DATA PROCESSING AGREEMENT

1 Background

This data processing agreement (Annex) is an inseparable part of the [ ] Services Agreement (the "Agreement") entered into between [ ] (Business ID: [ ]) (”**Supplier”)** and Management Events International Oy LTD (Business ID: 1015730-0) (”**Customer**”) [. .20].

This Annex is applied to the data protection and information security of the Customer's personal data in the Supplier's services. This Annex constitutes a written agreement between the parties in accordance with the EU General Data Protection Regulation (679/2016) regarding the processing of personal data.

In the event of any conflict between the terms and provisions of this Annex and the Agreement regarding the processing of personal data, the provisions of this Annex shall prevail.

The categories of personal data and categories of data subjects processed in the Services, the nature and purposes of the processing of personal data in the Services and the instructions given by the Customer regarding the processing are set out in Processing Specification Form in Annex A ("**Annex 1**"), unless otherwise agreed in the Agreement and its annexes, e.g. in the orders.

The terms ”controller”, ”processor”, ”data subject”, ”personal data”, ”data breach”, and ”processing” used in this Annex correspond to the terms defined in the General Data Protection Regulation (”**GDPR**”) 2016/679 of the European Union.

2 Data protection and processing of personal data

2.1 General

The Supplier processes the Customer's personal data on the Customer's behalf of and under the instructions of the Customer on the basis of the Agreement. The Customer or its principal is the Controller of the personal data processed in the Service and the Supplier is the Processor. The Parties undertake to comply with the legislation, regulations and instructions and guidelines of the authorities in force in Finland and the European Union regarding the processing of personal data and, if necessary, to amend the terms and provisions of this Annex to comply with them.

The Supplier is entitled to process the Customer's personal data and other information of the Customer only in accordance with the Agreement, this Annex and the Customer's written instructions and only to the extent and in the manner necessary to provide the Services. [The Customer's written instructions are attached as Annex 2 to this Annex.] The Supplier shall immediately notify the Customer if it finds that the Customer's instructions violate the GDPR or other data protection provisions.

2.2 Customer’s undertakings

As the Controller, the Customer is responsible for ensuring that it has the necessary rights and has obtained the necessary consent for the processing of personal data. The Customer is responsible for drafting and keeping available a privacy policy and for providing information to data subjects.

The Customer has the exclusive right and obligation to determine the purposes and means of the processing of personal data. The subject, nature and purpose of the processing are further defined in the Agreement. The categories of personal data processed in the Services and the categories of data subjects are defined in the Processing Specification Form, Annex 1.

2.3 Supplier’s undertakings

The Supplier shall have documented processes and procedures for risk management in place. The Supplier shall be responsible for detecting and identifying data protection and information security risks relating to the Services and for taking the necessary measures to prevent and minimise such risks.

The Supplier must have sufficient expertise and resources to implement the security and data protection measures specified in this Annex. The Supplier shall cooperate with the Customer's employees responsible for data protection and information security, where necessary.

The Supplier is obliged, taking into consideration the nature of the processing of personal data and the information available to the Supplier, to assist the Customer in ensuring that its obligations under the law are complied with. These obligations may include information security, notifying of breaches, data protection impact assessment and prior consultation obligations. The Supplier is obligated to assist the Customer only to the extent required by the obligations imposed on the data Processor by applicable data protection legislation.

2.4 Subcontractors

The Supplier shall not use subcontractors to process the Customer's personal data without the Customer's written general, or subcontractor-specific prior consent. In addition, the Supplier shall inform the Customer of all its subcontractors and any changes thereto. The Customer shall have the right, for justified reasons, to prohibit the use of new subcontractors.

The Supplier shall enter into a written agreement with its subcontractors and is responsible for ensuring that the subcontractors the Supplier uses comply with the provisions of this Annex and any other instructions given by the Customer. The Supplier shall regularly monitor the performance of its subcontractors and shall be liable for the performance of its subcontractors as if for its own performance.

2.5 Data transfers

Customer's data may not be stored, transferred, disclosed, modified, used or otherwise processed in real time, archived, backed up or in any other form in any country outside the EU/EEA without the prior written consent of the Customer.

In the absence of a European Commission decision on the adequate level of data protection in the country concerned, the transfer of personal data will generally be subject to an agreement in accordance with the standard contractual clauses adopted by the European Commission ("**Standard Contractual Clauses**"). Other legally recognized means of transfer may also be used as an alternative to the Standard Contractual Clauses. The Supplier shall inform the Customer in advance of the means of transfer to be used, how the means of transfer can be accessed and the non-EU/EEA countries to which the personal data will be transferred, so that the Customer can comply with its obligations as a Controller under the GDPR.

When using Standard Contractual Clauses or other legally approved data transfer means, the Supplier shall be responsible for taking the measures required by applicable law and regulatory guidance to ensure the legal validity of the data transfer means and an adequate level of data protection in the third country of transfer, and for properly assessing and implementing safeguards that complement the means of data transfer. Upon request, the Supplier shall promptly provide a documented assessment of the transfers and the safeguards accompanying the means of transfer. The assessment must take into consideration the circumstances of the transfer, the legislation of the third country and the means of transfer. If the assessment indicates that it is not possible to implement adequate additional safeguards in the transfer in question, the Supplier shall inform the Customer without delay and, at the Customer's request, suspend the transfer of data to the third country in question.

2.6 Requests from data subjects

The Supplier shall immediately forward to the Customer any requests received from data subjects for the inspection, rectification, erasure or objecting the processing of personal data and any other requests concerning personal data. At the Customer's request, the Supplier shall assist the Customer in fulfilling the requests made by the data subjects. The Supplier shall be responsible for fulfilling the data subject's statutory requests.

2.7 Communications with the authorities

The Supplier shall forward all enquiries from the data protection authorities directly to the Customer and shall await further instructions from the Customer. The Supplier is not authorized to represent the Customer or to act on behalf of the Customer in dealings with the authorities supervising the Customer, unless otherwise agreed in writing.

2.8 Auditing

The Supplier shall be obliged to demonstrate on request that the Supplier and its subcontractors comply with the terms and provisions of this Annex and any other instructions given by the Customer. The Customer or an auditor authorized by the Customer (other than a competitor of the Supplier) may annually verify that the Supplier and its subcontractors process the Customer's data in accordance with this Annex and any other instructions given by the Customer by giving 14 working days' notice prior to the audit. The Supplier shall promptly remedy any defects and deficiencies identified at its own expense. Each party is to bear their own expenses

related to the audit. The Customer or an auditor authorized by the Customer may review the adequacy of the remedies performed by the Supplier. If the audit reveals that the Supplier has acted materially contrary to this Annex or other written instructions of the Customer, the Supplier shall reimburse the Customer for the external costs of the audit and the resulting remedies, according to the auditor's invoice.

3 Information security

The Supplier is obliged to implement appropriate technical and organizational security measures, as required by the applicable data protection legislation, to protect the personal data it processes. The establishment of safeguards shall consider the available technical options, the particular risks involved in the current processing activities, and the special categories of personal data being processed. For example, the processing must comply with the following rules:

1) The Supplier shall ensure that the Supplier's personnel involved in the processing of personal data or the personnel of any subcontractor used by the Supplier are bound by non-disclosure or are subject to a legal obligation of confidentiality.
2) The systems and communications used by the Customer to process the data are protected by appropriate and up-to-date security solutions in accordance with industry best practices.
3) The personal data shall not be used for the development, testing or other purposes of the Supplier's own services.

The Supplier is responsible for backing up the Customer's data it processes, unless otherwise agreed in writing.

A more detailed description of the technical and organizational security measures taken by the Supplier in response to this Annex is set out in Annex 2.

4 Handling of data breaches

The Supplier shall inform the Customer without delay of any data security breaches of which it becomes aware, such as data breaches, accidental or unlawful destruction, erasure, alteration, unauthorized disclosure or access to data. The notification must describe what happened, whose data and what data was affected by the breach, and the estimated numbers involved.

The Supplier shall promptly investigate the causes and likely effects of the breach and take the necessary measures to stop the breach, mitigate its adverse effects and prevent similar breaches. The Supplier shall promptly document to the Customer the results of the investigation and the measures taken.

The Supplier shall cooperate with the Customer and ensure that the Customer has the documentation required by law and data protection authorities in relation to data breaches.

5 Liabilities

The Supplier shall be fully liable for all liabilities, damages, actions and claims (including reasonable attorneys' fees) incurred by the Customer and/or its management, officers, employees or contracting parties arising from the Supplier's processing of the Controller's personal data or other information in violation of law, this Appendix or the Customer's written instructions.

Administrative sanctions imposed by the competent authorities or claims for damages brought by the data subject on the basis of this Annex shall be the liability of the Controller and Processor of personal data, as provided by law. Without prejudice to any limitation of liability, if a party compensates a data subject based on a legally binding judgment for damages caused by a breach of data protection law, that party is entitled to claim as a compensation a proportion of the compensation paid to the data subject from any other party involved in the same processing operation, corresponding to their liability for the damages.

6 Miscellaneous

Upon termination of the Agreement, the Supplier shall return and/or erase the Personal Data in accordance with the instructions provided by the Customer. If the Customer has not instructed the Supplier within one (1) month after the termination of the Contract, the Supplier shall without undue delay request instructions in writing from the Customer for the erasure and returning of the Personal Data. The Supplier shall assist the Customer to the extent requested by the Customer in transferring the Customer's data. The Supplier shall arrange for the destruction of copies of the Customer's Data held by the Supplier and its subcontractors and shall confirm the destruction of such copies to the Customer in writing.

The Supplier shall inform the Customer in writing of any changes that may affect the Supplier's ability or capacity to comply with the provisions of this Annex and any written instructions given by the Customer. Any additions or amendments to this Annex shall be agreed by the Parties in writing.

This Annex shall enter into force upon signature by both Parties. This Annex shall remain in force (i) for as long as the Agreement is in force or (ii) for as long as the parties have obligations to one another arising from the processing of personal data.

Obligations which, by their nature, are intended to continue to be in force notwithstanding the expiry of this Annex shall remain in force after the expiry of this Annex.

7 Signatures

[Date and place]

[**Oy**] [**X Oy**]

_____	_____
Name:	Name:
Role:	Role:

APPENDICES

1. [Processing Specification Form]
2. [Security measures]

PROCESSING SPECIFICATION FORM (ANNEX 1)

This Processing specification form is an inseparable part of the Annex concerning Personal Data Processing. The Processing Specification Form specifies a processing assignment the Processor performs for the benefit of the Controller in the manner provided for in the Agreement and this Annex.

1 Services	The Processing shall concern the following services (fill out the service description)
2 Approved Subcontractors (Special/General Prior Approval)	The following subcontractors are used in the provision of the service:
3 Geographical Location of Personal Data	The Personal Data is Processed[1] in the following countries or areas:
4 Sets of Data Subjects	The Personal Data Processed concerns the following sets of Data Subjects[2]:
5 Types of Personal Data	The Personal Data Processed in the service consists of the following types of Personal Data[3]: Special sets of Personal Data[4] :

[1] I.a. saving, storage, correction and maintenance services and capacity services.
[2] E.g. employees, customers, potential customers, suppliers.
[3] Types of personal data processed may be e.g. customer data, and the supplier's data, such as name, title, home address, telephone number, e-mail address, date of birth, gender, customer number, purchasing and service use history; as well as financial data; employee and personnel data; as well as IT-management data, such as system data concerning offered service, including technical identification, user names, location, contact information, and technical actions concerning offered services, such as system and application log data and security log data, premises and system surveillance data and data of data security breaches. Note the collection of social security numbers or background checks in this section.
[4] Race or ethnic origin, political opinions, religious or philosophical beliefs, membership in trade union, processing of genetic or biometric data for the unambiguous identification of a person, data regarding health, or data concerning sexual orientation or behavior.