DATA PROCESSING AGREEMENT

This DataForApps Data Processing Agreement (the '**DPA**') forms part of the DataForApps Terms of Service (the '**Terms**'), the agreement between Client (hereinafter '**Client'**, '**you**') and DataForApps (hereinafter '**Company**', **'DataForApps'**, '**we**', '**us**', or '**our**'), which is owned and operated by DataForSEO OU, company №14502291, registered in the Republic of Estonia. This Agreement is governing the processing of personal data that Client uploads or otherwise provides us in connection with the services and/or the processing of any personal data that DataForApps provides to Client on their behalf in connection with the performance of services, hereinafter referred to individually as a '**Party**' or together as the '**Parties**'.

1. Definitions

"**Standard Contractual Clauses (SCC)**" means Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj.

"**General Data Protection Regulation (GDPR)**" means 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, and repealing Directive 95/46/EC.

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

"**Service Data**" means Personal Data that the Company transfers or otherwise provides to Client on his/her behalf in connection with the performance of SEO services via the Company's API with respect to which Client is a data controller and DataForApps is a data processor.

"**Other Data Protection Laws and Regulations**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states applicable to the processing of Personal Data under the Terms as amended from time to time, other than the GDPR.

"**Public Authority**" means a government agency or law enforcement authority, including judicial authorities.

"**Supervisory Authority**" means an independent public authority to be responsible for monitoring the application of the data protection legislation.

2. Roles and Responsibilities

If GDPR applies to your processing of Service Data, you acknowledge and agree that with regard to the processing of Service Data, you are a controller and we are a processor (as defined by the GDPR) acting on your behalf, as further described in the Standard Contractual Clauses agreed under this DPA (the '**Clauses'**) and Appendix I with corresponding Annexes.

3. Instructions

The Parties agree that this DPA and the Terms constitute your complete and final documented instructions regarding our processing of Service Data on your behalf (the '**Instructions**'). Any additional or alternate instructions must be consistent with the terms and conditions of this DPA and the Terms.

4. Your Obligations

Within the scope of the DPA and Terms and your use of the Services, you will be solely responsible for complying with all requirements that apply to you under the GDPR and Other Data Protection Laws and Regulations. You represent and warrant that you will be solely responsible for:

(i) the accuracy, quality, integrity, confidentiality and security of collected Service Data;

(ii) complying with all necessary transparency, lawfulness, fairness and other requirements under GDPR and Other Data Protection Laws and Regulations for the collection and use of the personal data by:

- establishing and maintaining the procedure for the exercise of the rights of the Data Subjects whose Service Data are processed on your behalf;
- ensuring compliance with the provisions of this DPA and Terms by its personnel or by any third-party accessing or using Service Data on your behalf.

(iii) implementing and maintaining appropriate technical and organisational measures to protect Service Data from personal data breaches (the '**Security Incidents**'), in accordance with security standards set out in Annex II to this DPA;

(iv) ensuring that your Instructions to us regarding the processing of Service Data comply with the GDPR and Other Data Protection Laws and Regulations, including complying with principles of data minimisation, purpose and storage limitation; and

(v) complying with all applicable laws, rules, regulations (including GDPR and Other Data Protection Laws and Regulations) in respect to any Instructions you issue to us.

5. Our Obligations

5.1. General Obligations.

With regard to the processing of Personal Data the Company shall:

(i) process Service Data only for the purpose of providing, supporting, and improving our services, using appropriate technical and organisational security measures, and in compliance with the instructions received from Client subject to Sections 3 and 4 of this DPA;

(ii) inform Client if DataForApps cannot comply with its obligations under this DPA, in which case Client may terminate this DPA or take any other reasonable actions, including suspending data processing operations;

(iii) inform Client if, in DataForApps' opinion, a Client's Instruction may be in violation of the provisions of the GDPR or Other Data Protection Laws and Regulations;

(iv) follow Client's instructions regarding the collection of Service Data (including with regard to the provision of notice and exercise of choice), in case DataForApps is obtaining Service Data from Data Subjects on behalf of Client under Terms;

(v) take reasonable steps to ensure that any employee/contractor to whom DataForApps authorises access to Service Data on its behalf comply with respective provisions of the Terms and this DPA.

5.2. Notices to Client.

Upon becoming aware, we shall inform you of any legally binding request for disclosure of Service Data by a Public Authority, unless DataForApps is otherwise forbidden by law to inform the Client, for instance, to preserve the confidentiality of investigation by Public Authority. DataForApps will inform the Client if it becomes aware of any notice, inquiry, or investigation by a Supervisory Authority with respect to the processing of Service Data under this DPA conducted between you and us.

5.3. Security Incident.

Upon becoming aware of a Security Incident, DataForApps shall: (i) notify you without undue delay after we become aware of the Security Incident; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by you; and (iii) promptly take reasonable steps to contain and investigate any Security Incident so that you can notify competent authorities and/or affected Data Subjects of the Security Incident. Our notification of or response to a Security Incident shall not be construed as an acknowledgement by us of any fault or liability regarding the Security Incident.

5.4. Confidentiality.

DataForApps will not access or use, or disclose to any third party, any Service Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with contractual and legal obligations or binding order of a public body (such as a subpoena or court order). We shall ensure that any employee/contractor to whom we authorise access to Service Data on our behalf is subject to appropriate confidentiality contractual or statutory duty obligations with respect to Service Data, including after the end of their respective employment or termination or expiration of contract.

5.5. Reasonable Assistance.

DataForApps agreed to provide reasonable assistance to Client regarding:

(i) any request from a Data Subject in respect of access to or the rectification, erasure, restriction, portability, blocking or deletion of Service Data that DataForApps on behalf of the Client. In the event that a Data Subject sends such a request directly to DataForApps, Section 7 of this DPA shall apply;

(ii) the investigation of Security Incident and communication of necessary notifications regarding such Security Incidents subject to Section 5.3. of this DPA;

(iii) preparation of data protection impact assessments and, where necessary, consultation of Client with the Supervisory Authority under Articles 35 and 36 of the GDPR.

6. Audit and Certification

If a Supervisory Authority requires an audit of the data processing facilities from which DataForApps processes Service Data to ascertain or monitor Client's compliance with GDPR or Other Data Protection Laws and Regulations, DataForApps will cooperate with such audit. The Client is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time DataForApps expends for any such audit, in addition to the rates for services performed by DataForApps.

Client may, prior to the commencement of processing of Service Data, and at regular intervals, thereafter, audit the technical and organisational measures taken by DataForApps. DataForApps may provide Client with all information necessary to demonstrate compliance with its obligations laid down in the Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client with respect to such processing.

DataForApps shall, upon Client’s written request and within a reasonable period, provide Client with all information necessary for such audit, to the extent that such information is within the Company’s control and DataForApps is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

7. Data Subject Request

In the event that a Data Subject contacts us with regard to the exercise of their rights under GDPR and Other Data Protection Laws and Regulations (in particular, requests for access to, rectification or blocking of Client Personal Data), we will use all reasonable efforts to forward such requests to you. If we are legally required to respond to such a request, we shall

immediately notify you and provide you with a copy of the request unless we are legally prohibited from doing so.

8. Transfers of Service Data

The Parties agree to abide by and process Service Data protected by the GDPR in compliance with the Standard Contractual Clauses approved by the European Commission decision 2021/914 of 4 June 2021 in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of natural and legal persons for transfer of personal data specified in the Addendum and Appendixes to this DPA.

ADDENDUM I
Standard Contractual Clauses
(Processor-Controller)

SECTION I

Clause 1. Purpose and Scope

For the purposes of the Clauses:

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter '**entity/ies'**) transferring the personal data, as listed in Annex I.A (hereinafter each '**data exporter**'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each '**data importer'**)

have agreed to these standard contractual clauses (hereinafter: '**Clauses**').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2. Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3. Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1 (b) and Clause 8.3(b);

(iii) *[non-applicable]*;

(iv) *[non-applicable];*

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4. Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5. Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6. Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7. Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8. Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data (7), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9. Use of sub-processors

[NOT APPLICABLE]

Clause 10. Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11. Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

Clause 12. Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13. Supervision

[NOT APPLICABLE]

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14. Local laws and practices affecting compliance with the Clauses

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15. Obligations of the data importer in case of access by public authorities

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests,

type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16. Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data

exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17. Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Estonia.

Clause 18. Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of the Republic of Estonia.

Appendix
Annex I

A. LIST OF PARTIES

Data exporter

Name: Dataforseo OÜ

Address: Vesivärava tn 50-201, Kesklinna linnaosa, Tallinn, Harju maakond, Republic of Estonia, 10152

Contact person's name, position, and contact details: Nick Chernets, the Director, +372 602 7642, info@dataforapps.com

Activities relevant to the data transferred under these Clauses:

- Collection;
- Recording;
- Organisation;
- Structuring;
- Storage;
- Adaptation or alteration;
- Retrieval;
- Consultation;
- Alignment or combination;
- Restriction;
- Erasure or destruction.

Signature and date: By entering into the Terms, data exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the effective date of the agreement.

Role: processor

Data importer

Name: 'Client', 'You'.

Address: the relevant information is contained in the Client's account on the Site and/or DataForApps Platform.

Contact person's name, position and contact details: the relevant information is contained in the Client's account on the Site and/or DataForApps platform.

Activities relevant to the data transferred under these Clauses:

- Collection;
- Recording;
- Organisation;
- Structuring;
- Storage;
- Adaptation or alteration;
- Retrieval;
- Consultation;
- Alignment or combination;
- Restriction;
- Erasure or destruction.

Signature and date: By entering into the Terms, data importer is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the effective date of the agreement.

Role: controller

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred:

Client's customers.

2. Categories of personal data transferred:

Contact information or other personal data, appearing on a search engine results page (SERP).

3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved:

Transferred data will not include social security numbers or other national ID numbers, passwords, security credentials, or sensitive personal information of any kind.

4. The frequency of the transfer:

The personal data is transferred on a continuous basis.

5. Nature of the processing:

Personal data processing consists of the following:

- Collection;
- Recording;
- Organisation;
- Structuring;
- Storage;
- Adaptation or alteration;
- Retrieval;
- Consultation;
- Alignment or combination;
- Restriction;
- Erasure or destruction.

6. Purpose(s) of the data transfer and further processing:

The purpose of this data transfer is to provide data exporter's clients with SEO services via API.

7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The personal data shall be stored for the duration of this DPA concluded between the data importer and the data exporter, unless otherwise agreed in writing or the data importer is required by applicable law to retain some or all the transferred personal data. Data regarding:

- API output will be retained for 31 days for SERP and 7 days for HTML respectively;
- pingback and postback results for will be retained for 6 months;
- client tasks, results, payload will be retained for 12 months.

Annex II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

- The data importer is committed to preserving the confidentiality, integrity, availability and resilience of all the personal data in question throughout the data importer processing activities and ensuring that personal data are protected against loss and destruction by implementing appropriate internal information security procedures.
- The data importer has implemented data pseudonymisation and encryption mechanisms to protect the privacy of data subjects by ensuring the security of personal data.
- The data importer has implemented measures designed to ensure that personal data, in the event of a physical or technical incident, may be restored in a timely manner via any of the available backup technologies.
- The data importer has implemented role-based access control designed to deny unauthorised persons access to processing equipment used for processing of personal data and prevent the use of automated processing systems by unauthorised persons.

- The data importer has implemented measures designed to ensure that the confidentiality and integrity of personal data are protected during transfers of personal data, namely using safe transfer protocols and other means that may ensure the safety of personal data.
- The data importer has implemented measures for the protection of data during storage including the use of reliable cloud solutions.