POLICY ON THE PROCESSING OF PERSONAL DATA OF SITE.PRO

GENERAL PROVISIONS

1. The policy on the processing of personal data (hereinafter referred to as the Policy) of UAB Site.pro (hereinafter referred to as the Company) shall be the publicly available part of the rules regarding the processing of personal data which regulate the purposes of the processing of personal data of natural persons carried out by the Company, lay down the procedures for the exercise of their rights, establish organizational and technical safeguards for data protection, and regulate the use of a processor.

2. The Policy is based on The General Data Protection Regulation (hereinafter referred to as the GDPR) and other legal acts governing the processing and protection of personal data.

3. The Policy shall apply to the processing of data of natural persons by automatic means, and to the processing of filing systems of personal data otherwise than by automatic means.

4. The Policy shall also lay down the rights, obligations, and responsibilities of the employees of the Company. The provided requirements shall be binding on all the employees of the Company involved in the processing of personal data or who have access to personal data during the performance of functions assigned to them.

5. Processors must also follow the Policy to the extent it is not provided for in their contracts or Data Processing Agreements concluded with the Company.

KEY DEFINITIONS

6. **Personal data** shall be any information relating to an identified natural person or a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, a personal number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, economic, mental, cultural or social identity of that natural person.

7. **Responsible employee** shall be an employee of the Company chosen from among the existing employees of the Company on the basis of his professional qualities, in particular his expert knowledge of data protection law and practices who will help meet the requirements in the implementation of accountability measures (e.g. perform data protection impact assessments and carry out or assist with audits).

8. **Employee** shall be a person who performs permanent functions under a contract or post in the name and/or on behalf of the Company.

9. **Processing** shall be any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, storage, structuring, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

10. **Controller** shall be Company which, when processing data of its Clients, other natural persons or Employees, shall determine the means and measures of the use of personal data.

11. **Data Subject** shall be a Client, other natural person or an Employee whose data are processed by the Controller.

12. **Processor** shall be an entity which processes personal data managed by the Company under existing service or other contracts.

13. **Client** shall be a natural person or a legal entity to which the Company provides agreed services.

14. **Superfluous Data** shall be data that are not necessary for the purpose for which they are collected.

PRINCIPLES AND PURPOSES OF THE PROCESSING OF PERSONAL DATA

15. When performing their functions and processing personal data Employees of the Company must:
    - 15.1. Process them lawfully, fairly and in a transparent manner;
    - 15.2. Collect them for specified, explicit and legitimate purposes and not process them in a manner that is incompatible with those purposes;
    - 15.3. Comply with the principles of expediency, proportionality and data minimisation and not require Superfluous Data from Data Subjects;
    - 15.4. Ensure their accuracy and, where necessary, update them;
    - 15.5. Rectify, complete, destroy or block the processing of inaccurate or incomplete personal data;
    - 15.6. Store them so as to permit the identification of Data Subjects for no longer than is necessary for the purposes for which the data were collected and processed;
    - 15.7. Process them 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 (‘integrity and confidentiality’).

16. The processing in the Company shall be supervised by the responsible employee.

17. All information concerning the Clients and the services provided to them shall be confidential and shall remain so after the termination of the services.

RIGHTS OF DATA SUBJECTS AND PROCEDURES FOR THEIR EXERCISE

18. Data Subjects shall have the following right:
    - 18.1. To know (be informed) about the processing of their data;
    - 18.2. Upon production to the Company of an identity document or identification by electronic means which allow proper identification of the person, to access to their personal data and their processing, to obtain information from which sources and which data have been collected, for which purpose they are being

processed, to which recipients they are provided or have been provided for at least the last one year, and to obtain copies of documents containing their personal data;

18.3. To request the rectification, erasure or restriction of processing of their personal data;

18.4. To object to the processing of their data;

18.5. To have their data transferred to another controller or to be provided directly to the Data Subject in a convenient form (only data provided to the Company by the Data Subject himself);

18.6. To lodge a complaint with the supervisory authority;

18.7. To withdraw consent (if the data are processed on the basis of consent).

19. In all cases, the Company must provide the Data Subject with the information requested by him (unless the Data Subject already has such information):

19.1. Its name, legal entity number and domicile;

19.2. Purposes and the legal basis for the processing of personal data of the Data Subject;

19.3. Recipients and categories of recipients;

19.4. The period for which the data will be stored, or the criteria used to determine that period;

19.5. Other additional information (which personal data the data subject is required to provide and the consequences of such omission, as well as information on the right of the Data Subject to access to his personal data and the right to rectification of incorrect, incomplete or inaccurate personal data) to the extent necessary to ensure that the personal data are processed fairly without prejudice to the rights of the Data Subject.

Exercise of the rights of the Data Subject

20. The Company must:

20.1. Provide the Data Subject with the conditions for exercising the rights provided for in these Rules, except in cases laid down in laws when it is necessary to ensure the security or defence of the State, public order and the prevention, investigation, detection or prosecution of criminal offences, important economic or financial interests of the State, the prevention, investigation and detection of violations of official or professional ethics, and the protection of the rights and freedoms of the Data Subject or of other persons;

20.2. Ensure that all information is provided to the Data Subject in a clear and comprehensible manner;

20.3. Reply to the Data Subject no later than within 20 (twenty) working days from the date of receipt of the request. If the provision of data is refused, a reasoned reply must be provided for non-compliance with the request;

20.4. Inform recipients without delay of any rectification or destruction of personal data requested by the Data Subject, any blocked processing operations, unless the provision of such information would be impossible or excessively difficult (due to the large number of data subjects, data period or unreasonable cost). In this case, the State Data Protection Inspectorate must be notified immediately.

20.5. The Company shall provide data to the Data Subject free of charge. In certain cases (where the Data Subject manifestly abuses his rights, unreasonably

resubmits his requests for information, extracts or documents) such provision of information and data may be subject to a fee.

20.6. To exercise their rights, Data Subjects may contact the Company at the ticket system.

Provision of data to recipients

21. The Company shall provide personal data of Data Subjects without prejudice to the requirements laid down by law and by respecting the confidentiality of the data.

22. In the case of a single disclosure of data, the Company shall give the priority to the provision of information by electronic means.

23. The provision of personal data to public and municipal authorities and bodies, where those authorities and bodies receive personal data on the basis of a specific enquiry for the purpose of carrying out the control functions laid down by law, is not to be regarded as the provision of data to recipients.

DATA PROCESSED BY SITE.PRO

24. Processing of data relating to natural persons or representatives of legal entities for the purposes of the provision of services.
    - 24.1. **Basis for the processing**: the conclusion and performance of the contract.
    - 24.2. **Processed data**: the name, title, personal ID number, language, VAT identification number (if any), telephone number, e-mail, other contact details. The processing may also be extended to other data necessary for the provision of Company services and/or other data provided by the Client or his representative.
    - 24.3. **Period of storage of data**: data shall be processed to the extent necessary to achieve the purposes for which they are processed.
      If their processing is required by the applicable legal acts, some data must be processed for a period laid down by law, but not longer than 10 years after termination of contract.
    - 24.4. **Data sources**: data shall be obtained directly from Data Subjects or their representatives.
    - 24.5. **Data storage locations**: a Client's card with his personal data shall be generated in the database of the Company.
      Data may also be processed by storing them in the form of documents created or received in the course of the provision of services or in the form of e-mail as well on Clients website.
    - 24.6. **Persons (groups of persons) to whom data are transferred**: data shall not be provided to third parties.
      Data may be provided to public authorities at the request of the Client or his representative and on a legitimate ground for the transfer, if this is necessary for the provision of services to the Client or if this is required by the applicable legal acts.
      Undertakings providing IT services to the Company might have access to the databases containing data of Client representatives.
      The Company shall require the processors to process data in accordance with the GDPR and other legal acts applicable in the European Union.

24.7. **Transfer of data to third countries (non-EU/EEC countries)**: personal data shall not be provided to third countries, unless it is necessary for the proper provision of services to the Client. The Company guarantees that if the data is transferred to the third countries, all rules and principles for data security and processing existing in the EU/EEC shall be applied.

24.8. **Processing of special categories of data and data of minors**: the Company does not process data of minors or special categories of data for this purpose.

24.9. **Have data subjects been made aware of the processing and of their rights?** Clients or they representatives are aware that personal data provided by them will be processed by the Company when they agree to the provision of services by the Company. The Policy, which is available on the website of the Company, also provides information to Client representatives of their rights.

25. For direct marketing purposes.

25.1. **Basis for the processing**: consent. In certain cases, personal data may also be processed based on a legitimate interest.

25.2. **Processed data**: the name, position, employer, e-mail, telephone number; other contact details may also be processed.

25.3. **Period of storage of data**: data shall be processed on the basis of consent for a maximum period of 4 years. Before the expiry of a period of 4 years, the Company may request the Data Subject to renew its consent. Once the consent is renewed, data shall be stored for a maximum period of 8 years (in total).
Where the processing is performed on the basis of a legitimate interest of both parties, the processing shall be carried out until such time as the Data Subject refuses such processing.

25.4. **Data sources**: data shall be obtained directly from Data Subjects.

25.5. **Data storage locations**: cards of Data Subjects shall be generated in databases of the Company. Data may also be stored in specialised applications or e-mails.

25.6. **Persons (groups of persons) to whom data are transferred**: data shall not be provided to third parties.
Undertakings providing IT services to the Company might have access to the databases containing data of Data Subjects.
The Company shall require the processors to process data in accordance with the legal acts applicable in the Republic of Lithuania and in the European Union.

25.7. **Transfer of data to third countries (non-EU/EEC countries)**: personal data shall not be provided to third countries.

25.8. **Processing of special categories of data and data of minors**: the Company does not process data of minors or special categories of data for this purpose. Nevertheless, the Company does not check the age of Data Subjects when collecting data for direct marketing purposes, as this would be considered the collection of Superfluous Data.

25.9. **Have data subjects been made aware of the processing and of their rights?** When they agree to the processing of data for direct marketing purposes, Data Subjects are made aware of their rights in the context of the protection of personal data. The Policy, which is available on the website of the Company, also provides information to Data Subjects of their rights.

26. **Cookies and similar technologies.** Cookies are small text files that a website puts on users' computer, phone or other devices, which contains information about the navigation on that website. They are widely used to make websites work, or work more efficiently, as well as to provide information to the owners of the site. The Company might use other similar tools to better understand website users' needs and to optimize their experience on the website.

26.1. **Types of cookies and similar technologies:**

Session cookies allow Data subjects to be recognized for the duration of a session so that any page changes or item selection are remembered. Session cookies are temporary and disappear once the Data subject close browser or leave the website.

Long-term cookies are stored on a Data subject computer for a specified period following the end of the browsing session, and they may record specific user settings or actions when the Data subject returns to the website.

First party cookies are necessary for the conventional functioning of the website.

Third-party cookies operated by other organizations through the Company website. For example, Google Analytics cookies used on the Company website are utilized to analyze the website traffic.

Other tools that alone or in relation with cookies help to analyze user profile and experience (e.g. how much time they spend on which subpages, which links they choose to click, what Data subject do and don't like, etc.) and enable the Company to improve the supply of its services.

26.2. **Basis for the processing**: Consent for analytics cookies or behavioural advertising cookies and tools. In other cases, the legal basis that allows Company to collect personal data is a legitimate interest in letting Data subject navigate on its website, performance of its website and user preferences (language, type of browser, country of origin, etc.).

26.3. **Processed data**: Details of a Data subjects visit to the website including traffic data, geolocation data, logs, etc. and information about Data subject's computer such as an internet connection, IP address, operating system or browser type, etc.

26.4. **Period of storage of data**: The Company might use different types of cookies and similar technologies to improve Data subject experience on its website. Most of them last only during the browsing session but some stay till Data subjects deletes them from its internet browser.

Many browsers allow Data subjects to activate a private browsing option whereby cookies are always deleted after their visit. Depending on each browser, this private navigation may have different names.

Other data collected to record Data subject profile or for analytics purposes can be processed by the Company for up to two years.

26.5. **Data sources**: data shall be obtained directly from Data Subjects during browsing sessions.

26.6. **Data storage locations**: The Company shall keep data obtained from cookies and similar technologies secure in its servers by taking appropriate technical and organizational measures against its unauthorized or unlawful processing and its accidental loss, destruction or damage.

The information generated by the third-party cookies can be transmitted and stored by third parties.

26.7. **Persons (groups of persons) to whom data are transferred**: The information obtained by cookies and similar technologies is used exclusively by the Company, except for those of third parties, which are used and managed by third companies and by the Company for statistical purposes.
Company website may use services of third parties that, on their own, collect information for statistical purposes.
Providers of IT services to the Company shall also have access to the databases containing the personal data. The Company shall require these processors to process data in accordance with the GDPR.

26.8. **Transfer of data to third countries (non-EU/EEC countries):** personal data shall not be provided to third countries.
Third parties such as "Google Inc." also has access to the data collected by using specific cookies but is committed to complying with the privacy standards of the EU and US.

26.9. **Processing of special categories of data and data of minors**: The Company does not process data of special categories of data for this purpose.
The Company does not knowingly collect personal information from minors. If Company learns it has collected or received personal data from a minor, it will instantly delete that information.

26.10. **Have data subjects been made aware of the processing and of their rights?** When they agree to the processing of data, Data Subjects are made aware of their rights in the context of the protection of personal data. The Policy, which is available on the website of the Company, also provides information to Data Subjects of their rights.

27. For internal administrative purposes, the Company may also process other personal data the processing of which is defined in the rules regarding the processing of personal data approved by the Company.

ORGANISATIONAL AND TECHNICAL SAFEGUARDS FOR THE PROTECTION OF PERSONAL DATA

28. The Company shall make maximum efforts to ensure that the organisational and technical safeguards it applies for the protection of data comply with the requirements of the GDPR and other legal acts. In order to protect personal data against accidental or unlawful destruction, alteration, disclosure or any other unlawful processing, the following infrastructural, administrative and telecommunication (electronic) measures shall be taken:
    28.1. Adequate layout and maintenance of technical equipment, maintenance of information systems, network management, security of Internet use and other information technology tools;
    28.2. Strict compliance with the standards laid down by the fire service;
    28.3. Proper organisation of work, and other administrative measures;
    28.4. Implementation of the necessary data security measures;
    28.5. Practical tests shall be carried out for emergency recovery of personal data;
    28.6. Assurance of recovery of data from the last available data backup copy in case of loss of data due to hardware failure, software error or other breach of data integrity;
    28.7. Other necessary measures.

29. Employees who process personal data shall observe the principle of confidentiality and shall be subject to the obligation of secrecy of any information relating to Data Subjects that they came to know in the course of their duties. This obligation shall continue to apply on transfer to another position in the Company or on termination of employment or contractual relationship with the Company.

30. Employees shall process personal data by automatic means only after they have been granted access to the relevant information system. Access to personal data may be granted only to a person who needs personal data for the performance of his functions. Upon termination of employment relationship, access shall be denied to the Employee.

31. Employees shall transfer documents containing personal data only to those Employees who, by virtue of their duties or individual assignments, are authorised to use personal data.

32. When performing processing data of a Data Subject, Employees must prevent any accidental or unlawful processing and must keep the documents in an appropriate and secure manner (avoiding the collection of unnecessary copies containing data of a Data Subject, etc.). Document copies containing data of a Data Subject shall be destroyed in such a way that their contents cannot be reproduced and identified.

33. Without there being any further need, files containing personal data shall not be reproduced digitally, i.e. copies of files shall be created on local computer disks, portable media, cloud storage, etc.

34. The use of secure protocols and/or passwords for the transmission of personal data via external data transmission networks shall be ensured in the Company.

35. The safety control of personal data contained in external data storage media and e-mails and their erasure after their use shall be ensured by transferring them to databases.

36. The Responsible employee shall ensure that appropriate organisational arrangements are in place to achieve the following objectives:
    36.1. Control of the access of unauthorised persons to the premises of the Company by means of a door locking system and a general security alarm system;
    36.2. Protection of the internal computer network of the Company.

37. Employees shall organise their work to limit as far as possible the possibility for other persons to find out personal data undergoing processing. This provision shall be implemented as follows:
    37.1. By making sure that documents containing personal data undergoing processing or a computer allowing to open files containing personal data are not left unattended in such a way that the information contained therein can be read by Employees unauthorised to use specific personal data, trainees or other persons;
    37.2. By keeping documents in such a way that they (or fragments thereof) cannot be read by random persons;
    37.3. Where documents containing personal data are transferred to other Employees, divisions of the Company or authorities by persons who are not authorised to

process personal data or by post or courier, they shall be transferred in a sealed opaque envelope. This provision shall not apply if the said notices are delivered in person and confidentially.

USE OF A PROCESSOR

38. Where the Company authorises the Processor to carry out personal data processing operations, data protection principles, rules and liability clauses shall be set out in the contract for the provision of services or, in the absence thereof, a separate written agreement shall be concluded between the parties on the proper processing of personal data.

39. Agreements on whether to transfer the processing of data of a Data Subject to the Processor shall be adopted by the Company CEO and, failing that, by other Employees of the Company who may act on behalf of the Company in accordance with the rules regarding the processing of personal data approved by the Company.

40. The Company must select the Processor who guarantees the necessary knowledge, reliability and resources to implement and ensure compliance with technical and organisational safeguards for the protection of data, including the technical and organisational safeguards for the protection of data covered by this Policy.

41. When authorising the Processor to process personal data, the Company shall prescribe that the processing of personal data shall be carried out in accordance with the instructions of and rules approved by the Company, and specify the processing operations to be carried out by the Processor. The Company shall also inform the Processor of the duration, nature, type of processing, categories of Data Subjects, the Processor's obligation to erase or return personal data at the end of the provision of services, and other data processing requirements approved by the Company.

42. When concluding a contract with the Processor, the Company must ensure that personal data are processed in a confidential manner and that the Processor obtains the prior written approval of the Company if it intends to involve third parties/sub-processors in the processing.

43. The Responsible employee keep, review and, where necessary, initiate the renewal/amendment/termination of contracts and cooperation with Processors.

FINAL PROVISIONS

44. The Company shall ensure that Employees authorised to process personal data are fully informed about the processing of such data and its rules. The Data Protection Officer shall be responsible for organising and providing adequate information for employees using personal data.

45. The Responsible employee shall be responsible for supervising compliance with the provisions of the policy and for monitoring and periodic updating of the provisions laid down therein.