

Table of contents

GENERAL DATA PROTECTION REGULATION:	3
Introduction:	3
1. Definitions:	4
2. Principles relating to processing of personal data:	7
3. General information relating to processing of personal data:	8
4. Information relating to specific processing of data:	9
4.1. Ticket purchasing at SZIGET Webshop:	9
4.2. Offline ticket purchasing:	9
4.3. Subscription to newsletter:	10
4.4. Personal data processing related to employees and job applicants:	10
4.5. Data processing during the check in process:	11
4.6. Data processing for the purpose of returning documents and IDs lost during events and festivals:	11
4.7. Electronic surveillance systems used by SZIGET for the purposes of personal and property protection:	12
4.8. Press accreditation:	12
5. Additional data processing occurring during events:	13
5.1. Data control and processing activities related to providing health services to participants:	13
5.2. Market research and opinion polls conducted at events and festivals:	14
5.2.1. Participation in subscription to newsletter:	15
5.3. Data processing related to hospitality activities of different commercial units, as well as services provided by kitchens and clubs at events and festivals :	15
6. In addition to the above, SZIGET uses data processing activities of the following data processors, and transfers data to the following recipients:	17
6.1. FestiPay integrated check in and payment card issued by SZIGET:	17
6.2. Festipay Cashless Payment Service Provider Ltd as data processor:	17
6.3. Myriad Payments LTD as data processor:	18
6.4. BIG FISH Kft. as data processor:	18
6.5. Event InfoTech Szolgáltató Bt. as data processor:	18
6.6. TRL Hungary LTD. as data processor:	18
6.7. Netpositive Information Technology Provider and Commercial LTD. as data processor:	18
7. Other data transfer:	19
8. General information regarding use of Cookies:	20

9.	Customer service and complaints, SZIGET's customer correspondence:	20
10.	Information related to rights of data subjects:	21
10.1	Right to information as well as right to access processed personal data:	21
10.2	Right to rectification:	22
10.3	Right to erasure ('right to be forgotten') :	22
10.4	Right to restriction of processing:	23
10.5	Right to data portability:	23
10.6	Right to object:	24
10.7	Right to withdraw consent:	24
10.8	Procedure in case of data subject's request regarding the exercise of the above rights:	24
11.	Data security procedures:	25
12.	SZIGET maintains the following data processing registers:	26
13.	Submission of comments, questions, complaints:	27
14.	Legal remedies:	27
15.	Addendums:	28

GENERAL DATA PROTECTION REGULATION

Introduction

Sziget Cultural Management Ltd (address: 1033 Budapest, Hajógyári sziget 237/96/58., company register no.: 01-10-049598, hereinafter „**SZIGET**” or “**Controller**”) recognizes as mandatory for itself the principles of general data processing and protection enumerated in present general data protection regulation (hereinafter Regulation), with other words the data protection and processing policy of present Regulation.

SZIGET is committed to ensuring that all data processing related to its activities complies with expectations defined in present regulation and current laws. SZIGET upholds its right, and is committed to unilaterally modify the contents of present Regulation in accordance with the laws and regulations in effect, in addition to the event of a change in its services.

Data subjects shall be notified by SZIGET on its web site www.sziget.hu of any changes to present Regulation concurrently to the changes.

In case you have any questions regarding present Regulation, please write to us at hello@sziget.hu email address, or to our data protection officer Richard Zima (dpo@sziget.hu), or contact us at any of the contact information provided under section 13.

Unless provided otherwise, this Regulation does not extend to services and data processing related to promotions, raffles, services, other campaigns, or content advertised or otherwise published by third parties not affiliated with SZIGET or the web site operators on web sites described in this Regulation below.

When creating the provisions of the Regulation, SZIGET was especially mindful of

provisions of:

- the 2016/679 regulation of European Parliament and Council (EU) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (Hereinafter „**GDPR**”)
- Act CXII of 2011 on Informational Self-determination and Freedom of Information (Hereinafter „**Infotv.**”)
- Act V. of 2013 on the Civil Code (“**Ptk**”)
- Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (Hereinafter „**Grt.**”),
- Act CVIII of 2001 on certain issues of electronic commerce services and information society services (Hereinafter „**Eker. tv.**”)
- Act CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing („**Direktmarketing tv.**”)
- Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators („**Szvtv.**”)
- 23/2011. (III.8.) government regulation on improving the safety of dance and musical events.

- Act C of 2000 on Accounting („**Számv. tv.**”)
- Act CL of 2017 on Taxation („**Art.**”).

At the drafting of the Regulation, the amendment of Infotv in light of the mandatory and direct implementation of GDPR starting on May 25, 2018, has not occurred yet. It must be emphasized, in light of this, that during the application of the above laws as well as the present Regulation, the provisions of GDPR must be considered primarily, and a deviation from them is acceptable only and to the extent when GDPR itself allows it, and in absence of such permission, only and to the extent when the discrepancy provides for a more strict provision than those of the GDPR.

1. Definitions

Definitions of present Regulation are identical to the definitions and relevant provisions of the GDPR, and as such:

- “**personal data**” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.
- „**data subject**”: any natural persons identified or identifiable by any information;
- “**genetic data**” means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question, in addition personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.
- “**biometric data**” means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data; The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person, SZIGET does not employ such specific technical means.
- “**data concerning health**” means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

- **“Processing of special categories of personal data”** Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited;
- **„processing”** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **“restriction of processing”** means the marking of stored personal data with the aim of limiting their processing in the future;
- **“profiling”** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements, the principle of fair and transparent data processing requires that data subject be notified of the fact and purpose of data processing;
- **“filing system”** means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
- **“pseudonymisation”** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- **„cookie”**: cookie is a short text file which is sent by our server to the data subject’s device (including any computers, mobile phones or tablets) and read back. There are temporary (session) cookies, which are automatically deleted from the user’s device when the browser is closed, and there are cookies with a longer life span, which remain longer on the device of the data subject (this depends on the settings of the device as well);
- **“consent”** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- **“controller”** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Hungarian law, the controller or the specific criteria for its nomination may be provided for by Union or Hungarian law;
- **“processor”** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **“recipient”** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 2However, public authorities which may receive personal data in the framework of a particular inquiry in

accordance with Union or Hungarian law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

- **“third party”** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;
- **“enterprise”** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
- **„group of undertakings”** means a controlling undertaking and its controlled undertakings;
- **“binding corporate rules”** means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;
- **„Third country”**: a country not a member state of the European Union or the European Economic Area;
- **„EEA-state”**: a member state of the European Union, and other states that are a member of the agreement on the European Economic Area, in addition, the state whose citizen enjoys the same rights as a citizen of a member state of the agreement on the European Economic Agreement based on the international treaty between the European Union and its member states and the state which is not part of the agreement on the European Economic Area;
- **„international organization”**: means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
- **“data security incident”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Data Protection Officer: SZIGET has appointed a data protection officer especially given that its data processing related to its event management activity and its marketing activity repeatedly (as in yearly during the festival season) include data processing activities that require the systematic, substantial surveillance of data subjects due to the nature, extent and/or purposes (such as deploying camera systems at festivals for personal and property protection reasons, also in relations to its marketing activity, behavior-based advertising, retargeting and profiling activities are undertaken based on consent of the data subject).

SZIGET ensures that the data protection officer gets involved on time and in an appropriate way in every case related to personal data protection. The data protection officer cannot accept instructions related to carrying out his/her obligations, nobody can order him regarding the carrying out of his obligations, and cannot be fired or sanctioned due to carrying out his obligations. The data protection officer has a responsibility only to the board of directors of SZIGET.

Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under GDPR.

The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, and regarding the handling of data.

The data protection officer shall have at least the following tasks:

- a) to inform and advise SZIGET and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
- b) to monitor compliance with GDPR, with other Union or Member State data protection provisions and with the policies of SZIGET in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- d) to cooperate with the supervisory authority; and
- e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Section 13 of this Regulation contains the name and contact information of SZIGET's data protection officer.

2. Information relating to the principles of data processing

SZIGET shall strive to process personal information lawfully, fairly and in a transparent manner in relation to the data subject.

SZIGET shall process the provided personal data with specified, explicit and legitimate purposes defined by this Regulation, and information and rules marked as an annex and part of this Regulation („**principle of purpose limitation**”), which shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed („**data minimization**”).

Based on the principle of accuracy, SZIGET strives furthermore to ensure, with relation to the processed personal data, that they are kept up to date; and SZIGET shall take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay („**principle of accuracy**”).

During data processing, SZIGET shall recognize that storage of personal data shall not be longer than is necessary for the purposes for which the personal data are processed (“principle of storage limitation”), and that data processing is carried out in a way that appropriate technical and organizational measures are implemented in order to ensure appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage (“**integrity and confidentiality**”).

SZIGET provides additional information in the Data security subsection of section 11. of present Regulation regarding security measures taken in compliance with these data processing principles.

SZIGET and its data processors shall maintain internal data processing logs in order to demonstrate compliance with present data processing principles (“**principle of accountability**”). The principles included in this Regulation inform upon our practices related to personal data processing.

Our data processing principles apply to all of SZIGET’s devices, websites, all paper-based data processing, customer service platform or other online application, which refers to them by online link or any other manner. However, where present Regulation refers to separate data processing information or regulation in connection with data processing operations, we provide data subjects with separate information or regulation so that they may be informed more clearly and legibly regarding the date processing activities of SZIGET and/or its partners, participants, and data processors.

These regulations and information are a part and annex of present Regulation, with that insofar as a regulation or notice that is an annex does not specifically states otherwise, the contains of present Regulation are adequate to govern.

3. General information regarding data processing

In general, SZIGET processes data subject’s personal data to provide services used by data subject, to enhance user experience of data subject, and in relation to its own operations. SZIGET conducts data processing involving personal data with relation to the activities listed as follows:

- 1. During ticket purchase at SZIGET Web shop.**
- 2. During subscription to newsletters.**
- 3. Personal data processing related to job applicants or employees.**
- 4. Data processing during entrance (“check in”).**
- 5. Data processing for the purpose of returning objects lost during events and festivals**
- 6. Electronic surveillance systems used by SZIGET for the purposes of personal and property protection.**
- 7. Press accreditation.**
- 8. Additional data processing occurring during events:**
 - 8.1. Data control and processing activities related to providing health services to participants.**
 - 8.2. Data control and processing activities related to market research and opinion polls conducted at events and festivals.**
 - 8.3. Data processing related to hospitality activities of different commercial units, as well as services provided by kitchens and clubs at events and festivals.**
- 9. Data processors and other recipients of data transfers**
- 10. General information regarding the use of cookies.**
- 11. Customer service and handling of complaints, SZIGET’s customer correspondence**

General information regarding the specific data processing above:

- a) **Data processor and contact information: Sziget Cultural Management Ltd** (address: 1033 Budapest, Hajógyári sziget 237/96/58., company register no.: 01-10-049598 telephone: +36 (1) 372 0681, e-mail: hello@sziget.hu),
- b) **Data protection officer and contact information:** Richard Zima, address: 1033 Budapest, Hajógyári-sziget 23796/58, telephone: +36 (1) 3720664, e-mail address: dpo@sziget.hu.
- c) Purpose and legal basis of personal data processing: defined below for specific data processing, as well as in corresponding annex.
- d) Duration of storage of data processing or considerations for defining this period: defined below for specific data processing, as well as in corresponding annex.
- e) IN accordance with section 10.1 of this notice, data subjects are entitled to request from SZIGET access, rectification, erasure or restriction of data processing, and may object to such processing of personal data, and may exercise his/her rights regarding data transfer.

IN every necessary case, SZIGET conducted, prior to the processing, an assessment of the data protection impact, is mindful of the requirement of the necessity and proportionality of the processing operations, principle of purpose limitation, requirement of prior notification.

4. Information related to specific data processing

4.1. Ticket purchasing at SZIGET Web shop

SZIGET informs the data subjects that in case of ticket purchasing at the web shop and ticket sellers the main purpose of data processing is the identification of the user as the ticket purchaser, as well as the identification of suspicious transactions during online payments, as well as to obtain knowledge regarding which person it created a business relation with.

Detailed information regarding ticket purchase at the web shop is included at the Data Processing Information on purchasing at SZIGET web shop, which is an annex of this Regulation and may be accessed at the following link: <https://en.szigetfestival.com/policy-getc>

4.2. Offline ticket purchase

Third parties, independent of SZIGET,(ticket sellers, ticket selling and marketing promoters, hereinafter “**data processors**”) may sell entry tickets to SZIGET events; they transfer to SZIGET personal data collected during the purchase based on their own data processing regulations. During the purchase, the data subject accepts SZIGET’s present rules as well.

Purpose of data processing	Range of processed personal data	Duration of processed data	Legal basis of data processing
Ticket purchase from promoters, ticket sellers, ordering, preparation of purchase receipt,	Transaction number, date and time, receipt’s contents, name, address, and tax identification number	Until the satisfaction of the contract, in case of possible civil claims arising from the purchase, for 5 years	In case of ticket sale and reservation, data subject’s consent based upon Info.tv. section 5.§ (1) a) and

registry of buyers, distinguishing buyers from each other, satisfaction of purchase orders, documenting purchase and payment, satisfying accounting requirements, reserving tickets, customer relations.	in case of VAT invoices, name and phone number of customer in case of reserving a ticket.	from the date of purchase, if the data is handled by the data processors, by reserving or ordering the tickets, or by processing the customer's name and telephone number until notification	GDPR article 6. section (1) a), and performance of contract GDPR article 6. section (1) b), in case of documenting purchase and payment, satisfying accounting requirements GDPR article 6. section (1) c), section (2) of article 169 of the Számv. tv.
--	---	--	--

Additional detailed information regarding ticket sellers and promoters is included at the Data Processing Notice on purchasing at SZIGET web shop, which is an annex of this Regulation and may be accessed at the following link: <https://en.szigetfestival.com/policy-gctc>

4.3 Subscription to newsletters:

During subscription to newsletters at SZIGET's different web sites, data subjects submit personal data, which SZIGET collects and processes for the purposes of sending marketing materials to them regarding SZIGET's products and services.

Additional detailed information regarding subscription to newsletters is included at the separate Notice on Data Processing for Newsletters, which is an annex of this Regulation and may be accessed at the following link: <https://en.szigetfestival.com/policy-gctc>

4.4 3. Personal data processing related to job applicants or employees

SZIGET informs data subjects that according to its general rule, it only advertises employment opportunities by identifying itself. Publishing anonymous advertisements of employment opportunities, and processing the submitted materials by SZIGET occurs only by taking into account the data protection authority's guidance in particularly justified, exceptional cases, and even then to a limited extent (for instance only for a short, temporary period of time).

SZIGET further informs data subjects that, as a general rule, it stores their application materials for a period of one year from the date they are received in order to use them for its possible recruiting needs during this period.

If the data subject submits materials not related to a specific advertisement, SZIGET always requests, within the shortest reasonable amount of time, that the applicant confirms in writing, within five work days, that SZIGET may store the received application materials and the personal data of the applicant according to the aforementioned procedure. If confirmation is not received within the required time period, SZIGET does not store and process the documents and personal data further.

Employer notifies job applicants of this on its web site as well as in each published employment advertisement. Accordingly, the legal basis for storage of application materials is the voluntary consent (subsection (1) a) of article 6. of GDPR). The application materials may be accessed by the

Human Resources team leader, the assigned staff of the human resources department, and staff members authorized for decision making during the selection process.

Additional detailed information on SZIGET's data processing regarding employees is included in the regulation regarding SZIGET's employee data processing, which is an annex of present Regulation, and which document is not public.

4.5 Data processing during event entry („check in”)

During the registration at the location of the events managed by SZIGET (as in during the application to a natural person a wrist band authorizing entry during the entrance procedure), SZIGET requests personal identification by a photo identification document, and records the data subjects' last name, first name, date of birth, country of origin, nationality, as well as gender, and photographs them. The registration will be available online as well. SZIGET requires that the online ticket holders register online.

If SZIGET requires that persons younger than 14 shall be added to the adult accompanying them, SZIGET may mutually add the wrist band data of the data subject child(ren) to the wrist band data of the adult accompanying the child(ren). The primary purpose of the data processing is the protection of the personal safety of the visitors at the mass event by identifying the entering persons. The secondary purpose of the data processing during entrance procedure is the identification of abuse concerning the entry. Based on the data processed for the aforementioned purposes, it shall be deemed a legitimate interest of SZIGET to notify the proper authority of potential criminal activities or threats to public safety, and to transfer to the authority any personal data related to same criminal activity or threat to public safety in individual cases or in several independent cases.

4.6 Data processing for the purpose of returning documents and IDs lost during events and festivals

If, during the events or festivals of SZIGET, a visitor finds any lost document that probably belong to someone else and which document may be used for personal identification purposes of the original owner or possessor of the document, and if it is handed to the appropriate SZIGET staff member, SZIGET will safeguard the found documents in a locked place until the official end of the events or festivals.

If the identity of the owner or the documents or person authorized to receive them can be identified without a doubt, and if information to notify the person is available, SZIGET's staff shall notify this person.

The data subject has the opportunity to receive the documents, IDs by the official end of the event or festival in case of notification or without it also, and a record shall be made of the receipt of the documents. In this case the legal basis of the personal data processing is a legitimate interest pursued by a third party under subsection f) of section (1) of Article 6 of GDPR.

If the person otherwise authorized to receive the documents does not appear until the event closes, SZIGET shall deposit the documents, IDs with the clerk or notary public of the appropriate jurisdiction.

4.7 Electronic surveillance systems used by SZIGET for the purposes of personal and property protection

SZIGET hereby notifies data subjects that it uses electronic surveillance systems (camera systems) at its headquarters as well as at its particular events. Sziget deploys camera systems at the following festivals: Sziget Festival, Volt Festival, and Balaton Sound. The camera system provides fixed surveillance at its headquarters, and direct as well as fixed surveillance in the case of the aforementioned festivals.

SZIGET hereby notifies data subjects regarding all camera systems that SZIGET uses them solely for purposes of personal and object protection in accordance with the provisions of Szvtv; in addition, regarding all camera systems, SZIGET's employees as well as persons not employed by SZIGET who enter SZIGET headquarters or the festival premises may be considered data subjects.

4.8. Press Accreditation

SZIGET hereby provides notice regarding personal data collection and processing of data subjects during registration at <https://partners.sziget.hu> web site as well as press accreditation process. The purpose of the registration is the management of the online accreditation of the press. Primarily the name and email address of the data subject is given, which serves the purpose of keeping contact, and the password given by the data subject is necessary for safely accessing the user account.

An additional purpose of the data processing is to enable SZIGET press department to verify that the applicant meets the requirements for accreditation, as well as for the accredited media to provide information to the public about the festival according to the provisions of article 10 of the Act CIV. of 2010. regarding fundamental rules on media content, as well as article 11 of the Charter of Fundamental Rights of the European Union.

SZIGET hereby notifies data subjects that data controlled during accreditation in Hungary is controlled by SZIGET jointly with PRESSCOM.HU Szolgáltató és Kommunikációs Betéti Társaság (2000 Szentendre, János street 13/A. Corporate registration number: 13-06-050286).

The joint controllers have defined their respective tasks regarding the exercise of data subjects' rights, including the provision of proper data protection and confidentiality.

Additional detailed information regarding press accreditation is included at the separate Notice on Data Processing for Press Accreditation, which is an annex of this Regulation and may be accessed at the following link: <https://en.szigetfestival.com/policy-gctc>

5. Additional data processing occurring during events

5.1. Data control and processing activities related to providing health services to participants

According to section (3) of article 9 of government regulation 23/2011. (III.8.), SZIGET provides for on the scene presence of personnel trained for administering first aid based on the number of visitors at events and festivals organized by SZIGET, which it accomplishes for the 2018 festival season on one

hand by ordering the services of **Magenta Idea Szolgáltató és Kereskedelmi Korlátolt Felelősségű Társaság** (address: 1136 Budapest, Tátra u. 5. B. ép. fszt. 1/C., corporate registration number: 01-09-320063, email: magentaideabtinfo@gmail.com), and on the other hand by commissioning the **National Ambulance Service** (address: 1055 Budapest, Markó street 22., email: info@mentok.hu)(hereinafter: „Service Providers”). Accordingly, SZIGET provides limited access to Service Providers of its own database collected during check in as described in section 4.5, solely in case of protecting data subject’s vital interests (therefore especially in case when the identification of data subject for administering emergency medical care by Service Providers is otherwise not possible).

During data transfer and/or providing access to data base, SZIGET exercises the highest standard of care possible in terms of data security.

In addition to the aforementioned, SZIGET hereby notifies data subjects that independent data control activities of Service Providers pursuant to Act XLVII. Of 1997 regarding processing and protection of personal data related to health care („Eüak.”) is outside the purview of SZIGET’s control.

SZIGET is not responsible for the processing and protection of personal, health related and special data collected, processed and stored pursuant to Eüak; this data processing activity is within the purview of Service Providers as autonomous data controllers, which are legally as well as actually independent of SZIGET.

Circumstances of data processing:

1. **Subject matter of data control by Data processor:** performance of service or special-order contract;
2. **Duration of data processing:** duration of contractual relationship;
3. **Nature of data processing by Processor:** SZIGET as Controller provides limited access to a range of personal data defined under section 5., to its database, namely to the enterprise resource planning system (ERP) operated by Netpositive LTD (address: 2021 Tahitótfalu, Pataksor street. 48., Corporate registration number.: 13-09-104997) when necessary for providing treatment, patient care, or immediate medical care in case of emergency.
4. **Purposes of processing:** assistance by SZIGET in providing services defined under the service or special-order contracts that are fast, efficient and adequate from a data security perspective;
5. **Range of processed personal data:** name, gender, nationality and country of origin of data subject;
6. **Categories of data subjects:** natural persons entering to, or participating in any capacity, in events or festivals as defined under the service or special-order contracts;
7. **Legal basis for data control and data transfer:** the vital interests of the data subjects under subsection (1)d of GDPR article 6.

Furthermore, SZIGET hereby notifies data subjects that it has entered into a processing contract with Service Providers as processors pursuant to article 28 of GDPR, under which parties are bound by a

duty of confidentiality, are also obligated to support data security with the required technical and organizational measures, as well as physical and IT solutions during processing of limited range of data, and Service Providers are further obligated to return all the data set containing personal data received from SZIGET after the end of the aforementioned data transfer, and destroy the data set stored in its data storage by deletion, and document this, with that according to the aforementioned, after identifying the data subject, Service Providers shall process data necessary for the independent provision of their service independently from SZIGET.

5.2. Market research and opinion polls conducted at events and festivals

SZIGET shall inform the data subjects that, according to a service contract with **Ipsos Media-, Advertisement-, Market- and Opinion Research LTD** (address: 1139 Budapest, Pap Károly street 4-6., corporate registration number: 01-10-046444, email: hu-accountsreceivable@ipsos.com , hereinafter: „ **Ipsos Zrt.**”), Ipsos Zrt has undertaken conducting research tasks such as measuring traffic and interviews in relation to festivals and events organized by SZIGET.

Within traffic counting, Ipsos Zrt conducts a research among festival visitors with the purpose of measuring the demographic data of the visitors (families in case of Children Island) via a short, one page questionnaire, for instance age, schooling, residence, and other demographic data). At Volt, Balaton Sound and Sziget events, the above procedure is substituted by analysis of anonymous data collected during check in.

SZIGET shall inform the data subjects in this Regulation regarding the use of data for statistical purposes, in limited amount and rendered always anonymous, derived from the dataset collected at the check in, with that pursuant to Recital 50 of the GDPR, the processing of personal data is permissible for purposes (here statistical) other than those for which the personal data were initially collected, if Hungarian law (with other words the Directmarketing law) specifically describes its circumstances, as well as the processing is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Facts, data, and other information obtained by Ipsos Zrt as a result of preparing analysis as well as research papers during the research are processed as strictly confidential business secrets. Ipsos Zrt does not, in any case, transfer data collected for market research purposes to SZIGET for direct commercial purposes. It ensures that the data provided during the opinion survey are provided voluntarily, and ensures full anonymity of the surveyed person at each phase of the processing of the answers.

Data collected for this purpose are stored at a strictly isolated database, which is protected by proper technical and organizational measures.

5.2.1. Participation in newsletter subscription

In addition to the above, during interaction with participants at the premises of Children Island, the staff of Ipsos Zrt records on tablets the name and email address of participants who are 16 years or older- following their permission given voluntarily, expressly and in possession of a proper notice- and later transfers to SZIGET the dataset for purposes of newsletter subscription.

Additional detailed information regarding newsletter subscription is included in the separate Notice on Data Processing, which is an annex of this Regulation and may be accessed at the following link: <https://en.szigetfestival.com/policy-gctc>

SZIGET further informs the data subjects that it entered into a processing agreement with Ipsos Zrt as processor, pursuant to article 28 of GDPR, given the above data processing activity, under which parties have an obligation of confidentiality, and are obligated to ensure with technical and personal measures required by data security, as well as via physical and information technology solutions, the secure transfer to SZIGET of the collected data, as well as recording in a log the data processing and transferring activities.

Following the reaching the goal of data transfer described above, Ipsos Zrt must destroy by deletion on its own electronic devices, and data storages all the stored personal data set, and credibly document this.

5.3. Data processing related to hospitality activities of different commercial units, as well as data processed in connection with services provided by kitchens and clubs at events and festivals

Merchants

General description:

SZIGET shall provide merchants the opportunity to operate pavilions for purposes of providing service and non-food commercial activities, and provides the opportunity to operate cooking facilities under the same conditions for a service fee paid by merchants who have a contractual relationship with SZIGET as well as the FestiPasy system user fee, pursuant to conditions included in the Hospitality and Commercial GTC and technical regulations. Accordingly, SZIGET provides an opportunity for merchants to purchase professional pass type tickets, which can be purchased solely by the specified representative of the given merchants, and which may only be accessed by the staff of the merchants, and shall not be traded.

In addition, SZIGET shall permit at its events the construction and operation of installations by parties operating clubs, who are in a contractual relationship with SZIGET, at agreed upon, suitable locations. Accordingly, SZIGET provides an opportunity for operators to purchase professional type tickets. SZIGET accomplishes the construction and operation of card-based FestiPay payment processing system by providing electronic payment points (which consist of NFC POS Terminals and NFC card readers); SZIGET provides training for the club operators to learn the operation of these.

The merchants and the operators of clubs, kitchens together hereinafter („Merchants”).

SZIGET assigns natural persons a wrist band authorizing entrance to the event during the entry procedure (check-in) in accordance with section 4.5. of this Regulation. Those stipulations, including the stipulations regarding the entry procedure, are controlling for the use of tickets described here as well.

General purpose of data processing by SZIGET are: service contract performance, assisting the performance of Merchants’ contracts, later the accreditation of contact persons on the partner portal

operated by SZIGET for the purposes of easier cooperation, and the verification of the performance of the contracts.

Detailed information regarding specific data processing described above.

Purpose of processing	Range and categories of processed data	Duration of processing	Legal basis of processing
Collection of personal data of contact persons authorized financial accounting during contracting of Merchants.	Name, personal ID number, address, phone number, email address, bank account number	8 years after creation of the contract, in accordance with section (2) of paragraph 169 of Számv.tv., under subsection (1) (c) of GDPR's article 6.	Processing is necessary for the contract formation and performance under GDPS article 6, section b., parties are unable to form and perform a contract without providing data
Conducting the transaction at purchasing of professional type tickets, documenting purchase and payment, performance of accounting obligations, Identifying the user as ticket buyer, correspondence with him/her, billing, option of processing payment, and identification of suspicious transactions during online payments	Last name, first name, email address, date of birth, address.	Until performance of contract, in absence of this, SZIGET deletes the data after the purchase date, in accordance with Ptk. Paragraph 6:22, 5 years after possible needs become due, 8 years after the transaction under subsection (1)-(2) of paragraph 169 of Számv. Tv.	Data processing is necessary for contract performance (GDPR 6.b), and satisfaction of legal requirement (GDPR 6.c) parties are unable to perform the contract without providing data
Collection and processing of personal data for the purpose of assigning wrist bands to individuals during the entry procedure	Photo, last name, first name, date of birth, country, nationality, gender, in case of "online check-in": e-mail adress	SZIGET automatically deletes the personal data 72 hours after the official ending of the event.	Legitimate interest pursuant to subsection (1)(f) of article 6 of GDPR.
Cash substituting payment solutions deployed at events organized by SZIGET	Last name, first name, email address, phone number	Until official ending of the event.	Data processing prior to contract performance , for the steps necessary for

(FestiPay system considered to be electronic vouchers, operated by use of RFID wrist bands, as well as PayPass contactless payment system) as well as conducting training for the proper and lawful use of cash registers.			performance (GDPR 6.b), and satisfaction of legal requirement (subsection (1)(c) of article 6 of GDPR, without collection of the data, the staff or employees of the merchants are unable to perform under contract
--	--	--	---

Whereas the data of the data subjects processed for the aforementioned purposes are transferred by third persons to SZIGET, the notification of the data subjects by SZIGET would be impossible or would require a disproportionately big effort, therefore SZIGET hereby notifies aforementioned third parties that the data transfer shall be undertaken when a proper consent from the data subject is in the possession of the third persons.

6. In addition to the above, SZIGET uses data processing activities of the following data processors, and transfers data to the following recipients

6.1. FestiPay integrated check in and payment card issued by SZIGET

From 2018, payments can be made by the wristband authorizing entry to Sziget. The main thing about the system is that the wristbands will be equipped by RFID chips, so they include a payment function in addition to containing every entry entitlement (days, camping, etc). This system works for weekly and daily pass holders as well, and practically the FestiPay payment card becomes built in to the wristband.

This way, data subject can upload his/her balance via the Sziget mobile application, and at the end of the festival, he/she will receive back the balance to his/her bank card over the limit amount specified by each event.

6.2. FestiPay Cashless Payment Service Provider Ltd as data processor

Name of processor	Range of processed data	Duration of processing
Festipay Cashless Payment Service Provider Ltd (address: 1135 Budapest, Reitter Ferenc street 46-48., CRNo.: 01-10-048644)	Personal data such as name, address, ID or passport number, phone number, from data subject' ID, passport or driver's license during balance transfer	Processor deletes the data from its own system after the given event or festival

6.3 Myriad Payments LTD as data processor

Name of processor	Purpose and nature of data processing activity

Myriad Payments LTD (address: Elmslie House, 51-53. Irish Town Gibraltar)	Payment fraud monitoring and prevention, claim and right enforcement related to payment fraud.
---	--

6.4. BIG FISH Kft. as data processor

Name of processor	Purpose and nature of data processing activity	Category of processed data
BIG FISH Kft. (address: 1066 Budapest, Nyugati square 1-2., CRNo.: 01-09-872150)	Processor provides complex, electronic payment support service named „BIG FISH Payment Gateway”, and operates a corresponding connected information technology system for SZIGET	name, transaction amount, IP address, transaction date and time, billing address

6.5. Event InfoTech Szolgáltató Bt. data processor

Name of processor	Purpose and nature of data processing activity	Category of processed data
Event InfoTech Szolgáltató Bt. (address: 1118 Budapest, Tűzkő street 2. 5. floor. 21., CRNo.: 01-06772582)	Manages electronic application process for selecting participants of SZIGET’s Civil Sziget program location, and stores applicants’ data on its own storage, which it deletes immediately upon data subject request.	Personal or business email address; during the management of the event, this is expanded by name and phone number of participants.

6.6. TRL Hungary Kft. as Data Processor

Name of data processor	Purpose and nature of data processing activity
TRL Hungary Kft. (CRNo.: 11-09-007772, address: 2510 Dorog, Mátyás Király street. 11/A.)	Provides Maconomy management ERP system, financial and accounting process support (ERP) system operation

6.7. Netpositive Information Technology Service Provider and Trading Ltd. as Data Processor

Moreover SZIGET also uses the services of the **Netpositive Information Technology Service Provider and Trading Ltd.**

Data and contact details of Netpositive Kft.:

Name: Netpositive Information Technology Service Provider and Trading Ltd.

Registered Office: Pataksor street 48., Tahitófalu, 2021

Company Register No.: 13-09-104997

E-mail Address: info@netpositive.hu

Nature and Purpose of the Data Processing Activity

It performs physical and operation system level operation of the servers for the administration system and online sales systems of SZIGET. SZIGET stores the given personal data on the servers in the Budapest server room of GTS Datanet under the address of Victor Hugo utca18-22., 13th District, Budapest. SZIGET uses Netpositive Kft.'s operator services to store its personal data. Data Processor is bound by confidentiality obligations in respect of all information, facts, data and other knowledge that have come to its knowledge during its activities, and this obligation shall remain effective after the termination of the legal relationship.

If it is necessary and requested, the Data Processor helps SZIGET or other data controller pursuant to sectoral law to fulfil its obligations deriving from data protection impact assessments and from preliminary consultation with controlling authority.

Data Processors do not make decisions on their own; they are entitled to proceed solely pursuant to the contract made with the Data Controller and in compliance with the received instructions.

Data Controller monitors the work of Data Processors.

Data Processors are entitled to employ further data processor only with the prior written consent of the Data Controller.

7. Other Data Transfers

SZIGET Supplies Data to Borgun as Recipient

During purchases done through the internet as to serve the fulfillment of the data processing purpose, personal data are transferred to B-Payment Szolgáltató Zrt. (registered office: Váci út. 4., Budapest, 1132, company register no. Cg. 01-10-047882), who makes electronic payment services available, to ensure the execution, security and tracking of purchase transactions.

Transferred data are name, birth name, mother's name, place and time of birth, address, contact details, necessary financial data

SZIGET forwards personal data, and also through the bank card accepting network of OTP Bank Nyrt. (Nádor u. 16., Budapest, 1051), to **OTP Mobil Szolgáltató Kft.** (registered office: Közraktár u. 30-32., Budapest, 1093, company register no. Cg. 01-09-174466, hereinafter **SimplePay**) as recipient to ensure the execution, security and tracking of purchase transactions. Transferred data are user's name, surname, first name, shipment address, billing address, telephone number, e-mail address and data related to the purchase transaction.

If the user purchases with a card or voucher offering a special discount (OTP SZÉP Card, MKB SZÉP Card, K&H SZÉP Card, Erzsébet Card, Edenred voucher), SZIGET transfers the required customer's data to the company supplying the discount;

1. OTP Pénztárszolgáltató Kft. (Mérleg u. 4., Budapest, 1051),
2. MKB Nyugdíjpénztárt és Egészségpénztárt Kiszolgáltató Kft. (Dévai u. 23., Budapest, 1134),
3. K&H Csoporszolgáltató Központ Kft. (Lechner Ödön fasor 9., Budapest, 1095),

4. Erzsébet Utalványforgalmazó Zrt. (Hermina út 63. I/1., Budapest, 1146),
5. Edenred Kft. (Kéthly Anna tér 1., Budapest, 1075)

The user may request information on the applying data management rules directly from the respective service provider company. SZIGET automatically processes identifiers and other data of such cards/vouchers only to the extent the service provider company requires it to execute the purchase and to supply the discounts.

In addition to the points mentioned above, personal data are not transferred to any third party. Data are transferred to a third party or recipient if you are informed on the potential recipient in advance, and a prior consent is given by you or it is imposed by law. During such data processing activity, personal data are not transferred to any third countries or international organisations.

8. General Information on the Use of Cookies

SZIGET informs the subjects concerned that it uses cookies on the webpage of szigetfestival.com, gourmetfesztival.hu, balatonsound.com, volt.hu, gyereksziget.hu.

What are cookies? How can you change the settings?

Cookie is a short textual file, which is sent to the device (a computer, mobile or tablet) of the subject concerned and is read back by our webserver. There are temporary (or so called session) cookies, which are automatically deleted from your device when you close the browser, and there are cookies that remain on your device for a longer time (depending also on your device's settings). We apply cookies managing personal and non-personal data on the webpage of szigetfestival.com, gourmetfesztival.hu, balatonsound.com, volt.hu, gyereksziget.hu.

Further detailed information **on cookies used by SZIGET** (including the option of changing the cookie settings later) is in the **Cookie Guide** forming the Annex hereto, and it can be accessed through the link of [.....](#).

Concerning cookies used by third parties, we draw your attention to the fact that links/ads on the above mentioned surfaces lead to webpages of third parties, and you can inform on their data management policy including the possible use of cookies from the respective service provider, SZIGET does not accept any responsibility for such cookies.

9. Customer Service and Complaint Treatment, the Customer Correspondence of SZIGET

SZIGET provides assistance to private persons using its services in case of receiving complaint, question or other observation through its e-mail addresses generated specially for this purpose on the webpages in its property and operation.

SZIGET provides customer service platform on three specific areas to the subjects concerned:

1. general
2. for press workers

3. for ticket purchasers

The purpose of data management is the examination and detailed administration of cases received via contact e-mail addresses at links on SZIGET webpages during the customer service activity, or the detailed administration of calls made with the call centre to make questions and observations on SZIGET activity available for SZIGET. Communication via e-mail is archived so the information is available in their original form in the event of a subsequent question or debate, and, if necessary, SZIGET may get into contact with the user in relation to the case.

Further detailed information is in the Data Management Guide on purchasing in the SZIGET Webshop forming the Annex hereto, and it can be accessed through link of: <https://en.szigetfestival.com/policy-gctc>

Information regarding data subjects' rights

10.1 Right to information and to access the processed personal data:

You have the right to receive feedback from SZIGET on whether your personal information is being processed, and if such processing of your data is under way, you have the right to access the personal data and the following information:

- a) the purposes of the data processing;
- b) the categories of the personal data in question;
- c) the categories of recipients to whom we disclosed or will disclose the personal data, especially with regards to third country recipients or international organizations;
- d)) the planned duration of the storage of the personal information in any case, or if it is not possible, the criteria for determining this duration;
- e) the right of the data subject to request from the controller the correction, deletion or restriction of processing their personal data, and may object to the processing of such personal data;
- f) the right to file a complaint with a supervisory authority;
- g) if the data was not collected from the person concerned, all available information regarding the data source;
- h) the fact of automated decision making, including profiling, as well as easy to understand information, at least in these cases, regarding the applied logic and the significance of such data processing, and the envisaged consequences for the data subject.

Where personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards pursuant relating to the transfer.

SZIGET shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, SZIGET may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided by SZIGET in a commonly used electronic form.

The right to obtain a copy referred to in the paragraph above shall not adversely affect the rights and freedoms of others.

The aforementioned rights may be exercised via the contact information specified in article 13.

10.2 Right to rectification

The data subject shall have the right to obtain from SZIGET without undue delay the rectification of inaccurate personal data concerning him or her.

Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

10.3 Right to erasure ('right to be forgotten')

The data subject shall have the right to obtain from SZIGET the erasure of personal data concerning him or her without undue delay where one of the following grounds applies:

- a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b) the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
- c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data processing relates to direct sales;
- d) the personal data have been unlawfully processed;
- e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- f) the personal data have been collected in relation to the offer of information society services.

Erasure of data may not be requested if the processing is necessary:

- a) for exercising the right of freedom of expression and information;
- b) for compliance with a legal obligation which requires processing by Union or Member State law or for the performance of a task carried out in the public interest;
- c) for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional, and these data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies;
- d) for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- e) for reasons of public interest in the area of public health and these data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies;

- f) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes if the right to erasure would probably seriously risk or make impossible such data processing¹; or
- g) for the establishment, exercise or defense of legal claims.

10.4 Right to restriction of processing

Upon data subject's request, SZIGET restricts the processing of data subject's personal data where one of the following applies:

- a) the accuracy of the personal data is contested by the data subject, in this case the restriction is for a period that enables the data subject to verify the accuracy of the personal data;
- b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- c) SZIGET no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;
- d) the data subject has objected to SZIGET's processing pursuant to public interest or compelling legitimate grounds, in this case the duration of the restriction is for the time period needed for the verifying whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted for the aforementioned reasons, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

A data subject who has obtained restriction of processing pursuant to the aforementioned reasons shall be informed by SZIGET before the restriction of processing is lifted.

10.5 Right to data portability:

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to SZIGET, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from SZIGET to which the personal data have been provided, where:

- a) the processing is based on consent pursuant to contract
- b) the processing is carried out by automated means.

In exercising his or her right to data portability pursuant to the aforementioned, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

¹ Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organizational measures are in place in particular in order to ensure respect for the principle of data minimization. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

The exercise of the right to data portability shall be without prejudice to the right to erasure ('to be forgotten'). That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The right to data portability shall not adversely affect the rights and freedoms of others.

10.6 Right to object:

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to SZIGET's processing of personal data concerning him or her where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in SZIGET, processing is necessary for the purposes of the legitimate interests pursued by SZIGET or by a third party, including profiling based on those provisions.

In this case, SZIGET shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

10.7 Right to withdraw consent:

The data subject shall have the right to withdraw his or her consent at any time if SZIGET's data processing is based on consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

10.8 Modalities in case of request by the data subjects on the exercise of the aforementioned rights:

The controller shall provide information on action taken on a request to the data subject without undue delay and in any event within one month (30 days) of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

SZIGET shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

If SZIGET does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

SZIGET shall provide the requested information and notification free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, SZIGET may either charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request.

SZIGET shall inform every such recipient of personal data, with whom personal data was shared, of all modification, erasure, or data processing restriction, unless this proves to be impossible, or requires an unreasonably large effort. Upon request of the data subject, SZIGET shall inform him/her of these recipients.

10. Data security measures:

Controller as well as the operator of the server network shall ensure security of the personal data with reasonably obtainable most up-to-date hardware and software support especially from unauthorized use, unauthorized alteration, transfer, publication, erasure or destruction, as well as accidental destruction or data loss, thereby serving data security

Under the general rule, data processed by Controller shall be only accessed by employees and other collaborators partaking in achieving the data processing purposes of Controller under this Regulation, and they are under confidentiality obligation based on employment contract, legal relationship related to the employment, furthermore other contractual relations, statutory provisions, or based on instruction of Controller in relation to all data they accessed.

A. Security of paper-based personal data

For the security of personal data processed on paper, SZIGET and Netpositive Kft shall take the following measures:

- Data shall only be accessed by authorized persons, no other may access them, nor shall they be revealed to them
- The documents shall be placed in a well locked, dry place equipped with fire protection and property protection equipment.
- Documents under continuous, active processing shall be accessed only by authorized persons,
- The staff performing data processing can only leave the data processing room at the end of the day, if he/she locks the documents under his/her responsibility, or locks the office.
- If the personal data processed on paper is digitalized, the security rules applicable to digitally stored documents shall be applied by SZIGET and its data processors.

B. Security of Personal Data Stored Digitally

To ensure the security of the personal data stored on a computer or network, SZIGET and its data processors proceed in compliance with the rules of the Information Security Regulations of Netpositive Kft. operating the backstage, in particular

- to have access to data stored on backstage only with valid, unique and identifiable authorization, at least with a user name and password,

- to log each access to data ensuring traceability,
- to provide continuous protection against viruses on the network managing personal data,
- to prevent unauthorized access to the network by the implementation of the available information technology devices

A possible security incident may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

As soon as SZIGET becomes aware that a security incident has occurred, it should notify the security incident to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless it is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification cannot be given within 72 hours, SZIGET shall describe the reason for the delay in the notification, and it shall give the specified information in parts.

In order to prevent security incidents, to maintain security and to prevent processing that infringes GDPR, the SZIGET or the data processor shall evaluate the risks inherent in the processing and shall implement measures to mitigate those risks, such as encryption. These measures shall ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transferred, stored or otherwise processed which may in particular lead to physical, material or non-material damage. Furthermore, to monitor measures relating to security incidents and to inform the subjects concerned, SZIGET keeps security incident records as described below.

11. SZIGET Keeps the Following Data Management Records

To monitor the legality of data transfer and to inform the subjects concerned, SZIGET keeps data transfer records including

- a) time of personal data transfers managed by it,
- b) legal basis of data transfers,
- c) addressees,
- d) description of transferred personal data types and
- e) other data prescribed by law on data management

To monitor measures relating to security incidents and to inform the subjects concerned, SZIGET keeps security incident records where all security incidents obligatory listed at least with the following details

- a) the affected personal data types
- b) types and number of subjects involved in the security incidents
- c) time, circumstances and effects of security incidents

- d) measures taken to solve the problem and
- e) other data prescribed by law on data management.

In addition, SZIGET keeps records of requests to terminate data management, of cases by subjects concerned and by authorities, and of subjects concerned accepting marketing communication to be sent. Data protection officer keeps security incident records, and records of cases by subjects concerned and by supervisory authorities, and the Marketing Department of SZIGET keeps records of subjects concerned accepting marketing communication to be sent, whereas data transfer records are kept by SZIGET's respective departments involved in the data transfer.

12. Comments, questions or complains:

Any questions or requests regarding your personal data stored or processed in our system should be sent to hello@sziget.hu e-mail address, or in writing to 1399 Budapest Pf.: 694/245 postal address. Please keep in mind that to serve your best interest, we are only able to provide information or take action regarding your personal data processing if you provide us with credible identification.

We hereby inform you that concerned parties may contact SZIGET's data protection officer regarding all questions on personal data protection and exercise of rights under GDPR. The data protection officer may be contacted at:

- i. Data protection officer: Richárd Zima,
- ii. Address: H-1033 Budapest, Hajógyári-sziget Hrsz:23796/58,
- iii. Telephone: +3613720664,
- iv. E-mail: dpo@sziget.hu.

13. Legal remedies:

Controller may be contacted with any questions or comments regarding data processing via contact information provided under article 13.

(1530 Budapest, Pf.: 5., phone: +36 (1) 391-1400, e-mail: ugyfelszolgalat@naih.hu, website: www.naih.hu) alleging infringement of rights concerning the processing your personal information or if an immediate threat of such infringement is impending, in addition

You may initiate an investigation at the National Data Protection and Freedom on Information Authority:

- i. Name: National Data Protection and Freedom on Information Authority
- ii. Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
- iii. Mailing address: 1530 Budapest, Pf.: 5.
- iv. phone: +36.1.391.1400
- v. Fax: 06.1.391.1410
- vi. Web: <http://www.naih.hu>
- vii. E-mail: ugyfelszolgalat@naih.hu

In case of infringement of your rights, you may seek judicial remedies against SZIGET as data controller. The court considers the case out of turn. SZIGET has the burden to prove that processing of the data was in accordance with the law. Decision of the case is within the jurisdiction of the court.

Legal proceedings may also be brought before the court where the data subject has domicile or residence.

SZIGET shall compensate for damages caused to others by unlawful processing of data subject's data, or a violation of the requirements of data security. Data subject may demand restitution (~~Ptk. 2:52. §~~) in case of invasion of privacy. Processor is indemnified from liability if the damage is caused by an unavoidable cause outside of the scope of data processing. SZIGET shall not compensate for damages, nor can restitution be demanded to the extent that it was caused by the gross negligence or willful conduct of the injured party.

14. Annexes

The present Regulations has the following Annexes

1. Data Management Guide on Purchasing in the SZIGET Webshop
2. Data Management Guide on Newsletters
3. Data Protection Regulations on Data Management at Work
4. Data Protection Guide on Press Accreditation
5. Cookie Guide
6. Data Protection Guide on the Application of the SZIGET Electronic Camera System
7. Privacy Notice for the Making of Video Recordings
8. Data Protection Guide on the Wish List App
9. Notice on Data Processing for Press Releases

