DATA PROCESSING AGREEMENT (“DPA”)

Where TAPTAP Digital S.L. accesses the personal data as data processor (hereinafter “Data Processor”) for the provision of the applicable service (hereinafter referred as to the “Agreement”) and in accordance 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 regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”), the processing of personal data by Data Processor in name and on behalf of the Data Controller will be carried out in accordance with the following

CLAUSES

1. Object

The purpose of this DPA is to enable the Data Processor to process on behalf of the Data Controller the personal data necessary to fulfill the purpose of the Agreement, and to define the conditions under which the Data Processor shall process personal data to which it has access during the execution of the Agreement and to establish the obligations and responsibilities derived from the data processing performed by the Data Processor exclusively for and on the occasion of the Agreement.

2. Description of the Processing

Annex I specifies the details of the processing operations and, in particular, the categories of personal data and the purposes for which personal data are processed on behalf of the Data Controller.

3. Obligations of the Parties

3.1. Instructions

a. The Parties agree that this DPA and the Agreement constitute Controller’s documented instructions regarding Data Processor’s processing of personal data detailed in Annex I (“Documented Instructions”). The Data Processor shall process personal data only in accordance with Documented Instructions from the Controller, unless it is required to do so by Union or Member State law applicable to the Data Processor. In such a case, the Data Processor shall inform the Data Controller of such legal requirement prior to processing, unless such law prohibits it for important reasons of public interest. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between Data Processor and Data Controller.

b. The Data Processor shall immediately inform the Data Controller if the instructions given by the Data Controller infringe, in the opinion of the Data Processor, the GDPR or the applicable provisions of Union or Member State data protection law.

3.2 Purpose limitation

The Data Processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex I, unless it receives further instructions from the Data Controller.

3.3 Duration of the processing of personal data

Processing by the Data Processor shall only take place for the duration specified in Annex I.

3.4 Record of Processing Activities

The Data Processor undertakes to maintain, in writing, a record of all categories of processing activities carried out on behalf of the Data Controller, containing at least all the information required by Article 30.2 of the GDPR.

3.5 Security of processing

a. The Data Processor shall implement the necessary technical and organizational measures to ensure the security of the personal data. In determining an 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 purposes of the processing, and the risks posed by the processing to the data subjects.

b. The Data Processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The Data Processor shall ensure that persons authorized to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. In addition, the Data Processor guarantees that it carries out the necessary training on personal data protection for the members of its staff authorized to process personal data.

3.6 Sensitive data

If the processing 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 ("sensitive data"), the Data Processor shall apply specific restrictions and/or additional safeguards.

3.7 Documentation and compliance

a. The Parties shall be able to demonstrate compliance with these clauses.

b. The Data processor shall deal promptly and adequately with inquiries from the Data Controller about the processing of data in accordance with these clauses.

c. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations that are set out in these clauses and stem directly from the GDPR. At the Controller's request, the Data Processor shall also permit 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 an audit, the Data Controller may take into account relevant certifications held by the Data Processor.

4. Declarations and guarantees of the Data Controller

a. The Controller declares and certifies to the Processor:

i. That the personal data which shall be processed by the Data Processor have a lawful origin, guaranteeing that they have been obtained in compliance with the requirements established in the GDPR.

ii. To have informed the data subjects, which personal data the Data Processor processes, of the purposes of use of their personal data, and to have provided sufficient information in compliance with Articles 13 and/or 14 of the GDPR.

b. The Data Controller shall make available to the Data Processor all information necessary to demonstrate compliance with the declarations that are set out in clause 4.a).

5. Assistance to the Controller

a. The Data Processor shall promptly notify the Data Controller of any request it has received from the data subject. It shall not respond to such a request itself, unless the Data Controller has authorized it to do so.

b. The Data Processor shall assist the Data Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with a) and b), the Data Processor shall comply with the Controller's instructions

c. In addition to the Data Processor's obligation to assist the Data Controller pursuant to clause 5.b), the Data Processor shall furthermore assist the Data Controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the Data Processor:

- **i.** The obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
- **ii.** the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; and
- **iii.** the obligations in Article 32 of the GDPR.

6. Notification of personal data breach

a. In the event of a personal data breach concerning data processed by the Data Processor, the Data Processor shall notify the Data Controller without undue delay after the Data Processor having become aware of the breach. Such notification shall contain, at least:

- **i.** Description of the nature of the personal data security breach including, when possible, the categories and approximate number of data subjects affected, and the categories and approximate number of personal data records affected.
- **ii.** The name and contact details of the Data Processor's Data Protection Officer (DPO) and another point of contact to obtain more information.
- **iii.** Description of the possible consequences of the personal data security breach.

b. The Data Processor shall cooperate with and assist the Controller to comply with its obligations under Articles 33 and 34 of the GDPR, where applicable, taking into account the nature of processing and the information available to the Data Processor.

7. Sub-processing

7.1. Necessary subcontracting

a. The Data Processor requires the subcontracting of third parties that will process the personal data under the responsibility of the Data Controller. Some of these subcontracts are necessary in order to provide the applicable service, since the operation of the Data Processor's systems and the provision of certain services depend on them. The necessary subcontracting is reflected in Annex II.

b. With all necessary sub-processors, the Data Processor maintains an agreement imposing data protection obligations that provide sufficient guarantees of implementation of technical and organizational measures appropriate to the processing.

c. The Data Controller hereby authorizes the subcontracting referred to in the current terms.

7.2. New subcontracting

a. When it is necessary to subcontract any other processing, the Data Processor may do so provided that the Data Controller has not expressed its opposition to the subcontract within ten (10) working days from the notification.

b. The Data Processor shall notify the Data Controller within a reasonable period of time and not less than ten (10) working days prior to the hiring of the sub-processor in question, together with the information necessary for the Data Controller to object. The identification of the sub-processor, its contact details and the indication of the processing intended to be outsourced shall be considered sufficient necessary information.

c. The subcontracting may be carried out as long as the Data Controller has not expressed its opposition to it within ten (10) working days from the notification.

d. In any case, the processing of data by the sub-processor shall comply with the instructions of the Data Controller, and the Data Processor shall enter into a contract with the sub-processor under the terms provided for in this DPA and in accordance with the provisions of 28 of the GDPR, with the sub-processor undertaking, expressly and in writing, to assume obligations identical to those established for the Data Processor under this DPA. In the event of non-compliance by the sub-processor, the Data Processor shall be fully liable to the Data Controller for the fulfillment of the obligations.

8. International data transfers

a. Transfers of data to a third country or to an international organization by the Data Processor may only be carried out upon documented instructions from the Data Controller or pursuant to an express requirement of Union or Member State law to which the Data Processor is subject; and shall be carried out in accordance with Chapter V of the GDPR.

b. The Data Controller agrees that, where the Data Processor uses a sub-processor in accordance with clause 7 to carry out specific processing activities (on behalf of the Data Controller) and such activities entail a transfer of personal data within the meaning of Chapter V of the GDPR, the Data Processor and the sub-processor may ensure compliance with Chapter V of the GDPR by using standard contractual clauses adopted by the Commission, pursuant to Article 46(2) of the GDPR, provided that the conditions for the use of such standard contractual clauses are met.

9. Liability

Each party shall indemnify the other party (hereinafter “the Indemnifying Party”) from and against all loss, cost, harm, liabilities or damage suffered or incurred by the other party (hereinafter “the Indemnified Party”) as a result of the party's breach of the data protection provisions set out in this DPA, and provided that: (i) the Indemnified Party gives the Indemnifying Party prompt notice of any circumstances of which it is aware that give rise to an indemnity claim under this DPA; and (ii) the Indemnified Party takes reasonable steps and actions to mitigate any ongoing damage it may suffer as a consequence of the Indemnifying Party's breach.

10. Applicable legislation and competent courts

a. In matters not provided for in this DPA, as well as in the interpretation and resolution of conflicts that may arise between the Parties as a consequence thereof, Spanish legislation shall apply.

b. For the resolution of any dispute that may arise from this DPA, both Parties will submit to the jurisdiction of the courts of the city of Madrid, expressly waiving any other jurisdiction that may correspond to them.

ANNEX I

PROCESSING DESCRIPTION

1. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS PROCESSED:	Publishers' website users whose data are collected by Sonata Platform.
2. CATEGORIES OF PERSONAL DATA PROCESSED:	Indirect identifiers, which means and includes any data or information accessible by the Data Processor, including, without limitation, device IDs, IP addresses, location and demographic data, audience data segments, browsing history, declared, or inferred purchase intent information and user online behavior.
3. SENSITIVE DATA PROCESSED (IF APPLICABLE) AND ANY RESTRICTIONS OR SAFEGUARDS APPLIED:	No sensitive data is processed.
4. NATURE OF THE PROCESSING:	The processing may consist on the collection, storage, disclosure, structuring, erasure, record, consultation, and combination of the personal data.
5. DURATION OF THE PROCESSING:	This DPA shall remain in force until the Agreement termination.

ANNEX II

NECESSARY SUBCONTRACTING

Pursuant to clause 7.1. of this DPA, the Data Processor needs to subcontract the following third parties, which will process the personal data under the responsibility of the Data Controller and which have been approved by the Data Controller:

Sub-processor	Description of contracted service
Amazon Web Services (AWS)	Server's hosting.
NetSuite - Oracle	Enterprise Resource Planning.