

PRIVACY NOTICE OF BO DMC

Last updated: 01.09.2019

Bo Event Kft. (registered seat: Dayka Gábor utca 3., 1118 Budapest, Hungary, registration No.: 01-09-873966, hereinafter referred to as “Bo Event” or “Controller”) describes in this informative document its practices concerning the collection, use and disclosure of personal data. This Privacy Notice (“Notice”) is intended to provide information on the data that Bo Event collects and analyses about the users of its services and the persons whose personal data becomes known to it during the course of its business. It also provides information on how these data are used, disclosed to third parties or otherwise processed and how the data subjects’ rights are being protected under the data protection guidelines.

I. DEFINITIONS

Dataset: all data in a set physically treated as a single unit;

Technical processing: performing technical tasks, whether automated or non-automated, in connection with the processing operations on personal data, irrespective of the method and means used to perform the operations and of the place of application, provided that the technical task is carried out on the data. Technical processing may include, for example, activities outsourced to an external company (e.g. payroll accounting);

Processor: a natural or legal person, an entity without legal personality, a public authority or any other body processing personal data on behalf of the Controller under a contract with the Controller. Processors may include, for example, couriers in the course of delivering mail or parcels as part of their services;

Processing: any operation or set of operations performed on personal data, irrespective of the procedure used, including, in particular, collection, recording, organisation, structuring, storage, alteration, use, retrieval, transfer, disclosure, alignment or combination, blocking, erasure and destruction, prevention of further use, photo, audio or video recordings and the recording of any physical characteristics suitable for the identification of a person;

Controller: a natural or legal person, an entity without legal personality, a public authority or any 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 Controller or the specific criteria for its nomination may be provided for by Union or Member State law. Bo Event, for example, is deemed to be a Controller with respect to the processing set forth in this Notice;

Data marking: assigning identification marks to the data for distinction purposes;

Data destruction: complete physical destruction of the data medium containing the data, making the data permanently unidentifiable and unrecoverable;

Data storage: preservation of the data permanently or for a limited period of time;

Data transfer: for the purposes of this Notice, providing access to the data for a designated third party;

Data erasure: making the data unrecognizable in such a way that its restoration is no longer possible in any form;

Data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transferred, stored or otherwise processed;

Pseudonymisation: 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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Data subject: a natural person identified or identifiable on the basis of any information. From the data protection perspective, any natural person about whom personal data is held shall be deemed to be a data subject. Such data may include, for example, contact details held with the purpose of maintaining a contractual relationship;

Third party: a natural or legal person or an organization without legal personality other than the data subject, the Controller or the Processors;

Third country: any state other than a member state of the European Economic Area (EEA);

Consent: 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; A consent can also be given in electronic form by, for example, signing up to a newsletter online or by conduct (e.g. sending a message to an email address linked to Bo Event);

Websites: web content accessible through online channels created and maintained by Bo Event with the aim to promote its business interests, such as the <http://bolive.hu> website;

Disclosure: making the data accessible to anyone;

Profiling: 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;

Personal identifying information: any or all of a person's surname, given name, maiden name, sex, place and date of birth, mother's maiden surname and given name, information identifying the person's place of residence or stay or other institutional identification information (e.g. social security number) that is or might be suitable for the identification of the data subject;

Personal data: any information relating to an identified or identifiable natural person, i.e. the 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. Personal data may include any information related to the data subject - in particular, the name of the data subject, any data recorded by an institution and suitable for the personal identification of the data subject as well as any knowledge related to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of the data subject and any conclusion that can be drawn from the data related to the data subject;

Objection: the data subject's statement whereby he or she objects to the processing of his or her personal data and demands the discontinuation of processing or the erasure of the personal data processed.

II. LEGISLATIVE BACKGROUND

The guidelines laid down in this document about personal data processing have been drafted by taking into account law provisions including but not limited to the following:

- 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 (GDPR)
- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (Privacy Act)
- Act V of 2013 on the Civil Code (Civil Code)
- Act CVIII of 2001 on certain aspects of electronic commerce services and information society services (E-commerce Act)

III. DATA PROCESSING PRINCIPLES

The personal data processed by the Controller and the Processors are adequate, relevant and limited in scope and duration to what is necessary in relation to the data processing purposes defined by the Controller. The personal data are processed by the Controller and the Processors with the greatest possible security and in a confidential manner, in accordance with the data processing guidelines set forth herein. Bo Event undertakes to carry out the necessary technical improvements and update these data processing guidelines and the related provisions if this becomes necessary due to changes in the legal or technical conditions.

Bo Event undertakes to comply with the following principles of the GDPR (Article 5) in the course of processing personal data:

lawfulness, fairness and transparency: personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;

purpose limitation: personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

data minimization: personal data shall be adequate, relevant and limited only to what is necessary in relation to the purposes for which they are processed;

accuracy: personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

storage limitation: personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

integrity and confidentiality: personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

Bo Event shall be responsible for complying, and be able to demonstrate compliance, with the above principles. If the Data Supplier provides data other than his or her own personal data, the Data Supplier shall be responsible for obtaining the data subject's consent and shall be liable for any damage resulting from its failure to do so.

IV. DATA AND CONTACT DETAILS OF THE CONTROLLER

Controller:

- **Bo Event Kft.**
Registered seat: Dayka Gábor utca 3., 1118 Budapest, Hungary
Registration No.: 01-09-873966
Tax No.: 13801894-2-43
Represented by Zsófia DOBOS (independently)

Data Protection Officer appointed by the Controller:

- **Name:** András CSÍKY
- **Contact details:** welcome@bodmc.hu

Processor:

- **Digitalwave Hungary Kft.**
(as the hosting service provider and website developer for the bolive.hu website)
Address: Pillangó park 9., 1149 Budapest, Hungary
Tax No.: 12832332-2-42
Email: hello@digitalwave.hu

Other service provider

- **Rackforest Kft. (Victor Hugo utca 18-22., 1132 Budapest, Hungary) – server provider (does not have access to personal data and is not deemed to be a processor!)**

V. DATA PROCESSING OPERATIONS

General provisions

The data processing operations by Bo Event are based on the legal bases set forth in the GDPR, especially including the following:

- consent freely given by the data subject
- performance of a contract
- legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

Legal basis: if data processing is based on a consent freely given by the data subject, the data subject shall have the right to withdraw his or her consent at any time.

Inability to perform a contract: in case the basis of processing is the performance of a contract and the data subject fails to supply his or her personal data, indispensable for the performance of the contract, Bo Event will not be able to enter into the contract or to provide services. Bo Event will not accept liability or shall not be held responsible for any damage that may result from such inability.

However, Bo Event may require the party demonstrably at fault to pay compensation for any damages or expenses incurred as a result of Bo Event's failure to perform due to such inability.

Source of the data: Bo Event mainly processes personal data originating directly from the data subjects. If, in the course of data processing, the data come from a source other than the data subject, such fact will be indicated on a case-by-case basis in connection with processing.

Persons with right of access: on the part of Bo Event, the personal data may become known to authorized employees only to whom such right is granted in the internal rules or the authorization rules for electronic databases.

Processors: if Bo Event uses the services of a Processor for any of its processing activities, this will be indicated in connection with the particular processing activity.

Data security: In addition to these data protection guidelines, the internal IT rules of the Controllers may also contain provisions on data security.

VI. FORMS OF DATA PROCESSING

1. PROCESSING FOR MARKETING PURPOSES

1. Email newsletter

Purpose of processing: Sending information on our products and services.
Legal basis for processing: Consent. [Article 6 (1) a) of the GDPR]
Data processed: Name, email address
Data subjects: Newsletter subscribers.
Duration of processing: Until such time as the data subject withdraws his or her consent.

2. CONTACT/COMMUNICATION

2.1. Making contact on the data subject's initiative via email

Purpose of processing: Communication with the data subject for the purpose initiated by him or her.
Legal basis for processing: Consent. [Article 6 (1) a) of the GDPR]
Data processed: Name, email address, phone number or any other detail shared by the data subject as well as the content of his or her request.
Data subjects: Persons sending the emails.
Duration of processing: Until such time as the data subject withdraws his or her consent.

2.2. Making contact on the Controller's initiative

Description: Any contact made for a purpose other than marketing or the fulfilment of a service via any - primarily online - communication channel (e.g. notification that the email storage capacity is full).
Purpose of processing: Contact and communication with the data subject.
Legal basis for processing: Legitimate interests of Bo Event. [Article 6 (1) f) of the GDPR]

Data processed:	Name, email address, phone number, other identification details for communication via electronic channels (e.g. Skype).
Data subjects:	The persons contacted.
Duration of processing:	Until the purpose is fulfilled.

2.3. Name cards, other data carriers or data files containing personal data

Description:	Name cards, other documents or data files containing personal data, becoming available to Bo Event during the establishment or maintenance of business contacts (e.g. contact files transferred between mobile devices).
Purpose of processing:	Contact building and maintenance.
Legal basis for processing:	Consent. [Article 6 (1) a) of the GDPR]
Data processed:	Name, email, phone number or any other personal data stored on a data carrier or data file received by Bo Event from the data subject.
Data subjects:	Persons whom the personal data belong to or who share such data with Bo Event.
Duration of processing:	Until such time as the data subject withdraws his or her consent.

2.4. Delivery of postal mail

Description:	Delivery of mail originating from Bo Event and tracking it up to the destination.
Purpose of processing:	Communication.
Legal basis for processing:	Legitimate interests of Bo Event and/or the data subject. [Article 6 (1) f) of the GDPR]
Data processed:	Name, email address, phone number or any other personal data qualified as essential information by the company in charge of delivery.
Data subjects:	Mail recipients.
Duration of processing:	Until the purpose is fulfilled.

2.5. Calls for bid by or to Bo Event

Description:	Calls for bids sent or received through electronic or other communication channels.
Purpose of processing:	Communication to establish future business relationships.
Legal basis for processing:	Legitimate interests of Bo Event. [Article 6 (1) f) of the GDPR]
Data processed:	Name, title, email address, phone number or any other personal data becoming available to Bo Event through the bidder or the contracting party or from a public or purchased database as well as the content of the call for bid.
Data subjects:	Contact persons of the bidder or the contracting party.
Duration of processing:	Period of validity of the call for bids / bids received but not longer than 1 year.

3. DATA PROCESSING DURING THE EXISTENCE OF A CONTRACTUAL RELATIONSHIP

3.1. Communication with clients

Description:	Communication and information supply in order that Bo Event can fulfil its services.
Purpose of processing:	Communication with the data subjects.
Legal basis for processing:	Legitimate interests of Bo Event and the client concerned. [Article 6 (1) f) of the GDPR]
Data processed:	Name, email address, phone number, other identification details for communication via electronic channels (e.g. Skype).
Data subjects:	Persons communicating on behalf of the clients.
Duration of processing:	Until the person concerned ceases to be a contact person or upon termination of the business relationship with the client represented by the contact person or until the end of the limitation period of the documents prepared for the business relationship and containing personal data of the data subject.

3.2. Invoicing

Description:	Data processing related to the invoicing of business transactions.
Purpose of processing:	Invoice sending.
Legal basis for processing:	Legitimate interests of Bo Event and the client concerned. [Article 6 (1) f) of the GDPR]
Data processed:	Name, email for invoice sending through electronic channels.
Data subjects:	Persons communicating on behalf of the clients with regard to invoicing.
Duration of processing:	Such period as specified in Para (2), Article 169 of the Accounting Act (8 years) and an additional 2 years for tax audit purposes.

3.3. Enforcement of rights

Description:	Data processing to enforce rights related to business transactions.
Purpose of processing:	E.g. sending demands for payment, initiating administrative or judicial proceedings.
Legal basis for processing:	Legitimate interests of Bo Event. [Article 6 (1) f) of the GDPR]
Data processed:	Name, title, email.
Data subjects:	Contact persons of clients in contractual relationship.
Duration of processing:	Until expiry of the limitation period specified in the Civil Code.

4. DATA PROCESSING RELATED TO HUMAN RESOURCES MANAGEMENT

4.1. Applications for vacancies

Description:	Processing of data related to job ads posted by Bo Event or obtained from a headhunter partner or published on a job portal.
Purpose of processing:	Selection of persons for particular positions and coordination of the process.
Legal basis for processing:	Consent. [Article 6 (1) a) of the GDPR]

Data processed:	Name, phone number, email and any other personal data shared by the applicant/selected person with Bo Event.
Data subjects:	Persons applying for the position, persons selected.
Duration of processing:	Until the process of selecting the right person for the position is closed but no longer than 1 year.

4.2. Employed persons

Description:	Personal data shared by Bo Event employees with the employer.
Purpose of processing:	Data processing as an essential element of creating an employment relationship.
Legal basis for processing:	Consent. [Article 6 (1) a) of the GDPR]
Data processed:	Name, date of birth, mother's name, address, phone number, email, social security ID (TAJ), tax ID, bank account number.
Data subjects:	Bo Event employees.
Duration of processing:	During the term of the employment relationship and for such time thereafter as specified in law regarding the retention period of employment-related documents.

5. ONLINE DATA COLLECTION

Description:	Personal and other data collected through any online channel or becoming known to Bo Event about the user in connection with online activities.
Purpose of processing:	As specified on the particular online platform.
Legal basis for processing:	Consent. [Article 6 (1) a) of the GDPR]
Data processed:	As specified on the particular online platform.
Data subjects:	Persons using the online platform.
Duration of processing:	As specified on the particular online platform.

Other data processing

For any other data processing not listed above, Bo Event will provide information in each case at the time of data recording and there may also be cases of occasional data processing by Bo Event where project- or event-specific guidelines will apply to data processing (e.g. online promotional sweepstakes).

VII. PERSONAL DATA FLOW

In general: based on interactions with the data subjects - where personal data were recorded - the data can be disclosed to third parties (e.g. courier services, banks, etc.) involved in performance so that the purpose of recording is fulfilled. Moreover, Bo Event as member of the Multeam360

Communication Group may share the data it processes in order to pursue its common business interests. However, such sharing shall include, as an integral part, the sharing of any other ancillary information related to the shared data which has enabled, and will in the future enable, the lawful recording, storage and use of the personal data. In addition, the data may be shared for the purpose of meeting legal requirements, enforcing rights and complying with agreements.

Transfer of data to comply with legal and other obligations

Personal data processed by the Controller regarding data subjects may be transferred for the following purposes:

- enforcing, or complying with, laws, instructions issued by public authorities or binding regulations,
- detection and prevention of security threats, fraud or other crime,
- enforcing the rights and/or protecting the property of the Controller or a third party and
- protecting the rights and personal safety of the employees of Bo Event and of third parties.

Data transfer to third parties

Bo Event uses the services of third parties to provide certain services. Such third parties may include, but are not limited to, mail delivery providers (Magyar Posta, courier services, etc.) or any other partner whose services are essential for Bo Event to meet its obligations.

The personal data collected and processed about the data subjects may be used and transferred by such service providers solely for the purpose of fulfilling the orders given by Bo Event.

In the event of an official audit (e.g. by the tax authority NAV), the data and documents that may contain personal data about the data subjects shall be made available to the particular authorities at their request. In other cases of right enforcement for economic purposes (e.g. demands for payment), Bo Event may transfer the required personal data processed by it to the authorised legal representative or other parties substantially involved in the proceedings.

Protection of rights

When there is reasonable cause to believe that the rights and assets of the Controller, suppliers, clients or a third party have or might have been violated, the personal data of the data subject may be used or transferred to protect such rights and/or assets.

Moreover, Bo Event reserves the right to disclose the personal data of the data subject if required by law or by orders of competent authorities or for the purpose of complying with the law and protecting the rights set forth herein.

VIII. RIGHTS OF THE DATA SUBJECTS

The data subject may request information on the processing of his or her personal data and may request the rectification of such personal data or erasure or blocking thereof unless data processing

was ordered by law. The data subject may also request restriction of processing and may object to processing. The data subject shall have the right to receive the personal data which he or she has provided, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from the Controller to which the personal data have been provided.

The data subject and those to whom the data have previously been transmitted for processing purposes shall be notified of any rectification, blocking, marking and erasure of the data. Notification may be omitted if this does not violate the legitimate interest of the data subject with respect to the purpose of processing.

If the Controller does not satisfy the data subject's request to rectify, block or erase the data, it shall advise the data subject in writing within 30 days of receipt of the request on the factual and legal causes of rejecting the request for rectification, blocking or erasure. In the event of rejection of the request for rectification, erasure or blocking, the Controller shall inform the data subject of his or her right to seek judicial redress or apply to the Authority.

Right of information/access

At the data subject's request, the Controller shall provide information on the data subject's personal data processed by the Controller or by the Processor on behalf of the Controller, the source of such data, the purpose, legal basis and duration of processing, the name, address and processing-related activities of the Processor as well as the legal basis and recipient of the data transfer in case of transfer of the data subject's personal data. The Controller shall provide the information in plain language in writing as soon as possible but not later than within 30 days of the date of submission of the data subject's request.

The information shall be provided free of charge if the person requesting the information has not yet submitted a request for information to the Controller in the current year for the same scope of data. In other cases, costs may be charged. The amount of the costs can be specified in the parties' contract. The costs already paid shall be refunded if the data have been processed unlawfully or the request for information has resulted in rectification due to an omission by Bo Event.

In the event of a refusal to provide information, the Controller shall inform the data subject in writing of the provision constituting the basis of refusal to provide information. In the event of a refusal to provide information, the Controller shall inform the data subject of his or her right to seek judicial redress or apply to the Nemzeti Adatvédelmi és Információszabadság Hatóság (National Authority for Data Protection and Freedom of Information) ("the Authority").

Right of rectification

If the personal data are incorrect and the correct personal data are available to the Controller, the personal data shall be corrected by the Controller.

Right of erasure/right to be forgotten

Personal data shall be erased if

- processing is unlawful;

- the data subject requests so;
- the data are incomplete or erroneous - and this situation cannot be lawfully remedied -, provided the erasure is not excluded by law;
- the purpose of processing has ceased or the statutory term for storing the data has expired;
- ordered by court or the Authority.

The Controller may not erase the data of the data subject if processing has been ordered by law. However, the data may not be transferred to the recipient if the Controller has agreed with the objection or the court has found the objection well-founded.

Right to restrict/block processing

Instead of erasure, the Controller shall block the personal data if so requested by the data subject or if it can be assumed from the information available that the erasure would affect the legitimate interests of the data subject. The personal data so blocked can only be processed while the purpose of processing excluding erasure exists.

The Controller shall mark the personal data processed by it if the data subject challenges the accuracy or correctness thereof but the inaccuracy or incorrectness of the personal data cannot be clearly ascertained.

Right to object

The data subject may object to the processing of his or her personal data

- if processing or transfer of the personal data is necessary for compliance with a legal obligation to which the Controller is subject or for the purposes of the legitimate interests pursued by the Controller, the recipient or a third party, except where processing is mandatory;
- if the personal data are used or transferred for the purposes of direct marketing, opinion poll or scientific research; and
- in other cases provided by law.

The Controller shall investigate the objection within the shortest possible time but not later than within 15 days, adopt a decision as to whether it is well-founded or not and notify the requester in writing of its decision.

If, according to the findings of the Controller, the data subject's objection is well-founded, the Controller shall terminate all processing operations - including data collection and transfer -, block the data involved and notify all recipients to whom any of these data had previously been transferred concerning the objection and the ensuing measures, upon which these recipients shall also take measures regarding the enforcement of the objection.

If the data subject disagrees with the decision taken by the Controller or if the Controller fails to meet the deadline, the data subject shall have the right to go to court within 30 days of the date of communication of the decision or of the last day of the deadline.

Compensation for damages

The Controller shall compensate for any damage caused to others by unlawful processing of the data of the data subject or failure to meet the data security requirements. The Controller shall also be liable to the data subject for any damage caused by the Processor. The Controller shall not be liable if it proves that the damage was caused by an unavoidable cause outside the scope of processing.

Remedies

Applications for redress or complaints can be lodged to the Nemzeti Adatvédelmi és Információszabadság Hatóság (National Authority for Data Protection and Freedom of Information):

Nemzeti Adatvédelmi és Információszabadság Hatóság

Address: Szilágyi Erzsébet fasor 22/c, 1125 Budapest, Hungary

Postal address: 1530 Budapest, Pf.: 5.

Phone: +36 (1) 391-1400

Email: ugyfelszolgalat@naih.hu

<http://naih.hu>

IX. DATA SECURITY

The IT and other resources used for data processing shall be chosen and operated by the Controller in such a manner as to ensure that the data processed:

- are available to the persons authorized to access such data (availability);
- can be authenticated and verified (authenticity);
- can be verified to be unchanged (integrity);
- are protected against unauthorized access (confidentiality).

The Controller shall guarantee the security of processing by technical and organizational measures that offer an appropriate level of protection against the risks associated with processing.

In carrying out its data protection activities, the Controller shall maintain

- confidentiality by protecting the information so that it can only be accessed by those authorized to do so;
- integrity by protecting the accuracy and completeness of the information and the processing method;
- availability by ensuring that authorized users can actually access the required information when they need it and that the resources required to do so are available.

The data may be accessed on a need-to-know basis by persons employed or otherwise contracted by the Controller who are authorized by the Controller to access such data and

- who are appointed to certain positions of the Controller/Processor or the Auditor;
- who have received appropriate instructions to that effect;
- who are also bound by confidentiality obligations.

Persons who have been granted access to the personal data of the data subject may only access such data for the purpose of carrying out their duties in relation to that data. Such persons shall be properly trained in advance so that they can prevent the loss, destruction, unauthorized use or unauthorized access to the data to the maximum extent practicable.

In addition to the above, the data may be accessed by third parties who perform certain ancillary activities on behalf of the Controller, including

- service companies (e.g. IT service providers providing cloud services or hardware to the Controller for the performance of its activities, etc.)
- public bodies or authorities, supervisory and controlling bodies to which the Controller submits reports and documents or, more generally, public officials or individuals filling public administration or public service positions;
- external consultants giving legal assistance and advice for the resolution of disputes;

The above organizations or their representatives shall carry out their duties as external data management consultants or auditors under the direction and supervision of the Controller.

Recording, correction, storage and protection of the data

- The data obtained from the data subject and required for processing shall be recorded. Any data storage device, method or technique ensuring the protection of the data and preventing access of unauthorized persons to protected data will be suitable for this purpose.
- Any erroneous data in the recorded documentation shall be corrected or erased in such a manner as the original (erroneous) data can be identified.

Protection of the data processing system environment

- The security of the Data Protection Officer designated by the Controllers shall ensure the security of the physical placement and storage of the media images and documentation.
- The designated data protection officer shall also be responsible for the security of the data processing system environment within each department with due regard to the special local circumstances, including the prevention of data breaches in agreement with the IT specialists of Bo Event.

Both the IT system and network of the Controller are protected against computer-assisted fraud, espionage, sabotage, vandalism, fire and floods as well as computer viruses, hacking and denial of

service attacks. The operator maintains security through server-level and application-level security procedures.

The Controller applies the following specific IT and physical measures to ensure security of the data:

- The servers used by the Controller for data processing are located in closed, secured, logged server rooms.
- The interfaces through which personal data can be accessed are accessible only with personal user identification.
- The IT devices are protected by firewalls.
- Data backups are made to separate devices which are also accessible with user identification.

In addition to the typical IT measures listed above, the following measures have been taken for data security:

- ensuring data confidentiality through internal policies and instructions: employees are required to use the data obtained solely for the purpose of processing and to the extent necessary in such a manner as to prevent that persons who do not need to process the data for their jobs may not get to know the data; the persons authorized to use the data processing system can access only the personal data specified in the access authorization;
- during the transmission of data or transportation of the data media, it is ensured that they cannot be accessed, copied, modified or erased without authorization,
- personal data are transferred on a proper legal basis only;
- personal data are processed no longer than necessary;
- in the event of a breakdown, the data processing system can be restored and it will be possible to restore the data files (backup), protect against viruses and physically protect the storage media;
- internal regulations are being put in place to maintain data security (e.g. regulations for internet use and the use of IT devices, antivirus policy, information security policy, etc.);
- IT compliance levels are regularly reviewed and improved if necessary;
- an internal regulation is being put in place to address data breaches and all necessary measures are available to avoid them.

X. MISCELLANEOUS

Bo Event reserves the right to unilaterally update the data processing guidelines specified in this document. The date of the latest update is shown in the "Last updated" section at the beginning of this document.