logging and monitoring are in place. While systems vary in terms of capabilities, in general unauthorized login attempts that exceed a threshold result in account lockouts. This functionality is verified during penetration tests.	• Access Control Policy • Password Policy • Vulnerability and Penetration Testing Management
	Access to networks	The organization restricts access to all networks and information systems.	• Information Security Policy • Access Control Policy
IT System Access Control	Requirement	Status	
	Access via mobile devices	The Organization has a Personal Device (BYOD) Policy implemented where access via devices must meet organization security requirements be approved by the Security Manager.	• Personal Devices (BOYD) Policy

c. Data Access Control

Data Access Control	Requirement	Status	References
Protection of data against access by unauthorized persons	Access to data only via access permissions.	The organization restricts access to data to authorized individuals with a legitimate business reason. Policies and controls are in place to approve and revoke access.	• Access Control Policy

	Authorization and withdrawal	The organization restricts access to data to authorized individuals with a legitimate business reason. Policies and controls are in place to approve and revoke access.	• Access Control Policy
	Control of granted authorization	The organization restricts access to data to authorized individuals with a legitimate business reason. Policies and controls are in place to approve and revoke access.	• Access Control Policy
	Controlled destruction of data and printouts	The Organization has a Data Retention and Disposal policy with appropriate supporting controls.	• Data Retention and Disposal Policy

d. Separation Control

Separation Control	Requirement	Status	References
Separation of data items that are processed for different purposes	Client separation of the system	The Training Arcade® is multi-tenant. The application applies logical access controls and business rules to separate data belonging to different subscribers.	• Information Security Policy • Change Management Policy
	Purpose limitation of the systems	The system is used only for the purpose of providing the service contracted by customers.	• Information Security Policy
	Purpose limitation of the data	Data is used only for the purpose of providing the service contracted by customers.	• Information Security Policy
	Separation of production and test data	Organization policy does not allow use of production data outside of the production environment.	• Information Security Policy

e. Pseudonymization and Encryption

Encryption	**Requirement**	**Status**	**References**
Encryption of Personal Data	Protection assessment	Personal Data is encrypted in transport and at rest.	• Information Security Policy • Network Security Policy • Key Management and Encryption Policy
	Definition and availability of encryption methods	The organization has a policy on the use of encryption and, in summary, only uses appropriate commercial encryption algorithms and protocols.	• Key Management and Encryption Policy
Pseudonymization	**Requirement**	**Status**	
Processing in a way that the data can no longer be assigned to a specific person without the need for additional information	Preferred pseudonymization of Personal Data	The Training Arcade® only collects the minimal Personal Data required to provide the service. It is not possible to anonymize or pseudonymize this data and still provide the data required by subscribers. However, customers have the option of providing an anonymous identifier instead.	• Information Security Policy • Privacy Impact Assessment Policy and Procedure

3. Integrity

a. Control of transfer

Control of transfer	Requirement	Status	References
Protection of data during storage or transmission against unauthorized copying, modification or deletion	Organizational specifications for the storage of data media	Data is not transferred on media. Data is encrypted in transit and at rest.	• Information Security Policy • Network Security Policy • Key Management and Encryption Policy
	Protected rooms for data storage	Physical security, including physical access control, is provided by the datacenter owner, Amazon Web Services. The organization regularly reviews the performance and compliance of all vendors.	• Vendor Management Policy
	Protective measures for data transmission over the Internet	Data is encrypted for transmission across public networks, including the Internet.	• Information Security Policy • Network Security Policy • Key Management and Encryption Policy
	Physical data transport, e.g., tapes, only by specialist companies	Data is not transported on media. It remains within the Amazon Web Services datacenters.	• Not applicable
	Encryption of data carriers	Data is not transported on media. It remains within the AWS datacenters.	• Not applicable
	Passing on the data to third parties	Data is not provided to third parties.	• Not applicable

b. Input control

Input	Requirement	Status	References
	Storage of system logs	Logs are collected on servers. A centralized log collection and analysis system is in place and applications are being updated to improve log collection and transport.	• Server Security Policy

4. Availability and Resilience

a. Availability

Availability	Requirement	Status	References
Protection of data against accidental destruction or loss	Regular backups	Regular backups implemented by AWS Backup Plans	• Information Security Policy • Disaster Recovery Plan

	Mirroring hard disks, e.g., RAID procedure	Data is stored using redundant storage in multiple AWS availability zones.	• Information Security Policy • Disaster Recovery Plan
	Protective measures against fire and water	Physical security, including protection against fire, flood, and other environmental threats, is provided by the datacenter owner, Amazon Web Services. The organization regularly reviews the performance and compliance of all vendors.	• Vendor Management Policy
	Uninterruptible power supply ("UPS")	Power, including UPS and generator, is provided by the datacenter owner, Amazon Web Services. The organization regularly reviews the performance and compliance of all vendors.	• Vendor Management Policy
	Separated storage	Data store separation is provided by the cloud services provider, Amazon Web Services. The organization regularly reviews the performance and compliance of all vendors.	• Vendor Management Policy
	Use of firewalls and anti-virus / anti-malware software and systems	Network-level controls, including AWS Security Groups, are used to block all network traffic that is not specifically required for the application to function. Based on the organization's risk assessment, anti-virus/anti-malware software is not required on Linux servers. Anti-virus software and firewalls are used on all workstations.	• Information Security Policy • Network Security Policy • Workstation Security Policy

5. Assistance by Processor and Sub-processor(s)

Transfers to (sub-)processors	Requirement	Status	References
Transfers to Processor	Technical and organizational measures to provide assistance to Controller	To assist controller in responding to requests to exercise rights granted to Data Subjects under Data Protection Laws, the organization will provide assistance as set forth in the DPA. The organization has created a policy document and internal procedures for responding to requests from Authorized Users regarding their data management requests which comply with Data Protection Laws, and maintains a detailed data subject rights request spreadsheet to track each step in the process of responding to data subject management requests. The organization regularly trains its relevant customer service personnel on communicating with the controller and Authorized Users on how to manage such requests in a timely fashion. To further assist controller in responding to enquiries and requests made by Data Subjects under Data Protection Laws	• Privacy Policy • Data Subject Rights Procedure and

		applicable to the organization, or for Data Protection Laws applicable to processing by controller, the organization also makes available to the controller the privacy officer of the organization, Richard J. Lowenthal, via email address (Richard.lowenthal@thegameagency.com) and via mobile phone (+1 310-863-8107) To assist controller in ensuring compliance with data security and data processing obligations under Data Protection Laws applicable to controller, the organization has established the technical and organizational measures described above in Tables 1 – 4. To assist controller in demonstrating compliance with its obligations pertaining to processors under Data Protection Laws applicable to controller and exercising audit and inspection rights available to controller thereunder, the organization shall make available certain internal guidelines, standards, process descriptions, internal documentation and other information relating to the Processing of Personal Data on behalf of controller that is reasonably requested for such purposes, subject to the parties execution of appropriate non-disclosure agreements.	
Transfers from Processor to Sub-processor(s)	Technical and organizational measures to be taken by Sub-processor to provide assistance to Data Exporter	The organization shall only engage sub-processors in accordance with the terms and conditions set forth in the DPA, and shall not engage any sub-processor unless the proposed sub-processor has agreed to adhere to standards that are substantially the same and no less robust than those that apply to processer under the Agreement and the EEA Standard Contractual Clauses or any other International Data Transfer Mechanism (where applicable).	• Privacy Policy

SCHEDULE C – JURISDICTION-SPECIFIC OBLIGATIONS AND INFORMATION FOR INTERNATIONAL TRANSFERS

1. EUROPEAN ECONOMIC AREA

1.1 In the event Controller has determined that the GDPR is applicable, the Parties hereby incorporate Module Two of the EEA Standard Contractual Clauses in **Exhibit A** (the "**SCCs**") for the Processing of Personal Data Pursuant to GDPR and for Transfers to TGA or its Sub-processors from the EEA that require an International Data Transfer Mechanism and also enter into and agree to be bound by the SCCs.

1.2 In the event Controller has determined that the GPDR is not applicable, the SCCs shall not apply.

2. SWITZERLAND

2.1 In the event Controller has determined that the Federal Act on Data Protection is applicable, the Parties hereby incorporate the EEA Standard Contractual Clauses attached in Exhibit A subject to the following modifications (the "**modified SCCs**") for the Processing of Personal Data subject to the Federal Act on Data Protection and for Transfers to TGA or its Sub-processors from Switzerland that require an International Data Protection Mechanism also enter into and agree to be bound by the modified SCCs:

(a) The Parties adopt the GDPR standard for all data transfers from Switzerland.

(b) Clause 13 and Annex I(C): The competent authorities under Clause 13, and in Annex I(C), are the Federal Data Protection and Information Commissioner and, concurrently, the EEA member state authority identified in Annex I(C).

(c) Clause 17: The parties agree that the governing jurisdiction is the Republic of Ireland.

(d) Clause 18: The parties agree that the forum is the Republic of Ireland. The Parties agree to interpret the EEA Standard Contractual Clauses so that Data Subjects in Switzerland are able to sue for their rights in Switzerland in accordance with Clause 18(C).

(e) The Parties agree to interpret the EEA Standard Contractual Clauses so that "Data Subjects" includes information about Swiss legal entities until the revised Federal Act on Data Protection becomes operative.

2.2 In the event Controller has determined the Federal Act on Data Protection is not applicable, the modified SCCs shall not apply.

3. UNITED KINGDOM

3.1 In the event Controller has determined that the UK GDPR is applicable, the Parties hereby incorporate the UK International Data Transfer Addendum to the EEA Standard Contractual Clauses in **Exhibit B** ("**UK Addendum**") for the Processing of Personal Data subject to the UK GDPR and for Transfers to TGA or its subprocessors from the United Kingdom ("**UK**") that require an International Data Protection Mechanism and also enter into and agree to be bound by the UK Addendum.

3.2 In the event Controller has determined that the UK GDPR is not applicable, the UK Addendum shall not apply.

EXHIBIT A

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/15.

information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 - Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without

prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall

contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, :] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Republic of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: Customer

   Address: As set forth in the Agreement.

   Contact person's name, position, and contact details: As set forth in the Agreement.

   Activities relevant to the data transferred under these Clauses: Identification process for the Controller's Authorized Users to access Processor's platform, associate the activity data to the corresponding user, and communicate with them regarding relevant activity for the service related to Authorized User.

   Processor shall provide Customer details set forth in the Agreement upon request of a concerned data subject, competent supervisory authority, or a competent court.

   Signature and date: These clauses have been signed and entered into by duly authorized representatives of the Parties to be effective as of the Effective Date of the Agreementincorporating the DPA and these Clauses by reference.

   Role (controller/processor): Controller

Data importer(s):

1. Name: The Game Agency, LLC

   Address: 470 West Avenue, Suite #2002, Stamford, CT 06902, USA

   Contact person's name, position and contact details:

   - Richard J. Lowenthal, Chief Operating Officer, richard.lowenthal@thegameagency.com, +1 (310) 863-8107
   - EU and UK Representative: Rickert Rechtsanwaltsgesellschaft mbH, Colmantstrasse 15, 53115 Bonn, Germany

   Activities relevant to the data transferred under these Clauses: Identification process for the Customer's Authorized Users to access the TGA platform and associate the activity data to the correct user for the Customer's Authorized User.

   TGA's Service receives the transferred data from Customer and uses it to gate access to the Service, provide the permitted level of Service to each Data Subject, and associate the relevant Service activity for each Data Subject.

   Signature and date: These clauses have been signed and entered into by duly authorized representatives of the Parties to be effective as of the Effective Date of the Agreementincorporating the DPA and these Clauses by reference.

   Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Authorized Users (as defined by the Agreement)

Categories of personal data transferred

Customer Data, as defined in the Agreement, less Prohibited Data, as defined in the DPA.

For purposes of clarity, such Customer Data includes the following: (i) first name, (ii) last name, (iii) email address, (iv) unique identifier such as employee ID # (if the email address is not used as the unique identifier), (v) internet protocol address ("IP Address") and (vi) the data associated with the game ranking/leaderboard and game analytics.

Customer is strictly forbidden from requesting Prohibited Data from its Users or otherwise submit Prohibited Data to the service and is entirely responsible for all consequences of doing so, including but not limited to indemnifying TGA from such submission.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A (none).

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Data is transferred during the term of the Agreement and a three-month period after the term expires ("**Post Expiration Period**"). Discrete data transfer occurs when a Customer's Authorized User signs into the service to create or edit a game or view the results of the games played by Customer's Authorized Users. Data transfer also occurs at the discrete times when an Authorized User logs into TGA's Service to play a game. The data transfer enables a particular Authorized User to access the Portal and for another Authorized User to access the games. A subsequent data transfer occurs when the User has completed playing a game and their activity in the game is transferred back to Controller's servers. The frequency of the data transfer is dependent on the number of games created by a particular Authorized User and played by other Authorized Users, the number of Authorized Users playing, the period of time in which the games are available, and the frequency by which the Authorized Users play the game. For more details on the frequency of transfer, please see the next section, "Nature of the processing".

Nature of the processing

Data is processed in connection with TGA's provision of a cloud-based customizable training game service and any related technical or customer support to Customer and its Authorized Users.

The first name and last name of the Authorized User is used two ways: (i) on game leaderboards (the Authorized User decides what identifying data will appear on a leaderboard) and (ii) to identify the Authorized User in the Service analytics. The data is transferred when an Authorized User starts a game and then again when they finish playing, as well as when the Authorized User accesses the Service analytics.

Email address is used to send Authorized Users (as applicable) password resets, invitations to participate in certain Service activities, and information on their performance in the Service activities. The frequency of the data transfer of email data is dependent on (i) whether the email address is used as the unique identifier for Controller Authorized Users, if so, the frequency of transfer is each time a game is started and then finished by an Authorized User, (ii) how often an Authorized User needs to be reminded of their

password, (iii) whether Controller invites Authorized Users to gamification activities, and (iv) the cadence of communication designated by a particular Authorized User for transmittal to other Authorized Users (none, weekly, or monthly).

A unique identifier (such as employee ID #) is used to confirm authorized access to the Service when the Controller uses single sign on for the Service and can be used to associate Service activity to a particular Authorized User in the Service analytics and to Service-related permissions for Authorized Users in the Service Portal. The frequency of the unique ID data transfer is directly proportional to the Service usage as indicated in the "frequency of the transfer" section.

The IP Address is used solely when fraudulent use of the Service requires identifying a specific user. The IP Address is transferred each time a user accesses the Service, and the frequency of its transfer is tied to the Service usage as indicated in the "frequency of the transfer" section.

The User's actions within the game/s of the Customer will be analysed in view of their response to questions and overall performance in the training.

Purpose(s) of the data transfer and further processing

The purpose of the data transfer is to (i) gate access to the Service to only the Authorized Users intended by Controller, (ii) deliver the results of the Authorized Users' activity on their local device to the database hosted in the cloud which resides in the United States for Controller to view, (iii) send Service-related emails to Authorized Users, and (iv) provide customer and technical support to Controller.

The purpose of the further processing regarding the data associated with the game ranking/leaderboard is to provide the Authorized Users with quantifiable general feedback on the Authorized User's performance relative to others in the Customer designated group of Authorized Users. The data associated with game analytics provides the particular Authorized User with specific insights into the Authorized User's performance in the training game (such as correct or incorrect responses), the Authorized User's learning progress, and the overall learning trends for all the Authorized Users playing a particular game.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The personal data is retained for the term of the Agreement and the Post Expiration Period. During the Post Expiration Period, Authorized Users can access and play the games. The personal data is needed during the Post Expiration Period for the reasons indicated in the section "Purpose(s) of the data transfer and further processing".

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter is indicated in the section "Nature of the processing." The transfers and sub-processing are to enable database and application hosting. In addition, Amazon Web Services (AWS) is used to send service-related emails to Authorized Users indicated in the section "Nature of the processing".

The duration of the processing is the term of the Agreement and the Post Expiration Period.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Ireland's Data Protection Commission

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The Parties agree that Schedule B of the DPA describes the technical and organizational measures applicable to the Transfer.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Name: Amazon Web Services (AWS)

Address: North America

Contact person's name, position and contact details: AWS Account Manager: Austin Rodriguez, aurodri@amazon.com, (512) 697-4556, 410 Terry Ave. North, Seattle, WA 98109

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Database and application hosting. Authorized Users can log-in to the Service to create training games, publish games for their Users to play, and review analytics for their User activity. In addition, AWS is used to send service-related emails to Users such as password resets, invitations to participate in certain Service activities, and overviews of their performance in those activities as compared to their peers.

EXHIBIT B

UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("UK Addendum")

Background

This UK Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other Party also agreeing to be bound by this UK Addendum.
2. Although Annex 1A and Clause 7 of the EEA Standard Contractual Clauses require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the EEA Standard Contractual Clauses and any part of the EEA Standard Contractual Clauses.

Interpretation of this Addendum

3. Where this UK Addendum uses terms that are defined in the EEA Standard Contractual Clauses or the DPA those terms shall have the same meaning as in the EEA Standard Contractual Clauses or the DPA. In addition, the following terms have the following meanings:

Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved UK Addendum	The template UK Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 15.
EEA Standard Contractual Clauses	As defined in the DPA.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
SCCs	The version of the EEA Standard Contractual Clauses which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Addendum	This UK International Data Transfer Addendum which is made up of this UK Addendum incorporating the SCCs.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy, and/or electronic communications in force from time to time in the UK, including the UK GDPR

	and the Data Protection Act 2018.

To the extent there is any conflict between the definition for a term set forth in this UK Addendum and in the DPA, the definition set forth in this UK Addendum shall prevail for the purposes of this UK Addendum.

4. This UK Addendum must always interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in SCCs amend the EEA Standard Contractual Clauses in any way which is not permitted under the EEA Standard Contractual Clauses or the Approved UK Addendum, such amendment(s) will not be incorporated in this UK Addendum and the equivalent provision of the EEA Standard Contractual Clauses will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this UK Addendum, UK Data Protection Laws applies.
7. If the meaning of this UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, reenacted and/or replaced after this UK Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the EEA Standard Contractual Clauses sets out that the EEA Standard Contractual Clauses prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved UK Addendum and the SCCs (as applicable), the Approved UK Addendum overrides the SCCs, except where (and in so far as) the inconsistent or conflicting terms of the SCCs provides greater protection for data subjects, in which case those terms will override the Approved UK Addendum.
11. Where this UK Addendum incorporates the SCCs which have been entered into to protect transfers subject to the GDPR then the Parties acknowledge that nothing in this UK Addendum impacts the SCCs.

Incorporation of and changes to the EEA Standard Contractual Clauses

12. This UK Addendum incorporates the SCCs which are amended to the extent necessary so that:
    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the SCCs; and
    c. this UK Addendum (including the SCCs incorporated into it) is (1) governed by the laws of England and Wales; and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. No amendments to the EEA Standard Contractual Clauses other than to meet the requirements of Section 12 may be made.
14. The following amendments to SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the SCCs;

b. In Clause 2, delete the words: "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.8(i) is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

e. References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws." References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

f. References to Regulation (EU) 2018/1725 are removed;

g. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

h. Clause 13(a) and Part C of Annex I are not used;

i. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

j. In Clause 16(e), subsection (i) is replaced with: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;"

k. Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales.";

l. Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

m. The footnotes to the EEA Standard Contractual Clauses do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this UK Addendum

15. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved UK Addendum, including correcting errors in the Approved UK Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved UK Addendum will specify the start date from which the changes to the Approved UK Addendum are effective and whether the Parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised UK Approved Addendum from the start date specified.

16. If the ICO issues a revised Approved UK Addendum under Section 15, if any Party selected in Table 4 "Ending the UK Addendum when the Approved UK Addendum changes", will as a direct result of the changes in the Approved UK Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the UK Addendum; and/or

    b. its risk under the UK Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved UK Addendum.

Part 2: Tables

Table 1: Parties

Start Date	The date of the Agreement.	
The Parties	**Data exporter: Customer or Controller**	**Data importer: TGA or Processor**
Parties' details	Full legal name: As set forth in the Agreement. Trading name (if different): As set forth in the Agreement. Main address (if a company registered address): As set forth in the Agreement. Official registration number (if any) (company number or similar identified): As set forth in the Agreement. Processor shall provide provide Customer's details set forth in the Agreement upon request of a concerned data subject, competent supervisory authority, or a competent court.	Full legal name: The Game Agency, LLC Trading name (if difference): N/A Main address: 470 West Avenue, Suite 2002, Stamford, CT 06902, USA Official registration number (if any): N/A
Key Contact	Full Name (optional): As set forth in the Agreement. Job Title: As set forth in the Agreement. Contact details including email: As set forth in the Agreement. Processor shall provide provide Customer's key contact information set forth in the Agreement upon request of a concerned data subject, competent supervisory authority, or a competent court.	Full Name: Richard J. Lowenthal Job Title: Chief Operating Officer Contact details including email: - The Game Agency, LLC - 470 West Avenue, Suite 2002 Stamford, CT 06902 USA - +1 (310) 863-8107 - richard.lowenthal@thegameagency.com

Table 2: Selected SCC, Modules, and Selected Clauses

Schedule C	Module Two of the EEA Standard Contractual Clauses which this UK Addendum is appended to, detailed below, including the appendix information: Date: The Start Date in Table 1.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for Module Two as set out in the Appendix of the EEA Standard Contractual Clauses (other than the Parties), and which for this UK Addendum is set out in:

Annex 1A: List of Parties	As set forth under Table 1.
Annex 1B: Description of Transfer	As described in Section B of Annex I in the SCCs.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	As described in Annex II in the SCCs.
Annex III: List of sub-processors	As described in Annex II in the SCCs, or if not provided there in Section 6 in Schedule A of the DPA.

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Ending this UK Addendum when the Approved UK Addendum Changes	TGA and/or Customer may end this UK Addendum as set out in Section 16.