Data Processing Agreement (DPA)

concluded in accordance with Article 28 of the Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter the "**GDPR**")

between the parties:

Controller: The Client who has concluded the Master Services Agreement and accepted the Provider's General Terms and Conditions (hereinafter referred to as the "**Controller**" or "**Client**")

and

Processor: Sited, s.r.o. Registered office: Jakuba Kraya 2411/20, 060 01 Kežmarok, Slovak Republic Company ID (IČO): 50543709 Registered in the Commercial Register of the District Court Prešov, Section: Sro, Insert No.: 37977/P (hereinafter referred to as the "**Processor**" or "**Provider**")

(the Controller and the Processor hereinafter collectively referred to as the "**Parties**")

Preamble

This Data Processing Agreement (hereinafter the "**DPA**") forms an integral part of the General Terms and Conditions (hereinafter the "**GTC**") and the Master Services Agreement (hereinafter the "**MSA**") concluded between the Parties. By accepting the GTC and concluding the MSA the Client becomes the Controller and the Provider becomes the Processor within the meaning of this DPA.

Article I.

Subject Matter and Purpose of the Processing

1. The Processor undertakes to process personal data for the Controller to the extent and under the conditions set out in this DPA.
2. **Subject-matter of the processing:** The provision of the Nugis Service in accordance with the MSA, which mainly includes the storage, management, and making available of personal data collected through the interactive content created by the Controller.
3. **Purpose of the processing:** The processing is carried out exclusively for the purposes determined by the Controller in relation to its Respondents (e.g., marketing, market research, lead generation). The Processor does not process personal data for its own purposes.
4. **Duration of the processing:** The processing of personal data shall take place for the duration of the MSA.

Article II.

Nature and Scope of the Data Processed

1. **Categories of data subjects:** Respondents – end-users who interact with the content created by the Controller (e.g., visitors to the Controller's website).
2. **Scope and type of personal data:** The scope and type of personal data processed are entirely at the discretion and under the responsibility of the Controller. It may include common personal data (e.g., name, surname, email, phone number, age, address, preferences) and, subject to legal conditions, special categories of personal data within the meaning of Article 9 of the GDPR.

Article III.

Rights and Obligations of the Processor

1. The Processor is entitled to process personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country, unless required to do so by Union or Member State law.
2. The Processor shall ensure that persons authorised to process the personal data have committed themselves to confidentiality.
3. The Processor shall take all measures required pursuant to Article 32 of the GDPR, which are further specified in **Annex No. 1** to this DPA (Technical and Organisational Measures).
4. The Processor shall respect the conditions for engaging another processor referred to in Article V of this DPA.
5. The Processor shall, taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights.
6. The Processor shall assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR.
7. At the choice of the Controller, the Processor shall delete or return all the personal data to the Controller after the end of the provision of the Service, and delete existing copies unless Union or Member State law requires storage of the personal data.
8. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the Controller.

Article IV.

Rights and Obligations of the Controller

1. The Controller is fully responsible for the lawfulness of the processing of personal data provided to the Processor for processing.

2. The Controller is responsible for ensuring a valid legal basis for the processing of Respondents' personal data and for fulfilling the information obligation towards them.
3. The Controller provides instructions to the Processor for the processing of personal data through the use of the Service and this DPA. Any further instructions must be in writing.
4. The Controller is obliged to promptly inform the Processor of any facts that could affect the performance of the obligations under this DPA.

Article V.

Sub-processors

1. The Controller grants the Processor a general authorisation for the engagement of other processors (sub-processors) in the processing operations.
2. The Processor undertakes to inform the Controller of any intended changes concerning the addition or replacement of other sub-processors, thereby giving the Controller the opportunity to object to such changes.
3. A list of the currently used categories of sub-processors is provided in the Processor's Privacy Policy.
4. Where the Processor engages another sub-processor, it shall impose on that other processor the same data protection obligations as set out in this DPA by way of a contract.

Article VI.

Final Provisions

1. This DPA is concluded for the duration of the MSA.
2. This DPA supersedes any prior agreements between the Parties regarding the processing of personal data.
3. In the event of a conflict between the provisions of the MSA and this DPA, the provisions of this DPA shall prevail.
4. This DPA shall enter into force and effect on the date of conclusion of the MSA.

Annex No. 1 to the DPA – Technical and Organisational Measures

The Processor undertakes to maintain and apply the following technical and organisational measures to ensure a level of security appropriate to the processing of personal data:

1. **Confidentiality (Article 32(1)(b) GDPR):**
    - **Access Control:** Access to systems processing personal data is protected by passwords and/or other authentication mechanisms. Rights are assigned based on the principle of least privilege ("need-to-know").
    - **Encryption:** All communication between the client (browser) and the Processor's servers is encrypted using the TLS protocol. Databases containing personal data are encrypted at rest.

- **Confidentiality Obligation:** The Processor's employees and contractors with access to personal data are bound by a duty of confidentiality.

2. **Integrity (Article 32(1)(b) GDPR):**
   - **Logging:** Access and significant changes in the systems are recorded in logs for the purpose of traceability and detection of unauthorised activities.
   - **Malicious Code Protection:** Deployment of antivirus and antimalware solutions on servers and endpoints.
3. **Availability and Resilience (Article 32(1)(b) and (c) GDPR):**
   - **Backup:** Regular automated data backups with recovery testing to ensure the ability to restore the availability and access to personal data in a timely manner in the event of an incident.
   - **Redundancy:** Use of cloud provider services with high availability and geographical infrastructure redundancy.
4. **Processes for Regular Testing and Evaluation (Article 32(1)(d) GDPR):**
   - **Vulnerability Management:** Regular scanning of the infrastructure for vulnerabilities and timely application of security patches.
   - **Incident Response:** An established process for handling and reporting security incidents in accordance with GDPR requirements.