DATA PROCESSING AGREEMENT (DPA)

This Data Processing Agreement ("DPA") applies to (and is incorporated within) the End User License Agreement(s) (as applicable) and all other agreements between Newline Interactive SL ("Newline Interactive") and the Customer governing the Customer's use of the Newline Interactive products and services.

This DPA is an agreement between you and the entity you represent ("Customer," "you" or "your") and Newline Interactive SL and any applicable Newline Interactive contracting parties (together "Newline Interactive"). Newline Interactive and the Customer, hereinafter jointly referred to as the "Parties" and individually as the "Party".

1. DEFINITIONS

1.1. "Data Protection Laws" means all and any applicable data protection or privacy laws, rules and regulations. It shall include as applicable (a) the EU e-Privacy Directive 2002/58/EC as implemented by countries within the EEA; (b) the GDPR, (c) and the UK Data Protection Act 2018 and the UK Privacy and Electronic Communications (EC Directive) Regulations 2003 as well as any regulations that could supersede them in the future.

1.2. "GDPR" means Regulation (EU) 2016/679 (General Data Protection Regulation).

1.3. "Personal Data," "Data Subject," "Processing," "Controller," "Processor", "Sub Processor" have the meanings given in the GDPR.

1.4. "Standard Contractual Clauses" mean the annex to the EU Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council as shall be amended from time to time (including without limitation, the standard contractual clauses adopted by the European Commission in its Implementing Decision (EU) 2021/91 of 4 June 2021).

2. PROCESSING OF PERSONAL DATA

2.1. Scope. The Parties agree that the Customer is the Data Controller and Newline Interactive Europe is the Data Processor in relation to Personal Data processed under the Agreement.

2.2. Subject Matter. The subject matter of the data processing under this DPA is the Customer Data.

2.3. Duration. The Processing shall take place for the term of the Agreement and, upon its termination or expiry, until all Customer Data is deleted by the Processor in accordance with this DPA.

2.4. Purpose. The purpose of the Processing is to provide the services to the Customer as specified in the Agreement, including, in particular, the processing of personal data strictly necessary to implement and maintain user registration methods, login functionalities, and credential recovery mechanisms.

2.5. Nature of Processing. The Processing may include collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing, erasing, or destroying data.

2.6. Categories of Data Subjects. May include employees, customers, and end users of the Customer.

2.7. The types of Personal Data that may be processed under this Agreement include, but are not limited to:

- Device Data: Including device serial numbers, device types, and other hardware-specific information related to the devices used in connection with the services.
- Configuration Data: Details about device settings, preferences, and configurations that are applied to the devices.
- Applied Policy Rules: Information regarding security policies, access controls, and rules applied to devices as part of the MDM solution.
- App Installation Lists: Information about apps installed on the devices as part of the service.
- Location Data (Optional): Data related to the physical location of the devices, as permitted by the device users, including geolocation information.
- User Information: Information about users, including linked accounts or other identifiers associated with the devices.
- Device Activity and Logs: Information regarding the use and activity of devices, including logs related to access, usage, and events that are recorded to ensure device security and compliance.
- Authentication Data: Limited personal data collected through third-party identity providers (such as Google or Microsoft) during the registration or login process,

including name, surname, email address, and profile photo, solely for the purpose of user verification and credential management.

3. CUSTOMER OBLIGATIONS

3.1. The Customer warrants that it has all necessary rights to provide Personal Data to Newline Interactive Europe for processing in connection with the Agreement.

3.2. The Customer shall comply with its obligations as a Data Controller under applicable Data Protection Laws.

4. NEWLINE INTERACTIVE EUROPE'S OBLIGATIONS

4.1. Newline shall process Personal Data only on documented instructions from the Customer unless required to do so by law.

4.2. Newline shall ensure that persons authorized to process the Personal Data have committed themselves to confidentiality.

4.3. Newline shall maintain a written record of all categories of processing activities carried out on behalf of the Customer, in accordance with Applicable Data Protection Laws.

4.4. Newline shall assist the Customer, where appropriate, in carrying out Data Protection Impact Assessments and, where required, in conducting prior consultations with the competent supervisory authority, in accordance with Applicable Data Protection Laws.

4.5. Newline shall not disclose Personal Data to any third party unless expressly authorized in writing by the Customer or in cases permitted by applicable law.

4.6. Newline Interactive Europe shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, but not limited to:

- Access Control: Limiting access to Personal Data based on roles and responsibilities within the organization to ensure that only authorized personnel can process the data.
- Data Encryption: Using encryption protocols for the storage and transmission of Personal Data to prevent unauthorized access.

- Pseudonymization and Data Minimization: Applying techniques to reduce the identifiability of data subjects and ensuring that only the data necessary for the purposes of the Processing is collected and retained.
- Regular Testing and Evaluation: Conducting periodic assessments and testing of the effectiveness of technical and organizational measures to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing systems and services.
- Physical Security: Ensuring that physical access to data processing facilities is restricted and monitored.
- Incident Response Plans: Having clear procedures in place to detect, respond to, and recover from any data security incidents or breaches.
- Data protection impact assessments: This includes a systematic evaluation of the nature, scope, context, and purposes of the processing, and helps to identify and mitigate potential data protection risks proactively.
- Employee Training and Awareness Programs: Implementing mandatory, periodic training programs for all staff handling personal data. These programs should ensure that employees are aware of applicable data protection principles, company policies on data protection, and how to recognize and respond to data security incidents effectively.

4.8. In the event of a Personal Data Breach affecting the Customer's Personal Data, Newline shall notify the Customer without undue delay and, in any case, no later than 48 hours after becoming aware of the breach. Newline shall provide the Customer with sufficient information to enable the Customer to comply with any obligations to notify or communicate the Personal Data Breach to competent supervisory authorities or Data Subjects in accordance with Applicable Data Protection Laws. At a minimum, Newline shall provide the following (if available):

a) A description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records affected;

b) The name and contact from whom further information can be obtained;

c) A description of the likely consequences of the Personal Data Breach; and

d) A description of the measures taken or proposed to be taken to address the breach, including measures to mitigate its possible adverse effects.

Where and insofar as it is not possible to provide all the required information at the same time, the information may be provided in phases without undue delay.

Newline shall reasonably cooperate in good faith with the Customer and take all reasonable steps, as agreed between the Parties or required under Applicable Data Protection Laws, to investigate, mitigate, and remedy the Personal Data Breach. This includes, where necessary, assisting the Customer in preparing any required notifications to supervisory authorities or data subjects.

4.9. Newline shall make available to the Customer all information necessary to demonstrate compliance with its obligations under this Agreement and applicable data protection law.

5. SUBPROCESSING

5.1. Newline engages several trusted sub-processors to support the functionality and delivery of its products and services. Each sub-processor is bound by a written agreement imposing data protection obligations equivalent to those set forth in this Data Processing Agreement, in accordance with Applicable Data Protection Laws. The current list of sub-processors includes:

- Radix – Provides the Mobile Device Management (MDM) platform that allows IT administrators to remotely manage and monitor Newline displays. Radix processes administrative user data solely for authentication and system logging purposes.
  Radix does not access personal data independently without Newline's intermediation, and its functionality is limited to the technical purposes contractually defined. This includes:
  - Monitoring and managing device configurations, security settings, and applied policies.
  - Enforcing security policies such as password requirements, encryption, and remote wipe capabilities.
  - Tracking device activity and generating logs to ensure proper security measures are in place.
  - Collecting device data, such as serial numbers, device types, and app installation lists, to monitor and secure the devices.
  - Optional collection of location data, where permitted, for devices to enhance security and track usage patterns.
  - Secure Data Storage: Ensuring that all Personal Data is stored securely, using encryption and other protective measures to prevent unauthorized access or breaches.

  For more information, please refer to Radix's Privacy Policy.

- Eshare – Offers the NewlineCast+ software solution for wireless transmission of screen content, audio, and video over Wi-Fi. Eshare collects only non-personally identifiable information (e.g., IP address, device type) to improve service functionality.
  For more information, please refer to Eshare's Privacy Policy.

- DisplayNote – Enables wireless screen sharing between personal devices and Newline displays. DisplayNote processes only the personal data necessary for service operation and stores all data securely within the EU.
  For more information, please refer to DisplayNote's Privacy Policy.

- Newline Signage Pro (NSP) – A cloud-based digital signage platform that allows users to remotely schedule and manage content across displays. NSP supports login via credentials or Google accounts and ensures all data is stored within the EU.
  For more information, please refer to NSP's Privacy Policy.

- AirgoDMS – Supports centralized, large-scale device management, allowing remote configuration and software updates. AirgoDMS processes only operational metadata and configuration parameters, with no collection of personal data unless explicitly provided during system registration.
  For more information, please refer to AirgoDMS's Privacy Policy.

- AirgoCast – A lightweight application used for wireless screen mirroring and streaming over Wi-Fi. AirgoCast does not collect personal data and encrypts all network communications.
  For more information, please refer to AirgoCast's Privacy Policy.

- Whiteboard – A local application enabling users to annotate and draw on Newline displays. The application does not collect or transmit user data by default. When AI features are used, it connects to MyScript solely to process visual inputs as text, formulas, or drawings, without storing or identifying user data.
  For more information, please refer to Whiteboard EULA.

5.2. Newline may engage new sub-processors or replace existing ones in order to maintain or enhance its services. Newline shall notify the Customer of any intended changes to sub-processors at least 30 days in advance, allowing the Customer to raise reasonable objections. Any such changes will be reflected in the list of sub-processors available in this DPA or its referenced documentation. Newline ensures that all sub-processors are bound by written agreements imposing data protection obligations no less protective than those set out in this DPA, in accordance with Applicable Data Protection Laws.

DATA SUBJECT RIGHTS

6.1. Newline shall assist the Customer in addressing data subject rights requests in accordance with Applicable Data Protection Laws.. Where Newline receives a request directly from a data subject and is able to identify the relevant customer, it will make reasonable efforts to notify the customer without undue delay.

6. DATA TRANSFERS

7.1. Newline stores all customer data within the European Economic Area (EEA). If data is transferred outside the EEA, such transfers will be conducted in accordance with applicable Data Protection Laws, including the implementation of appropriate safeguards pursuant to Chapter V of the GDPR, such as Standard Contractual Clauses, adequacy decisions, or other lawful transfer mechanisms.

7.2. Upon request, Newline shall provide the Customer with information regarding the countries or third-party recipients involved in such transfers, and the safeguards applied, where applicable.

7. DELETION OR RETURN OF PERSONAL DATA

8.1. Upon termination of the Agreement, Newline will delete or return all Personal Data to the Customer, unless otherwise required by law.

8. AUDIT RIGHTS

9.1. Upon request, Newline shall make available to the Customer all information necessary to demonstrate compliance with this DPA. The Customer may also carry out an on-site audit or appoint a third-party auditor, provided that the parties agree in advance on the timing and scope of such audit.

9. LIABILITY

10.1. Each Party's liability arising out of or related to this DPA shall be subject to the limitations of liability set forth in the Agreement.

10. GOVERNING LAW AND JURISDICTION

11.1. This DPA shall be governed by the laws of Spain. Any disputes shall be subject to the exclusive jurisdiction of the courts of Spain.