APPENDIX 8

THE DATA PROTECTION REGULATION OF SZIGET KULTURÁLIS MENEDZSER IRODA KORLÁTOLT FELELŐSSÉGŰ TÁRSASÁG

Sziget Kulturális Menedzser Iroda Kft. (the "Data Controller") executes the processing and protection of personal and other data related to the services (the "Service") provided by them in accordance with the following regulations (the "Regulations").

1. Principles of data processing

1.1 Throughout applying these regulations, the subject is any defined, identified or identifiable natural person who can be directly or indirectly identified based on their personal data

1.2 The controller of the personal data collected and recorded in connection with the operation of the Data Processing Service is the Data Controller.

1.3 The purpose of data processing performed in connection with the operation of the Service is that the services available, within the framework of the services, should be effectively available by matching the data provided by the customer (name, address, telephone number, email address, mother's name, birth details).

1.4 Data processing is voluntary in all cases. Personal data is only used by the Data Controller for the purpose of the service chosen by the registered customer in accordance with and within the framework of the consent granted by them. The data processing serves this purpose in every phase. The legal foundation of the data processing performed by the Data Controller is the consent given by the previously informed subjects, which the subjects provide upon accepting the conditions of registration.

1.5 The data is stored in servers in Hungary and is not transferred to any data processor located in a third country. Throughout its activity, the Data Controller ensures the security of the data and the enforcement of data and privacy protection regulations by technical and organisational measures and by developing safety regulations.

1.6 The Data Controller and the operator of the server network vows to protect the data with the most up-to-date hardware and software support to prevent unauthorized access, alteration, transfer, making it public, erasure and destruction, accidental damage and destruction, thus serving to preserve the security of the data.

1.7 As a main rule, the data processed by the Data Controller is only accessible to employees who take part in performing the data processing activities

defined by the current Regulations, who – as defined in their employment contract, and by legal regulations regarding their job or based on their employers' instruction - have privacy obligations regarding all the data that becomes known to them.

1.8 Throughout its activity, the Data Controller is entitled to place brief, informative messages or messages with marketing purposes in the messages sent out to the customers - based on their consent - in connection with the data processing service. The subject receiving the messages in connection to the service can send their objection, relating to the receiving of marketing content, at any time in written, identifiable form to the Data Controller. In this case, upon receiving the written objection, the Data Controller is not entitled to place marketing content in the messages sent out in connection with the service to the objecting subject. The Data Controller is only entitled to send messages containing solely marketing content providing the Subject's definite consent is given in advance.

1.9 Subjects of data processing carried out by the Data Controller can initiate, in a written message sent to the Data Controller, the withdrawal of their consent given to data processing any time. Furthermore, they can restrict their consent to certain data or data processing operations. The customers are subsequently entitled to object against the processing of their personal data in the cases as defined by Act CXII of 2011, regarding the right of informational self-determination and freedom of information.

However, we call the customers' attention to the fact that in case they request the deletion of the minimal data necessary for the service being provided, the Data Controller will not be able to provide the Service for these customers any longer. In this case, the Data Controller is entitled to terminate the contract unilaterally.

1.10 Based on its data protection policy and in accordance with standard legal regulations, the Data Controller maintains its right to publicize and transfer to a third person the statistical data collected from the customers (which does not qualify as personal data) regarding the composition of the data base.

2. Corresponding the legal regulations

2.1 The Data Controller treats the personal and any other data of the customers confidentially and in accordance with the effective Hungarian legal regulations.

2.2 The data protection policy of the Data Controller corresponds to effective Hungarian law, as well as to the most important international directives, especially with respect to the following:

a) The content of the expressions used in the current Regulations correspond to the content set in the regulation of the Act CXII of 2011 (3. §) about the right of informational self-determination and freedom of information;

b) Act VI of 1998 about the Protection of Individuals with Regard to Automatic Progression of Personal Data Agreement, dated Strasbourg, 28 January, 1981;

c) Questions as defined by Act CVIII of 2011 in connection with electronic marketing services and the services in connection to the informational society;

2.3 The Data Controller maintains the right and at the same time accepts responsibility to unilaterally change its privacy policy and the content of the current Regulations in accordance with the operative legal regulations or in case of the change of the Service. The Data Controller informs its customers about any changes in the data protection policy in advance on the www.sziget.hu website.

3. Registration

3.1 In order to have use of the Services, the Data Controller requests its customers to register with the Data Controller (signing the contract).

Through registration the customers shall provide at least the following personal data:

a) name, mother's name and address, postal address, invoice address, telephone number (which are necessary for possible notices, responses, preparing and sending invoices)

b) ID number or tax number

d) in case of online registration, email address (which is necessary for sending out the tickets which constitute as part of services, sending possible notices, responses)

During registration, only that data can be requested from the customer (subject), which is necessary for the executing of the Service, and is suitable for achieving the purpose.

3.2 The Data Controller does not transfer the personal data collected during registration or make it accessible to any third parties, nor does the Data

Controller connect it to other data processing without the expressed consent of the subject. However, the Data Controller informs the subjects in order to fulfil the Services that the transferring the data or the connecting of data processing might become necessary for previously defined persons as defined in the Appendix B of the current Regulation. Throughout the transfer and the connecting of data processing, the Data Controller acts with complete consideration regarding the safety of the data, and makes sure that those persons who are at the receiving end of the data transfer shall process the data under efficiently secure conditions. The Data Controller can only transfer the data to the persons listed in Appendix B if it is required for the fulfilment of the defined service and shall only transfer the necessary data required for it.

3.3 Upon registering, the customer (subject) gives their consent for his/her personal data to be stored freely, and to the efficient process of the Data Controller's current Regulations (data protecting policy). Upon the expiry of the contract with the customer, the Data Controller deletes the processed data.

4. Notices, advertisements

4.1 Throughout the period of providing the services, the Data Controller contacts the customers directly, primarily via email. The Data Controller is solely entitled to send messages containing information in connection with the use of the Service or information that might occur in connection with it; the only exception being as defined in point 1.8. Service Provider is also entitled to send news, newsletters, advertisements, promotional offers to customers and holds the right to use the data for marketing-related researches and evaluations. Other than that the Data Controller provides further information for its customers on www.sziget.hu, and through their customer service department.

4.2 With regard to the content of point 1.8, the Data Controller only sends messages that are classified as advertisements to its customers in a clean, unambiguously identifiable form and only with the previous consent of the customers. In accordance with the relevant legal regulations, the Data Controller keeps a record of those persons who announced in writing that advertisement messages can be sent to them. The Data Controller shall not send advertisements to those people who do not appear in the records. The Data Controller is allowed to hand over the record to a third party only with the customer's (subject's) previous consent with respect to the content of point 3.2, in which case the data is transferable.

4.3 In case the customers do not wish to receive any messages that can be considered as an advertisement in future, they can cancel it at the Data Controller, by using the options available on the www.sziget.hu website or at the customer service of the Data Controller.

5. Information and options for legal remedy

5.1 In case of further questions, notifications arising on top of the content of the current Regulation, we request the customer to get in touch with the Data Controller on the following phone number or via the email address provided below:

Phone number: +36 1 372 0650

e-mail address: ugyfelszolgalat@emezrt.hu, info@sziget.hu

5.2 The customer can request information about the processing of their personal data at any time.

If requested, the Data Controller shall provide a detailed account of the customer's (subject) data processed by the Data Controller, and about the data processed by the data processing person appointed by it. The account shall provide information about their sources, about the purpose of the data processing, about its fundamental right, duration, as well as about the name, address of the person processing the data and their activity in connection to the data processing. Furthermore – in the case of transferring the subject's personal data – it will detail the fundamental right and recipient of the data transfer.

The Data Controller provides the information within the shortest possible time after the request is made, and within the maximum of 30 days, in writing, and in a comprehensible way and posts it to the address (postal address) provided by the customer, providing that the customer provided such contact details. In the case of default, the standard 30-day deadline of the Data Controller can only be considered expired when the customer provides their contact to the Data Controller in a justifiable way.

5.3 The customer can furthermore request the correction or deletion – apart from the data processing commanded by law – of their personal data at any time.

5.4 If the personal data is false, and if the accurate data is available to the Data Controller, the Data Controller corrects the personal data.

5.5 The Data Controller informs their customers that their data needs to be deleted in the following cases:

a) if the processing of the data is illegitimate;

b) if the customer (subject) requests as such;

c) if the data is incomplete or inaccurate and the situation cannot be rectified legally;

d) if the purpose of data processing has ceased; and

e) if the court or the Hungarian National Authority for Data Protection and Freedom of Information enacts it.

Instead of deletion the Data Controller blocks the personal data if the subject requests, or if based on the available information it is presumed that deletion would violate the legitimate interests of the subject. Data blocked in this way can only be controlled as long as the data controlling purpose that excluded the deletion of the personal data prevails.

However, the Data Controller informs its customers that upon deletion of their data they cannot provide the Service any longer for the given customer.

5.6 The Data Controller marks the personal data processed by them if the subject contests its correctness or accuracy but the incorrectness or inaccuracy of the data in question cannot be ascertained unambiguously.

5.7 The customer can object to the processing of their personal data in accordance with the applicable legal acts.

The objection – and at the same time, the suspension of the data processing – will be examined by the Data Controller in the shortest possible time following the sending of the request, but within a maximum of 15 days. The Data Controller informs the customer about the result of the examination in writing, sending it to the contact detail (postal address) given by the customer, given that the customer provided such detail in their request. In the case of default, the standard 15-day deadline for the Data Controller can only be considered expired when the customer provides their contact details to the Data Controller in a justifiable way.

In case the objection is justified, the Data Controller ceases to process the data – including data recording and data transfer – locks the data, and informs about the objection and the measures taken based on it all the people concerned for whom it has previously transferred the personal data and who are liable to act in order to validate the right of objection.

In case customers disagree with the decisions made by the Data Controller based on their objection, they can lodge a complaint in a court of law 30 days following its announcement.

5.8 In the case of violating the law regarding the personal data of the customers, the customers can turn to court. The court of law will prioritize the case. Based on the decision of the customer, the court case can be undertaken in a court based on the registered address of the Data Controller or at the place of residence of the customer (subject).

In effect as of: 01.11.2012