SZIGET KULTURÁLIS MENEDZSER IRODA KORLÁTOLT FELELŐSSÉGŰ TÁRSASÁG
(SZIGET CULTURAL MANAGEMENT LIMITED)
DATA PROTECTION POLICY

Sziget Kulturális Menedzser Iroda Korlátolt Felelősségű Társaság (hereinafter "Data Controller") performs the management and protection of personal and other data in accordance with the following regulations (hereinafter "Regulations").

The Data Controller organizes events, and to these events and for the related services it sells tickets, furthermore, it conducts these events and the check-in process, moreover, at the events it gives access to services provided by it or its contracted partners.

Pursuant to the resolution issued by the Hungarian National Authority for Data Protection and Freedom of Information, the Data Controller is entitled to perform data management under registration number 40778 and in compliance with legal regulations. The objective of these Regulations is to ensure, for all individuals, that the rights and basic freedoms, in particular the right to privacy, are respected during the automatic processing of their personal data (data protection) in the course of the Data Controller's activities described in the previous paragraph.

Furthermore, the purpose of these Regulations is to set out the data protection and data management principles applied by Sziget Kulturális Menedzser Iroda Korlátolt Felelősségű Társaság (1033 Budapest, Hajógyári-sziget top. lot no. 23796/58, company registration no. Cg. 01-09-263756, registering authority: Court of Registration of the Budapest Metropolitan Court, tax no.: 10837410-2-41) as well as the Company's data protection and data management policy.

1./ Principles of Data Management

1.1. For the purpose of the application of these Regulations, the subjects concerned are any specific natural persons who may – directly or indirectly – be identified on the basis of their personal data.

1.2. The Data Controller is the manager of personal data collected and recorded in relation to the operations of the Data Controller.

1.3. During customer registration, the objective of data management is to ensure that the services available are actually and effectively available, by matching the data provided by the given user. During the check-in process, the objective of data management is to ensure the personal security of visitors attending the event. During the event, a further objective of data management is (provided that it is technically feasible and the service provider deems it necessary to check the subject's eligibility [e.g. age] to a certain service available at the event) to secure that the service provider is capable to ascertain the subject's eligibility by checking the subject's personal data.

1.4. Data management is voluntary in all cases, and the Data Controller only uses the personal data provided for the purposes of providing the service selected by the subjects

concerned, in line with and within the framework of the consent granted by such subjects. Data management is in line with this objective in all its phases. The legal basis for the data management performed by the Data Controller is the informed consent by the subjects concerned; they grant this consent by accepting the terms and conditions during customer registration, by participating in the identification procedure during the check-in process, and by participating in the event in the respect of data management during the event.

1.5. Data is stored on servers in Hungary, and are not forwarded to any data controllers or data processors in any third countries. During its activities, the Data Controller ensures the security of data and the enforcement of data protection and privacy regulations through technical and organisational measures and by putting the rules of the security procedure in place.

1.6. The Data Controller and the operator of the server network protects the data using state-of-the-art hardware and software support, in particular against unauthorised access, alteration, transfer, disclosure, deletion or destruction, as well as against accidental destruction and damage, thereby providing data security.

1.7. In line with the general rule, only employees of the Data Controller participating in the implementation of data management purposes set out in these Regulations will have access to the data managed by the Data Controller; these employees are bound by confidentiality obligations in respect of all data that come to their knowledge pursuant to their employment contract, legal provisions applicable to their employment or based on the instructions of the Data Controller.

1.8. During its activities, in messages sent out in relation to the service provided in connection with data management, the Data Controller is entitled to include short, informative or marketing purpose messages to customers, based on their consent. If the subjects concerned at any time forward their objections to the marketing content received in messages related to the Service, and send these objections to the Data Controller in a written and identifiable form, after receipt of these objections the Data Controller shall no longer be entitled to place marketing content in messages related to the provision of the service sent to those customers. Messages containing only marketing content can only be sent by the Data Controller if it is granted prior and express consent to do so by the subjects concerned.

1.9. Subjects affected by the data management performed by the Data Controller can at any time revoke the consent granted to the Data Controller for that data management by sending the Data Controller a written message, or they may limit the consent to certain data or data management procedures. Furthermore, subjects are also entitled to object to the management of their personal data in the cases set out in Act CXII of 2011 on Informational Self-Determination and Freedom of Information. At the same time, the Data Controller also calls the attention of customers to the fact that if they request the deletion of the minimum data required for the provision of any of its services, it will no longer be able to provide the given service to such customers. In such cases, the Data Controller is entitled to terminate the legal relationship with any such customers unilaterally and with immediate effect.

1.10. The Data Controller uses the data collected from customers for statistical purposes and anonymously – in other words, in a manner that does not allow the relationship between data and customers to be restored – in line with governing legal provisions, and is also entitled to disclose such data and forward it to third parties.

2./ Compliance with Legal Regulations

2.1. The Data Controller treats the personal and other data of customers in compliance with the Hungarian legal regulations in effect.

2.2. The Data Controller's data protection policy is in compliance with the applicable Hungarian legal regulations in effect as well as key international recommendations, in particular with the following:

(i) the content of terms and expressions used in these Regulations is identical to the content set out in the Definitions section (Article 3) of Act CXII of 2011 on Informational Self-Determination and Freedom of Information;
(ii) Act VI of 1998 on the Promulgation of the Strasbourg Convention of 28 January 1981 on the Protection of Individuals with regard to Automatic Processing of Personal Data;
(iii) Act CVIII of 2001 on Certain Issues of Electronic Commerce Activities and Information Society Services.

2.3. The Data Controller reserves the right, and at the same time undertakes to amend its data protection policy as well as the content of these Regulations unilaterally and in line with the currently effective legal regulations, or in the event of a change in the services, in line with that. The Data Controller informs customers of any changes to the data protection policy simultaneously with that change taking force, through the www.sziget.hu website.

3./ Customer Registration

3.1. In order to be able to use the various services provided by the Data Controller then, during the conclusion of the agreement, customers must register themselves on the Data Controller's website. As part of the registration procedure, customers must – depending on the type of services purchased – provide the following personal data (hereinafter: "Customer Data"): name, mother's maiden name, address, billing address, telephone number, date of birth, email address and vehicle registration plate.

3.2. The personal data collected during registration are at no time transferred by the Data Controller, disclosed to any third parties or linked to any other data management procedures without the express consent of the subjects concerned. At the same time, the Data Controller informs the subjects concerned that, in the interest of providing the service, the transfer of data and linking data management procedures may become necessary to persons determined in advance or set out in the annex to these Regulations.

3.3. During data transfer and the linking of data management procedures, the Data Controller acts while taking data security aspects fully into account and ensures that the persons to whom the data is transferred manage such data under the appropriate security conditions.

3.4. The Data Controller only transfers data to persons listed in the annex these Regulations in the event this is absolutely necessary to provide the service in question and only transfers the data absolutely required for this purpose.

3.5. By registering, customers (subjects concerned) grant their consent to the free of charge storage of their personal data and to the management of such data in line with these

Regulations. The Data Controller retains the Customer Data managed by it, and only deletes such data at the specific request of the customer.

4./ Identification During the Check-in Process

4.1. During the check-in process (assigning the admission wristband to the natural person identified during the check-in procedure) at the site of events organised by the Data Controller, the Data Controller requests identity to be verified with a photo identification document. As part of this process, the Data Controller reads, records, stores and manages the data of the subjects concerned as shown in the identification documents; furthermore, it makes audio and video recordings of the subjects concerned, which it also records, stores and manages (the personal data collected during admission and the recordings made of the subjects concerned are hereinafter collectively referred to as: "Identification Data"). If the Data Controller requests children under the age of fourteen (14) to be connected to the adult escorting them, then it is entitled to mutually connect, during the entry process, the wristband data of the children concerned to the wristband data of the adult escorting them. If the persons wishing to gain admission to the Data Controller's event do not grant, or revoke, their consent to any of the data management specified in this Section 4.1, the Data Controller is entitled to invalidate the wristband and deny admission to the event.

4.2. The personal data collected during identification are at no time transferred by the Data Controller, disclosed to any third parties or linked to any other data management procedures without the express consent of the subjects concerned. At the same time, the Data Controller informs the subjects concerned that if law or an order from a court or other authority requires it to do so, then it may transfer, make available, or link the subject's personal data to other data management procedures, in the scope and to the persons set out in such law or order.

4.3. During data transfer and the linking of data management procedures, the Data Controller acts while taking data security aspects fully into account and ensures that the persons to whom the data is transferred manage such data under the appropriate security conditions.

4.4. By checking in to the event, customers (subjects concerned) grant their consent to the free of charge storage of their personal data and to the management of such data in line with these Regulations. The Data Controller deletes Identification Data after seventy-two (72) hours following the official closing of the event at which these data were recorded, except where a well-founded suspicion of abuse arises or if actions violating, endangering or threatening the lives, physical well-being or health of participants have arisen, in which cases such Identification Data shall be retained by the Data Controller for a maximum period of one year or for the period determined by the authorities if they order it to do so.

5./ Identification at the Event

5.1. If at the Data Controller's event it is technically feasible and the service provider deems it necessary to check the subject's eligibility [e.g. age] to a certain service available at the event, then the Data Controller may use the Identification Data collected from the subject during the check-in process to ascertain, by checking the subject's personal data, if the subject is eligible to such services.

5.2. The personal data set out in Section 5.1 are at no time transferred by the Data Controller, disclosed to any third parties, or linked to any other data management procedures without the express consent of the subjects concerned, however the information about the eligibility for a certain service (e.g. reaching the legal age) may be disclosed to the third party service provider.

5.3. By entering into the event, customers (subjects concerned) grant their consent to the free of charge storage of their personal data and to the management of such data in line with these Regulations. The Data Controller deletes Identification Data after seventy-two (72) hours following the official closing of the event at which these data were recorded.

6./ Notifications, Advertisements

6.1. The Data Controller directly contacts its customers ("Ticket Buyers") registering on its website via email, over the phone or through text messages (SMS). The Data Controller may send Ticket Buyers messages containing information arising in relation to the use of the service or in the interest of the use of the service, except in those cases set out in Section 1.8. Furthermore, the Data Controller may also send news items, newsletters, advertisements and promotional offers related to events organised by it and may use data for marketing research and surveys. Moreover, the Data Controller provides further information for Ticket Buyers on its website at www.sziget.hu.

6.2. With a view to the contents of Section 1.8 as well, the Data Controller only sends messages qualifying as advertisements to Ticket Buyers with the prior consent of Ticket Buyers, in a clearly identifiable manner. In line with applicable legal regulations, the Data Controller keeps records of persons that have indicated in writing that advertising messages may be sent to them. The Data Controller does not send any advertisements to persons not in these records. The records may only be handed over to any third party with the prior consent of the customers (subjects concerned), with a view to the contents of Section 3.2, in which case data may be transferred.

6.3. If Ticket Buyers no longer wish to receive messages qualifying as advertisements, they can cancel this at the Data Controller using the option available on the www.sziget.hu website or in person at the registered office of the Data Controller.

7./ Provision of Information and Legal Remedy

7.1. If, beyond the contents of these Regulations, customers have any other questions or observations, the Data Controller requests such customers to contact it at the telephone number or email address listed below:

Telephone number: +36 1 372 0650
Email address: info@sziget.hu

7.2. Customers may request information on the management of the personal data at any time. At their request, in each case the Data Controller provides detailed information on the data of the customers (subjects concerned) managed by it, as well as the data processed by the data processor commissioned by it, the source of such data, the purpose, legal basis and duration of data management, the name and address and data management-related activity of the data processor, as well as the legal basis and addressees of data transfers (if the personal

data of the subjects concerned are transferred). The Data Controller provides such information within the shortest possible time from receipt of such request, but within thirty (30) days at the most, in writing, clearly, sent (postal address) to the contact details provided by the customers, provided those customers have provided such contact details in their request. In the absence of such contact details, the 30 day deadline set for the Data Controller shall only be deemed expired when customers provide their contact details to the Data Controller in a verifiable manner.

7.3. Furthermore, customers may request the correction or deletion (with the exception of data management set out in legal regulations) of their personal data at any time.

7.4. If the personal data provided are false and the correct personal data is available to the Data Controller, the Data Controller will correct the personal data in question.

7.5. The Data Controller informs customers that it shall delete the data in the following cases:

(i) if the management of such data is against the law;
(ii) if requested to do so by the customer (subjects concerned);
(iii) if the data are incomplete or false and this cannot be lawfully corrected;
(iv) if the purpose of data management has expired;
(v) if ordered to do so by the Court or the Hungarian National Authority for Data Protection and Freedom of Information.

Instead of deletion, the Data Controller blocks the personal data if requested to do so by the subjects concerned or if, based on the information available, it may be assumed that deletion would violate the legal interests of the subjects concerned. Data thus blocked may only be managed as long as the data management purpose that has prevented the deletion of the personal data exists. At the same time, the Data Controller informs customers that, in the event of the deletion of their data, it cannot continue to provide the Service to the given customers.

7.6. The Data Controller flags the personal data managed by it if the subjects concerned contest the correctness or accuracy of such data but the incorrectness or inaccuracy of the personal data disputed cannot be clearly determined.

7.7. Customers may object to the management of their personal data in accordance with the applicable legal regulations. Objections – with the simultaneous suspension of data management – are reviewed by the Data Controller within the shortest possible time from receipt of such request, but within 15 days at the most, and the Data Controller sends the results of its review to the customers in writing, sent (postal address) to the contact details provided by the customers, provided customers have provided such contact details in their request. In the absence of such contact details, the 15 day deadline set for the Data Controller shall only be deemed expired when customers provide their contact details to the Data Controller in a verifiable manner. If the objection is justified, the Data Controller terminates data management – including all further data collection and data transfers – it blocks the data, and informs all those to whom it has transferred the personal data affected by the objection, as well as those obliged to act in the interest of enforcing the right of objection, of the fact of objection and the measures taken on the basis of the objection. If customers do not agree with the decision of the Data Controller made on the basis of their objection, they can lodge a complaint in a court of law within 30 days of the disclosure of the decision.

7.8. In the event of the violation of their rights related to the management of personal data, customers may turn to the Court. The Court will give priority to such cases. Court proceedings, depending on customer choice, may be opened in a court of law competent according to the registered office of the Data Controller or according to the place of residence of the given customer (subject concerned).

ANNEX TO
DATA PROTECTION POLICY

1) Data transfer in relation to Meex Student Tickets:
Scope of transferred data:
name, mother's maiden name, place of birth, date of birth, student ID no., name of education institution, email address, telephone number, barcode of ticket purchased, billing address, billing name

M Group International Korlátolt Felelősségű Társaság,
Company registration number: Cg.01-09-991540,
Tax number: 24123459-2-41,
Registered office: 1033 Budapest, Hajógyári sziget 23796/58.

2) Data transfer in relation to Transfer Tickets:
Scope of transferred data:
name, date of birth, email address, telephone number, barcode of ticket purchased, other information related to the use of the service as provided by the buyer during the purchasing process

Festival Travel International Korlátolt Felelősségű Társaság
Company registration number: Cg.01-09-991628
Tax number: 24125262-2-43
Registered office: 1095 Budapest, Soroksári út 48.

3) During the online purchasing process, for the purposes of transaction identification, the following data are transferred:
Start of purchasing process, end of purchasing process, transaction identifier, purchase amount

BIG FISH Internet-technológiai Kft.
Company registration number: Cg.01-09-872150,
Tax number: 13767213-2-42,
Registered office: 1066 Budapest, Nyugati tér 1-2.

4) During the online purchasing process, in the event of purchasing polyfoam mats, mattresses, inflatable beds, camping sets and safe deposit tickets, the following data are transferred: product type and name, time of sale, product barcode.

ATTROY Kereskedelmi és Szolgáltató Korlátolt Felelősségű Társaság
Company registration number: Cg.01 09 204309
Tax number: 25177509243
Registered office: 1125 Budapest, György Aladár utca 25. A. ép. Fszt 3.

5) During the online purchasing process, in the event of purchasing festival watches and festival tags, the following data are transferred: product type and name, time of sale, product barcode.

iPOS Kereskedelmi és Szolgáltató Korlátolt Felelősségű Társaság
Company registration number: Cg.13-09-121394
Tax number: 14213126-2-13

Registered office: 2724 Újlengyel, Dózsa György utca 15.

6) During the online purchasing process, in the event of purchasing Budget Parking products, the following data are transferred: product type and name, time of sale and product barcode, as well as other information related to the use of the service as provided by the buyer during the purchasing process.

Star Parking Korlátolt Felelősségű Társaság
Company registration number: Cg.01-09-933409
Tax number: 12416495-2-41
Registered office: 1137 Budapest, Ditrói Mór utca 3.