Data Processing Agreement (DPA)

Document Control

Date	22nd September 2023
Document Status	Live
Version	2
Date of Next Review	31st July 2024

Openplay Data Processing Agreement (DPA)

1. Definitions.

The definitions below are additional defined terms specific to this DPA. Any capitalised terms used in this DPA , which are not specifically defined below, shall have the meaning set out in the Definitions included in the Order Form of the Agreement above.

'Customer' means the Customer Company Name in the Order Form;

"**Account"** means Customer's account in the Service, in which Customer stores and processes Customer Data.

"Customer's Personal Data" means the types of Personal Data that the Customer may instruct Openplay to Process as specified in clause 3.5(f) below on behalf of the Customer and if applicable on behalf of the Affiliate;

"**Data Controller**" means an entity that determines the purposes and means of the Processing of Personal Data and for the purposes of this DPA would be the Customer or if applicable the Affiliate

"Data Protection Laws" means (i) Regulation 2016/679 of the European Parliament and of the Council 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) ("GDPR"); (ii) the United Kingdom's Data Protection Act 2018 (as well as any subsequent data protection law enacted by the United Kingdom); and (iii) any local, national or international laws, rules and regulations related to privacy, security, data protection, and/or the Processing of Personal Data, as amended, replaced or superseded from time to time.

"Data Processor" means Open Play that Processes Personal Data on behalf of a Data Controller.

"**Data Subject**" means the identified or identifiable natural person to whom the Personal Data relates.

"Personal Data" means (a) information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person or household; and (b) any information defined as "personal data", "personal information," or other similar terms under applicable Data Protection Laws.

"**Processing**" shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination and "**Process**", "**Processes**" and "**Processed**" will be interpreted accordingly.

"**Purposes**" shall mean (i) OpenPlay's provision of the Services under the Agreement, including Processing initiated by Customer Users in their use of the Services, and (ii) further documented, reasonable instructions from Customer agreed upon by the parties.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data.

"**Services**" means the Technical Services and Moves Rewards Platform specified in the Order Form above and any other services that may be provided by OpenPlay under the Agreement

"**Sub-processor**" means any other Data Processors engaged by OpenPlay to Process Customer Personal Data.

2. **Scope and Applicability of this DPA.** This DPA applies where and only to the extent that OpenPlay Processes Customer Personal Data on behalf of the Customer or Authorised Affiliates as Data Processor in the course of providing the Services.

3. **Roles and Scope of Processing.**

3.1 **Role of the Parties**. The Customer or as applicable the Affiliate are the Data Controller of Customer Personal Data.

3.2 **Customer Instructions**. OpenPlay will Process Customer Personal Data only for the Purposes. The Customer shall ensure its Processing instructions are lawful and that the Processing of Customer Personal Data in accordance with such instructions will not violate applicable Data Protection Laws. The parties agree that the Agreement (including this DPA) sets out Customer's complete and final instructions to OpenPlay for the Processing of Customer Personal Data. Any Processing outside the scope of these instructions will require prior written agreement between the Customer and OpenPlay.

3.3 **Authorized Affiliate.** OpenPlay's obligations set out in this DPA shall also extend to Authorized Affiliates, subject to the following conditions: (a) Customer must communicate any additional Processing instructions from its Authorized Affiliates directly to OpenPlay; (b) Customer shall be responsible for Authorized Affiliates' compliance with this DPA and all acts and/or omissions by an Authorized Affiliate with respect to Customer's obligations in this DPA shall be considered the acts and/or omissions of Customer; and (c) Authorized Affiliates shall not bring a claim directly against OpenPlay. If an Authorized Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against OpenPlay ("**Authorized Affiliate Claim**"): (i) Customer must bring such Authorized Affiliate Claim directly against OpenPlay on behalf of such Authorized Affiliate, unless Data Protection Laws require the Authorized Affiliate be a party to such claim; and (ii) all Authorized Affiliate Claims shall be considered claims made by Customer and shall be subject to any liability restrictions set out in the Agreement, including any aggregate limitation of liability.

3.4 **Customer Processing of Personal Data**. the Customer agrees that it: (a) will comply with its obligations under Data Protection Laws with respect to its Processing of Customer Personal Data; (b) will make appropriate use of the Services to ensure a level of security appropriate to the particular content of the Customer Personal Data; and (c) has obtained all consents, permissions and rights necessary under Data Protection Laws for OpenPlay to lawfully Process Customer Personal Data for the Purposes, including, without limitation, Customer's sharing and/or receiving of Customer Personal Data with third-parties via the Services.

3.5 **Details of Data Processing.**

(a) Subject matter: The subject matter of the Processing under this DPA is the Customer Personal Data.

(b) Duration: Notwithstanding expiry or termination of the Agreement, this DPA will remain in effect until, and will automatically expire upon, deletion of all Customer Personal Data as described in this DPA.

(c) Purpose: OpenPlay shall Process Customer Personal Data only for the Purposes.

(d) Nature of the Processing: OpenPlay provides Services as described in the Agreement.

(e) Categories of Data Subjects: The categories of Data Subjects to which Customer Personal Data relate are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Students
(ii) Employees
(iii) Members
(iv) Residents

(f) Customer Personal Data: The types of Customer Personal Data are determined and controlled by Customer in its sole discretion, and may include, but are not limited to:

(i) Identification and contact data (name, address, title, contact details);
(ii) Financial information (credit card details, account details, payment information);
(iii) Employment details (employer, job title, geographic location, area of responsibility); and
(iv) IT information (IP addresses, usage data, cookies data, location data).

(g) Special Categories of Personal Data (if applicable): Subject to any applicable restrictions and/or conditions in the Agreement and under the Data Protection Laws, Customer may also include 'special categories of personal data' or similarly sensitive personal data (as described or defined in Data Protection Laws) in Customer Personal Data, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Customer Personal Data revealing racial or ethnic origin, or data concerning health, illness or disability and physical activity levels.

4. Sub-processing.

4.1 **Authorized Sub-processors**. Customer generally authorizes the engagement of Sub-processors and specifically consents to those listed at Anex 2as of the Effective Date and any Affiliate of OpenPlay. For clarity, this Section 4 (Sub-Processing) constitutes Customer's general consent for OpenPlay's engagement of onward sub-processors.

4.2 **Sub-processor Obligations**. OpenPlay shall: (a) enter into a written agreement with each Sub-processor imposing data protection obligations no less protective of Customer Personal Data as OpenPlay's obligations in this DPA to the extent applicable to the nature of the services provided by such Sub-processor; and (b) remain liable for each Sub-processor's compliance with the obligations in this DPA. Upon written request, OpenPlay shall provide Customer all relevant information it reasonably can in connection with its applicable Sub-processor agreements where required to satisfy Customer's obligations under Data Protection Laws.

4.3 **Changes to Sub-processors.** OpenPlay shall provide such notification at least thirty (30) days in advance of allowing any new Sub-processor to Process Customer Personal Data (the "**Objection Period**"). During the Objection Period, Customer may object in writing to OpenPlay's appointment of the new Sub-processor, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss Customer's concerns in good faith with a view to achieving resolution. If Customer can reasonably demonstrate that the new Sub-processor is unable to Process Customer Personal Data in compliance with the terms of this DPA and OpenPlay cannot provide an alternative Sub-processor, or the parties are not otherwise able to achieve resolution as provided in the preceding sentence, Customer, as its sole and exclusive remedy, may terminate the Order Form(s) with respect only to those aspects of the Services which cannot be provided by

OpenPlay without the use of the new Sub-processor by providing written notice to OpenPlay. OpenPlay will refund Customer any prepaid unused fees of such Order Form(s) following the effective date of termination with respect to such terminated Services.

5. Security.

5.1 **Security Measures**. OpenPlay shall implement and maintain appropriate technical and organizational security measures designed to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data in accordance with its security practices, Includeing the measures set out at Annex I to this DPA ("Security Measures"). OpenPlay may review and update its Security Measures from time to time, provided that any such updates shall not materially diminish the overall security of the Services or Customer Personal Data.

5.2 **Confidentiality of Processing**. OpenPlay shall ensure that any person who is authorized by OpenPlay to Process Customer Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

5.3 **No Assessment of Customer Personal Data by OpenPlay**. OpenPlay shall have no obligation to assess the contents of Customer Personal Data to identify information subject to any specific legal requirements. Customer is responsible for reviewing the information made available by OpenPlay relating to data security and making an independent determination as to whether the Services meet Customer's requirements and legal obligations under Data Protection Laws.

6. Customer Audit Rights.

6.1 Upon written request and at no additional cost to Customer, OpenPlay shall provide Customer, or its appropriately qualified third-party representative (collectively, the "**Auditor**"), access to reasonably requested documentation evidencing OpenPlay's compliance with its obligations under this DPA (collectively, "**Reports**").

6.2 Customer may also send a written request for an audit (including inspection) of OpenPlay's facilities. Following receipt by OpenPlay of such request, OpenPlay and Customer shall mutually agree in advance on the details of the audit, including reasonable start date, scope and duration of, and security and confidentiality controls applicable to, any such audit. OpenPlay may charge a fee (rates shall be reasonable, taking into account the resources expended by OpenPlay) for any such audit. The Reports, audit, and any information arising therefrom shall be OpenPlay's Confidential Information.

6.3 Where the Auditor is a third-party, the Auditor may be required to execute a separate confidentiality agreement with OpenPlay prior to any review of Reports or an audit of OpenPlay, and OpenPlay may object in writing to such Auditor, if in OpenPlay's reasonable opinion, the Auditor is not suitably qualified or is a direct competitor of OpenPlay. Any such objection by OpenPlay will require Customer to either appoint another Auditor or conduct the audit itself. Expenses incurred by Auditor in connection with any review of Reports or an audit, shall be borne exclusively by the Auditor.

7. Data Transfers

7.1 **Hosting and Processing Locations.** OpenPlay will only host Customer Personal Data in the region(s) offered by OpenPlay and selected by Customer on an Order Form or as Customer otherwise configures via the Services (the "**Hosting Region**"). Customer is solely responsible for the regions from which its Users access the Customer Personal Data, for any transfer or sharing of Customer Personal Data by Customer or its Users and for any subsequent designation of other Hosting Regions (either for the same Account, a different Account, or a separate Service). Once the Customer has selected a Hosting Region, OpenPlay will not Process Customer Personal Data from outside the

Hosting Region except as reasonably necessary to provide the Services procured by Customer (provided that for any such Processing, the Processing shall only involve remote access and will not involve relocating the storage location of Customer Personal Data to a new country), or as necessary to comply with the law or binding order of a governmental body.

8. **Return or Deletion of Data.** Customer may retrieve or delete all Customer Personal Data upon expiration or termination of the Agreement as set out in the Agreement. Any Customer Personal Data not deleted by Customer shall be deleted by OpenPlay promptly upon the later of: (a) expiration or termination of the Agreement; and (b) expiration of any post-termination "retrieval period" set out in the Agreement. Upon Customer's written request, OpenPlay shall confirm such deletion in writing.

9. Security Incident Response.

9.1 **Security Incident Reporting.** If OpenPlay becomes aware of a Security Incident, OpenPlay shall notify Customer without undue delay, and in any case notify Customer within seventy-two (72) hours after becoming aware. OpenPlay shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

9.2 **Access Control**

9.2.1 **Preventing Unauthorized Product Access** Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: We host our product infrastructure with outsourced infrastructure providers. We do not own or maintain hardware located at the outsourced infrastructure providers' data centres. Production servers and client-facing applications are logically and physically secured from our internal corporate information systems. The physical and environmental security controls are audited for ISO 27001 and Cyber Essentials Plus compliance, among other certifications.

Authentication: We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorisation: Customer Data is stored in a single tenant storage system accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorisation to data sets is performed through validating the user's permissions against the attributes associated with each data set.

9.2.2 **Preventing Unauthorized Product Use:** We implement industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: We implement a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Code stored in our source code repositories is checked for best practices and identifiable software flaws using automated tooling.

Penetration testing: We maintain relationships with industry-recognized penetration testing service providers for penetration testing of the OpenPlay web application at least annually. The intent of these penetration tests is to identify security vulnerabilities and mitigate the risk and business impact they pose to the in-scope systems.

9.2.3 **Limitations of Privilege & Authorization Requirements:** Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, product development and research, to troubleshoot potential problems, to detect and respond to security incidents and implement data security.

9.3 **Input Control**

Detection: We designed our infrastructure to log extensive information about the system behaviour, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by technical, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to you will be in accordance with the terms of the Agreement.

9.4 **Availability Control**

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and heating, ventilation and air conditioning (HVAC) services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online DB backups: Production databases are backed up and maintained using at least industry standard methods.

Disaster Recovery Plans: We maintain and test at least annually a disaster recovery plan to help ensure availability of information following interruption to, or failure of, critical business processes.

Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime.

9.5 **Security Incident Communications.** OpenPlay shall provide Customer timely information about the Security Incident, including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by OpenPlay to mitigate or contain the Security Incident, the status of OpenPlay's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. Notwithstanding the foregoing, Customer acknowledges that because OpenPlay personnel do not have visibility to the content of Customer Personal Data, it will be unlikely that OpenPlay can provide information as to the particular nature of the Customer Personal Data, or where applicable, the identities, number or categories of affected Data Subjects. Communications by or on behalf of OpenPlay with Customer in connection with a Security Incident shall not be construed as an acknowledgment by OpenPlay of any fault or liability with respect to the Security Incident.

10. Cooperation.

10.1 **Data Subject Requests.** To the extent legally permitted, OpenPlay shall promptly (and in any case within five (5) days) notify Customer if OpenPlay receives a request from a Data Subject that identifies Customer and seeks to exercise the Data Subject's right to access, rectify, erase, transfer or port Customer Personal Data, or to restrict the Processing of Customer Personal Data ("**Data Subject Request**"). The Service provides Customer with a number of controls that Customer may use to assist it in responding to a Data Subject Request and Customer will be responsible for responding to any such Data Subject Request. Taking into account the nature of OpenPlay's Processing, OpenPlay shall (upon Customer's written request) provide commercially reasonable cooperation to assist Customer in responding to any Data Subject Requests.

10.2 **Data Protection Impact Assessments.** OpenPlay shall provide reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by Data Protection Laws, so long as Customer does not otherwise have access to the relevant information.

11. Relationship with the Agreement.

11.1 The parties agree that this DPA shall replace and supersede any existing data processing addendum, attachment or exhibit that OpenPlay and Customer may have previously entered into in connection with the Services.

11.2 Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Data.

11.3 **Subject to indemnity terms set out in clause 12 below ,** and notwithstanding anything to the contrary in the Agreement or this DPA, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or relating to this DPA and any other data protection agreements in connection with the Agreement (if any), shall be subject to any aggregate limitations on liability set out in the Agreement.

11.4 In no event shall this DPA or any party restrict or limit the rights of any Data Subject or of any competent supervisory authority.

11.5 This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement.

12. Indemnity

The Parties agree , that : If either Party has by their act or omission caused a breach of the 'Data Protection Laws' (as defined in this DPA) , it will be liable to indemnify the other party for any cost, charge, damages, expenses or loss it has incurred, including a claim arising from any third party, such as a data subject or the UK data protection regulator. Indemnification is contingent upon (a) the Party seeking to enforce this indemnity clause notifying the other party of any claims and (b) OpenPlay being given the opportunity to co-operate with the Customer in defence or settlement of the claim.

Annex 1 – Data Protection Security Measures

OpenPlay will implement and maintain appropriate technical and organizational measures to meet its obligations under applicable Data Protection Laws. For example, OpenPlay will:

1. inform all employees that Customer Personal Data is confidential and subject to contractual and legal protections;
2. instruct employees to access or display Customer Personal Data only in secure locations;
3. require that all devices used to store or transfer Customer Personal Data are encrypted and subject to a strong password policy that requires a password at initial startup and upon waking from sleep;
4. require multi-factor authorization and other account protection as available;
5. protect servers behind a firewall and perform annual vulnerability tests;
6. use reasonable technical and organizational measures to ensure that Customer Personal Data is (i) encrypted when in transit; and (ii) anonymized or pseudonymized where appropriate in light of the purposes of the relevant Processing activities; and

   use secure AWS (or comparable service provider) service to allow the restore of Customer Data. OpenPlay takes daily snapshots of data which gives it restore points that it can implement should it ever need to.

Annex 2 - List of OpenPlay Sub-processors

The following table sets out the list of Sub-processors that OpenPlay has specifically authorized as of the Effective Date.

Entity Name	Entity Country / Processing location	Description of Service/Processing Activity
Amazon Web Services	EU (Ireland)	Infrastructure, Database, Application hosting
Datadog	EU (Germany)	Metrics & Logs
Opayo/Elavon	UK and Eu (Ireland)	Online payments
GoCardless	UK	Direct debits
CoursePro	EU (Ireland)	Course Management
Innovatise	EU (Ireland and Germany)	Mobile Integration
Zendesk	EU (Ireland and Germany)	Customer Support