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

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.

In the course of ticket purchase, of check-in process, and of giving access to services at the events it is necessary that the Data Controller obtains certain personal data of ticket purchasers and visitors.

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, email: info@sziget.hu) as well as the Company's data protection and data management policy.

I PRINCIPLES OF DATA MANAGEMENT

1/ Scope 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. The Data Controller manages personal data in the following cases:

(i) during ticket purchase;
(ii) during registration to newsletters;
(iii) during the check-in process;
(iv) at the event, during its term.

(i) During ticket purchase, the main objective of data management is to secure compliance with applicable law, especially to enable the Data Controller to meet its accounting and tax obligations prescribed by law. The secondary objective of data management during ticket purchase is to ensure that (a) the Data Controller has knowledge about the identity of the person with whom it has entered into a legal relationship in the subject of the purchase of an event ticket and/or other service, (b) to identify, in the case of international purchases, which partner of the Data Controller is entitled to a commission after the purchase, (c) to identify fraudulent transactions made during online payment. The data management in question also renders the services provided by or through the Data Controller effectively available.

(ii) The main objective of data management during registration to newsletters is to send marketing communication to the subjects who explicitly authorise the Data Controller to do so.

(iii) During the check-in process, the main objective of data management is to ensure the personal security of visitors attending the event by identifying the people entering the event. A secondary objective of data management during the check-in process is to identify any entry-related fraud.

(iv) During the event, the 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.

Special provisions pertaining to the separate data managements described in Paragraphs (i)-(iv) above are set forth in Article II of these Regulations. The Data Controller only manages the personal data gathered pursuant to the aims defined herein and in the applicable law.

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, voluntary consent by the subjects concerned, given beforehand. The subjects concerned grant this consent in the following way:

(i) by commencing the purchase process during ticket purchase;
(ii) by ticking the checkbox required for registration and providing their email-address during registration to newsletters;
(iii) by participating in the identification procedure during the check-in process;
(iv) by participating in the event in the respect of data management during the event.

2/ General information on data management

2.1. During data management by the Data Controller, 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.

2.2. The Data Controller and the operator of the server network protects the data using, within reasonable boundaries, 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.

2.3. In line with the general rule, only employees and contractors 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 people are bound by confidentiality obligations in respect of all data that come to their knowledge pursuant to their employment or other professional contract, legal provisions applicable to their employment or based on the instructions of the Data Controller.

2.4. 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.

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

2.6. It is the aim of the Data Controller during all data management to ask only for the most inevitable personal data.

2.7. 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.

II DESRIPTION OF THE CASES OF DATA MANAGEMENT

1/ Data Management During Ticket Purchase

1.1. By commencing the purchase process, customers (subjects concerned) acknowledge that providing personal data voluntarily is a condition of completing the purchase, therefore they grant their explicit and voluntary consent in advance to the management of their personal data specified in this Clause II/1 by the Data Controller in line with these Regulations. The subjects acknowledge, by commencing the purchase process, that they explicitly give their consent to the Data Controller.

Besides that, independent third parties may also sell tickets or services to the Data Controller's events. Such third parties may forward the customers' personal data obtained during the purchase to the Data Controller on the basis of their own data policies. During the purchase, the subjects concerned also accept these Regulations of the Data Controller and give their consent to the Data Controller to the management of their personal data being forwarded.

1.2. In order to be able to purchase tickets or other services online to the Data Controller's events, customers must provide the following personal data (hereinafter: "Customer Data"): name, address (both country and street address), billing address, date of birth, email address. If the customer participates in the respect of any event in the Student Ticket Program organized by the Data Controller and Festival Travel International Korlátolt Felelősségű Társaság (1095

Budapest, Soroksári út 48., tax. No.: 24125262-2-43), then he/she shall also be required to provide the following Customer Data (personal data) as well: name of the education institution where he/she studies, and the number of his/her student ID. In case the subject purchases from the Data Controller a ticket or service specified in Annex 1 hereto, then – depending on the type of ticket or service purchased – he/she must also provide the Data Controller with further Customer Data (personal data), as specified therein.

1.3. The personal data collected during purchase – with the exception stated in the second sentence of this paragraph – 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 by the Data Controller, the transfer of data and linking data management procedures may become necessary to persons determined in advance. In case the subject purchases a ticket or service specified in Annex 2 hereto, then his/her personal data specified therein may be forwarded to the persons determined in Annex 2.

1.4. During data transfer and the linking of data management procedures, the Data Controller acts while taking data security aspects fully into account.

1.5. The Data Controller only transfers data to persons listed in Annex 2 of 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.

1.6. The Data Controller retains the Customer Data managed by it, and only deletes such data at the specific request of the customer. The Data Controller is obliged to retain the subject's billing data for a period of eight years pursuant to Act 92 of 2003 on taxation.

1.7. The Data Controller directly contacts its customers purchasing tickets or other services on its webpage via email. The Data Controller may send the subjects messages containing information arising in relation to the use of the service or in the interest of the use of the service.

1.8. Data management under this section has been registered by the Hungarian National Authority for Data Protection and Freedom of Information under registration number 40778.

2./ Data Management During Registration to Newsletters

2.1. The subjects may register on webpage www.szigetfestival.com to newsletters containing advertisements, promotions, and program offers related to the Data Controller's own events and services. Registration may be revoked by the subject at any time, without conditions and limitations by clicking on the "Unsubscribe" link at the bottom of the newsletter or by sending an email in the subject to info@sziget.hu. The personal data managed in connection with newsletter-registration is the email-address used for the registration.

2.2. The Data Controller may use data for marketing research and surveys. In line with applicable legal regulations, the Data Controller keeps records of persons that have registered to newsletters. 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 the exception of Section 1.3 of Chapter II, in which case data may be transferred without consent.

2.3. Data management under this section has been registered by the Hungarian National Authority for Data Protection and Freedom of Information under registration number 98300.

3/ Data Management During the Check-in Process

3.1. 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.

By participating in the check-in process, customers (subjects concerned) acknowledge that providing personal data voluntarily is a condition of participating in the event, therefore they grant their explicit and voluntary consent in advance to the management of their personal data specified in this Clause II/3 by the Data Controller in line with these Regulations. The subjects acknowledge, by participating in the check-in process, that they explicitly give their consent to the Data Controller.

During check-in, the Data Controller reads, records, stores and manages the following data of the subjects concerned as shown in the identification documents: citizenship, name, type, number and expiry of the identification document, date of birth, gender.

Simultaneously, the Data Controller 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 3.1, the Data Controller is entitled to invalidate the wristband and deny admission to the event.

3.2. 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.

3.3. During data transfer and the linking of data management procedures, the Data Controller acts while taking data security aspects fully into account.

3.4. 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 beyond seventy-two (72) hours, but for a maximum period of one year, or, if determined otherwise by a competent authority, for the period they have compelled the Data Controller to do so. The Data Controller deletes Identification Data after it has handed them over to the competent authority.

3.5. Data management under this section has been registered by the Hungarian National Authority for Data Protection and Freedom of Information under registration number 73838.

4/ Data Management at the Event

4.1. 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. In addition, the Data Controller operates a camera system at its events due to personal and event safety reasons. By entering into the event, the subject acknowledges that he/she has given his/her voluntary consent referred herein to the Data Controller.

4.2. The personal data set out in Section 4.1 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.

4.3. The Data Controller deletes Identification Data in all cases after seventy-two (72) hours following the official closing of the event at which these data were recorded.

III GEOLOCATION DATA, IP-ADDRESSES, COOKIES, AND DATA COLLECTION FOR STATISTICAL PURPOSES

1/ In the course of the ticket purchase written in Clause II/1 of these Regulations, the Data Controller, in order to identify fraudulent transactions, stores the geolocation data and IP-address of the user's computer, which data is not considered to be personal data. The user, by completing purchase transaction, consents to the use of these data by the Data Controller.

2/ During the use of the Data Controller's webpages written in Annex 3 hereto (hereinafter jointly the "Webpages") cookies (computer data of the person using the Webpages) generated in the course of using the Webpages shall be stored. Cookies are logged by the Data Controller upon visiting and leaving the Webpages without a separate legal declaration made by the user. The purpose of these data is to compile statistics related to the use of the Webpages and to develop the IT systems of the Data Controller.

Data obtained in this way is only managed by the Data Controller anonymously and in an aggregated form, and shall not be linked to the person or the personal data of the user.

The user, by using the Websites, accepts the use of cookies by the Data Controller. Cookies may be deleted by the user from his/her computer at any time. If the user forbids the use of cookies, then the use of the Webpages may not be of full value.

The codes used by the Data Controller for this purpose are written in Annex 3.

IV PROVISION OF INFORMATION AND LEGAL REMEDY

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

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, on the circumstances and effects of any data protection incident, 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 twenty-five 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 twenty-five-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.

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.

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.

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.

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.

4/ 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 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 line with the terms and conditions pertaining to such service. If revocation of the consent affects Identification Data collected during the check-in process, then the Data Controller shall be entitled to invalidate the wristband received by the subject without any obligation to refund the purchase price, and refuse entry for the event. If the revocation of the consent affects data management in relation to any other service, then the Data Controller is entitled to terminate the legal relationship with any such customers unilaterally and with immediate effect.

5/ 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.

6/ In the event of the violation of their rights related to the management of personal data, customers may turn to the Court or to the Hungarian National Authority for Data Protection and Freedom of Information (22/C Szilágyi Erzsébet fasor, 1125 Budapest, Hungary; phone: +36 1 3911400; fax: +36 1 3911410; email: ugyfelszolgalat@naih.hu). 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).

Annexes:

1. Further Customer Data managed during purchasing certain tickets and services
2. Data forwarding
3. Data related to cookies

DATA PROTECTION REGULATIONS
ANNEX 1

In case of purchasing the following products, the Data Controller also manages the subject's following personal data.

1./ 7-day ticket purchase in the Student Program

Further personal data: number of student ID

Purpose of data management: verification of student status

DATA PROTECTION REGULATIONS
ANNEX 2

In the below cases, the Data Controller may forward the subject's personal data.

1./ During the online purchase process

Personal data forwarded: name of customer, address of customer (country, city, postal code, street and house address), email address

Reason of data forwarding: execution and identification of purchase transaction

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

2./ During the online purchase process

Personal data forwarded: name of customer, address of customer (country, city, postal code, street and house address), email address

Reason of data forwarding: execution and identification of purchase transaction, fraud monitoring

Recipient:
OTP Mobil Szolgáltató Kft.
Registered office: 1093 Budapest, Közraktár utca 30-32.
Company registration number: Cg. 01-09-174466
Tax number: 24386106-2-43

DATA PROTECTION REGULATIONS
ANNEX 3

Cookies are stored on the Data Controller's following websites:

szigetfestival.com
volt.hu
gyereksziget.hu
gourmetfesztival.hu
balatonsound.com

The Data Controller applies the following statistical codes:

Google Analytics
Hotjar

The Data Controller applies the following tracking codes:

Facebook pixel
Google remarketing
Optinmonster
Adverticum