eventscase

DATA PROCESSING AGREEMENT

UNDER ARTICLE 28 OF THE EU REGULATION 2016/679

BETWEEN

EventsCase **client / platform user** (hereinafter referred to as “Principal” or as “Data Controller”)

AND

Eventscase Ltd, with registered office in 40 Islington High St, – London N1 8XB, United Kingdom, in the person of its *pro tempore* legal representative Iván García Villar, CTO (hereinafter referred to as “Agent” or as “Data Processor”).

WHEREAS

1. The Principal and the Agent executed an agreement (hereinafter referred to as “Agreement”) concerning the use of the Agent’s Service called “EventsCase”, which can be used on a SaaS basis to manage data related to events by the Principal (hereinafter referred to as “Service”).
2. The Services provided by the Agreement include the processing of personal data in accordance with the EU Regulation 2016/679.
3. The Principal is the Data Controller for processing the personal data of his employees and decides on the processing purposes and methods.
4. The Agent has appropriate skills and knowledge to carry out the activities included in the Service, as well as an adequate expertise according to the purposes and the methods provided for the regulations on personal data protection.
5. The Agent ensures technical and organisational measures (e.g. equipment, human resources and materials), which comply with all the tasks for carrying out the operations included in the Service and with the purposes and methods provided for by the regulations on personal data protection.
6. The Principal intends to appoint the Agent – who intends to accept this appointment – as Data Processor of any activity provided by the Service.
7. The Principal shall authorise any activity carried out by the Agent other than those above-mentioned and included in Annex 1: List of subcontractors.
8. Regarding to this appointment, the Parties wish to regulate through this Agreement their mutual relationship on the processing of personal data carried out by the Data Processor on behalf of the Principal.

1. OBJECT

Through this appointment, in accordance with the EU Regulation 2016/679 on the processing of personal data (hereinafter referred to as “Regulation”), the Principal appoints the Agent as “Data Processor” for any activity concerning the processing of personal data. These activities are defined below, in compliance with the provisions included in the Article 28 of the Regulation.

Execution of the contractually agreed data processing shall occur exclusively in a Member State of the European Union, or in another signatory state to the EEA Treaty. Any transfer to a third country requires the prior agreement of the Customer and may only occur if the specific prerequisites of Article 44 ff. EU-GDPR (e.g. EU Commission adequacy decision, standard data protection clauses, approved codes of conduct) are fulfilled.

2. PROCESSING OPERATIONS WITHIN THE SCOPE OF THIS APPOINTMENT

The processing is aimed at performing any operation required by the Service.

3. OBLIGATIONS OF THE DATA PROCESSOR

The Data Processor processes personal data only upon specific instructions of the Data Controller, also in case of transfer of personal data to third countries or to an international organization, without prejudice to the Article 28, § 3 of the Regulation.

In accordance with the law and with the Agreement entered into with the Data Controller, the Data Processor must guarantee the confidentiality, the integrity and the quality of the data and their exclusive use for the purposes hereby specified. These obligations are also extended to the staff the Data Processor employs to carry out its activity and related processing operations.

The Data Processor can appoint another Data Processor only with prior written authorization of the Data Controller and in accordance with the provisions included in the article 28, § 4, of the Regulation.

The Data Processor shall provide the Data Controller any information required to confirm the respect of the obligations included in this Agreement.

The Data Processor shall aid the Data Controller in impact assessments under the article 35 of the EU Regulation 2016/679, where necessary.

The Data Processor shall co-operate with supervisory authorities (such as the ICO) in accordance with Article 31.

4. OBLIGATIONS OF THE DATA CONTROLLER

The Data Controller must inform the Data Processor immediately and fully, if it determines errors or irregularities in relation to data protection provisions in the order-related results.

5. DATA SUBJECTS REQUESTS

The Data Processor may receive requests from data subjects, aimed at exercising their specific rights. the Data Processor shall:

- provide prompt written communication to the Data Controller
- verify the data subject's identity, in order to control the legitimacy of the request,
- check, in collaboration with the Data Controller, the accuracy of the information to give the data subject according to the request forwarded.
- meet these rights – within the Data Processor's functions – within the term provided for by the law and by forwarding any information concerned to the Data subject.

6. SECURITY MEASURES

The Data Processor shall control the adoption of any appropriate security measure provided for by the articles 32 and 36 of the Regulation, in order to ensure an adequate security level against risks. In verifying the security level ensured by the Data Processor, the Data Controller shall take in particular consideration the risks that could derive from the specific processing of the Service and especially from the destruction or the loss, even the accidental one, of the data. The Data Controller shall also pay specific attention to the risks that could be caused by any non-authorized access or processing incompatible with the purposes of the data collection.

The Data Processor shall support the regular evaluation of the entire level of security's adequacy, with particular regard to any new technological knowledge, to the nature of the data and to the specific features of the processing carried out under its responsibility.

With reference to any possible variation in the operations or in the data processed for the Service, the Data Processor adopts any appropriate urgent measure to safe the confidentiality, the integrity and completeness of the data processed as above, pursuant to the applicable law on this matter. The Data Processor adopts security efficient measures to be communicated to the Data Controller with due advance.

7. PRESERVATION OF DOCUMENTS

The Data Processor shall handle any paper or digital document concerning the requirements provided for by this appointment, by law and by the Data Protection Authority through the adoption of specific procedures, of efficiency criteria and by ensuring the safekeeping of the data.

8. COLLABORATION WITH THE DATA CONTROLLER

At Data Controller's request, the Data Processor shall assist the same Data Controller in its defense before any ordinary court, even by the prompt submission of documentary evidences related to its functions.

9. CONTROLS AND AUDITS

The Data Processor allows the Data Controller to verify the fulfilment of its appointment under the law and any applicable provision.

Examinations and controls conducted by the Agent or an auditor contracted by it shall be carried out during normal business hours without disruption to operating procedures after notification with an appropriate notice period. The Principal may make such examinations and controls dependent on signature of a non-disclosure declaration in respect of the data of other clients and the technical and organizational measures arranged. If the auditor contracted by the Agent is in a competitive relationship with the Principal, the Principal has a right to veto such a person.

10. DATA BREACH

If the Data Processor discovers a breach of security which caused the destruction, the loss, the modification, the unauthorized disclosure or the access to personal data processed on behalf of the Data Controller (hereinafter referred to as “incident”), the Data Processor undertakes:

- to verify the severity of the incident, in terms of consequences and damage;
- to adopt enforcement actions in order to limit and lessen the incident until its eventual resolution;
- to inform the Data Controller about the incident within 48 hours since the moment it becomes aware of the same incident. This communication shall include detailed information on the incident, such as description, the related consequences suffered by the personal data processed and, where necessary, the actions carried out by the Data Processor to remedy and/or resolve the problem and to avoid similar incidents;

11. TERMINATION OF THE PROCESSING

In case of termination of the processing operations for any reason or the appointment concerned, the Data Processor shall fully destroy all the personal data.

An exception to this general rule applies if the processor is required to retain the personal data by law.

12. COMMENCEMENT AND DURATION

This appointment will be effective from the date of subscription by both the Principal and Agent and will remain in force until its expiry or termination by any other reason.

13. LIABILITY / COMPENSATION

The Customer and Contractor are liable to affected persons in accordance with the provisions of Article 82 GDPR.

eventscase

ANNEX 1
List of subcontractors

Company name	Address	Purpose used for
Amazon Ireland	Ireland	Physical servers including backups (Secondary server for scalability purposes and future main servers of the platform, we will inform you accordingly)
720tech	Spain	Scalability and infrastructure assessment and monitorisation