GENERAL DATA PROTECTION REGULATION

Introduction

Weekend Event Korlátolt Felelősségű Társaság (registered office: 1122 Budapest, Városmajor utca 48. B. ép. fszt. 2., company register no.: 01-09-695549, hereinafter "**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. Controller is committed to ensuring that all data processing related to its activities complies with expectations defined in present regulation and current laws.

Controller reserves 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 Controller on its website molnagyonbalaton.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 adat@nagyonbalaton.hu email address, 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 Controller or the web site operators on web sites described in this Regulation below.

When creating the provisions of the Regulation, Controller 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.**").

During the application of 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, Controller 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;

2. Information relating to the principles of data processing

Controller shall strive to process personal information lawfully, fairly and in a transparent manner in relation to the data subject. Controller 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, Controller strives furthermore to ensure, with relation to the processed personal data, that they are kept up to date; and Controller 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, Controller 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"**). Controller 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. Controller 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 Controller'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 Controller 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, Controller 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. Controller especially conducts data processing involving personal data with relation to the activities listed as follows:

1. **During ticket purchase at Controller Webshop.**

2. **During subscription to newsletters.**
3. **Personal data processing related to job applicants or employees.**
4. **Data processing for the purpose of returning objects lost during events and festivals**
5. **Electronic surveillance systems used by Controller for the purposes of personal and property protection.**
6. **Data processing related to hospitality activities of different commercial units, as well as services provided by kitchens and clubs at events and festivals.**
7. **Data processors and other recipients of data transfers**
8. **General information regarding the use of cookies.**
9. **Customer service and handling of complaints, Controller's customer correspondence**

Otherwise, if - in case of certain activities, promotions, games, prize games etc. - data processing occurs, Controller informs the data subject about it in a separate privacy notice.

General information regarding the specific data processing above:

a) **Data controller and contact information: Weekend Event Korlátolt Felelősségű Társaság** (registered office: 1122 Budapest, Városmajor utca 48. B. ép. fszt. 2., company register no.: 01-09-695549, telephone: +36 (1) 372 0681, e-mail: adat@nagyonbalaton.hu),
b) Purpose and legal basis of personal data processing: defined below for specific data processing, as well as in corresponding annex.
c) Duration of storage of data processing or considerations for defining this period: defined below for specific data processing, as well as in corresponding annex.
d) In accordance with section 10.1 of this notice, data subjects are entitled to request from Controller 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. The data subjects are informed in a separate privacy notice about the rights that may be exercised concerning each data processing, if those rights are different from the aforementioned rights.

In every necessary case, Controller 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 Controller's Webshop

Controller informs the data subjects that in case of ticket purchasing at the webshop 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 webshop is included at the Notice on Data Processing for Webshop Purchasing, which is an annex of this Regulation and may be accessed at this link.

4.2. Offline ticket purchase

Third parties, independent of Controller, (ticket sellers, ticket selling and marketing promoters, hereinafter "**data processors**") may sell entry tickets to Controller events; they transfer to Controller personal data collected during the purchase based on their own data processing regulations. During the purchase, the data subject accepts Controller'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, registry of buyers, distinguishing buyers from each other, satisfaction of purchase orders, documenting purchase and payment, satisfying accounting requirements, reserving tickets, customer relations.	Transaction number, date and time, receipt's contents, name, address, and tax identification number in case of VAT invoices, name and phone number of customer in case of reserving a ticket.	Until the satisfaction of the contract, in case of possible civil claims arising from the purchase, for 5 years 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	In case of ticket sale and reservation, data subject's consent based upon 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 Notice on Data Processing for Webshop Purchasing, which is an annex of this Regulation and may be accessed at this link.

4.3. Subscription to newsletters:

During subscription to newsletters at Controller's different web sites, data subjects submit personal data, which Controller collects and processes for the purposes of sending marketing materials to them regarding Controller's products and services. By registering for newsletter the data subject consent that any activities (such as opening it or clicking on links) with the newsletters sent to the email address of the data subject can be monitored and used by Controller in order to display advertisements – even third parties' advertisement - on its own or on partner's webpage.

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 this link.

4.4. Personal data processing related to job applicants or employees

Controller 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 Controller 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).

Controller 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, Controller always requests, within the shortest reasonable amount of time, that the applicant confirms in writing, within five work days, that Controller 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, Controller 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 management and the Chief Financial Officer.

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

4.5. Data processing for the purpose of returning documents, IDs and objects lost during events and festivals

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

If the identity of the owner of the documents, IDs, objects or the person authorized to receive them can be identified without a doubt, and if information to notify the person is available, Controller's staff shall notify this person. The data subject has the opportunity to receive the documents, IDs, objects 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, IDs, objects.

In case of documents, IDs, 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, IDs does not appear until the event closes, Controller shall deposit the documents, IDs with the clerk or notary public of the appropriate jurisdiction.

In case of other lost objects (in case of receipt of the object: name, address, signature; in case of searching for an object: name, contact telephone number, signature) the legal basis of the personal data processing is – in case of the receipt of the object - a legitimate interest pursued by a third party under subsection f) of section (1) of Article 6 of GDPR, in case of searching for an object the legal basis is the consent of the data subject pursuant to subsection a) of section (1) of Article 6 of GDPR. The data subject will be informed by a privacy notice about the data processing mentioned in this section at the venue.

4.6. Electronic surveillance systems used by Controller for the purposes of personal and property protection

Controller hereby notifies data subjects that it uses electronic surveillance systems (camera systems) at its particular events. Controller deploys camera systems at the following festivals: SopronFest Festival, ZamJam Festival, Balaton Piknik Festival, BMYLAKE Festival and Strand Festival. The camera system provides direct (live) and fixed surveillance in case of the aforementioned festivals. Controller hereby notifies data subjects regarding all camera systems that Controller uses them solely for purposes of personal and object protection in accordance with the provisions of Szvtv; in addition, regarding all camera systems, Controller's employees as well as persons not employed by Controller who enter Controller festival premises may be considered data subjects. Controller provides privacy notice regarding each festival's electronic surveillance system on its webpages and at the venues of the festivals.

Additional detailed information regarding the use of electronic surveillance system is included in the Privacy Notice, which is an annex of the present Regulation and may be accessed at this link.

5. Additional data processing occurring during events

Data processing also occurs related to hospitality activities of different commercial units at events and festivals.

General description:

Controller 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 Controller as well as the FestiPasy system user fee, pursuant to conditions included in the Hospitality and Commercial GTC and technical regulations.

Accordingly, Controller 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, Controller shall permit at its events the construction and operation of installations by parties operating clubs, who are in a contractual relationship with Controller, at agreed upon, suitable locations. Accordingly, Controller provides an opportunity for operators to purchase professional type tickets. Controller 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); Controller provides training for the club operators to learn the operation of these.

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

General purpose of data processing by Controller are: service contract performance, assisting the performance of Merchants' contracts, later the accreditation of contact persons on the partner portal operated by Controller 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, 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, Controller 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
Cash substituting payment solutions deployed at events organized by Controller (FestiPay system considered to be electronic vouchers, operated by use of cards, as well as PayPass contactless payment system) as well as conducting training for the proper and lawful use of cash registers.	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 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 Controller, the notification of the data subjects by Controller would be impossible or would require a disproportionately big effort, therefore Controller 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, Controller uses data processing activities of the following data processors, and transfers data to the following recipients

6.1. 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 Controller	name, transaction amount, IP address, transaction date and time, billing address

6.2. Netpositive Számítástechnikai Szolgáltató és Kereskedelmi Kft. as Data Processor

Moreover Controller also uses the services of **Netpositive Számítástechnikai Szolgáltató és Kereskedelmi Kft..**

Data and contact details of Netpositive Kft.:

Name: Netpositive Számítástechnikai Szolgáltató és Kereskedelmi Kft.

Registered Office: Pataksor street 48.**,** Tahitótfalu, 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 Controller. Controller 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. Controller 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 Controller 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.

6.3. Hidden Design Korlátolt Felelősségű Társaság as Data Processor

Moreover Controller also uses the services of the **Hidden Design Korlátolt Felelősségű Társaság** (1095 Budapest, Gát utca 21. fszt. 1., Company register No.: 01-09-278702, tax number: 23089655-2-43).

Nature and Purpose of the Data Processing Activity:

The Hidden Design Kft. provides a runtime environment for the Websites of Controller. The Hidden Design Kft. resorts to the following sub-processors (the data are exclusively stored at servers located in the European Union):

the **Contabo GmbH** (Aschauer Straße 32a, 81549 Munich, Germany, Company registration number: HRB 180722, registry court: AG München, tax number: DE267602842, telephone number: +49 89 3564717 70, Fax: +49 89 216 658 62, e-mail: info@contabo.com), and the **DigitalOcean LLC** (101 Avenue of the Americas, 10th Floor, New York, NY 10013, United States).

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 Controller 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

Controller 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), Controller 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 Kiszolgáló Kft. (Dévai u. 23., Budapest, 1134),
3. K&H Csoportszolgáltató 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. Controller 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 by Controller on the potential recipient in advance, and a prior consent is given by the data subject 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

Controller informs the subjects concerned that it uses cookies on the webpage of molnagyonbalaton.hu, balatonpiknik.hu, strandfesztival.com, zamjam.hu, sopronfest.hu, bmylake.hu and nagyszinpad.com.

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 the device for a longer time (depending also on the device's settings). Controller applies cookies managing personal and non-personal data on the webpage of molnagyonbalaton.hu, balatonpiknik.hu, strandfesztival.com, zamjam.hu, sopronfest.hu, bmylake.hu and nagyszinpad.com

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

Concerning cookies used by third parties, Controller draws 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, Controller does not accept any responsibility for such cookies.

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

Controller 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.

Controller 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 Controller webpages during the customer service activity, or the detailed administration of calls made with the call centre to make questions and observations on Controller activity available for Controller. 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, Controller may get into contact with the user in relation to the case.

Further detailed information is in the Notice on Data Processing for Webshop Purchasing forming the Annex hereto, and it can be accessed through this link.

10. 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 Controller 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.

Controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, Controller 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 Controller 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 Controller 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 Controller 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 processing[1]; or
g) for the establishment, exercise or defense of legal claims.

10.4. Right to restriction of processing

Upon data subject's request, Controller 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) Controller 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 Controller's processing pursuant to public interest or compelling legitimate grounds, in this case the duration of the restriction is for the time period

[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.

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 Controller 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 Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from Controller 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.

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 Controller'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 Controller, processing is necessary for the purposes of the legitimate interests pursued by Controller or by a third party, including profiling based on those provisions. In this case, Controller 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 Controller'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:

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.

Controller 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 Controller 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.

Controller 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, Controller 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.

Controller 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, Controller shall inform him/her of these recipients.

11. 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, Controller 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 aplied by Controller 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, Controller 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 Controller 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, Controller 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 Controller 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, Controller keeps security incident records as described below.

12. Controller Keeps the Following Data Management Records

To monitor the legality of data transfer and to inform the subjects concerned, Controller 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, Controller 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, Controller 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.

13. Comments, questions or complains:

Any questions or requests regarding your personal data stored or processed in our system should be sent to adat@nagyonbalaton.hu e-mail address, or in writing to 1122 Budapest, Városmajor utca 48. B. ép. fszt. 2. 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 Controller regarding all questions on personal data protection and excercise of rights under GDPR. Controller may be contacted at:

i. Address: H-1122 Budapest, Városmajor utca 48. B. ép. fszt. 2.,
ii. Telephone: +3613720664,
iii. E-mail: adat@nagyonbalaton.hu

14. Legal remedies:

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

You may initiate an investigation at the Hungarian National Authority for Data Protection and Freedom of Information:

i. Name: Hungarian National Authority for Data Protection and Freedom of Information
ii. Address: 1055 Budapest, Falk Miksa utca 9-11.
iii. Mailing address: 1363 Budapest, Pf.: 9.
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 Controller as data controller. The court considers the case out of turn. Controller 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.

Controller 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. Controller 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.

15. Extras

This General Data Protection Regulation was written in Hungarian, although its English version is also accessible. In the event of contradiction between Hungarian and English version, the Hungarian language version shall prevail.

16. Annexes

The present Regulations has the following Annexes

1. Notice on Data Processing for Webshop Purchasing
2. Notice on Data Processing for Newsletters
3. Privacy Notice Regarding the Use of Electronic Surveillance System
4. Cookie Notice
5. Data Protection Regulations on Data Management at Work (this annex is not public)