DATA PROCESSING AGREEMENT

This Data Processing Agreement (**“Agreement”**) applies to the processing of Client Data (as defined below) by Screen9 AB (hereinafter **“Screen9”** or **“Processor”**) and you as a customer of Screen9´s Services (hereinafter **“Client”** or **“Controller”)** (Screen9 and Client hereinafter individually also referred to as a **“Party”** and together as the **“Parties”**).

1. Introduction

1.1. The subject of this Agreement is the collection and processing of Client Data (as defined below) in connection with the Services provided by Screen9 to the Controller as specified in the Contract.

1.2. The Controller appoints Screen9 as a processor to process Client Data (as defined below) for the purposes described in this Agreement and the Contract, or as otherwise agreed in writing by the parties (**“Permitted Purpose”**).

1.3. Each party must comply with the obligations that apply to it under Applicable Data Protection Law.

2. Definitions

2.1. In this Agreement, the following terms will have the following meanings:

2.1.1. **“controller”**, “**processor**”, “**data subject**”, “**personal data**”, “**processing**”, “**process**” and “**special categories of personal data”** will l have the meanings given in the Applicable Data Protection Law;

2.1.2. **“Applicable Data Protection Law”** will mean: (i) prior to 25 May 2018, the EU Data Protection Directive (Directive 95/46/EC) and any national legislation implementing the EU Data Protection Directive; (ii) on and after 25 May 2018, the EU General Data Protection Regulation (Regulation 2016/679); and (iii) any national legislation implementing the Privacy and Electronic Communications Directive 2002/58/EC (as amended by Directive 2009/136/EC) in the applicable EU member state (including any future national or European legislation replacing such legislation)

2.1.3. **“Instruction”** means a direction, either in writing, in textual form (e.g. by e-mail) or by using a software or online tool, issued by the Controller to the Processor and directing the Processor to process Personal Data.

2.1.4. **“Client Data”** means all electronic data which is (i) submitted to the Processor by the Controller or (ii) which is collected, used and processed by the Processor specifically for the Controller or via the Controller´s digital properties.

2.1.5. **“Screen9 Affiliate”** means any entity that directly or indirectly controls, is controlled by, or is under common control of Screen9.

3. Scope of Data Processing

3.1. The Processor must process the Client Data exclusively in accordance with the Contract and this Agreement, which together will constitute the Instructions of the Client. The Client agrees that Screen9 may process and use Client Data for the purposes of providing the Service, fraud detection, forecasting and reporting in aggregate form. Details on the data provided by the Client, including the nature of data processing, the type of data being processed and the categories of data subjects concerned, are described in Annex A (Processing Activities) to this Agreement and in the Privacy Policy.

4. Processor's Obligations

4.1. Technical and organizational security measures: The Processor must implement technical and organizational security measures necessary to protect the Client Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the Client Data (**"Security Incident"**), in compliance with Applicable Data Protection Law.

Security Incidents: If it becomes aware of a confirmed Security Incident, the Processor must inform the Client without undue delay and it must provide reasonable information and cooperation to the Client so that the Client can fulfil any data breach reporting obligations it may have under (and in accordance with the timescales required by) Applicable Data Protection Law.

The Processor must further take such reasonably necessary measures and actions to remedy or mitigate the effects of the Security Incident and must keep the Client informed of all material developments in connection with the Security Incident.

4.2. Cooperation and data subjects' rights: The Processor must provide reasonable and timely assistance to the Client (at the Client's expense) to enable the Client to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law; and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Client Data. In the event that any such request, correspondence, enquiry or complaint is made directly to the Processor, the Processor must promptly inform the Client providing full details of the same. Upon request, the Processor must provide the Client with contact details of the individual(s) to approach with privacy-related queries.

4.3. Data Protection Impact Assessment: If the Processor believes or becomes aware that its processing of the Client Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it must inform the Client and provide reasonable cooperation to the Client (at the Client's expense) in connection with any data protection impact assessment that may be required under Applicable Data Protection Law.

4.4. Deletion or return of Client Data: Upon termination or expiry of this Agreement and the Contract, as appropriate, the Processor must destroy all Client Data in its possession or control. This requirement will not apply to Client Data it has stored on back-up systems. Client Data will in no case be stored for longer than 90 days.

4.5. Confidentiality of processing. The Processor must ensure that any person it authorizes to process the Client Data protects the Client Data in accordance with the Processor's confidentiality obligations under this Agreement and the Contract.

4.6. Audit. The Client acknowledges that the Processor is regularly audited by independent third party auditors. Upon request, the Processor must supply a summary copy of its audit report(s) to the Client, which reports shall be subject to the confidentiality provisions of this Agreement and the Contract. If the need for audit/audit questions stems from an incident (security or routine breach) caused by the Processor, each party is responsible for its own costs. Such audits are in addition to the yearly audit.

At the Client's expense, the Processor must also respond to any written audit questions submitted to it by the Client, provided that the Client does not exercise this right more than once per year.

4.7. Sub-contracting. The Client authorizes that Processor may use any Screen9 Affiliates as subprocessors. The list of Screen9 Affiliates is available at https://www.screen9.com/gdpr/ and will be updated by Processor from time to time. Where it has been agreed that Client Data is processed by third party subprocessor, the Client further consents to the Processor engaging third party subprocessors to process Client Data for the Permitted Purpose provided that: (i) the Processor maintains an up-to-date list of its subprocessors, which it must update with details of any change in subprocessors at least 30 days' prior to any such change; (ii) the Processor imposes data protection terms on any subprocessor it appoints that require it to protect the Data to the standard required by Applicable Data Protection Law; and (iii) the Processor remains liable for any breach of this Clause that is caused by an act, error or omission by its subprocessor.

Screen9 shall notify Client, at the by the Client provided email address (for GDPR updates), at least 30 days prior to any changes of subprocessors.

The Client may object to the Processor's appointment or replacement of a subprocessor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, the Processor will either not appoint or replace the subprocessor or, if this is not possible, the Client may suspend or terminate this Agreement or the Contract (without prejudice to any fees incurred by the Client prior to suspension or termination).

5. Client’s Obligations

5.1. Personal Data. All personal data which the Client transfers to, makes available for, submits to, or grants Screen9 access to must be obtained by the Client in accordance with Applicable Data Protection Law. If Screen9 comes into possession of or obtains access to Personal Data from the Client, which has not been collected in accordance with Applicable Data Protection Law, the Client must cease any such transfer or submission without undue delay. Screen9 reserves the right to block any transfer or submission of unlawfully obtained Personal Data, and to delete any such data from its systems, in its sole discretion. The Client is solely liable for all Personal Data it uploads to the system.

5.2. Information Obligation. The Client must inform the Processor as soon as reasonably possible of any legitimate inspection or audit of the Client Data processing by any competent authority which relates to the Data processing by the Processor.

5.3. Data Subject Requests. The Client must inform the Processor as soon as reasonably possible of any request from a data subject to enforce their rights under Applicable Data Protection Law.

5.4. The Client understands that it is responsible for ensuring that (i) any Client Data it provides to Screen9 for processing when delivering the agreed services under the Contract has been collected in accordance with Applicable Data Protection Law, and (ii) any Client Data provided to Screen9 may lawfully be processed by Screen9 in the manner necessary to deliver the agreed services under the Contract.

6. Term, Termination

6.1. This Agreement is entered into for as long as the Processor processes data on behalf of the Client in accordance with the Contract. It may be terminated in accordance with the Contract. The right to terminate for cause without notice will remain unaffected.

Annex A

Processing Activities

1. Information we may collect

1.1 We may collect information, including the following:

(a) User login information such as: email address, user name, password, IP-address

(b) device and browser fingerprints;

(c) information collected through cookies, players and other technologies;

(d) demographic information and automatically accessible information through the use of the Service; and

(e) aggregated information.

1.1.2 User accounts are needed in order to access content and/or support. By setting up a user account, the user gives his/her consent to the collection of the information set forth in 1.1 above.

1.2 We may collect information in a variety of ways. These include:

1.2.1 Through internet browser

Certain information is collected by most websites, such as users' IP addresses, screen resolution, operating system type and version, Internet browser type and version, ISP, time of the visit and the page(s) visited. We use this information for purposes such as calculating usage levels, presenting users with relevant usage statistics, improving the service, helping diagnose server problems, and administration.

1.2.2 Using software such as the Player and the App

The Player and the App include software which tracks and captures user activity. This enables us to track and capture user activity and experience to optimize the Service and present users with relevant usage statistics.

1.2.3 By aggregating information

We may aggregate and use collected information for improving the Service to the benefit of the Client a long as (i) no personal identifiable information is kept, and (ii) information is no longer associated with Client (anonymized both from end user and Client).