valid from:
2020.01.01

Privacy Policy

I. Introduction

Netpositive Ltd. (registered seat: 2021 Tahitótfalu, Pataksor u. 48., headquarters: 1031 Budapest, Záhony u. 7., postal address: 1031 Budapest, Záhony u. 7., company registration number: 13-09-104997, tax number: 12643565-2-13; hereinafter: “Data Controller”) complies with the following policy (hereinafter: “Policy”) when processing and protecting personal and other data.

As a commissioner of the Event Organizer, Data Controller undertakes the selling of tickets and related services for events organized by the Event Organizer.

For ticket purchases, admission to the events, using the services at the events, as well as for assessing future demands, Data Controller requires access to the personal data of ticket holders. The purpose of the displayed rules is that the rights, fundamental freedoms and the right to protection of privacy is respected when processing the personal data of each person purchasing tickets and related services for the events.

Data Controller declares that its data processing activities are carried out – by implementing appropriate internal policies and technical and organisational measures – at all times in conformity with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter: “Regulation”) and with the provisions of Act CXII of 2011 on Informational Self-Determination and Freedom of Information (“Privacy Act”).

Data Controller may unilaterally amend the Policy, with any such amendments taking effect upon publication at the website.

II. Purpose of the Policy

The purpose of the Policy is to establish internal rules and to provide a foundation for measures that ensure fair and transparent data processing, compliance with relevant legislation, and the protection of personal and other data.

III. Scope of the Policy

The scope of this Policy extends to the processing of personal data concerning natural persons by the Data Controller.

IV. Definitions

For easier identification we provide the meaning of the most important terms.

1. “**Personal data**” means any personal 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, location data or an online identifier. Scope of collected and processed personal data: name, e-mail, phone number, country, postal code, city, address, GeoIP data, VAT number (the latter only in case of requesting an e-invoice).

2. “**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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3. “**Data 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 Member State law, the Data Controller or the specific criteria for its nomination may be provided for by Union or Member State law;

4. “**Processor**” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller;

5. “**Third party**” means a natural or legal person, public authority, agency or body other than the data subject, Data Controller, processor and persons who, under the direct authority of the Data Controller or processor, are authorised to process personal data;

6. “**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.

V. Basic principles of processing

Data Controller shall carry out processing in the following cases:

1. in the course of purchasing tickets;
2. in newsletter registrations;
3. during the admission process.

The legal basis for processing is your freely given, specific, informed and unambiguous consent, which extends to the processing carried out for the purposes specified in this privacy policy.

Primary objectives of processing your personal data:

- to provide a process for ticket purchasing, to ensure uninterrupted compliance with legislation on the Data Controller's part, including in particular Data Controller's compliance with accounting and tax obligations prescribed by law;
- collecting statistical data for market research;

Secondary objectives of processing your personal data:

- ensuring that Data Controller is aware of its business partner's identity when selling a ticket and/or other services to an event;
- maintaining contact by electronic means (telephone, email);
- sending information and/or newsletters about the Company's products, services, terms and conditions, and discounts;
- analysing website use and user patterns.

VI. Processing for ticket purchase:

Making a purchase in the webshop operated by Data Controller constitutes a contract in line with Article 13/A of Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services and with Government Decree 45/2014. (II. 26.) on the Detailed Provisions of Contracts Concluded Between Consumers and Companies.

Data Controller shall handle the personal data and address of natural persons making purchases at the webshop for the purposes of drawing up the contract for the service, determining and modifying the contents thereof, monitoring the performance thereof, billing the charges arising therefrom as well as enforcing the claims related thereto on the legal basis of Subsection 13/A (1) of Act CVIII of 2001, and shall handle e-mail addresses and online identifiers by consent.

For purchases in the webshop, the legal basis for processing in case of tickets purchased after 25 May 2018 is the contract. (With the entry into force of REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.)

Duration of the processing of personal data: for the duration of the service, or until a withdrawal of consent (request for erasure) by the data subject, or in case of a purchase for 5 years following the purchase.

The legal basis for processing your data is your consent; your data is processed until you withdraw your consent.

VII. Entitled data processors

Based on contracts signed by the parties Data Controller transmits personal data elements to specific service providers who act as data processors in order to fulfill their contractual obligations.

Event organizers
Event organizers receive all personal data of customers along with the details of their purchases (date of purchase, type and number of purchased tickets, voucher identifiers) in order to ensure proper identification and validation of the tickets at the venue of the event. Also these data enables Event organizer’s Customer Support to look into and resolve any issues and reply to customer inquiries.

Payment gateway provider
During the online payment process initiated in the webshop Data Controller (merchant) transmits the following pieces of personal data to BIG FISH Payment Services Ltd. (seat: H-1066 Budapest, Nyugati tér 1-2.) as data processor: first name, last name, IP-address, billing address, country, phone number, e-mail address, the first six and the last four digits of the card number, the brand of the card. The purpose of the data transmission is to execute the necessary data communication between the merchant's and the payment service provider's system to conclude payment transactions and to ensure the traceability of the transactions for the merchant by storing the transmitted data in the data processor's transaction logs.

Payment service provider
Depending on the payment method chosen by the customer, Barion Payment Inc. (seat: H-1117 Budapest, Infopark sétány 1.) or OTP Mobile Ltd. (seat: H-1143 Budapest, Hungária körút 17-19.) as data processor receives the following pieces of personal data via

the payment gateway provider: data necessary for completion of bank transfer payment (such as name, email, phone number); purchase data (e.g. amount of purchase, detailed shopping cart content name). The purpose of the data transmission is to provide necessary data for concluding payment transactions and to ensure the traceability of the transactions for the merchant by storing the transmitted data in the data processor's transaction logs.

Invoicing service provider
KBOSS.hu Ltd. (seat: 2000 Szentendre, Táltos u. 22/B.), operator of számlázz.hu, as data processor receives billing data and receipt data necessary to create e-invoice and e-receipt for the customer. The scope of data elements required and thus transmitted is determined by the related law.

VIII. Special rules of processing related to the newsletter service

If you would like to receive news from the events organised by the Event Organizer, please grant your consent by checking the appropriate checkbox for receiving regular emails and for having your data processed. You can unsubscribe from the newsletter any time through a statement made in writing or by email, resulting in the withdrawal of your consent. In such cases we promptly erase all data of the person unsubscribing.

IX. Processing during entry

During the admission process at the venue of the event (that is when the wristband entitling for admission is associated with the person presenting the purchased ticket/voucher and the eligibility for admission is checked), the Event Organizer’s or Data Controller’s authorised agent may request that you identify yourself with a photo ID.

X. Data security

In respect to data processing for all purposes and legal basis, to ensure the security of personal data, Data Controller shall take all technical and organisational measures and has implemented such procedural rules as necessary for the enforcement of relevant legal provisions.

Data Controller shall apply appropriate measures to prevent accidental or unlawful destruction, loss, alteration, breach, unauthorised disclosure of, or access to, personal data.

Data Controller shall use a firewall and antivirus protection to protect the information technology system.

Data Controller shall classify and treat all personal data as confidential information. Data processed by Data Controller shall, as a rule of thumb, only be disclosed to those employees and agents of Data Controller that are engaged in implementing the data processing objectives specified in this Policy and whose contract of employment or contract of agency obliges them to confidentiality in respect to all data made known to them, in line with the legal regulations concerning their employment or by Data Controller's instructions.

Data Controller may use the data collected from data subjects for statistical purposes if such data is rendered anonymous – i.e., in such a manner that the data subject is not or no longer identifiable – in compliance with the governing legal provisions, and is entitled to publish and transfer such data to third parties.

Data Controller shall carry out electronic processing and maintain records via computer software that conforms to the requirements of data security. The software shall ensure that access to data is under purpose limitation and supervision, available only to those whose tasks necessitate such access.

In respect of automated personal data processing, Data Controller and processors shall implement additional measures designed to:

- prevent the unauthorized entry of data;
- prevent the use of automated data-processing systems by unauthorized persons using data transfer devices;
- ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data transfer devices;
- ensure that it is possible to verify and establish which personal data have been entered into automated data-processing systems and when and by whom the data were input;
- ensure that installed systems may, in case of malfunctions, be restored; and
- ensure that faults emerging in automated data-processing systems is reported.

For the purpose of protecting personal data, Data Controller shall ensure that incoming and outgoing electronic communication is monitored.

Data involved in ongoing projects and processing shall be available only to authorised employees and agents.

Data Controller shall ensure adequate physical protection of data and their relevant data carriers and documents.

Data Controller possesses adequate hardware and software tools and undertakes to implement technical and organisational measures ensuring the legality of processing and the protection of data subjects' rights

XI. Rules pertaining to processing

Data Controller (Data Controller as data processor or the authorised data processor) shall:

- warrant that he shall implement the technical and organisational measures ensuring compliance with relevant legal provisions, in particular in expertise, reliability and resources, including processing safety.
- ensure that in the course of Data Controller's activities, the persons authorised to access data subject's personal data, unless compelled to maintain confidentiality by law, shall undertake confidentiality obligations in respect to the personal data disclosed to them.
- possess adequate hardware and software tools and shall undertake to implement technical and organisational measures ensuring the legality of processing and the protection of data subjects' rights.

XII. Data Controller's rights and obligations

Taking into account the current state of science and technology and the costs of implementation, the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, Data Controller shall implement appropriate technical and organisational measures to ensure data security in line with the relevant levels of risk.

Data Controller shall take steps to ensure that any natural person acting under the authority of Data Controller who has access to personal data does not process them except on instructions from Data Controller, unless he or she is required to do so by Union or Member State law.

Data Controller shall ensure that stored data is accessible via the internal system or by direct access only to those duly authorised, and only in relation to the purpose of processing.

Data Controller shall ensure the necessary and regular maintenance and development of the equipment used. The device storing the data shall be kept in a closed room with adequate physical protections where Data Controller shall ensure physical protection thereof.

Data Controller is obliged to only engage persons with appropriate skills and expertise to carry out the tasks specified in the contract. Furthermore, Data Controller shall ensure that the persons thus engaged are trained in the applicable legal regulations on data security, the obligations described herein, and the purpose and method of data collection.

Data Controller undertakes to engage another processor only under the terms specified in the relevant legal regulations. Data Controller hereby grants general permission to Processor to engage other processors (subcontractors). Prior to engaging another processor, Processor shall duly notify Data Controller about the other processor's identity and the planned activities to be carried out by the other processor. In case Data Controller, based on the above information, raises objections against engaging the other processor, Processor shall only be entitled to engage the other processor if the requirements specified in the objection are met.

Where a processor engages another processor for carrying out specific processing activities on behalf of Data Controller, they shall conclude a contract in writing where the contract shall apply the same data protection obligations as set out in this contract concluded between Data Controller and the processor, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfill its data protection obligations, the initial processor shall remain fully liable to the Data Controller for the performance of that other processor's obligations.

XIII. Data Controller's rights and obligations in case of authorising a data processor

Data Controller shall conclude a written contract with Processor for the processing activities.

Data Controller is entitled to inspect that activities carried out by Processor conform to the terms of the contract.

Data Controller shall be held liable for the legitimacy of his instructions concerning the tasks specified in the contract; however, Processor shall promptly notify Data Controller if Data Controller's instructions or the implementation thereof is against the law.

Data Controller shall be held liable for informing the natural persons in question about the processing work under this contract, and to obtain their consent if so required by law.

XIV. Requesting information, your rights and options for legal remedy

In case of any questions or comments exceeding those contained in this Policy, Data Controller requests that you contact its Data Protection Officer at the following email address:
data.protection.officer@netpositive.hu

You may **request information** about the processing of your personal data anytime. Upon your request Data Controller shall provide detailed information concerning the data relating to you (data subject), including those processed by a data processor on its behalf, the sources from where they were obtained, the purpose, grounds and duration of processing, the name and address of the data processor and on its activities relating to data processing, and – in case of data transfer – the legal basis and the recipients.

Data Controller must comply with requests for information without any delay, and provide the information requested in an intelligible form, in writing at your request within not more than 30 days, emailed to the contact address listed by you, provided that such an email address was listed in the request. Failing that, the thirty-day time limit prescribed for Data Controller shall only be considered expired after you have provided your email address to Data Controller in a verifiable manner.

Furthermore, you may request the **rectification or erasure** of your personal data anytime – except data processing prescribed by law –, while Data Controller is entitled to refuse admission to the event concurrently with the erasure of such data.

Data Controller informs you that Data Controller is obliged to erase the data in the following cases:

- if data are unlawful;
- if requested by the client (data subject);
- if data are incomplete or inaccurate and lawful rectification is not possible;
- if the purpose of processing has ceased;
- if ordered by court or by the National Authority for Data Protection and Freedom of Information.

Instead of erasure, Data Controller may block personal data if so requested by the subject, or if it is assumed based on the available information that erasure is likely to violate the subject's lawful interests. Personal data thus blocked may only be processed for as long as the purpose for processing that prevented the erasure exists. However, Data Controller informs the client that in case of an erasure of data, Data Controller can no longer provide its services to the given client.

You may object to such processing of your personal data in accordance with the provisions of the applicable law. Data Controller shall review your objection – concurrently with suspending the processing – as soon as possible, but not later than within fifteen days of the objection and shall notify the client in writing at the contact address (postal address) listed by client, provided that such contact address had been listed in client's request. Failing that, the fifteen-day time limit prescribed for Data Controller shall only be considered expired after client has provided his address to Data Controller in a verifiable manner. In case the objection is justified, Data Controller shall cease data processing, including all further data recordings and transfers, and shall block the data, and notify all parties about the objection and the measures taken on that basis to whom such objected data had been transferred and who are obliged to act to enforce the right to object. If the client finds the decision made by Data Controller in response to the objection questionable, Client may bring action at a court within thirty days of having learned of the decision.

You may **seek ruling from a court** if your rights concerning the processing of your personal data have been violated. The case shall be given priority at the court. Action may be brought, as per your choice, at the court of Data Controller's registered seat or at the court of your (the data subject's) domicile (residence).

You have the right to transparent information, which we seek to provide with this Policy.