WOICE d.o.o.
DATA PROCESSING ADDENDUM TO THE GENERAL TERMS AND CONDITIONS

February 2025

INITIALLY

F i r s t l y: WOICE, razvoj digitalnih produktov, svetovanje in prodaja, d.o.o., Ulica škofa Maksimilijana Držečnika 6, 2000 Maribor, matična številka: 8610061000, davčna številka: SI 42243017 ("**Processor**") provides a subscription software as a service product for a/b testing and split testing ("**Services**") to its users ("**Controller**"), whereby the said Services may require the Processor to process Personal Data on behalf of the Controller. This Data Processing Addendum ("**Addendum**") establishes a framework to govern the rights and obligations of the Controller and the Processor in relation to the processing of personal data. Parties will process personal data ("**Personal Data**") when performing their obligations under Principal Agreement, whereas Controller shall provide Personal Data to Processor for further processing;

S e c o n d l y: This Addendum sets out the additional terms, requirements, and conditions under which the Processor will process Personal Data in the provision of the Services in accordance with the Processor's general terms and conditions ("**Principal Agreement**"). This Addendum supplements the Parties' Principal Agreement, which shall form an integral part of Principal Agreement.

T h i r d l y: This Addendum contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation (EU) 2016/679 for contracts concluded between controllers and processors and other data protection legislation requirements ("**Data Protection Laws**").

Agreed terms

1. PROCESSING OF PERSONAL DATA

1.1 Processor undertakes:

(a) to comply with the applicable provisions of this Agreement and the Data Protection Laws when processing Personal Data; and

(b) not to process Personal Data otherwise than in accordance with the documented instructions of the Controller ("**Permitted Purpose**").

1.2 The Processor will not retain, use, disclose or otherwise process Personal Data obtained in the course of the provision of the Services for any purpose other than for Permitted Purposes or where otherwise required by Data Protection Laws.

2. INFORMATION ON PROCESSING OF PERSONAL DATA

2.1 **Purpose of processing Personal Data.** The Processor processes Personal Data for the following purposes:

(a) providing you the Services in accordance with Principal Agreement;

(b) for the purposes of order placing and payment;

(c) to manage your account and your requests;

(d) to manage our relationship with you (through support, newsletters, marketing e-mails etc);

(e) to administer and protect our business (including troubleshooting data analysis, testing, system maintenance, support, reporting and hosting of Personal Data);

(f) to deliver relevant content on our website.

2.2 **Categories of Personal Data.** The processing of Personal Data by the Processor includes the following categories of Personal Data:

(a) **Identity Personal Data** (such as your first and last name);

(b) **Contact Data** (includes your e-mail address);

(c) **Payment details** (such as cardholder name, billing address, country of residence, billing e-mail; if the user is a legal entity we process Personal Data, such as company's legal name or tax ID number, billing address, country of residence, e-mail address).

1.2 **Categories of Data Subjects.** The Processor processes Personal Data of the following categories of Data Subjects:

(a) Flowout customers;

(b) Newsletter Signups.

1.2 **Retention period of Personal Data.** The processing of Personal Data by the Processor on behalf and for the account of the Controller shall start with the date of commencement of Principal Agreement and will continue as long as you have a registered user account on our Website or as long as you use our Services (have a valid subscription to one of our available subscription plans). If we keep any of your Personal Data for longer, we keep it for a maximum of 5 years, as required by tax regulation.

1.3 **Technical and Security Measures.** The Processor undertakes to implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data and against accidental or unlawful loss, destruction, alteration, such as:

(a) Access Control

- Establish user access levels based on job responsibilities.
- Regularly review and update user access rights.
- Implement Two-Factor Authentication (2FA) for access to all critical systems, including but not limited to Google Workspaces, Slack, Asana, and other sensitive platforms.
- Utilize 1Password as the designated password sharing platform to securely manage and share credentials.

(b) Data Encryption

- All sensitive information transmitted over the network, including data within Google Workspaces, Slack, Asana, and other platforms, is encrypted

to protect against unauthorized access, shared only within the organization (or at times with trusted partners), all accounts with access should have Two-Factor Authentication (2FA) enabled.

(c) Password Policy

- Enforce strong password requirements.
- Regularly update and change passwords.
- Implement Two-Factor Authentication (2FA) for access to Google Workspaces, Slack, Asana, and other sensitive systems.
- Utilize 1Password to ensure secure password management and sharing practices.

(d) Security Awareness Training

- Mandate periodic training for all employees, including specific guidance on the secure use of Google Workspaces, Slack, Asana, and other collaboration tools, as well as best practices for password management with 1Password.

(e) Bring Your Own Device (BYOD) Policy

- If employees use personal devices to access Google Workspaces, Slack, Asana, or other organizational systems, provide guidelines for secure usage and mandate 2FA.

2. Processor Personnel

2.1 The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of the Processor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of Terms and Conditions, and to comply with Data Protection Laws in the context of that individual's duties to the Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

2.2 At the request of the Controller, the Processor will demonstrate that the persons under the control of the Data Processor are subject to the confidentiality requirements as stated in point 3.1 and have access to the Personal Data only when the access to the Personal Data is strictly necessary.

3. Security of Processing

3.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of data processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Data Processor shall in relation to the Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

3.2 In assessing the appropriate level of security, Data Processor shall take account in particular of the risks that are presented by data processing, in particular from a Personal Data breach.

4. SUB-PROCESSING

4.1 Data Processor shall not appoint (or disclose) any Personal Data to any sub-processor unless required or written authorized by the Controller.

4.2 The Processor will make any request for approval to use the services of a sub-processor(s) at least 30 days before the use of the services of the sub-processor(s) concerned.

4.3 The Processor requires its Sub-processors to satisfy equivalent obligations as those required from the Processor, as set forth in this Addendum. Authorised Sub-processors are listed below:

(a) **Google Analytics.** We use Google Analytics to monitor your behaviour and patterns when you engage with our Website. This feature helps us to track our Website's traffic, helps us with information who visits our site and our users and visitors browsing behaviours, so that we can manage and adapt the Website.

(b) **Vercel.** We use Vercel to launch and maintain a fast and responsive Website. It helps us deliver a top-notch user experience, optimize performance and scalability so that Website load quickly and run smoothly, even when traffic of our users and visitors is high.

(c) **Neon.tech**. We use Neon.tech to host our database and database data, as well as serve it to our back-end.

4.4 Where the Processor appoint another sub-processor to carry out specific processing activities on behalf of the Controller, that sub-processor shall be subject to the same data protection obligations as set out in this Addendum, in particular to provide sufficient guarantees for the implementation of appropriate technical and organisational measures in such a way that the processing will comply with the requirements set out in this Addendum and Data Protection Laws.

4.5 Data Processor shall be responsible for requiring that the sub-processor complies at least with the obligations applicable to the Processor under this Addendum and Data Protection Laws.

5. DATA SUBJECT RIGHTS

5.1 Taking into account the nature of the Personal Data processing, Data Processor shall assist Data Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Data Controller obligations, as reasonably understood by Data Controller, to respond, to requests and to exercise data subject rights under the Data Protection Laws.

5.2 Processor shall:

(a) promptly notify the Controller if it receives a request from a data subject under any Data Protection Laws in respect of Personal Data, including requests by a data subject to exercise rights in Chapter III GDPR, and shall provide full details of that request; and

(b) ensure that it does not respond to that request except on the documented instructions of the Controller or as required by Data Protection Laws to which the Processor is subject.

6. Personal Data breach

6.1 The Processor shall notify the Controller without undue delay upon the Processor becoming aware of a Personal Data breach affecting Personal Data, providing the Controller with sufficient information to allow the Controller to meet any obligations to report or inform data subjects of the Personal Data breach under the Data Protection Laws.

6.2 The Processor shall reasonably cooperate with the Controller and take reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation, and remediation of each such Personal Data breach.

6.3 The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments, and prior consultations with supervising authorities or other competent data privacy authorities, which the Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Laws, in each case solely in relation to processing of Personal Data.

7. Deletion or return of Personal Data

7.1 Upon termination of a Principal Agreement that involves the processing of Personal Data, the Processor shall, within 10 business days of the date of cessation of any services involving the processing of Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those Personal Data.

8. Audit rights

8.1 The Processor shall make available to the Controller on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by the Controller or an auditor mandated by the Controller in relation to the data processing of the Personal Data.

8.2 Information and audit rights of the Controller only arise under the previous section to the extent that this Addendum does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Laws.

9. Data Transfer

9.1 The Processor may not transfer or authorize the transfer of Personal Data to countries outside the EU and/or the European Economic Area ("**EEA**") without the prior written consent of the Controller.

9.2 If Personal Data processed under this Addendum is transferred from a country within the EEA to a country outside the EEA, the Parties shall ensure that the Personal Data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses or any other mechanism or safety measure by which the transfer of Personal Data shall be in accordance with Data Protection Laws.

10. Final Provisions

10.1 **Validity**. This Addendum shall remain in effect for as long as the Principal Agreement between the Controller and the Processor are in effect.

10.2 **Applicable Law**. This Addendum shall be governed by the law of the Republic of Slovenia.

10.3 **Jurisdiction**. Disputes arising out of or relating to this Addendum shall be resolved amicably. If this is not possible, disputes shall be resolved by a court of competent jurisdiction in Ljubljana.

In Ljubljana, 9. 8. 2024

WOICE d.o.o.