Based on the Law on Personal Data Protection1 (hereinafter: the Law), the director of House of Win Beograd-Palilula, Vojvode Micka Krstića 1M, Belgrade, registration number: 64957163, tax ID: 110696602, on 01/01/2020, hereby adopts the following:

PRIVACY POLICY

1. INTRODUCTORY PROVISIONS

1.1. By this document (hereinafter: the Privacy Policy), Users are informed about which personal data are collected by the Controller's website located at the internet domain https://houseofwin.net/, the purpose and legal basis of their processing, the data retention period, information about Users' rights, procedures in case of incidents, as well as the User's consent that the website may collect, process, and store their personal data, as further prescribed herein.

1.2. The website uses User data in accordance with this Privacy Policy and undertakes to protect the privacy of all Users, to collect only the necessary and basic data about Users, i.e. data necessary for the operation of the service, provision of services, and informing Users, in accordance with good business practice and for the purpose of providing a quality service, all in accordance with this Privacy Policy.

1.3. The website displayed at the internet address https://houseofwin.net/ (hereinafter: the Website) is owned and controlled by House of Win Beograd-Palilula, Vojvode Micka Krstića 1M, Belgrade, registration number: 64957163, tax ID: 110696602 (hereinafter: the Controller).

1.4. This Privacy Policy has been drafted in accordance with the rules prescribed by the Law, and for all matters not regulated by this Privacy Policy, the provisions of the Law shall apply, whereby, in the event of any inconsistency, the provisions of the Law shall prevail.

2. MEANING OF TERMS

2.1. The terms used in this Privacy Policy shall have the following meanings:

- CONTROLLER – the company referred to in Article 1.3 that processes personal data;
- SERVICES – the services provided by the Controller include market research, public opinion polling, organization of focus groups, chatbot research and communication, digital marketing, neuromarketing, and political marketing;
- USER – a person who accesses the Website and contacts the Controller for the purpose of reviewing the Services and the prices of the Services provided by the Controller;
- LAW – the Law on Personal Data Protection of the Republic of Serbia (Official Gazette of the RS, No. 87 of 13 November 2018) (hereinafter: the Law);

1 ("Official Gazette of the RS", No. 87/2018)

- GDPR – the General Data Protection Regulation of the European Union (2016/679);
- CONSENT – any freely given, specific, informed, and unambiguous indication of the User's wishes by which, through a statement or a clear affirmative action, the User gives consent to the processing of personal data relating to them;
- PERSONAL DATA – any information relating to a natural person whose identity is determined or identifiable, directly or indirectly, in particular on the basis of an identifier such as a name and identification number, location data, identifiers in electronic communication networks, or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity;
- PROCESSING OF PERSONAL DATA – any operation or set of operations which is performed, whether by automated or non-automated means, on the User's personal data, such as collection, recording, classification, grouping, or structuring, storage, adaptation or alteration, disclosure, inspection, use, disclosure by transmission or delivery, duplication, dissemination or otherwise making available, comparison, restriction, erasure, or destruction;

- PROCESSOR – a natural or legal person engaged by the Controller to process the User's personal data on behalf of and for the account of the Controller;
- THIRD PARTY – a natural or legal person, or public authority, other than the User, the Controller, or the Processor, as well as a person authorized to process personal data under the direct supervision of the Controller or Processor;
- COMPETENT AUTHORITIES – public authorities competent for the prevention, investigation, and detection of criminal offences, as well as for the prosecution of offenders or execution of criminal sanctions, including the protection against and prevention of threats to public and national security, as well as any legal person authorized by law to perform the above tasks;
- COMMISSIONER or SUPERVISORY AUTHORITY – an independent public authority established pursuant to the Law, competent for supervising the implementation of the Law and performing other tasks prescribed by the Law.

3. DATA CONTROLLER

3.1. The Controller is the company further defined in Article 2.1, item 1, with contact details as set out in Article 15.

3.2. The company referred to in Article 3.1, in its capacity as Controller, is responsible for the personal data collected from Users, in the manner and to the extent provided by this document and the Law.

3.3. The Controller undertakes the necessary technical, organizational, and staffing measures to ensure that processing is carried out in accordance with the Law and to be able to demonstrate this to Users, taking into account the nature, scope, circumstances, and purpose of processing, as well as the likelihood and severity of risk to the rights and freedoms of Users.

3.4. Information on which employees or other persons engaged by the Controller have access to personal data and who their administrator is shall be contained in the Record of Processing Activities referred to in Article 13.

4. USER DATA COLLECTED AND PROCESSED

4.1. For the purpose of providing services to interested persons, i.e. Users, as well as for compliance with legal obligations, legitimate interests, and reasons of improvement, more efficient and lawful operation of the Controller, or on the basis of the User's consent, as further explained below, the Controller collects and processes Users' personal data.

4.2. The Controller collects and processes the following User data:

- first name;
- last name;
- e-mail address;
- telephone number;
- message content;
- data collected from internet browsers.

4.3. Special categories of personal data

4.3.1. The Controller does not process data revealing racial or ethnic origin, political opinions, philosophical beliefs, nor genetic data, biometric data for the purpose of uniquely identifying a person, or data concerning the sex life or sexual orientation of a natural person.

4.4. Data obtained from the User's internet browser – Cookies.

4.4.1. In order to improve the service on our website and enhance the User's browsing experience, the Controller collects data from the User's internet browser while the User is browsing the website, i.e. Cookies.

5. PURPOSE AND LEGAL BASIS FOR PROCESSING PERSONAL DATA

5.1. The Controller processes the data referred to in Article 4:

- on the basis of the User's consent, which may have a separate form or may be given through a conclusive act in accordance with the Law, within the meaning of Article 12, paragraph 1, item 1 of the Law;
- on other legal grounds prescribed by the Law, according to which the Controller is obliged to collect, store, and process User data.

5.2. The Controller processes the data referred to in Article 4 for the following purposes:

- for the purpose of providing Services to interested persons;
- for the purpose of enabling contact with the Controller in order to provide the necessary information about the Services;
- for other purposes for which the User's consent has been given, unless such consent has been withdrawn in accordance with the Law and this Privacy Policy;
- for other purposes in accordance with the Law.

For each special category of data referred to in Article 4, the purpose and legal basis of processing are determined in the Record of Processing Activities referred to in Article 13.

5.3. Processing for other purposes

5.3.1. If processing for a purpose other than the purpose for which the data were collected is not based on the law or on the consent of the data subject, the Controller, while observing adequate security measures, shall assess whether such other purpose of processing is compatible with the purpose of processing for which the data were collected, taking into account in particular:

- whether there is a link between the purpose for which the data were collected and the other intended purpose of processing;
- the circumstances in which the data were collected, including the relationship between the Controller and the User;
- the nature of the data;
- the possible consequences of further processing for the User.

5.4. Through the continuous application of appropriate technical, organizational, and staffing measures, the Controller shall ensure that only those personal data which are necessary for achieving each individual purpose of processing are always processed. This applies to the number of data collected, the scope of their processing, the retention period, and their availability.

6. CONSENT TO THE PROCESSING OF PERSONAL DATA

6.1. Consent given by the User shall be provided in a separate form, which may also be electronic, with a clear and prominent title "Consent" or another title, provided that the form unequivocally indicates that it is consent, and that its content is described in an informed, transparent, understandable, and accessible manner, using clear and simple language, in the manner prescribed by the Law.

6.2. The User shall not be conditioned into giving consent in order to be provided with a service or part of a service for which consent is not necessary for that service to be performed, and such consent shall therefore be considered voluntary, unless, without the processing for which consent is requested, it is not possible to enable the User to exercise their right.

6.3. The User has the right to withdraw consent at any time. Withdrawal of consent shall not affect the lawfulness of processing carried out on the basis of consent prior to its withdrawal. Before giving consent, the data subject must be informed of the right to withdraw consent, as well as the effect of such withdrawal. Withdrawal of consent must be as simple as giving consent.

7. WHAT RIGHTS DOES THE USER HAVE IN RELATION TO PERSONAL DATA PROTECTION

7.1. Right to be informed and right of access to information:

7.1.1. The Controller is obliged, in a concise, transparent, intelligible, and easily accessible manner, using clear and simple language, at the User's request, to provide the User with the following information about:

- the identity and contact details of the Controller and of the employee or other person engaged by the Controller who is responsible for processing;
- the purpose of the intended processing and the legal basis for processing;
- the existence of the legitimate interest of the Controller or a third party, where processing is based on legitimate interest;
- the recipient or categories of recipients of the personal data, if any;
- the fact that the Controller intends to transfer personal data to another state or international organization;
- the retention period of personal data or, if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the Controller access to, rectification or erasure of their personal data, as well as the right to restriction of processing, the right to object, and the right to data portability;
- the existence of the right to withdraw consent at any time and the fact that such withdrawal does not affect the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with the Commissioner;
- whether the provision of personal data is a statutory or contractual obligation or a necessary requirement for entering into a contract, and whether the data subject is obliged to provide their personal data and the possible consequences if such data are not provided;
- the existence of automated decision-making, including profiling, if the Controller carries out such processing.

7.1.2. In response to a request referred to in Article 7.1.1, the Controller must reply within 30 days, provided that this period may be extended by an additional 60 days if necessary, taking into account the complexity and number of requests. The Controller is obliged to inform the User of the extension and the reasons for the extension within 30 days from receipt of the request, and if the User submitted the request electronically, the information must be provided electronically if possible.

7.2. Right to rectification and completion

7.2.1. The User has the right to have inaccurate personal data rectified without undue delay, where possible. Depending on the purpose of processing, the User has the right to have incomplete personal data completed, including by providing an additional statement.

7.2.2. If rectification can be carried out by correction, deletion, and entry of different data by the User, the User shall perform the rectification referred to in Article 7.2.1 independently.

7.2.3. If the User is unable to make the rectification and completion in the manner referred to in Article 7.2.2, the User shall submit a request to the Controller.

7.3. Right to erasure

7.3.1. If the legal conditions are met, the Controller is obliged, at the User's request and without undue delay, to erase the personal data referred to in Article 4 in the following cases:

- the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
- the User has withdrawn the consent on which the processing was based, in accordance with the Law, and there is no other legal basis for processing;

- the User has objected to processing in accordance with the Law, and there is no other legal basis for processing which overrides the legitimate interest, rights, or freedoms of the data subject;
- the personal data have been unlawfully processed;
- the personal data must be erased in order to comply with the legal obligations of the Controller;
- the personal data were collected in connection with the use of information society services within the meaning of the Law.

7.4. Right to restriction of processing

7.4.1. Users have the right to request from the Controller the restriction of processing of data relating to them if the processing is unlawful, if the accuracy of the data is contested, if an objection to processing has been submitted in accordance with the Law, as well as for other reasons prescribed by law.

7.5. Right to object

7.5.1. Depending on the specific case, and if the User considers it justified, the User has the right at any time to object to the Controller regarding the processing of their personal data carried out on the basis of consent, and the Controller is obliged to stop processing the data of the User who has submitted the objection.

7.5.2. The Controller is not obliged to stop the processing in the manner referred to in Article 7.5.1 if it has shown the User that there are legal grounds for processing which override the interests, rights, or freedoms of that User, or if the processing is related to the submission, exercise, or defense of legal claims.

8. WHERE AND HOW USERS' PERSONAL DATA ARE STORED

8.1. In electronic form, the data referred to in Article 4.2 are stored on the server of mCloud d.o.o., located in Belgrade, in a TIER 3 data center and protected by CXS and Patchman. They are also protected by cPanel SSL certificates held by the provider mCloud d.o.o. Belgrade.

8.2. Information on the storage location for each individual data item is recorded in the Record of Processing Activities referred to in Article 13.

8.3. In the event of a change in the storage location referred to in Article 8.1, the Controller shall amend and supplement the Privacy Policy, which will be posted on the platform.

9. ACCESS TO DATA BY THIRD PARTIES / PROCESSORS OF PERSONAL DATA

9.1. For the purpose of providing services, carrying out payment transactions, complying with legal obligations, maintaining the service, and improving its operation, the Controller is authorized to use the services of accounting agencies, programmers, IT consultants, and other external and internal associates, for whose work and results it shall be responsible in accordance with the law.

9.2. Processors for each specific data item are designated in the Record of Processing Activities referred to in Article 13.

9.3. The Controller guarantees that the Processor shall apply the necessary technical, organizational, and staffing measures so that processing is carried out in accordance with the Law and adequate protection of Users' personal data is ensured.

9.4. For the purpose of ensuring the conditions set out in Article 9.3, the Controller and the Processor may conclude a data processing agreement, which shall form an integral or accompanying part of the basic agreement and which shall, among other things, contain all the necessary elements prescribed by the Law.

10. DATA SECURITY

10.1. When assessing the required level of established security of personal data, the Controller takes into account and monitors the level of technological development and the costs of implementation, as well as the nature, scope, circumstances, and purpose of data processing, and on the basis of these parameters assesses the probability of risk occurring, i.e. the potential level of risk to Users' rights and freedoms.

10.2. In relation to the circumstances referred to in Article 10.1, the Controller implements appropriate technical, organizational, and staffing measures in order to achieve the required level of organizational security in relation to the risk.

10.3. When sending data to Processors, the Controller is obliged to ensure a secure communication channel through which the data travel, as well as to make sure that the data are securely stored with appropriate security standards in place.

10.4. In electronic form, data are protected on the server of mCloud d.o.o., located in Belgrade in a TIER 3 data center and protected by CXS and Patchman. They are also protected by cPanel SSL certificates held by the provider mCloud d.o.o. Belgrade.

10.5. A description of the organizational and technical security for each individual data item referred to in Article 4 is contained in the Record of Processing Activities referred to in Article 13.

11. PROCEDURE IN THE EVENT OF A PERSONAL DATA SECURITY BREACH

11.1. If the data referred to in Article 4, or the security measures referred to in Article 10, are compromised, the Controller shall take all necessary notification and protection measures prescribed by the Law, including notifying the competent Supervisory Authority, as well as Users if the conditions under this Privacy Policy and the Law are met.

11.2. In the event of a data breach, the Controller is obliged to notify the Supervisory Authority of a personal data protection breach that may create a risk to Users' rights without undue delay, and no later than within 72 hours from becoming aware of the breach. If this deadline is not met, the Controller shall explain the reasons for the delay.

11.3. The Controller's notification to the Supervisory Authority referred to in Article 11.2 must contain at least the following information:

- a description of the nature of the personal data protection breach, including the categories of data and the approximate number of Users to whom the data of those categories relate, as well as the approximate number of personal data records whose security has been breached;
- the name and contact details of the person from whom information about the breach may be obtained;
- a description of the possible consequences of the breach;
- a description of the measures that the Controller has taken or whose taking has been proposed in relation to the breach, including measures taken to mitigate the harmful consequences.

11.4. In the event of a breach of the right to personal data protection, the Controller is obliged to notify Users of a personal data breach that may create a risk to the rights and freedoms of natural persons.

11.5. The notification to the User referred to in Article 11.4 must clearly and understandably describe the nature of the data and provide the information referred to in Article 11.3.

11.6. The Controller is not obliged to notify Users in the situation referred to in Article 11.4 if:

- it has taken appropriate technical and organizational measures of protection in relation to the personal data whose security has been breached;
- it has subsequently taken measures ensuring that the personal data breach with a high risk to the rights and freedoms of the data subject can no longer produce consequences for that person;

- notifying the data subject would require a disproportionate expenditure of time and resources, in which case the Controller is obliged to ensure that the data subject is notified by means of public notification or another effective manner.

12. DATA RETENTION PERIOD AND ERASURE

12.1. The data referred to in Article 4 are retained in accordance with the information available in the record of processing of Users' personal data referred to in Article 13, as a separate document maintained and updated by the Controller.

12.2. The data referred to in Article 4 shall be retained for as long as necessary to fulfill the purpose for which they are processed.

12.3. Data regarding the retention period of cookies are stored in accordance with the Cookie Policy.

13. RECORD OF PROCESSING ACTIVITIES OF USERS' PERSONAL DATA MAINTAINED BY THE CONTROLLER

13.1. The Controller maintains a record of the processing activities concerning Users' personal data referred to in Article 4 of this Privacy Policy.

13.2. In addition to the name and business details of the Controller, the record consists of the following information: categories of persons whose data are processed, categories of personal data, purpose of processing, third parties to whom the data have been disclosed, retention period of the data, description of protection measures, and the form in which the data are stored.

13.3. The record referred to in Article 13.1 is kept in electronic form and stored permanently, in accordance with the Law.

14. COMMISSIONER / SUPERVISORY AUTHORITY

14.1. The supervisory authority for personal data protection in the Republic of Serbia is the Commissioner for Information of Public Importance and Personal Data Protection of the Republic of Serbia. The authority may be contacted at Bulevar kralja Aleksandra 15, 11000 Belgrade, Republic of Serbia, by e-mail at office@poverenik.rs or by telephone at +381 11 3408 900.

14.2. The Controller cooperates with the Commissioner in the exercise of its powers, in accordance with the obligations prescribed by the Law.

15. CONTROLLER CONTACT DETAILS

15.1. If interpretation of the provisions of the Privacy Policy is required, if the User wishes to exercise the rights referred to in Article 4, or for other issues prescribed by the Law, Users may contact the Controller using the following contact details:

- Business name of the Controller: House of Win Beograd-Palilula, registration number: 64957163, tax ID: 110696602;
- Address: Vojvode Micka Krstića 1M, Belgrade;
- Controller's e-mail: info@houseofwin.net;
- Controller's contact telephone: 0643987291;
- Working hours:
  - on working days: 08:00–20:00
  - on Saturdays: 08:00–20:00
  - on Sundays: 08:00–20:00

16. FINAL PROVISIONS

16.1. By giving consent to use the services, the User confirms that they accept the Privacy Policy, that they have read and understood it, and that they agree with the legal bases and purposes of data processing as prescribed by this document.

16.2. All changes to the Privacy Policy shall be publicly available in the place designated for that purpose on the Controller's website, and Users shall be informed through the same means of communication in such a way that they are enabled to read the new document.

17. APPLICABLE LAW AND JURISDICTION

17.1. The substantive law applicable to the processing of Users' personal data, in relation to processing carried out by the Controller, shall be the law of the Republic of Serbia, the Law on Personal Data Protection, as well as the GDPR where applicable.

17.2. For administrative and judicial proceedings, the competent authorities and courts of the Republic of Serbia shall have territorial jurisdiction in accordance with the positive legislation of that state.

In Belgrade,

01/01/2020

For the Controller:

PREDRAG SPASOJEVIĆ PR

HOUSE OF WIN