



## **Lyyti Data Protection Appendix**

This appendix ("Data protection appendix") regarding the processing of personal data forms an inseparable part of the agreement ("Agreement") between Lyyti Oy ("Supplier") and Nordic Institute for Advanced Training in Occupational Health ("Customer"). The Customer and the Supplier shall be referenced in the text separately with "Party" and together with "Parties."

If the Agreement and its other appendices are found to be in conflict with this Data protection appendix, preference is given to this Data protection appendix, regardless of what is stated in the Agreement or the other appendices thereof. The terms used in this appendix are in accordance with the terms specified in the European Union's General Data Protection Regulation (GDPR). The Supplier has the right to revise these terms in case it proves justifiable due to a change in legislation or interpretation thereof or due to changes in the Supplier's operational environment or business operations.

### **Data controller and personal data processor**

Based on the Agreement the Supplier shall, in the role of data processor and on behalf of the Customer acting as the actual Controller, process Personal data for the purpose defined by the Customer and in accordance with the instructions given by the Customer as defined in this appendix. The purpose of the data processing is to enable 1) the collecting of personal data of persons who have registered for events organised by the Customer or personal data collected for other purposes to the extent required by the event organization or said other purpose; 2) the processing of data produced by various surveys; and 3) other form of analysis of the aforementioned data as defined by the Customer and permitted by applicable legislation.

## Personal data to be collected

For each event, the Customer shall define which data is to be collected. Regarding each event, the Supplier shall collect and store the processed data as defined by the Customer. This type of data may include, for example, the name of the person, required contact information, and, if required, the age of the person as well as other necessary additional information ("Personal data") needed for event registration, participation, and payment. The data is processed for each event for the duration defined by the Customer. The Customer shall comply with a privacy policy required in the GDPR. The Supplier shall comply with the instructions of the Customer which are in accordance with the appropriate privacy protection legislation.

## Processing of personal data

**Principles.** The Customer shall be responsible for possessing the required rights and consent to process the Personal data. The Customer shall be responsible for verifying the age of the data subject. The Parties shall be responsible for the drafting and availability of a privacy policy and for informing the registered of the processing activities of the parties, according to the article 30 of the GDPR and other applicable legislation. The Supplier undertakes to process the Personal data in compliance with appropriate data security processes and in accordance with applicable legislation, the Customer's written instructions as confirmed in this Agreement and specifications provided by Customer in the Lyyti system. The Supplier undertakes to inform the Customer in case the Supplier considers the Customer-provided instructions or specifications being unlawful or if the Supplier is unable to process the Personal data in accordance with the Customer's instructions or specifications. If required, the Supplier shall cooperate with the Customer's staff responsible for data protection and security. The Personal data and the Lyyti system are located in the EU/EEA-area. The Supplier shall not transfer personal data outside of the EU/EEA-area, apart from transfers which take place according to the Customers instructions and specific conditions of this data protection appendix. If the Customer demands or agrees to transfer the personal data outside of the EU/EEA-area, the Customer is responsible for ensuring that the transfer fulfils the conditions set out in the GDPR and if necessary, that the registered have given consent for the transfer. The Supplier shall help the Customer in complying with the



requirements set for the controller in the GDPR. In exchange, the Supplier shall have the right to charge a reasonable fee in case the provision of this type of assistance requires activities outside the Supplier's customary operations.

**Storing the data.** Unless a transfer of payment or any other justified interest of the Supplier or legislation require any part of the Personal data to be stored for a longer period of time, the Personal data shall be anonymized at the latest when the Customer so requires or when the Agreement ceases to be in force. In case the Supplier receives a request from the Customer before having anonymized the data, Supplier shall return all Personal data to the Customer.

**Persons who process the data.** The Supplier undertakes to ensure that the Personal data is processed only by persons having committed to keep the processed data confidential. The Customer agrees that the Personal data may be processed, at Supplier's discretion, by persons other than the Supplier and the Supplier's staff. In case the data is processed by such a third party, the Supplier is responsible for securing that the third party in question undertakes to comply with the Supplier's obligations under this Data protection appendix. At the request of the Customer, the Supplier shall provide necessary information about a third party processing the Personal Data. The Customer authorises the Supplier to engage another processor to process the Customer's Personal Data in accordance with Processing Instructions on the condition that the Supplier shall notify the Customer of the engagement of any such subprocessor. If the Customer wishes to object to the change of subprocessor, the Customer shall have the right to terminate the Agreement.

**Rights of the data subject.** By providing technical interfaces, the Supplier shall help the Customer to fulfil the Controller's obligation of addressing requests related to the rights of a data subject. Furthermore, the Supplier shall help the Controller to ensure that the processing-related security issues have been adhered to taking into account the nature of the Personal data. The Supplier shall, without delay, notify the Customer of any personal data breaches that the Supplier becomes aware of, and furthermore, assist the Customer in notifying the supervisory authority and the data subject of such data breach. Where applicable, the Supplier shall assist the Customer in data protection impact assessment and prior consultation procedure. The Supplier shall have the right to charge the Customer for reasonable extra costs incurred thereof. For the sake



of clarity, it shall be stated that the fee for ordinary processing activities shall be included in the fee agreed in the Master Service Agreement. However, the Supplier shall have a right to claim extra fee and costs for processing activities that are not included in the ordinary responsibilities of a processor of personal data.

**Ensuring data protection.** When requested, the Supplier shall deliver the required documentation and information to the Customer, permit audits, and assist in such audits to prove that the Supplier complies with this annex and data protection legislation. The party performing the audit shall commit to keeping any information obtained during the audit confidential. The Supplier shall have the right to deny an audit in case the auditing party proves to be a direct or indirect competitor of the Supplier or a party whose expertise or reliability may reasonably be questioned. The Customer shall be responsible for all costs incurred in connection with such audits. The Supplier shall forward any Customer-related queries of the supervisory authorities to the Customer as well. The Supplier shall neither act as the Customer's representative nor act on Customer's behalf in data protection -related matters.

**Liability for damages.** The Parties accept that any liability following an administrative sanction imposed by a competent authority, or a claim for damages by the registered made according to this appendix or the applicable data protection legislation, shall be borne by the Parties in proportion to their individual failure to comply with the obligations set in the applicable legislation. In case of such sanction or claim, the Party that has neglected or breached its obligations shall be liable for the imposed sanctions and damages according to the decision of the entitled authority or the court. The Parties shall have the right to claim compensation retrospectively from the other Party according to the applied privacy protection legislation, if the other Party has paid a full or partial sanction or compensation to the registered following an action which is against privacy protection legislation from which the other Party is partly or entirely responsible. The liabilities for possible other damages and the restrictions of liability have been agreed in the Master service agreement, which this document is an appendix of.

**Data security.** The Supplier shall be responsible for applying documented and appropriate risk management and data security processes to all its activities



related to processing Personal data. The Supplier shall take adequate technical and organisational protective measures, as required by the data protection legislation and this Agreement, to protect the Personal data. Taking into account the sensitive nature of the Personal data as defined by the Customer and the level of risk related thereto, the Supplier shall protect the data traffic and the systems used in data processing by appropriate security measures to ensure that the confidentiality, integrity and availability of the Personal data are secured until the Personal data is erased from Supplier's system in accordance with this Agreement.

