BRENUM LTD

# PRIVACY POLICY

**1. Introduction**

This privacy policy (hereinafter: the Policy) governs the method and extent of recommended procedures for collecting, processing and storing personal information by BRENUM Ltd, Mlini HR-20207, Makoše 29, Croatia, PIN 17768963437, (hereinafter: the Company). This Policy defines guidelines that aim to comply, to the extent possible with regard to the circumstances of each particular case, with the 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 (General Data Protection Regulation).

The purpose of this Policy is to define standards for management personnel, employees and other associates during their employment and professional activity in the Company regarding the handling of personal data. The ultimate objective is to minimize the risk associated with any potential non-compliance with the applicable regulations, which depends on a prompt and adequate response by the employees in each individual case.

Concerning this matter, employees are invited to refrain from and cease any activity, and immediately contact the competent data protection officer for further guidance and instructions in case any provisions of this Policy are not fully understood or should any ambiguity regarding its implementation or any other uncertainty in conjunction with any current and future collection, processing and storage of personal data arise.

Personal data protection is one of the fundamental human rights. The Company is fully aware that reliable and safe processing of personal data of its guests, employees and other natural persons whose personal information it collects and processes is of paramount importance.

With this Policy, the Company creates a unique and high protection level for the personal data that it processes.

In particular, the Company ensures personal data protection in the following ways:
a) by adopting this Policy regulating the general rules regarding the personal data protection by the Company,
b) by adopting special internal regulations and protocols that govern personal data processing in more detail,
c) by implementing staff-related, organizational and technical measures for personal data protection,
d) by appointing a data protection officer,
e) by keeping detailed records about data processing activities,
f) by continuously educating its employees about the importance of data protection.
2. Definitions and understanding key terms

For better understanding of the terms used throughout numerous provisions of the Policy, the following definitions are given below:

**2.1. Personal data**
This term refers to the data of an individual whose identity has been determined or may be determined either directly or indirectly, or by using identifiers such as name, ID number, location data, network identifier or one or multiple factors that are distinctive to that individual's physical,

physiological, genetic, mental, economical, cultural or social identity.

**2.2. Personal data processing and storage**

The processing of personal data refers to any procedure or sets of procedures performed on personal data or personal data sets, that are either automated or non-automated, for the purpose of collecting, recording, organizing, structuring, storing, adapting or changing, finding, inspection, use, disclosing by means of transmitting, disseminating or making available in any other way, harmonizing or combining, limiting, deleting or destroying personal data.

The collection, processing or storing of personal data may be performed on personal data in any form, either non-automated (such as forms or documents obtained from the client, employees, or by manually entering personal data), semi-automated (manually populating Excel sheets or scanning for further processing), or automated (via the electronic forms or access cards, web pages, etc.).

The already processed data or the data being processed is stored within certain systems, i.e. in the structured personal data set that is accessible and classified under special criteria (personal data categories, either general or special), and irrespective of whether they are centralized, decentralized or dispersed on a functional or geographical basis. Certain exceptions may apply to the personal data being processed for scientific, public or statistical purposes.

**2.3. Personal data subject and recipient**

A personal data subject is any natural person whose information the Company collects, i.e. that submitted this information to the Company, or whose personal data is provided to the Company for legal reasons (e.g. clients, current or prospective employees of the Company, external collaborators, etc.).

A recipient of personal data refers to any natural or legal person, pubic authority, agency or any other body to which personal data is being disclosed for certain reasons.

**2.4. Controller and processor**

The data processing controller is the Company that either alone or together with another data processing controller (e.g. when personal data is being collected together with a partner company) determines the purposes and means for personal data processing. The data processor is any natural or legal person, public authority, agency or any other body that processes personal data for the Company (e.g. external accounting department).

**2.5. Automated individual decision-making and profiling**

Automated individual decision-making refers to a situation when the Company's computer program, based on its technical settings and software, processes the subject's personal data without human intervention, i.e. only by using a pre-defined algorithm (e.g. the program that automatically accepts or declines a certain request made by the subject based on particular requirements).

Profiling refers to any form of automated data processing that involves using personal data for evaluating certain aspects about an individual, and in particular for analyzing or predicting that individual's work performance, economic status, health, personal preferences, interests, reliability, behavior, location or movement (e.g. a program that analyses consumer habits and sends offers based on them).

In order to prevent any uncertainties, the Company does not use automated individual decision-making. Any decisions regarding a data subject or that may affect it in a significant way and involve legal effects are made with considerable human intervention.

**2.6. Pseudonymisation**

This term refers to the processing procedure by which personal information can no longer be traced back to an individual without using additional information, subject to condition that such additional information is being stored separately and is subject to technical and organizational measures ensuring that personally identifiable information can no longer be traced back to an individual whose identity is or may be determined.

**3. Policy use**

The Policy shall apply whenever personal data of natural persons is being collected or processed, irrespective of the current stage (initial preparations or under process).

Personal data to which this Policy does not apply is in particular

a) information about legal entities (e.g. companies, associations, public bodies)

b) information about deceased persons, and

c) information by which natural persons cannot be identified either independently or by associating it with some other information (e.g. pseudonymisation).

This Policy is a constitutional document of the Company and applies to any and all personal data processing activities performed by the Company, such as in particular:

a) processing of personal data of the employees during the conclusion, performance and processing of an employment agreement, as well as for contacting prospective employees during the selection processes before an employment agreement is concluded,

b) processing of personal data of the natural persons that the Company employs under a temporary service agreement, copyright agreement, or similar agreements,

c) processing of personal data of the personnel employed by the Company's suppliers,

d) processing of personal data of the pupils and students on an internship at the Company or which perform temporary pupil or student work, as well as during the selection process, agreement conclusion and granting scholarships to the pupils and/or students by the Company,

e) processing of personal data of the employees' family members to the extent necessary for implementation of the legal provisions or exercising rights under the collective agreement (e.g. right to tax relief, paid leave, reward for the birth of a child, appropriate gift for the child and such),

f) processing of personal data related to the conclusion, implementation and processing of the hotel services agreements with business and private users, and implementation of the appropriate advertisement and market research activities for the purpose of informing the service users and interested third parties about the services offered by the Company,

g) processing of personal data related to the conclusion, implementation and processing of other types of agreements whose subject matter consists of providing one of the services that fall within the scope of the registered business activities of the Company (such as catering agreements, irrespective of the nature of the contract),

h) processing of personal data of the Company's stakeholders or shareholders, depending on the legal form of the Company,

i) any other personal data processing activities currently performed by the Company or that may be performed in the future either on a temporary or permanent basis.

This Policy is binding for all organizational units of the Company.

This Policy is also binding for all entities for which the Company may request to accept it (e.g. data processors).

The provisions of this Policy are intended to ensure high and unique levels of protection of personal data in the Company. Any existing or future obligations under laws or

regulations relating to the personal data processing and use with a broader scope than the principles set forth in this Policy, with which obligations the Company must comply with shall not be affected by this Policy.

The provisions of this Policy shall not affect the applicability of the national regulations relating to the national security, defense or public safety, or for the purpose of preventing and investigating criminal offences and prosecuting perpetrators.

**4. Addressees**

All management personnel, employees and associates of the Company (hereinafter: the Employees) shall be the addressees of the implementation of this Policy, i.e. responsible officers when properly collecting, processing and storing personal data. In addition, the said responsibility shall be one of the work obligations of each individual employee.

The stated addressees act in good faith and with due diligence when performing any of the stated and/or similar actions and/or in any of the stated situations, while simultaneously acting in the best interests of all subjects whose personal data is being collected, processed and stored, since this is an indispensable prerequisite for the proper implementation of this Policy.

The rules applicable to the individual data processing areas within the Company shall be more detailedly regulated with individual rules that must comply with the relevant data protection regulations and this Policy.

For the purposes of more detailedly regulating the individual data processing areas, the Company may adopt acts (e.g. an IT safety policy, regulation on personal data processing of the employees and other individuals hired by the Company, CCTV regulation, Archives and registry protection regulation, etc.). The Company may at any time adopt regulations it deems necessary in order to achieve higher personal data protection level within one business unit, and these regulations shall serve to supplement the provisions of this Policy and may not contradict them.

**5. Principles**

Any and all actions under this Policy are based upon the following principles which must be observed at all times when handling personal data.

**5.1. The principle of legal, fair and transparent** data handling, according to which any handling of data must comply with the laws and other applicable regulations, as well as carried out in a fair and transparent way.

In order to clarify to the data subjects that their personal information is being collected and processed, and for which purpose, the Company notifies the subjects about the purpose of the processing among other things, which includes information about what personal data is being collected, processed and used, for which applications, for how long it is stored, and which recipients this data is disclosed to. The subjects are notified through different channels, depending on the circumstances of the particular case, and these may include: notices via the Company's web site, written notifications in the Company's premises, written notifications on forms that the Company uses, written notifications as part of the agreement that the Company enters into with the subject, email notifications, verbal notifications by the Company's employees, and other methods if necessary.

In particular, the Company notifies the subjects about their rights and the way they may exercise them. The data protection officer's contact information is publicly available.

**5.2. The principle of data collection for legal reasons only**, according to which the data may be collected only for the specific, explicit and legal purposes, and may not be processed in any other way that is contrary to the indicated purposes.

**5.3. The principle of the data volume limit and proportionality**, according to which any personal data collection must be limited to the minimum necessary and only data that is relevant and proportional to the purpose for which is are processed may be collected.

**5.4. The principle of data accuracy and currency**, according to which the accuracy of the data being collected and entered into the databases must be verified, and necessary measures taken in order to immediately delete or rectify the incorrect information, while taking the purpose for which it is being processed into account.

**5.5. The principle of limited storage**, according to which the need to keep the data that allows natural persons to be identified must be limited with the purpose for which the personal data is processed. Personal data may be stored in a form that enables data subjects to be identified only for as long as necessary according to the purpose for which the personal data is processed. Whenever possible, the Company may apply techniques for deleting personally identifiable information (anonymisation) or replacing the personally identifiable information with other properties (pseudonymisation).

The retention periods for various personal data categories are given in the data processing activities records (if kept) for each personal data type separately. The data retention periods are determined based on the legal requirements and the needs to protect the Company's interests.

With the Archives and registry protection regulation, the Company may regulate the documentation retention periods for each individual business units of the Company.

**5.6. The principle of personal data safety**, according to which any handling of personal data must be performed in a way that ensures the highest possible level of protection of this data, including protection against unauthorized and/or unlawful processing, accidental loss, destruction or damages by using appropriate technical and organizational measures.

## 6. The purpose of personal data processing

It is important that any collection or processing of personal data has its purpose, that is a reason for which that particular personal data is collected or processed. The stated reasons are determined, defined and itemized below, and must be unequivocally indicated whenever personal data processing is performed:

### 6.1. Subject's consent

Data collection and processing is based upon the subject's consent/approval given for one or multiple specific purposes.

### 6.2. Contract performance

Data collection and processing is necessary for the performance of the agreement to which the subject is a party, or in order to take actions upon subject's request before the contract is entered into (e.g. for the conclusion of the agreement, the contractual parties need to be defined that may be identified by personal information only).

### 6.3. Legal obligation of the Company

The collection and processing of certain data on the part of the Company arises from the legal obligation that compels the Company to perform the aforementioned activities as well as cooperate with the public authorities (e.g. data collection about the employees for the Croatian retirement and health insurance institute, tax office,

customs office, independent administration bodies, the Croatian national tourist board).

**6.4. Legitimate interests of the Company or third party**
Data collection and processing is needed for a legitimate interest of the Company or a third party, except when superseded by the interests or fundamental rights and freedoms of the subject that require the personal data protection, and especially if the subject is a child (e.g. legitimate interest of the Company to install a CCTV system to ensure safety of the surveilled area).

In case when the Company processes personal information based on its legal interest that is obvious, the Company shall note the nature of its legitimate interest and circumstances based on which it concluded that its legal interest supersedes the subject's interests, rights and freedoms in the data processing activities records, if obligated to keep them. In cases when the Company's legitimate interest is not obvious and therefore requires a more elaborate proportionality test and a deeper analysis, the Company shall document the reasons based on which it determined that the its legal interest prevails in more detail and in written form.

**6.4.1. Data processing for the direct marketing purposes**
It can be reasonably assumed that the Company has a legal interest to process personal data for direct marketing purposes. In this regard, the data concerned must be personal information that was previously legally collected by the Company, and the use of data for direct marketing purposes must be in accordance with what the subject may reasonably expect based upon its relationship with the Company in its capacity as a data processing controller. As opposed to this, processing of personal data for direct marketing purposes may not be based upon the legitimate interest, but only upon the subject's express consent.

If the personal data is processed for direct marketing purposes based on the legitimate interest of the Company, the subject may appeal against the personal data processing for direct marketing purposes at any time, including profiling that is associated with such direct marketing. Not later than during the initial communication with the subject, the subject is warned about this in a clear and distinct way and separately from any other information given. If the subject opposes the data processing for direct marketing purposes, its personal information may no longer be processed for such purposes.

In order to eliminate any doubt, the Company confirms that sending its different written communications (e.g. newsletter and news about the Company's benefits and services) is only possible upon the subject's consent given by filling out the corresponding fields on the Company's web site after being notified about the processing of personal data and a subsequent verification by clicking on the link sent to the email address specified for receiving notifications.

Except when specified by the subject itself, the Company shall not collect email addresses or other information in any other way for sending newsletters to the subjects. Any and all such communications transmitted to the subject contain a clearly highlighted unsubscription option from receiving communications. By unsubscribing, the subject's consent is deemed as revoked. In case of unsubscribing, the Company deletes the subject's personal data it collected for direct marketing purposes.

**6.5. Matter of public interest**
Data collection and processing is required for performing a public interest matter or when exercising official authorization.

**6.6. Protection of the key interests of the subject or other natural person**

Data collection and processing is required for the purpose of protection of the key interests of the subject or other natural person.

## 7. Subject's consent

Subject's consent is a sound basis for collecting personal data, if the said consent is communicated to the Company with a distinct confirmatory action that represents a voluntary, explicit, deliberate and unequivocal agreement by the subject that may be expressed in a written, electronic or verbal form.

It is important to bear in mind that the Company bears the burden of proving that the subject actually gave its consent for collecting or processing its personal information. In view of the foregoing, obtaining a consent given only verbally is generally not recommended.

Irrespective of the form of the consent, the communication with the subject relating thereto must be in an easy to understand way, using clear and simple language and without any unfair conditions.

**7.1. Subject's written consent**

The subject may give its consent in a written form, preferably with a signature and the date of consent.

Equally, in case the Company requests a consent in a written form that contains requests for information other than the consent (such as statements or other answers), the actual request must be presented in a way to allow it to be clearly distinguished from the other questions, meaning that it may not be presented in a way that could confuse the subject.

**7.2. Subject's electronic consent**

The subject may give its consent in an electronic form. The Company's request for consent must be clear, concise and may not unnecessarily disturb the use of the service it is used for (e.g. aggressive cookies disrupting access to the content, etc.).

Taking the fact that the consent must be unequivocal and voluntary into account, it is necessary to keep in mind that it is not allowed to "force" the consent, especially by checking the consent box in advance, or in some other way that significantly affects the use of a web page, or by adjusting the technical settings, but rather the choice in hand must be "neutral". When drawing up the consent form, it must also be considered that silence, i.e. inactivity of the subject may not be construed as consent in any case whatsoever.

**7.3. Voluntariness of the consent**

Free choice must indeed be offered to the subject in forms and requests, where rejecting the request or withdrawing the consent does not involve any consequences.

In cases where the form or request to disclose personal information is closely connected with the service provision or performance of the offered contract, the Company requests only information necessary for providing the said service or performing the said contract.

**7.4. Procedure in case of withdrawal of consent**

The subject has the right to withdraw its consent, and the Company enables the subject to easily withdraw its consent at any time, which possibility is subject to a prior notification and must be enabled through simple contact with the Company, by a written instrument or via the Internet. After the consent has been revoked, any further processing of the subject's personal data is forbidden. A potential revocation of the consent does not affect the lawfulness of the processing of data at issue prior to the revocation.

**8. Fulfilling the obligation of prior notice to the subject**

The Company receives the subject's personal data from the subject itself, as well as from other sources. In both cases, the Company gives all relevant information to the subject relating to the personal data collection and processing that pertains to the subject.

However, the obligation of notice must not be fulfilled if
a) the subject already has such the information,
b) recording and disclosure of personal information is expressly required by law, or
c) providing such the information to the subject is impossible or would involve a disproportionally large effort, and if
d) the personal data must remain classified under the obligation of professional secrecy, that may be prescribed by applicable regulations or the statute.

**8.1. Information given by the Company to the subject in case of direct data collection**

During the initial collection of personal data from the subject, the Company provides the following information to the subject relating to the data processing:
a) identity and contact information of the Company, i.e. the Company's representative (appoint an employee to be the contact person)
b) contact information of the data protection officer, if appointed
c) the purpose of the personal data processing and the legal basis for the processing, and in case the purpose is based upon the Company's legitimate interests, they need to be defined
d) recipients of the personal data, if any, i.e. entities who this personal data will be provided to, if it is intended to transfer the data outside of the Company,
e) if applicable, the fact that the Company intends to transfer personal data to a third country or international organization, as well as an existing or non-existing adequacy decision of the Commission for that particular country, or a reference to the appropriate and relevant protection measures, and the methods of securing the copy of the data or the place to which it is made available.
f) the period for which the personal data is being stored or, if this is not possible, criteria for defining that period (or for as long as the legal basis for processing or an internal limitation exists, e.g. 1 year)
g) inform the subject about its rights, that is the (I) right to access to, (II) right to rectification or erasure, (III) right to restriction of processing, (IV) right to object, (V) right to transfer the data to another controller, (VI) right to withdraw consent, (VII) right to object with the competent monitoring authority, as well as about how to exercise the said rights (e.g. by a written instrument, email, filling out a form, etc.)
h) information about whether providing personal data is a legal or contractual obligation, or a requirement necessary for concluding a contract, and whether the subject is obligated to provide personal data and what are the possible consequences in case of not providing it
i) information about whether an automated decision-making system is in place, including subject profiling

Furthermore, in case the collected data is further processed for any purpose other than the one for which the data was initially collected, the Company is obligated to provide information about the new purpose for data processing and other relevant information given above.

**8.2. Information given by the Company to the subject in case of data collection from other sources**

In the present case, the Company provides the same information pursuant to item 8.1, except of that under h), and in addition indicates the source of the received personal information (or if the source is publicly available). The Company provides the stated information within a reasonable time, and at the latest one month from the day of receiving the corresponding subject's personal data. However, there are two exceptions to the stated rule, in which case the procedure differs, as indicated below:

a) if the intended use of the collected personal data is to communicate with the subject, the Company shall provide this information to the subject when the initial communication is established at the earliest, and
b) if the data is intended to be disclosed to another recipient, the Company shall provide this information when the personal data is first disclosed at the latest.

Furthermore, the Company shall also provide all relevant information, if the personal data at issue is subsequently processed for a purpose other than the initial.

**9. Personal data retention period**

With regard to the retention period for specific personal data, there is personal data for which the retention period is regulated by law (such as special regulations on job track records for students prescribing a six-year retention period for data upon termination of employment, or on accounting records prescribing an 11-year data retention period from the date of creation), and personal data for which the retention period is not regulated by law.

In any case, the Company stores the data for a minimum period as allowed by law or as needed according to the Company's business activities and deletes it immediately after. If deemed necessary, the Company may determine with an internal act which data shall be manually or automatically deleted after a certain period of time (e.g. 1 year, 2 years, etc.), or with regard to a certain occurrence (e.g. end of fiscal year).

**10. Processing of special categories of personal data**

In principle, the following types of personal data are not processed: data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of the unique identification of individuals and data related to health, sex life or an individual's sexual orientation.

The above-mentioned personal data categories are nevertheless processed by the Company in the following situations:
a) the data subject has given explicit consent to the processing of this personal data for one or more specified purposes, except when the applicable regulations provide that such the consent does not produce effect
b) the processing is required for the purposes of performing obligations and exercising specific rights of the Company or the subject in the field of employment and social security and social protection law in so far as it is authorized by applicable law or collective agreement
c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
d) processing relates to personal data which is manifestly made public by the data subject
e) processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity
f) processing is necessary for reasons of substantial public interest, on the basis of applicable law, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
g) processing is necessary 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 applicable laws.

Collecting, processing or storing special categories of personal data must be carried out with special care by the employees.

There is a possibility of further changes to the applicable regulations pertaining to the handling of special categories of personal data, for which purpose regular consultation with the data protection officer is needed concerning this matter.

**10.1. Specifics of processing of personal data obtained by CCTV**

The Company processes personal data obtained by CCTV only for the purpose that is necessary and justified for the protection of persons and property, while taking into account that the subjects' interests contrary to the processing of data obtained by CCTV do not prevail.

A notice carrying relevant information that the entire premises or a specific area is under video surveillance, as well as the Company's contact information by which a subject may exercise its rights is attached in a clearly visible location.

Processing of personal data of the employees obtained by CCTV is carried out only if conditions under this law are met together with the conditions under occupational safety regulations, and if the employees were individually notified in advance about this measure and only if the Company informed its employees prior to making the decision about installing a CCTV system. The said video surveillance may not be installed in the recreation rooms, personal hygiene rooms and dressing or changing rooms.

Only authorized persons may access the personal data obtained by CCTV, and video footage obtained by CCTV may be stored for a period up to a maximum of 6 months, except if a longer retention period is prescribed by law or such video footage serves as a means of proof in a legal, administrative, arbitration, or other similar proceedings.

**10.2. Specifics of processing of biometric data and photos**

The Company processes biometric data only if prescribed by law and necessary for the protection of individuals, property, classified information, trade secrets, or for unique and secure identification of service users, while taking into account that the subjects' interests contrary to the processing of biometric data referred to in this article do not prevail.

The legal basis for the processing of the subject's biometric data for secure identification is the express consent by the subject.

The Company processes biometric data of its employees for the purpose of keeping records of working time, as well as entry and leaving of offices, if prescribed by law and if such processing is carried out as an alternative to another solution for keeping records of working time, i.e. entry and leaving of offices, provided that the employee has given express consent for such processing of biometric data.

Processing of photos should not be considered as processing of specific categories of personal data, since, strictly speaking, these are only included under the definition of biometric data processed by special technical means, enabling a unique identification or authentication of an individual, which is why personal data of this kind must not be processed, except when permitted in special cases.

**10.3. Specifics of processing of personal data about children**

The applicable regulations provide special protection for personal data about children, especially the ones under 16, for a reason that this subject category may generally be less aware of the potential risks and consequences.
The above applies in particular to the use of personal data about children for the marketing or individual or user profiling purposes, as well as the collection of personal

data about children during the provision of services offered directly to children.

Processing of personal data at issue is generally lawful only under the condition that the consent was given by a person having parental authority (parent, legal guardian, etc.). The Company makes a reasonable effort to, with regard to the available technology, check or verify whether the said consent of a parent or guardian exists (e.g. via the web form). However, the consent of a person having parental authority is not needed within the meaning of preventive services or counseling services offered directly to children.

**11. Procedure when the subject exercises its rights**

The subject has certain rights relating to its own personal data that is collected and processed by the Company, which must be respected when the subject wishes to exercise them.

The Company proves the identity of the person claiming to be the data subject and requests access to personal data or assertion of other right. The identity is proven by inspecting the identity document such as an ID card, passport or driving license, or a client reference number by web identification. If deemed necessary, the Company keeps records of all inquiries and activities that have been performed relating to the said inquiries. The above procedure is performed at the expense of the Company, however, in case of multiple inquiries by one subject administrative charges may be incurred.

**11.1. Exercising the right to access to personal data by the subject**

In case of a request to access personal data in written or electronic form, the Company issues a confirmation about whether the subject's personal data is processed, and specifies what exact data is being processed, i.e. grants access to the data (and hands over a copy of the personal data, except if the copy contains data of other subjects).

In addition, the Company also specifies the information about:
a) the purpose of processing,
b) the categories of personal data at issue,
c) recipients or categories of recipients to which the personal data is or will be disclosed, and in particular recipients in third countries or international organizations,
d) the provided time period, when possible, for which the data is stored, or, when not possible, the criteria for determining such time period,
e) the right of the data subject to request a rectification or erasure of personal data, or restriction of processing of personal data from the Company, or to object to such processing, or the right to lodge a complaint with a supervisory authority,
f) any available information about the source of personal data, if not collected by the subject,
g) information about whether an automated decision-making system is in place, including subject profiling

**11.2. Procedure for exercising rights**

The subject may exercise its rights by sending a written request to the data protection officer by email or post. Data protection officer's contact information is publicly available on the Company's web site.

For specific subject categories (e.g. employees), further or additional contact persons may be appointed by special regulations to whom the subjects may appeal in order to exercise their rights in the easiest possible way.

In case any employee of the Company receives a data subject's request in any form, it undertakes to immediately forward it to the data protection officer, or to notify its superior who then undertakes to forward it to the officer. The Company is obligated to instruct its employees to comply with this procedure. Exceptionally, it is not necessary to notify the officer when an authorized

employee of the Company updates their personal information upon the employee's request in the records kept by the Company.

After receiving the subject's written request, the officer undertakes to review it. Depending on the complexity of the request, the officer decides whether to reply to the request itself, or whether the draft reply upon the subject's request shall be prepared by the Company's employee under whose job duties the subject's request falls. In the latter case, the officer undertakes to review the reply before dispatching the reply to the data subject.

**11.3. Exercising the right to rectification and erasure of personal data**

In case of a request in hand, the Company rectifies the incorrect personal data of the data subject without unnecessary delays, and supplements incomplete personal data upon receipt of an additional declaration by the subject.

In addition to the above, the Company notifies all recipients of the personal data at issue about the rectifications, i.e. supplements performed, and notifies the subject about the said recipients upon the subject's request.

**11.4. Exercising the right to erasure of personal data**

The Company erases personal data either upon the data subject's express request or if one of the following conditions is met:

a) personal data is no longer needed for the purposes for which it was collected or otherwise processed,

b) the data subject has revoked its consent upon which the data processing is based and there are no further legal bases for the processing,

c) the data subject objects to the processing of personal data and there are no stronger legitimate reasons for processing, or the data subject objects to the processing of personal data for direct marketing purposes,

d) personal data is processed contrary to the legal provisions,

e) personal data must be erased in order to comply with the legal obligation under the applicable legal regulations,

f) personal data is collected relating to the offer of services by an IT company (social networks, for example).

The Company erases personal data in such a way as to enable permanent deletion of the specified data from the main systems, with a record of erasure (in order to prove that the erasure procedure has been actually performed) and determined methods for data destruction (e.g. data in written form, on a USB or CD medium).

In case the Company has publicly disclosed personal data, it is obligated, considering the available technology and execution costs, to take reasonable technical measures to delete any and all links to the data, i.e. copies or reconstructions thereof, and is furthermore obligated to inform any other related controllers processing the data that the data subject has requested its erasure.

The Company is obligated to notify any recipients of the personal data at issue about its deletion and inform the data subject about those recipients upon data subject's request.

The Company determines the time period within which the need to process and store personal data shall be re-examined and erases the data that no longer needs to be processed or stored.

**11.4.1. Restriction of complying with the request for erasure of personal data**

In spite of the data subject's request or proof of the grounds referred to in item 11.3, the Company does not perform the erasure of personal data to the extent for which the processing is necessary:

a) in order to comply with legal obligations under which the processing is provided and to which the Company is subject, or to perform a service of public interest,

b) in order to respect the right to freedom of speech and information,

c) for public interest in the area of public health,
d) for public interest, historical or scientific research, or statistical purposes, i.e. for asserting or defending legal claims.

**11.5. Exercising the right to restriction of processing**

Upon the data subject's request, the Company restricts the processing of personal data in such a way as to allow processing of specific personal data only with the subject's consent (with the exception of the need to assert or defend legal claims or protect other natural or legal person's right or for an important public interest), in case that:
a) the subject objects to the personal data accuracy, for a time period that allows the Company to verify the accuracy of personal data,
b) data processing is unlawful, and the data subject objects to the erasure of personal data and requests restriction of its use instead,
c) the Company no longer needs the personal data for processing, but the data subject requests it for establishing, asserting or defending legal claims,
d) the subject has lodged a complaint with the Company and awaits confirmation of whether the data processing controller's legitimate reasons outweigh the subject's reasons for erasure,
e) the Company notifies the subject when restriction of processing has been obtained and subsequently cancelled, in which case such notification must take place prior to the cancellation.

The Company notifies all recipients of the personal data at issue about the imposed restrictions of processing and informs the data subject about the said recipients upon its request.

In practice, the method for restriction of processing in hand would involve temporary relocation of the selected personal data to another data processing system, making the selected data inaccessible to the users, or temporary removal of the disclosed data from the web page. In automated storage systems, the restriction of processing must be ensured through technical means by making the data unavailable for further processing and impossible to alter, and by clearly denoting that processing of the personal data at issue is restricted.

**11.6. Exercising the right to data portability**

Upon the data subject's request, the Company delivers the requested personal data in a structured, commonly used and machine-readable format, in order to enable the data subject to easily transfer the data at issue to another potential processing controller (the subject also decides whether to request data erasure together with the transfer).

Where technically possible and requested by the subject, the personal data at issue is transferred directly to another controller as selected by the subject, provided that the processing is performed automatically and is based on the subject's consent, or if the processing is necessary for performance of a contract.

However, it has to be considered that the data transfer will not be carried out if that would compromise other subjects' personal data.

**12. Objections procedure**

**12.1. Objection to the processing of personal data whose purpose is a legitimate interest of the Company**

The subject may at any time object to the processing of personal data whose purpose is the preservation of legitimate interests of the Company. In such an occurrence, the Company discontinues any processing of personal data, and conducts an assessment of the proportionality of the interests of the subject against the interests of the Company for processing personal data.

If legitimate interests of the Company prevail over the data subject's interests in any particular case, or processing of personal data is necessary for establishing, asserting or defending legal claims, the processing of personal data continues. If the data subject's interests prevail over the legitimate interests of the Company, personal data at issue may no longer be processed. When conducting the aforementioned proportionality test, consultation with the data protection officer is absolutely necessary.

**12.2. Objection to processing of personal data for direct marketing purposes**

The data subject may at any time object to processing of personal data for direct marketing purposes, including profiling to the extent related to such direct marketing. In such a case, the Company discontinues any further processing of the personal data at issue.

**13. Specifics of automated individual decision-making, including profiling**

The data subject has the right that a decision based solely upon automated processing including profiling does not apply to it, which decision produces legal effects that apply to or significantly affect the data subject. The above conditions are met for example, when the Company's computer system is, based on the technical settings and software, selecting certain subjects with regard to their data without human intervention.

However, the above does not apply when the automated decision in hand is necessary for conclusion or performance of a contract between the data subject and processing controller and permitted under applicable regulations or based on the express consent of the subject (in which cases the subject is entitled to express its position or object to the decision at issue).

The said decision-making is not permitted relating to the special categories of personal data, except upon data subject's express consent or in case that proper safeguards for rights and freedoms and legitimate interests of the subject are in place and exist.

When conducting an assessment whether profiling occurs in a particular case or not, it is taken into account whether the end goal is the collection of personal data based upon which a certain image of the data subject and its preferences is formed (above all, in case of tracking the data subject's web activities) and subsequent sending of specific offers, suggestions or similar based on such an image (e.g. a profile about services that the data subject usually uses is created based on which offers that are closely related to such services are sent). If the answer to the above question is yes, the Company informs the subject relating thereto.

**13.1. Creation and keeping records about personal data processing activities**

If provided for by statutory regulations, the Company creates and keeps records of the data processing activities, in which it records all activities relating to the personal data processing that is entered, i.e. listed. This is either a written or an electronic document containing the below information:

a) name and contact information of the Company and, if applicable, the common data processing controller, the controller's representative and the data protection officer,
b) purpose for the processing,
c) description of the data subject categories and personal data categories,
d) recipient categories to which personal data is or will be disclosed, including recipients in third countries or international organizations,
e) if applicable, personal data transfers to a third country or international organization, including identification of that third country or international organization, and

f) prescribed periods for erasure of different data categories, when possible,
g) description of the technical and organizational safety measures.

The Company allows access to the records upon request of a supervisory authority.

These records are not kept if the Company has less than 250 employees, except when the data processing performed by it may likely cause high risks for the data subjects' rights and freedoms, if the processing of data is not periodical or if it involves special data categories, or the personal data is related to criminal convictions or offenses.

**14. Maintaining personal data security**

The Company pays particular attention at all times to the protection of personal data that is collected and processed, in which regard it carries out pseudonymisation and encryption of personal data, ensures permanent confidentiality, integrity, availability and reliability of the data processing systems and services, maintains archival records of personal data and accesses them in the event of physical or technical incidents (back-up servers for the personal data affected), and establishes a process for regular testing, evaluation and assessment of efficiency of the technical and organizational measures for ensuring processing security together with the potential risks such as accidental destruction or loss of personal data, unauthorized disclosure or access to the personal data that is transferred, stored or otherwise processed.

14.1. Encryption
If deemed necessary, the Company protects personal data with encryption, by using the so-called asymmetric encryption algorithms which may be decrypted only with a key known to authorized persons (for example, AES [Advanced Encryption Standard] or TDEA [Triple Data Encryption Algorithm] are recommended). The above applies in particular to the systematic data storage, transfer of data outside of the Company, storage of data on portable media such as USB drives etc., or to the processing of special categories of personal data.

**14.2. Secure access to personal data**
The Company keeps personal data in a physical or electronic form stored on portable media such as CD, USB or hard drives in a secure place such as archives or vaults to which only authorized personnel have access. In case of data in electronic form, they are kept in computer applications which may only be accessed by means of a secure login, password and a system requiring strict identification of authorized persons (especially in the event of special categories of personal data).

It is recommended to maintain records of all personal data transfers and uploads, in order to be able to detect any possible unauthorized uses of or sending personal data, by means of a system that would automatically mark authorized persons performing the upload at issue, the location of the data, date and time stamp, and the contents of this data.

Any personal data sent electronically should be transmitted only by secure HTTPS URLs, and it is recommended to provide access to the data via the web through an OAUTH authentication.

**14.3. Data backup system**
If deemed necessary, the Company shall maintain the security of personal data from accidental destruction in case of failure of the computer system or similar events, in a way as to create and commission a specific backup system for preventing this (e.g. a backup server or hard drive).
15. Review of personal data processing and security

If deemed necessary, the Company shall conduct an internal review of the personal data protection for the purpose of locating potential security-related issues and risks, and to erase personal data that no longer needs to be stored.

The said internal review is performed by the Company's authorized persons with the collaboration of the data protection officer.

If necessary, the Company shall also conduct an independent review by a third party, which review may not involve persons who participated in the implementation of the security measures and personal data processing, which methodology shall determine any possible issues related to any aspect of data collection, processing and storage as well, in conjunction with the consultations on how to improve the safety and security.

## 16. Procedure in case of a breach of personal data

### 16.1. Breaches in general

Despite all appropriate measures for protection of personal data implemented by the Company in order to prevent breaches of personal data, the possibility of breaching personal data cannot be ruled out completely. In addition to the protection measures that are intended for preventing breaches, the Company also takes technical measures with the goal of establishing whether a breach has occurred.

The breach of personal data may involve a series of adverse consequences for the data subjects, which is why a prompt reaction by the Company to an event of breach is of utmost importance.

The breach of personal data is a violation of security leading to accidental or unlawful destruction, loss, modification, unauthorized disclosure of or access to the personal data transferred, stored or otherwise processed.

Data destruction implies that personal data no longer exists or does not exist in a form that the Company needs for the purposes for which it processes it.

Data loss implies that personal data exists, but the Company no longer has control over or access to it, or that the Company is otherwise no longer in possession of the data. The loss may be temporary or permanent.

Modification implies that the data is no longer complete, correct or up-to-date as a result of changes performed.

Unauthorized disclosure of or access to personal data implies disclosure to persons that have no authorization.

### 16.2. Reporting to the Data protection authority

If the Company discovers a breach of personal data which is likely to cause risks for the subject's rights and freedoms, the Company must immediately and without delay report to the Data protection authority, and within 72 hours at the latest (in case of a later notice, the explanation for the delay must be provided).

This report must include the

a) description of the nature of the breach of personal data, including, where possible, the categories and approximate number of data subjects from the category and the approximate number of the related personal data records,

b) name and contact information of the data protection officer or other contact point from which further information may be obtained,

c) description of the likely consequences of the breach of personal data,

d) description of the measures taken or suggested by the Company for resolving the potential breach of personal data, including measures for minimizing its adverse consequences where necessary.

If the Company is for whatever reason unable to provide the above information in a single report, it may provide it successively, but without unnecessary delays.

The Company undertakes to document any violation of personal data, including facts relating to the breach of personal data, consequences, as well as measures taken for repairing the damage.

After notifying the Authority, the Company follows any orders given by the Authority. Consultations with the competent data protection officer are also necessary in the said procedure.

**16.3. Reporting to the data subject**

The Company undertakes to immediately and without delay inform the data subject about the breach which likely represents high risk for the rights and freedoms of the affected subject. In the present notice, the Company provides a description of the breach together with the information referred to under b), c) and d), in clear and simple language.

However, no notice is sent to the data subject if at least one of the below conditions is met:

a) appropriate technical and organizational protection measures have been taken, and in particular ones that render the data unintelligible to any person who is not authorized to access the data, such as encryption,

b) additional measures have been taken ensuring that high risk for the subject's rights and freedoms is no longer probable,

c) disproportionally large effort is required to notify the data subject. In such a case, some sort of public notice or a similar measure must be in place for notifying the data subjects in an equally effective manner.

**16.4. Course of action by employees in case of a breach**

It is the responsibility of all employees of the Company to immediately inform the data protection officer about a breach, or the suspicion of a breach and the circumstances from which the suspicion arises.

In case that the officer is absent, the person responsible for human resources and/or legal business must be notified, who takes over the officer's responsibilities until the latter assumes its position or gives explicit instructions.

**16.5. Course of action by the officer in case of a breach**

The job of the data protection officer is to investigate the circumstances under which the breach occurred, or circumstances related to the alleged breach, within 48 hours. For that purpose, the data protection officer is authorized and obligated to conduct the necessary investigations that includes interviewing the relevant employees and other persons who may have knowledge about the breach, as well as consultations with IT experts employed with the Company.

The data protection officer prepares a written report about the actions taken, which it presents to the Company management, and that must contain the information stated below among others:

a) a description and result of the actions and investigations conducted by the officer,

b) a description of the nature of the breach of personal data, including, where possible, the categories and approximate number of data subjects from the category and the approximate number of the related personal data records affected by the breach,

c) a description of the risk and probable consequences of the breach of personal data,

d) a description of the suggested measures to be taken for resolving the breach of data, including measures for minimizing its possible adverse consequences,

e) a concluding proposal addressed to the Company management about whether the officer deems necessary that the notification of the supervisory authority (AZOP) is advisable (which notification is not required, if it is unlikely that the breach will cause risks for the rights and freedoms of an individual), or notification of the data subject (which

notification is necessary if it is likely that the breach will cause high risk for the rights and freedoms of an individual).

In order to ensure greater consistency, the Company may prepare a form to be used for reporting breaches.

## 17. Data protection impact assessment

The Company shall perform an assessment of the impact on data protection if it is likely that the implementation of a new processing technique or type, and in particular by introducing new technologies, while taking the nature, extent, context and purposes for the processing into account, will cause high risk for the rights and freedoms of the individuals. In the process, one assessment may include a series of similar processing procedures that represent equally high risks. When performing the said assessment, the Company will call in the data protection officer.

This assessment is mandatory in the following situations:
a) in the case of systematic and comprehensive assessment of the individual's personal aspects based on the automated processing, including profiling, based upon which processing decisions are made that produce legal effects relating to or significantly affecting the individual
b) in the case of comprehensive processing of special categories of personal data or data relating to the criminal convictions or criminal acts, or
c) in the case of systematic monitoring of a publicly available area to a significant extent.

The data protection authority and other supervisory authorities also undertake to establish and publish a list of procedures for which the said assessment needs to be performed.

### 17.1. Contents of the assessment

The assessment must contain the following information:
a) a detailed description of the planned processing procedures and purposes, including, if applicable, the Company's legitimate interest,
b) an assessment of the necessity and proportionality of the processing procedures related to their respective purposes,
c) an assessment of the risk for the subjects' rights and freedoms, i.e. assessment of the probability that the breach at issue may cause physical, material or immaterial damage or lead to discrimination, identity theft or fraud, financial loss, reputational damage, loss of confidentiality of the personal data protected with a trade secret, unauthorized reversal of pseudonymisation, or any other significant economic or company losses; or if the data subjects may be deprived of their rights and freedoms or be prevented from monitoring their personal data; if special categories of personal data are being processed; if personal aspects are being processed, in particular the analysis and the prediction of the aspects relating to the work performance, economic status, health, personal preferences or interests, reliability or behavior, location or movement for the purpose of creation and using personal profiles; if data of sensitive individuals is processed, especially children; or if the processing involves a large volume of personal data and affects a large number of data subjects,
d) measures provided for resolving risk issues, including protection measures, security measures and mechanisms for ensuring protection of personal data and proving compliance, with regard to the rights and legitimate interests of the subjects and other included individuals.

The Company is not obligated to perform the assessment if the purpose for processing is a legal obligation of the Company and if the regulations from which the obligation arises provide for special processing procedures or sets

thereof, meaning that the said assessment of the effect on data protection has already been performed, except when the applicable regulations expressly state otherwise.

**17.2. Consultation with the supervisory authority**

The Company consults the supervisory authority prior to potentially risky processing if the previously performed data protection impact assessment suggests that the processing may pose high risk, unless specific security measures are implemented.

For the consultation with the supervisory authority, the following must be specified:

a) relevant data of the Company, common data processing controllers and data processors involved with the processing, especially for processing inside of an entrepreneurial group,

b) the purpose and means for the intended processing,

c) protection measures and other measures for safeguarding the rights and freedoms of the data subjects,

d) the contact information of the data protection officer,

e) a data protection impact assessment,

f) any other information that the supervisory authority requests.

If the supervisory authority determines that the intended processing would violate the applicable regulations, and in particular if the risk involved is not adequately identified and minimized, the supervisory authority advises the Company in writing within eight weeks from the day of receipt of the request (this period may be extended for another six weeks) by using any of its legal powers such as direct orders, obtaining access to the personal data or conducting a review of the personal data protection.

**18. Procedure in case of transfer of personal data to third countries**

If the personal data being collected and processed is transferred outside of the EU in a third country or international organization (such as foreign association of hospitality companies), the Company verifies that a permission for sending personal data for that particular country exists, the so-called adequacy decision, which is made by the European Commission in the Official Journal of the European Union. In light of the above, further actions differ with regard to three potential situations:

a) if the adequacy decision exists, the transfer is permitted.

b) if the adequacy decision does not exist, the transfer is in principle not permitted, but may be possible, provided that the Company or the processor has provided for the appropriate protection measures and provided that the subjects have enforceable rights and effective judicial protection at their disposal. These measures include in particular standard data protection clauses.

c) even if neither such the decision nor appropriate measures referred to in b) exist, the transfer is still possible, if the subject has given its express consent to such a transfer after being informed about the potential risks, or if the transfer is necessary within the scope of contractual obligations, or relating to the establishment, assertion or defense of legal claims and if another important public interest or data subject's interest exists.

Within the meaning of item b) from the previous paragraph, the Company endeavors to favor the protection measure that provides a higher protection level (e.g. using the standard contractual clauses approved by the European Commission, or the special contractual clauses approved by the supervisory authority), except when under the circumstances of the case application of a derogation for specific situations from the Article 49 of General Regulation is more appropriate.

The object of the business activities of the Company is to host guests from different countries, whereby the Company may receive personal data of its guests from foreign travel agencies or foreign online booking platform operators. In relation to the Company, the above subjects act as separate data processors, for whose actions the Company is not and cannot be held responsible. These subjects may be located in countries in which an adequate protection level is not ensured. With these partners, the Company may exchange certain personal data about guests for the purpose of billing the provided services, such as period of stay of a particular guest and information about the guest's consumption. These exchanges of personal data with the said partners are based upon Article 49 (1) it. c) of General Regulation (the transfer is necessary for the conclusion or performance of a contract between the controller and another natural or legal person for the data subject's interests; cf. c)).

In cases where there is a doubt whether the transfer of personal data in a country that does not ensure adequate protection is permitted, it is necessary to seek advice and opinion from the data protection officer in advance.

**19. Data processor**

The Company may entrust a data processor with processing a portion of the personal data (e.g. auditors, lawyers, or the like).

The data processor must sufficiently guarantee the observance of all appropriate technical and organizational measures compliant with the applicable data protection regulations, and act only according to the Company's instructions. The relationships with the data processors relating to the personal data are regulated with special agreements or within the scope of basic contracts.

**19.1. Conclusion of contracts with data processors**

The Company may decide whether to entrust certain aspects of data processing to the processors who undertake to process personal data in the name and according to the instructions of the Company. The Company may engage the services of data processors that sufficiently guarantee the observance of appropriate technical and organizational measures for protection of personal data.

The Company is obligated to conclude a written agreement with the data processor, by which the object and the duration of the processing, the nature of and the purpose for processing, the type of personal data and the subject category, as well as the rights and obligations of the Company and the data processor are regulated. In the context of such an agreement, the data processor gives certain guarantees to the Company relating to personal data protection.

Depending on the circumstances of a particular case, and in accordance with the type and scope of processing performed by the data processor, the Company may perform investigations it considers reasonable and necessary before engaging the services of a data processor, such as:

a) request information whether the processor has appointed a data protection officer,

b) request information whether the data processor uses subcontractors, who they are and in which countries are they located,

c) check with the data processor whether it keeps records of data processing activities,

check with the data processor whether it has any internal policies and procedures in place for personal data protection,

d) conduct interviews about the way in which the data processor's relevant processes are organized,

e) request information whether the data processor possesses a certificate aligned with GDPR (certification is not mandatory, but is useful to specify),

f) request information whether the data processor has any ISO certificates in the area of IT security,
g) consider to what extent the Company has monitoring capabilities over the processor,
h) visit the data processor's business premises,
i) concerning the data processor with whom the Company cooperates for a longer period of time, the data processor's commitment and proper performance of its contractual obligations up to that moment may also be taken into account.

For the purpose of continuous monitoring of the data processor, the Company may request from the data processor to provide a written declaration of compliance on a yearly basis or more frequently, if necessary. A draft declaration may be enclosed to the contract signed with the data processor by the Company.

The data processor specifies the Company in the record of the data processing activity (if obligated to keep it) together with all investigations which the Company conducted prior to enlisting its services. The human resources and business activities department keeps the list of processors and the contracts with the processors.

In general, the Company will avoid cooperation with the data processors who may potentially transfer personal data into a third country (outside of the EU). However, cooperation with such processors may be entered into if appropriate protection measures are implemented pursuant to Chapter V. General Regulation.

**19.2. Contracts that include exchange of data with other recipients**

When conducting its business activities, the Company may enter into legal relationships with other natural and legal persons with whom it neither acts as a common processing controller nor does it enlist their services as its data processors. In such legal relationships, certain personal information may be exchanged. Equally, personal data may be also exchanged with public authorities.

In all such cases, depending on the circumstances, the Company assesses whether a written agreement defining the contracting parties' rights and obligations needs to be concluded, as well as whether and to what extent such written contract, apart from the general provision on the contracting parties' obligation of secrecy and confidentiality pertaining to any and all information and personal data received from each other for the purpose of performance of the respective contractual obligations, should include additional provisions on exchange of personal data.

Any such additional provisions on exchange of personal data may in particular include the provisions specifying the purpose of the personal data exchange, the type of data transferred, the legal basis for the data transfer, restriction relating to the downstream recipients of personal data, the obligation of secrecy and confidentiality, the period during which the recipient will store personal data, the consequences of the personal data breach, and the like.

Any and all personal data exchanged with the recipients will be limited to the minimum necessary for fulfilling the purpose for which the data is transferred.

**20. Use of cookies**

The Company's web site uses cookies. Cookies are small pieces of text data stored on the visitor's computer when visiting the web site. The purpose of the cookies is to remember the visitor and recognize it during the next visit, as well as to store its preferences.

The cookies may collect information about the IP address, city and country of the web site visitor, its age and sex, as well as other data. Introductory provision of GDPR (30)

expressly prescribes that network identifiers such as cookies may be used for profiling of individuals and their identification. For this reason, the Company informs the visitors of the web site about the automated processing logic and the consequences of profiling for the individuals.

In order to eliminate any doubt, the Company does not aim to identify the individuals by using cookies but uses them only for the purpose of data control. The Company collects and processes personal data for the purpose of reservations and management of guests, receipts and charges, marketing campaigns, and satisfaction surveys. The data is intended for the Company and its service providers. The subject may inspect, gain access to, rectify or object to such processing by contacting our data protection officer.

Using electronic communication networks for data storage or access to the stored data in the users' terminal equipment is only permitted when the user/subject has given its consent, but only after being clearly and completely informed thereof in accordance with the special data protection regulation, and in particular about the purposes of personal data processing. In accordance with the above provision, the Company asks for the visitor's consent prior to setting cookies.

When visiting the Company's web site, the visitor is provided information about the type of cookie used by the web site and its purpose. After that, the visitor may select the cookies whose installation it wants to permit, and cookies which he wishes to reject.

On the Company's web site, information about cookies is made available to the visitor, as well as the method for modifying the cookie settings and deletion of previously set cookies.

The Company undertakes to re-examine the above course of action relating the use of cookies in a timely manner, and review if necessary, after adopting the regulation at the EU level governing the area at issue (e-privacy Regulation).

**21. Rights and obligations of the data protection officer**

The data protection officer acts autonomously and independently and is authorized to undertake all necessary active measures in order to ensure that the business activities of the Company are compliant with the data protection regulation.

The data protection officer reports directly to the Company management for its work.

When making the decision on the appointment of the data protection officer, the Company will keep in mind that the appointed person possesses the necessary expert knowledge for implementing all measures and activities for the purposes of data protection. The officer must have the necessary technical qualifications, and in particular expert knowledge about the law and practices in the area of personal data protection. Although certificates obtained by the officer may be helpful, continuing education is of much greater importance for discharging the job duties of the data protection officer, as well as knowledge of the Company's processes and IT system, the legal framework of the Company's business activities, and its needs for security and protection of data.

It's at the management's discretion whether the data protection officer will enter into an employment relationship with the Company, or the services of an external service provider will be enlisted by contractual agreement.

In the case of an employment relationship, the data protection officer may be a part-time or full-time employee. In addition to the job duties as a data protection officer, the officer may also perform other duties that do

not conflict with the interests arising from the officer's duties.

The data protection officer is a person who must be included with any and all issues relating to the personal data protection in a Company in a proper and timely manner, which is why all personnel and third parties are referred to the data protection officer in case of any doubts relating to the data protection. The Company ensures that all its organizational units, from the management staff to the employees furthest down the hierarchy, know about the data protection officer within the Company and its duties, and the importance of informing the data protection officer during the development of new services, intended use of new technologies, new types of personal data processing, personal data breaches, and requests for the exercise of rights on data protection by the data subjects.

The Company undertakes to ensure the following:
a) in case of planned new types of processing of personal data, or planned personal data processing for a purpose other than the current purpose, or use of new technologies, the officer must be involved in the relevant meetings at the earliest possible stage, in order to be able to express its opinion and lend its advice,
b) the Company shall endeavor to ensure that the officer is present at the regular management and senior management meetings, in order to be able to give its contributions to the data protection, especially at the meetings that may have influence over personal data processing,
c) ensuring that the officer has appropriate personnel, organizational and technical resources at its disposal, in order to be able to perform its job duties,
d) all organizational units of the Company are obligated to immediately inform the officer about any fluctuations and changes relating to the Company's business that may affect personal data protection,
e) before amending any policies and acts relating to personal data protection, the management shall seek the officer's opinion,

When performing its duties, the data protection officer may not receive any instructions on how to perform the duties and may not be relieved of its duties nor punished for performing these.

The officer is obligated to perform its job duties personally, diligently and carefully. The data protection officer is responsible for implementing all measures and activities with the goal of achieving the objects of the Company's privacy policy and personal data protection, and enforcing laws, regulations and other binding acts in the area of personal data protection.

The obligations and duties of the data protection officer include in particular:
a) informing and advising the Company's management and employees about the relevant obligations under the General Regulation and other applicable data protection laws and regulations,
b) continuously educating the Company's employees in the field of data protection, in order to instruct them about the legal and the Company's internal requirements relating to personal data protection,
c) conducting internal reviews for the purpose of checking whether the business activities and practices of individual organizational units comply with the requirements under the General Regulation and the Company's internal acts, and preparing written reports on the conducted reviews, describing the results of the inspection and any possible identified deficiencies,
d) performing a periodical review of the Company's policies and acts relating to personal data protection,
e) preparing and reviewing the documentation relating to the personal data protection (e.g. contracts with data processors, contracts with common processing controllers, contracts based upon which personal data is

exchanged with the recipients, notices to the data subjects, internal policies and procedures, etc.),
f) reviewing any and all changes in data processing activities records and helping the responsible employees to fill them out,
g) preparing, i.e. reviewing written replies to the requests for the exercise of rights on data protection by the data subjects referred to in Part three of this Policy, and keeping records of received requests for the exercise of rights on data protection and replies to such the requests,
h) keeping records of the breaches of personal data and acting in accordance with the provisions referred to in Part six of this Policy in the event of a breach, as well as actively participating in the investigations of and reporting on the personal data breaches it finds out,
i) preparing data protection impact assessments referred to in Article 35 of General Regulation (when such obligation exists),
j) continuously upgrading its education by attending training courses for data protection officers as agreed upon with the management, as well as following the changes and the practices in the area of personal data protection by its own accord, and in particular the guidelines and opinions of AZOP, guidelines of the Working Party established under the Article 29 of Directive 95/46/EC and the Personal data protection committee established under the General Provision,
k) cooperating with the supervisory authority and acting as a contact person for the supervisory authority relating to the data processing,
l) performing other activities that contribute to the increased protection of personal data.

The officer is authorized to verbally warn the employees when a course of action contrary to the General Regulation or this Policy is determined, and to instruct them on how to remedy the irregularities.

The officer warns the Company management about any determined non-compliances in the area of personal data protection. The Company management subsequently decides on measures to be taken in order to eliminate such the non-compliances.

If damage is incurred to data subjects, the Company, or other individuals as a result of a mistake on the part of the data protection officer, the officer may be directly held liable for the damages, if these are caused by the officer's intent or negligence, which will be determined in accordance with the applicable legal regulations.

The data protection officer is obligated to permanently keep the confidentiality of any information and personal data which it came into possession of while performing its duties.

**22. Employee education and training**

All employees are obligated to sign special confidentiality statements or are bound by the employment contract to permanently keep the confidentiality of personal data. However, in order to help raise awareness about the importance of data protection, the Company is obligated to educate its employees about the relevance of and methods for the personal data protection within the first month on the job. The educational training is organized by the responsible person of the HR department's education and training unit.

In accordance with the current state of personal data protection, changes in legal regulations or internal policies, the number of breaches, or otherwise upon suggestion by the data protection officer, the Company conducts periodical employee trainings during the term of the employment contract for the purpose of increasing personal data protection and raising awareness among the employees about the need to protect its secrecy. These educational courses are to be held once a year at minimum.

The holding of these courses must be documented.

The training program is determined by the data protection officer in coordination with the Company management, while taking the risk level of the individual workplaces into account, in order to adapt the training content to the employee's job duties and to the scope in which the employees come into contact with personal data.

In the scope of the training programs, employees are instructed to report any and all deficiencies and non-compliances relating to the personal data protection to the data protection officer.

**23. Responsibility**

The Company is responsible for the compliance with the applicable data protection regulations and it must be possible to prove the said compliance, that is acting in accordance with the law.

**24. Conclusion**

This Policy represents codified good practice relating to personal data protection and serves as a specific guidance. This Policy aims to cover most of the foreseeable situations that may occur, but this is of course not possible, which is why each situation should be evaluated based on the circumstances that are unique to each individual situation.

This Policy is construed in accordance with the General Regulation and the applicable laws of the Republic of Croatia in the area of personal data protection. Any inquiries relating to this Policy may be submitted to the data protection officer who undertakes to reply to the applicant's request in the within the shortest possible time, and within one month at the latest.

To any and all possible disputes arising from the personal data breach committed by the Company the applicable laws and regulations of the Republic of Croatia shall apply, and court at the place of Company's registered office having the subject matter jurisdiction shall be the competent court.

This Policy ceases to be in force if the Company makes such a decision, or in case the Company is liquidated or some other status change occurs that results in a dissolution or termination of the Company. However, the abrogation of this Policy does not exempt the Company's employees from their obligations of protection of personal data collected and/or processed up to that point.

The subject of personal data protection is wide-ranging and complex, which is why it is of the utmost importance that all employees approach this matter seriously, diligently and composedly, since that is the only way to respond quickly to all challenges imposed by this ever-changing field to the everyday business activities of the Company.

BRENUM Ltd – PIN 17768963437

a Croatia, HR - 20207 Mlini, Makoše 29, Croatia
e info@brenum.com
w www.brenum.com
t | f +385 20 357 755 | +385 20 610 164

DPO:
**KATARINA RAGUŽ**

a HR - 20207 Mlini, Makoše 29
e dpo@brenum.hr
w www.brenum.com
m +385 91 219 55 35
t | f +385 20 357 755 | +385 20 610 164