**ad**page

# DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Schedule 1, (**"DPA"**) is an addendum and forms part of the **General Terms and Conditions of Service AdPage.io** or other written or electronic agreement between **AdPage.io** and **Customer** for the purchase of Server Side Tracking services from AdPage.io (identified either as "Services" or otherwise in the applicable agreement, and hereinafter defined as **"Services"**) (the **"Agreement"**) to reflect the Parties' agreement with regard to the Processing of Personal Data.

The customer enters this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations.

While providing the Services to Customer pursuant to the Agreement, AdPage.io may process Personal Data on behalf of the Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

**HOW TO EXECUTE THIS DPA:**

1. This DPA consists of two parts: the main body of the DPA, Schedule 1 and corresponding annexes.

2. This DPA has been pre-signed on behalf of AdPage.io as a data processor. Annex I has been pre-signed by AdPage.io as the data importer.

3. To complete this DPA, Customer must:

    a. Complete the information in the signature box and sign **on page 5 and 18.**
    b. Sign the document in the AdPage Tagging portal.

**HOW THIS DPA APPLIES**

Except as otherwise expressly provided in the Agreement, this DPA will become legally binding upon receipt by AdPage.io of the validly completed DPA at **support@adpage.io**.

To avoid any doubt, signature of the DPA on page 5 shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses, including Annex II and Annex III.

If the Customer signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, AdPage.io is party to this DPA.

**IT IS AGREED AS FOLLOWS**

**1**  DEFINITIONS AND INTERPRETATION

1.1  In this DPA, the following terms shall have the meanings set out below:

**AdPage.io:** is a trade name of AdPage BV (KVK: 75440482), with its registered address: Velmolenweg 54 A 5404 LD, Uden the Netherlands. Also referred as **"Processor"**

**Agreement:** means written or electronic agreement between AdPage.io and Customer for the purchase of Server Side Tracking services from AdPage.io.

**Clauses:** means Module Two (Controller to Processor Transfers) of the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 as set out in Schedule 1 of this DPA.

**Customer:** means the legal entity or Consumer with whom AdPage.io has entered into a legally binding agreement. Also referred as **"Controller"**.

**Controller:** means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

**Customer Data:** includes all data and information submitted by or for Customer to AdPage.io to provide Services.

**Data Processing Addendum (DPA):** is this data processing addendum, including the Annexes, as amended from time to time.

**Data Protection Laws** means all applicable laws relating to the protection of personal data or privacy which have effect in the European Economic Area and the United Kingdom from time to time, including (but not limited to) EU GDPR, UK GDPR, and the UK Data Protection Act 2018, and any other applicable law relating to data protection of the privacy of individuals.

**EU GDPR** means EU General Data Protection Regulation 2016/679.

**Parties:** Both AdPage.io and Customer.

**Personal Data** means any information relating to an identified or identifiable living individual that is processed by the Processor on behalf of Controller as a result of, or in connection with, the provision of the Services under the Agreement, the details of which are set out in Part B of Annex I to Schedule 1 of this DPA, which may be amended from time to time by mutual agreement between the Parties.

**Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

**Service(s):** All Services made available to Customers via AdPage.io online platform, plugins, third-party websites or any other Service offered by AdPage.io.

1.2  The terms, "**third country**", "**Member State**", "**data subject**", "**personal data breach**", "**processing**" and "**supervisory authority**" shall have the same meaning as in the EU GDPR, and their cognate terms shall be construed accordingly.

1.3  In the case of conflict or ambiguity between:

1.3.1 any provision contained in the body of this DPA and any provision contained in the Schedule 1, the provision in Schedule 1 will prevail; and

1.3.2 any of the provisions of this DPA and the provisions of the body of Agreement, the provisions of this DPA will prevail with respect to the subject matter of this DPA.

**BACKGROUND**

(A) The customer runs a website or web shop and wants to achieve more leads and sales.

(B) AdPage.io is a provider of specialized analytics Server Side Tracking Services, and Customer wishes to procure AdPage.io 's services in relation to correctly measure the results of ads by using Proxy server.

(C) The parties have entered into an Agreement which sets out the legal framework under which AdPage.io will assist Customer and under which AdPage.io has agreed to provide the Services to the Customer.

(D) The Services provided by AdPage.io under the Agreement enable AdPage.io to access and process Personal Data (as defined above) as Processor on behalf of the Customer (who acts as a Controller).

(E) To ensure the secure, correct and lawful processing of Personal Data by AdPage.io on behalf of Customer, the Parties have agreed on the terms and conditions as set forth in this data processing addendum.

**2 ROLE AND OBLIGATIONS OF THE PARTIES**

2.1 Customer and AdPage.io agree and acknowledge that:

2.1.1 for the purposes of the Data Protection Laws, AdPage.io is acting as a Processor on behalf of Customer (who acts as a Controller);

2.1.2 the processing of the Personal Data by AdPage.io shall be governed by the Standard Contractual Clauses (as set out in Schedule 1 of this DPA); and

2.1.3 for the purposes of the Standard Contractual Clauses, Customer is the exporter and the AdPage.io is the importer of the Personal Data;

2.1.4 it is the **responsibility of the Customer to enable pseudonymisation of the personal data**. If pseudonymization is disabled, Adpage cannot guarantee that adequate supplementary measures are in place to ensure essential equivalence to EU levels of protection.

**3 DELETION OR RETURN OF CONTROLLER'S PERSONAL DATA**

3.1 Subject to clause 5.3 (Term and Termination), the obligations of AdPage.io set out in clause 8.5 of the Standard Contractual Clauses shall be completed within 30 days after the end of the provision of the Services under the Agreement.

3.2 AdPage.io may retain Personal Data to the extent required by EU, UK or Member State law and only to the extent and for such period as required by EU, UK or Member State law and always provided that AdPage.io shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only processed as necessary for the purpose(s) specified in the relevant EU, UK or Member State law requiring its storage and for no other purpose.

**4 ASSISTANCE PROVIDED PURSUANT TO SCHEDULE 1**

4.1 AdPage.io shall provide the assistance set out in clauses 8.3, 8.6, and 10 of the Clauses at no extra cost to the Customer.

**5 TERM AND TERMINATION**

5.1 This DPA shall enter into force upon receipt by AdPage.io of the validly completed DPA at email address and shall terminate on the later of:

(i) the date on which the Agreement terminates; or

(ii) the date on which AdPage.io ceases processing Personal Data.

5.2 Any provision of this DPA which expressly or by implication is intended to come into or continue in force on or after termination of this DPA shall remain in full force and effect.

5.3 Termination or expiry of this DPA shall not affect any rights, remedies, obligations, or liabilities of the Parties that have accrued up to the date of termination or expiry, including the right to claim damages in respect of any breach of this DPA which existed at or before the date of termination or expiry.

**6 LIABILITY**

6.1 Subject to clause 6.2, the liability of each Party in relation to all and any claims, losses, proceedings, actions, or regulatory penalties arising under or in connection with this DPA shall be governed by the provisions set out in the Agreement and shall not be modified by this DPA.

6.2 Notwithstanding the foregoing, nothing in this DPA or the Agreement shall limit the liability of either Party in respect of its obligations under the Clauses.

**7 MISCELLANEOUS**

7.1 All notices to a Party under this DPA shall be in writing and sent to its address as set forth in the beginning of this DPA or to such other address as communicated in writing by a Party.

7.2 Any Party's failure to exercise any of its rights pursuant to or in connection with this DPA shall not constitute a waiver of such rights or in any other way prejudice such rights.

7.3 This DPA may be amended only by written agreement between the Parties.

7.4 If any provision of this DPA is declared void or unenforceable by any court or tribunal of competent jurisdiction, the other provisions of this DPA shall remain to be of effect, unless the latter provisions must be deemed to be indissolubly connected with the void or unenforceable provision. In the event that the other provisions remain valid, both Parties shall endeavor to

replace the void or unenforceable provision by a valid provision which reflects the Parties' original intent to the greatest possible extent.

**8   GOVERNING LAW**

8.1  This DPA and any dispute or claim arising out of or in connection with this DPA (including non-contractual disputes or claims) shall be governed by and construed in accordance with the laws of the Netherlands. Each Party irrevocably agrees that the court of Den Bosch in the Netherlands shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this DPA (including non-contractual disputes or claims).

Executed in two (2) original copies, each party acknowledging receipt of one (1) original copy.

Signed by _____          Signed by _____

Name:                                      Name:

Title:                                     Title:

For and on behalf of                       For and on behalf of the **AdPage.io**

**SCHEDULE 1 - STANDARD CONTRACTUAL CLAUSES**

<u>**SECTION I**</u>

*Clause 1*

***Purpose and scope***

(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), 8.9(a), (c), (d) and (e);

    (iii) Clause 9(a), (c), (d) and (e);

    (iv) Clause 12(a), (d) and (f);

    (v) Clause 13;

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

    (vii) Clause 16(e);

    (viii) Clause 18 - Clause 18(a) and (b);.

(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 – Optional*

**Docking clause**

*(omitted)*

### 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 importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b)     The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2     Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

**8.3     Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.4     Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

**8.5      Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

**8.6      Security of processing**

(a)      The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b)      The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c)      In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d)      The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the

competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

**8.7      Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

**8.8      Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i)      the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii)      the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii)      the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv)      the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

**8.9      Documentation and compliance**

(a)      The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b)      The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c)      The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d)      The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e)     The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

## Clause 9

### Use of sub-processors

(a)     The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least [30 days] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b)     Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.8 The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c)     The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d)     The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e)     The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

## Clause 10

### Data subject rights

(a)     The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b)     The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c)    In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

### 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.

(c)    In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(d)    Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i)    lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13; or

  (ii)    refer the dispute to the competent courts within the meaning of Clause 18.

(e)    The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(f)    The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

  The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

### 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.

(a)    The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(b)    Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of

a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(c)     The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(d)     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.

(e)     The Parties agree that if one Party is held liable under paragraph (e), 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.

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

*Clause 13*

**Supervision**

(a)     The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b)     The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

*Clause 14*

***Local laws and practices affecting compliance with the Clauses***

(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***

**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.

(g)     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.

(h)     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 one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Netherlands.

*Clause 18*

***Choice of forum and jurisdiction***

(i)     Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(j)     The Parties agree that those shall be the courts of the Netherlands.

(k)     A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(l)     The Parties agree to submit themselves to the jurisdiction of such courts.

**ANNEX I**

## A. LIST OF PARTIES

**Data exporter(s):**

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: The *receipt* by the exporter of specialised analytics Server Side Tracking services from the importer in relation to correctly measure the results of ads by using Proxy server as set out in further detail in the Agreement between the exporter and the importer.

Signature and date: _____

Role (controller/processor): **Controller**


**Data importer(s):**

Name: AdPage BV

Address: Velmolenweg 54 A 5404 LD, Uden, the Netherlands

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: The *provision* by the importer of specialised analytics Server Side Tracking services to the exporter in relation to correctly measure the results of ads by using Proxy server as set out in further detail in the Agreement between the exporter and the importer.

Signature and date: _____

Role (controller/processor): **Processor**


## B. DESCRIPTION OF TRANSFER

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

Clients, leads and website visitors of the Customer.

2. **Categories of personal data transferred**

The data to be transferred to analyse and measure the results of ads consist of**:**

- Website;

- Link tracking in URL's;

- User identifier;

- IP address;

- Other identifiers (CRM, unique identifier, etc.);

- Other identifying data like e-mail address, first name, last name, phone number; and

- Pseudonymised data.

3. **Sensitive data transferred and applicable restrictions of safeguards**

The Personal Data transferred concern the following special categories of data:

□ personal Data revealing racial or ethnic origin;

□ political opinions;

□ religious or philosophical beliefs;

□ trade-union membership;

□ genetic data;

□ biometric data for the purpose of uniquely identifying a natural person;

□ data concerning health;

□ data concerning a natural person's sex life or sexual orientation.

4. **The frequency of the transfer**

Data Transfer is continuous depending on the use of the Services.

5. **Nature of the processing**

The Personal Data transferred will be subject to the following processing activities:

- Data will be pseudonymised and forwarded to Google Tag Manager Server Side;

- Filtered data will be used to measure ads results.

6.     **Purpose of the data transfer and further processing**

The purpose of the transfer and processing necessary is necessary to perform the services of analysis and measuring of ads results as instructed by Controller.

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

Unless the exporter instructs the importer to return or delete the data at an earlier date, all personal identifiers will be kept up to a maximum of 6 (six) months.

After this period, all personal data will be irreversibly deleted.

8.     **Transfers to (sub-)processors**

The personal data might be transferred to sub-processors.

Full list of authorised sub-processors is provided in Annex III.

**C. COMPETENT SUPERVISORY AUTHORITY**

In accordance with Clause 13, competent supervisory authority is Dutch Data Protection Authority (Autoriteit Persoonsgegevens), 2509 AJ The Hague, Netherlands.

**ANNEX II**

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

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Adpage shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:

- Measures of pseudonymisation and encryption of personal data;
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing.

**If enabled by the Consumer, Adpage will ensure that data is pseudonymised prior to being shared with Google Tag Manager Sever Side.**

Taking into account European Data protection Board (EDPB) *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021*[1] it is considered that pseudonymization is sufficient and effective supplementary measure to ensure security of data when transfer is taking place in third country; if processor first pseudonymizes data it holds, and then transfers it to a third country for analysis, e.g., for purposes of ads tracking.

Previous is justified under four conditions:

1) If data exporter transfers personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group without the use of additional information;
2) That additional information is held exclusively by the data exporter and kept separately in a Member State or in a third country, by an entity trusted by the exporter in the EEA or under a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA;
3) Disclosure or unauthorized use of that additional information is prevented by appropriate technical and organizational safeguards, it is ensured that the data exporter retains sole control of the algorithm or repository that enables re-identification using the additional information; and

---

[1] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, available for download: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en (last accessed 18 February 2023)

4) The controller has established by means of a thorough analysis of the data in question - taking into account any information that the public authorities of the recipient country may be expected to possess and use - that the pseudonymized personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information.

**It is the responsibility of the Controller to take appropriate measures to avoid that the data could be cross-referenced, for example by using other third-party cookies or trackers.**

Sub processor security measures are described in Annex III.

**ANNEX III**

**LIST OF SUB-PROCESSORS**

The exporter has authorised the use of the following sub-processors:

**1) Scaleway**

Registered office: 8 rue de la Ville l'Evêque, 75008 Paris, France

VAT number: FR 35 433115904

Director of publication: Arnaud Brindejonc de Bermingham

Hosted by: SCALEWAY SAS BP 438 75366 PARIS CEDEX 08 FRANCE

Scaleway provides choice to the world of cloud computing, offering customers the ability to choose where their customer's data resides, to choose what architecture works best for their business, and to choose a more responsible way to scale.

Scaleway processes personal data provide the services that AdPage have requested or authorized as an integral part of the contract for the provision of Scaleway's Services entered into between the AdPage and
Scaleway and governs instances when Scaleway processes Personal Data on the AdPage's behalf as a Data Processor within the meaning of the GDPR.

Scaleway Data Processing Addendum can be found here. (last accessed 28 January 2025)

Scaleway General Terms of Services can be found here. (last accessed 28 January 2025)

Scaleway takes all steps required to protect the personal data processed and carefully selects all its partners and service providers who may have to access costumer's data. Data is processed electronically and/or manually and, in both cases, Scaleway ensures an appropriate level of security, protection and confidentiality based on the sensitivity of data, using administrative, technical and physical measures preventing any loss or theft or any unauthorised use, disclosure or alteration of costumer's data.

Scaleway Information Systems Security Policy can be found here. (last accessed 10 January 2023)

Personal data is processed by Scaleway, its subcontractors and partners, to manage the contract and provide the services customers have requested or authorised.

Costumer's data may also be transferred to third parties, providing services or support and advice to Scaleway.

On request, it may also be transferred to the persons and authorities granted access to personal data under applicable laws or regulations or provisions adopted by legally competent authorities.

**AdPage will provide notice of any new sub-processors or changes to the list of sub-processors in Annex III of this DPA and give you the opportunity to object to such changes.**