

**Budapestevent Company Ltd., as Data Management Organization
(briefly: Data Manager or Organization)**

Privacy Policy

In case of misunderstanding or trouble of interpretation, the original Hungarian version is the standard and has to be applied.

Application of the Data Protection and Privacy Policy

Information of Data Management Organization

Name of Data Manager	Budapestevent Co. Ltd.
Based:	Budapest, Koszta J. u. 26., 1124 Hungary
Tax number:	13777339-2-43
Company registration no.:	01-09-872629
Responsible for the content:	Tamás Koltai
Date of entry into force:	25. May 2018.

This policy sets out the adequacy of the protection of personal data and the privacy of personal data. The Data Controller performs personal contact with the person in charge of his / her personal contact and personal data handling. Customer has the right to disable data management. The provisions of this Code shall apply to the issuance of specific data management activities and instructions and information governing data management. The Data Protection Officer of the Organization does not apply. When handling personal data, the Data Controller adheres to the right to information self-determination in 2011 CXII. law. Given that data management is handled by the Data Handler as a customer relationship and business related, so data protection privacy registration is not required in 2011 CXII. (a) of Section 65 (3): - the data of the personnel, except financial organizations, member organizations, dormitory memberships or parent companies, public utility suppliers, customers of electronic communications service providers.

Scope of the regulation

This regulation is valid until the date of revocation, extending to the officials and employees of the Organization.

Purpose of the regulation

The purpose of these Rules is to harmonize, in respect of data management activities, the other internal rules of the Organization for the protection of the fundamental rights and freedoms of natural persons and to ensure the proper management of personal data. The Organization wishes to fully comply with the statutory requirements for the processing of personal data, in particular the provisions of Regulation (EU) No 2016/679 of the European Parliament and of the Council.

An important purpose of issuing the policy is also to enable the employees of the Organization to be able to legitimately handle the handling of natural persons by knowing and observing them.

Essential concepts, definitions

- GDPR (General Data Protection Regulation) is the new EU Privacy Policy

"data controller" means a natural or legal person, public authority, agency or any other body that determines the purposes and means of handling personal data individually or with others; where the purposes and means of data management are defined by Union or national law, the data controller or the particular aspects of the designation of the data controller may also be defined by Union or national law;

- Data Handling: means any operation or operation in any automated or non-automated way of personal data or data files, such as collecting, recording, rendering, compiling, storing, modifying or modifying, querying, inspecting, using, communicating, transmitting, distributing or otherwise disclosure, coordination or interconnection, restriction, deletion or destruction;

- data processor: a natural or legal person, a public authority, agency or any other body that manages personal data on behalf of the data controller;

- personal data: any information relating to an identified or identifiable natural person (s) concerned; a natural person may be identified, directly or indirectly, based on one or more factors relating to the physical, physiological, genetic, intellectual, economic, cultural or social identity of an identifier such as name, number, positioning data, online identifier or natural person identified;

- third party: a natural or legal person, a public authority, an agency or any other body other than the data subject, the data controller, the data processor or any person authorized to manage personal data under the direct control of the data controller or the data processor ;

- the consent of the person concerned: a voluntary, concrete and appropriate and informed and clear statement of the will of the person concerned, indicating his or her consent to the handling of personal data affecting him by means of a declaration of intent or a manifest error of expression;

- Restrictions on data management: the designation of stored personal data to limit their future management;

- pseudonymization: the handling of personal data in a way that, without the use of additional information, no longer identifies the specific natural person of the personal data provided that such additional information is stored separately and provided with technical and organizational measures, that this personal data can not be linked to identified or identifiable natural persons;

-"registration system" means the personal data in any way, centralized, decentralized or functional or geographic, accessible on the basis of defined criteria;

- privacy incident: a breach of security resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise handled;

Data Management Policy

The processing of personal data shall be carried out legally and fairly and in a manner transparent to the person concerned. Collecting personal data can only be done for a specific, clear and legitimate purpose. The purpose of personal data management is to be appropriate and relevant and only to the extent necessary.

Personal data must be accurate and up-to-date. Inaccurate personal data should be deleted immediately.

Personal data should be stored in a form that allows the identification of the data subjects for a limited time only. The storage of personal data for longer periods of time may only take place if the storage takes place for public interest archiving, for scientific and historical research purposes or for statistical purposes.

Personal data should be handled in such a way as to ensure adequate security of personal data, including the protection against unauthorized or unlawful handling, accidental loss, destruction, or damage to data by using appropriate technical or organizational measures.

The principles of data protection apply to all identified or identifiable natural person information.

The organization's data management employee has disciplinary, compensation, punitive and criminal liability for the lawful handling of personal data. If the employee becomes aware of the fact that the personal data he manages is defective, incomplete or timeless, he or she must correct it or rectify it by the employee responsible for recording the data.

Handling personal data

As natural persons can be associated with online identifiers such as IP addresses and cookie identifiers provided by the devices, applications, devices, and protocols they use, these data can be combined with other information and can be used to create a profile of natural persons, identify.

Data handling can only take place if the person concerned provides a voluntary, specific, informed and explicit consent to the processing of data by a clear reinforcement act, such as written, including electronically, or verbal declarations. This includes the personal data of Budapestevent Kft as a Data Management Organization registered on the web pages of the website and the personal data provided by e-mail to the given e-mail addresses, whereby the Customer (the person concerned) declares that, subject to the terms and conditions of use and this Data Handling Notice intention of establish a customer relationship with the Organization,

in which you consent to the personal data provided by Budapestevent Kft. In view of this availability, the Data Management Organization (Budapestevent Kft.) Treats the registered person as a customer, in compliance with the provisions regarding the customers in the processing of data.

Contribution to data management is also considered when the person concerned displays a check box when viewing the web site. Silence, the foreground check, or non-action are not considered as contributions.

A consent is also given to a user making technical adjustments to the use of electronic services or making a statement or act that clearly indicates the consent of the person concerned to the management of his / her personal data in that context.

Personal data should be handled in a way that ensures their level of security and confidentiality, including in order to prevent unauthorized access to or the unauthorized use of personal data and personal data management tools. All reasonable steps must be taken to correct or delete inaccurate personal data.

Data processing activity by Budapestevent Co. Ltd.

Nature and purpose of data processing: personal data necessary for the use of the services of Budapestevent Kft., Personal data necessary for business contacts, personal data required for issuing the invoice, personal data for the reception of the account and personal data of the prospective employees.

Category concerned:

- personal data provided on websites operated by Budapestevent Co. Ltd.
- personal data provided by e-mail received by Budapestevent Co. Ltd.

Managed data category: name, address, e-mail address, telephone number, tax ID, and employee registration TAJ number, birth data (place, date, mother's name).

The data management part-activity performed by Budapestevent Ltd. as a Data Controller covers the recording, storage and deletion of such personal data. Budapestevent Kft. As a Data Administrator treats the personal data provided by the person concerned no later than the withdrawal of the written consent of the person concerned or, in the case of administrative data handling, the processing of personal data will be subject to the scrapping of the document on which the treatment is based.

The person concerned may withdraw his consent at any time by sending an e-mail to the Data Manager info@budapestevent.hu e-mail.

Legality of data management

The handling of personal data is lawful if one of the following is true:

- the person concerned has consented to the processing of his / her personal data for one or more specific purposes;
- Data management is necessary for a business offer or for the performance of a contract or for the performance of a contract in which the party concerned is required to take action on one of the parties or prior to the conclusion of the contract;
- data processing is necessary to fulfill the legal obligation for the data controller;
- data processing is necessary for the protection of the vital interests of the concerned or another natural person;
- data management is necessary for the performance of a task in the public interest or in the exercise of a public authority exercised on the data controller;
- Data handling is necessary for the legitimate interests of the data controller or a third party, unless the interests or fundamental rights and freedoms of the data subject that require the protection of personal data, especially if the child concerned, are the priority of those interests.

According to the above, data management is considered legitimate if it is required in the context of a contract or a willingness to conclude a contract or a bid.

If the data is handled in the context of the fulfillment of a legal obligation for the data controller or if it is necessary for the execution of a public interest task or for the exercise of a public authority, data management must have legal basis in Union law or in the law of a Member State.

Data management shall be considered legitimate when it is protected in the interests of the person concerned or of any other natural person mentioned above. By reference to the vital interests of a natural person with regard to personal data management, it may in principle only be possible if the data processing in question can not be performed on other legal grounds.

Some types of personal data management may serve at the same time important public interest and the vital interests of the person concerned, for example, when data management for humanitarian reasons, including when it comes to monitoring epidemics and spreads or humanitarian emergencies, especially natural or man-made disasters need.

The data controller, including the data controller with which he or she may share personal data, or a legitimate interest of a third party, may provide a legal basis for data handling. Such a legitimate interest may arise, for example, when there is a relevant and adequate link between the data subject and the data controller, for example in cases where the data subject is in the client's or his application.

The essential handling of personal data to prevent fraud is also a legitimate interest of the data controller concerned. Handling personal data for direct business purposes can also be considered as a legitimate interest.

In order to establish the existence of a legitimate interest, consideration must be given, inter alia, to whether the data subject can reasonably expect to be able to handle data for the purpose at the time of collection of personal data and in the context of the collection of personal data. The interests and fundamental rights of the data subject may take precedence over the data controller's interest if the personal

data are handled under circumstances in which the data subjects do not count for further data handling.

The legitimate interests of the data controller concerned are those of public authorities, computer emergency response units, network security incident units, providers of electronic communications networks and services, and personal data management implemented by security service providers, which is absolutely necessary and proportionate to guarantee network and IT security.

The handling of personal data for purposes other than the original purpose of collecting it is permitted only if the data processing is compatible with the original purpose of data handling for which the personal data was originally collected. In this case, there is no need for a separate legal basis other than the legal one that allowed the collection of personal data.

The handling of personal data by officially recognized religious organizations by the authorities in the context of constitutional or international public law is considered to be in the public interest.

Contribution and conditions of the person concerned

- If the data management is based on a contribution, the data controller must be able to demonstrate that he / she has consented to managing the personal data of the person concerned.
- If the party concerned gives its consent in the form of a written statement that also applies to other matters, the request for consent must be communicated in a clearly distinct manner from these other cases.
- You have the right to withdraw your consent at any time. Revocation of the contribution does not affect the lawfulness of the consent based on consent, prior to the withdrawal. Before consent is given, the person concerned shall be informed thereof. The withdrawal of the consent must be allowed in the same simple way as the granting of the consent.
- In determining whether a contribution is voluntary, account shall be taken, to the greatest extent possible, of the fact that the contribution to the management of the contract, including the provision of services, is conditional on the contribution to the management of personal data that are not required for performance of the contract.
- The handling of personal data provided directly to children for information society services is lawful if the child is 16 years of age. In the case of a child who is not 16 years of age, the treatment of the child's personal data is legitimate only if the consent has been granted or authorized by the parent control over the child.

Decisions on the determination of criminal liability and the processing of personal data relating to criminal offenses and related security measures may only take place in the case of data processing by the public authority.

Unspecified data management

If the purposes from which the data controller handles personal data does not require the data controller to be identified by the data controller, the data controller is not required to retain additional information.

If the data controller can prove that he or she is not in a position to identify the data subject, he / she shall, if possible, inform him accordingly.

Information and rights of the person concerned

The principle of fair and transparent data management requires that the information concerned be informed of the fact and purpose of the data handling.

Information related to the management of personal data relating to the data subject should be provided to the data subject at the time of the data collection, or if the data are collected from other sources but not from the data subject, must be provided within a reasonable time taking into account the circumstances of the case.

The data subject has the right to have access to the data collected for it and to exercise that right in a simple and reasonable manner in order to establish and verify the lawfulness of data processing. Everyone concerned should have the right to know, in particular, the purposes for which personal data are to be handled and, if possible, about the duration of personal data management,

In particular, the data subject is entitled to erase his personal data and to no longer handle it when personal data is collected or otherwise handled in connection with the original purposes of the data management or if the data subjects have withdrawn their consent to the processing of the data.

You can exercise your rights in the following contact details:

Post address: Budapestevent Kft. 1015 Budapest, Széna tér 7.

E-mail: info@budapestevent.hu

If personal data is handled for direct business, the data subject must be entitled to protest free of charge at any time against the handling of personal data relating to it.

Review personal information

Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, az adatkezelő törlési vagy rendszeres felülvizsgálati határidőket állapít meg. Regular review period established by the Head of Organization: 1 year.

Tasks of the data controller

The data controller uses appropriate internal data protection rules for legitimate data management. This regulation covers the powers and responsibilities of the controller.

The Data Controller is obliged to take appropriate and effective measures and to be able to demonstrate that the data management activities are in compliance with the applicable legislation.

This regulation shall be taken in the light of the nature, scope, circumstances and objectives of data handling and the risks to the rights and freedoms of natural persons.

The data controller shall take appropriate technical and organizational measures, taking into account the nature, scope, circumstances and purposes of data handling and the risk of varying probabilities and seriousness reported to the rights and freedoms of natural persons. On the basis of these rules, the other internal policies are reviewed and, if necessary, updated.

The data controller shall keep a proper record of the data management activities performed by his / her competence. Each data controller and data processor shall cooperate with the supervisory authority and make such records available upon request to verify the data handling operations concerned.

Rights related to data management

The right to request information

Any person may, through the specified contact information, request information about the Organization's data, what legal basis, what kind of data management purpose, how long and how long it handles it. Upon request, information must be sent promptly, but not later than within 30 days.

Right to rectification

Any person can request the modification of any of the specified contact information. Upon request, you must take action without delay, but within 30 days, and provide information on the provided contact details.

The right to cancel

Any person can request the cancellation of their data through the specified contact information. At your request this must be done promptly, but within 30 days, and information must be sent to the given contact details.

The right to block or restrict

Any person can ask for your data to be locked through the specified contacts.

Locking takes place until the indicated reason makes it necessary to store the data. The request must be made promptly, but not later than 30 days, and information must be sent to the given contact details.

Right to protest

Any person may object to data handling through the specified contact details. The protest must be examined within the shortest possible time, but not later than 15 days, on the grounds of its validity, and information on the decision must be sent to the given contact details.

Enforcement of data management

National Privacy and Freedom Authority

Postal address: 1530 Budapest, Pf.: 5.

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22 / c

Phone: +36 (1) 391-1400, Fax: +36 (1) 391-1410

E-mail: service@naih.hu

URL <https://naih.hu>

Coordinates: 47 ° 30'56 "N; 18 ° 59'57 "E

In case of violation of the rights of the data subject, the data controller can turn to the court against the data controller. The court proceeds out of court. The lawsuit may be initiated by the person concerned, according to his choice, before the competent court of domicile or residence.

Data Security

Data shall be protected against any unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as any unintentional destruction or damage resulting from a change in the technique used.

In order to protect electronically managed files in the registers, an appropriate technical solution should ensure that the data stored in the records can not be directly linked and assigned to the data subject.

When designing and applying data security, consideration must be given to the current state of the art. There are several possible data management solutions to choose from, providing for a higher level of protection of personal data, unless disproportionate to the data controller.

Privacy incident

The data protection incident shall be notified to the competent supervisory authority without undue delay within 72 hours at the latest unless it can be demonstrated in accordance with the principle of accountability that the privacy incident is unlikely to pose a risk to the rights and freedoms of natural persons.

The person concerned shall be informed without delay if the data protection incident is likely to have a high risk to the rights and freedoms of the natural person in order to take the necessary precautionary measures.

Management and registration data management

The Organization may treat personal data in cases of its activity or for administrative and registration purposes. Data management is based on a voluntary and explicit consent based on the relevant information of the person concerned. The detailed information, covering the purpose, legal basis and duration of the data processing and the rights of the person concerned, shall be notified to the person concerned of the voluntary nature of the data handling. Contribution to data processing must be recorded in writing (either electronically).

Data management for administrative and accounting purposes serves the following purposes:

- data management of members and employees of the Organization, which is based on statutory obligations;
- the data processing of persons in the mandate of the Organization for contact, settlement and registration purposes;
- contact details of other organizations, institutions and businesses in business relationship with the Organization, which may be the contact and identification data of natural persons;

Data processing on the one hand is based on a statutory obligation on the one hand and, on the other hand, the person expressly contributed to the processing of his / her data (eg for work contract or as a partner on the website, etc.)

The consent of the person concerned must be presumed in the case of documents (including CVs, job-search applications, other submissions, etc.) which have been submitted in writing to the Organization, including personal data. After expiration, the documents must be destroyed on the basis of the written notice of the person concerned.

In the case of administrative data management, personal data are included only in the records of the case and in the records. The treatment of these data will last until the document underlying the treatment is disposed of.


Data management for administrative and accounting purposes - to ensure that personal data is stored for the duration required - to be reviewed annually, inaccurate personal data should be deleted immediately.

In the case of data management for the purposes of administrative and registration purposes, compliance with the law must also be ensured.

Legislation underlying data management

- 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 Regulation (EC) No 95/46 / General Data Protection Regulation).
- 2011 CXII. law on information self-determination and freedom of information.
- Act LXVI of 1995 on Public Works, Public Archives and the Protection of Private Archives Material. law.
- Decree 335/2005 on the General Requirements for Document Management of Public Servants (XII.29.) Government decree.
- CVIII of 2001. Act on Electronic Commerce Services and Information Society Services Issues.
- Act C of 2003 on electronic communications.

Date: 18. May 2018.


.....
Head of Organization

BUDAPESTEVENT RSZ. KFT.
H-1124 Budapest, Kosztka J. u. 26.
Tel.: +36 1 980 9960 Fax: +36 1 202 0010
Adószám: 15777339-2-43
AXA Bank Rt. 77000019-11636391