Data Processing Agreement

1 Preamble

1.1 This Data Processing Agreement ("**DPA**") is an appendix and an integral part of Mopinion's General Terms and Conditions ("**GTC**") that form the basis for the agreement entered into with the Customer. When the Customer renews or purchases a Service, the then-current DPA will apply and will not change during Customer's subscription for that Service, except for changes agreed under Section 16(2) of this DPA.

1.2 This DPA sets out the rights and obligations of the Customer as the data controller ("**Controller**") and Mopinion B.V. ("**Mopinion**") as the data processor ("**Processor**") when processing Personal Data on behalf of the Controller.

1.3 Mopinion B.V. is a member of the Netigate Group. Mopinion may engage other Netigate Group entities as Sub-Processors in the delivery of the Services, subject to the conditions in Section 10 of this DPA.

1.4 This DPA has been designed to ensure the parties' compliance with Article 28(3) of Regulation 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 (General Data Protection Regulation "**GDPR**") as well as national laws supplementing the GDPR and the laws implementing EU Directive 2002/58/EC and any amendments thereto ("**EU Data Protection Laws**").

1.5 The terms used in this DPA, such as "Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as defined in the EU Data Protection Laws.

2 Scope of this DPA

2.1 In the context of the provision of the cloud-based software-as-a-service solution and related consulting services (the "**Services**") in accordance with the GTC, the Processor will be processing Personal Data on behalf of Controller. This

DPA applies to all activities where Processor, Processor's employees or third parties commissioned by Processor in accordance with this DPA, on Controller's behalf get access and/or process, collect, save or use Personal Data for which Controller is responsible, in connection with the provision of the Services.

2.2 This DPA shall take priority over the similar provisions for the processing and handling of Personal Data contained in the GTC or other agreements between the parties.

2.3 Annex 1 is attached to and forms an integral part of this DPA, and contains instructions and details about the processing of Personal Data, including the purpose and nature of the processing, type of Personal Data, categories of Data Subject and duration of the processing.

2.4 This DPA along with appendices shall be retained in writing, including electronically, by both parties.

2.5 This DPA shall not exempt Processor from obligations to which Processor is subject pursuant to the GDPR or other legislation.

3 Duration of this DPA

3.1 This DPA shall apply as long as Processor processes Personal Data on Controller's behalf in connection with the provision of the Services. During this time, this DPA cannot be terminated unless other clauses governing the provision of Personal Data processing services have been agreed between the parties.

3.2 If the provision of Personal Data processing services is terminated, the Personal Data will be deleted or returned to Controller pursuant to Section 15(2) and Annex 1. This DPA is automatically terminated as well.

3.3 The obligations to maintain confidentiality according to Section 6 of this DPA as well as the legal and contractual storage obligations of Processor continue beyond the end of this DPA.

4 Rights and Obligations of Controller

4.1 Controller is responsible for ensuring that the processing of Personal Data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and this DPA.

4.2 Controller has the right and obligation to make decisions about the purposes and means of the processing of Personal Data.

4.3 Controller shall be responsible, among other things, for ensuring that the processing of Personal Data which Processor is instructed to perform has a legal basis.

5 Processor's Responsibility to Act According to Instruction

5.1 Processor shall process Personal Data only on documented instructions from Controller, unless required to do so by Union or Member State law to which Processor is subject. Controller's instructions to Processor are specified in this DPA and in Annex 1. Subsequent instructions can also be given by Controller throughout the duration of the processing of Personal Data, but such instructions shall always be documented and kept in writing, including electronically, in connection with this DPA. Instructions that go beyond the contractually agreed services shall be treated as a request for a change in performance and shall entitle Processor to a reasonable remuneration.

5.2 Processor shall immediately inform Controller if instructions given by Controller, in the opinion of Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5.3 Controller shall immediately inform Processor of changes that affect Processor's obligations according to this DPA. Controller shall inform Processor in case anyone else, either alone or jointly with Controller, is Data Controller(s) of the Personal Data.

5.4 Processor has the right to anonymise Personal Data derived from Controller and store, process and exploit it in an aggregated format, containing no Personal Data for the following purposes: maintaining and improving security, product improvement, create statistical analyses and anonymous benchmarks, and for research and development purposes.

6 Confidentiality

6.1 Processor shall only grant access to the Personal Data being processed on behalf of Controller to persons under Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis (Art. 28(3) GDPR). Access to Personal Data can be withdrawn if access is no longer necessary, and Personal Data shall consequently not be accessible anymore to those persons.

6.2 Processor shall at the request of Controller demonstrate that the concerned persons under Processor's authority are subject to the abovementioned confidentiality.

6.3 Processor undertakes to not disclose information about the processing of Personal Data covered by this DPA or any other information that Processor has received as a result of the provision of Services or this DPA to a third party. This obligation does not apply to information that Processor has been compelled to disclose by law or legal process. Processor undertakes to notify Controller in writing of any injunction of such disclosure that has been issued.

6.4 Processor shall, where applicable, comply with national legislation applicable to classified or confidential information.

6.5 The confidentiality obligations continue to apply after the expiration or termination of the Agreement and this DPA.

7 Security of Processing

7.1 Processor shall implement technical and organisational measures ("TOMs") as required by the EU Data Protection Laws to ensure a level of security according to Article 32 GDPR, to ensure a level of security that is appropriate with regards to the risk and to protect Personal Data being processed from accidental or unlawful destruction, loss or alteration, or unauthorised disclosure of, or access to, the Personal Data being processed. Processor shall take 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. The latest TOMs shall be available on www.netigate.net/legal.

7.2 Depending on the risk assessment, the measures may include the following:

(a) pseudonymisation or encryption of Personal Data;

(b) the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

7.3 To the extent necessary and reasonable, Processor shall assist Controller in ensuring that the obligations under Articles 32–36 of the GDPR are fulfilled, by inter alia providing Controller with information concerning the technical and organisational measures already implemented by Processor pursuant to Article 32 GDPR along with all other information necessary for Controller to comply with Controller's obligation under Article 32 GDPR.

7.4 The technical and organisational measures are subject to technical progress and further development. In this respect, the Processor is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures must not be undercut. Significant changes shall be documented.

8 Assistance to Controller

8.1 Taking into account the nature of the processing, Processor shall assist Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of Controller's obligations to respond to requests for exercising the Data Subject's rights laid down in Articles 12–23 GDPR.

8.2 This entails that Processor shall, insofar as this is possible, assist Controller in Controller's compliance with:

(a) the right to be informed when collecting Personal Data from the Data Subject;

(b) the right to be informed when Personal Data have not been obtained from the Data Subject;

(c) the right of access by the Data Subject;

(d) the right to rectification;

(e) the right to erasure ('the right to be forgotten');

(f) the right to restriction of processing;

(g) notification obligation regarding rectification or erasure of Personal Data or restriction of processing;

(h) the right to data portability;

(i) the right to object;

(j) the right not to be subject to a decision based solely on automated processing, including profiling;

(k) Processor shall promptly notify Controller if it receives a request from a Data Subject under EU Data Protection Laws in respect of Controller Personal Data. Processor shall not respond to such requests except on the documented instructions of Controller or as required by applicable laws to which Processor is subject, in which case Processor shall, to the extent permitted by applicable laws, inform Controller of that legal requirement before Processor responds to the request.

8.3 In addition to Processor's obligation to assist Controller pursuant to Section 7.3, Processor shall furthermore, taking into account the nature of the processing and the information available to Processor, assist Controller in ensuring compliance with:

(a) Controller's obligation to without undue delay after having become aware of it, notify the Personal Data Breach to the competent Supervisory Authority, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons;

(b) Controller's obligation to without undue delay communicate the Personal Data Breach to the Data Subject, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons;

(c) Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data (a data protection impact assessment);

(d) Controller's obligation to consult the competent Supervisory Authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by Controller to mitigate the risk.

9 Notification of Personal Data Breach

9.1 In case of any Personal Data Breach, Processor shall, without undue delay after having become aware of it, notify Controller of the Personal Data Breach to enable Controller to comply with Controller's obligation to notify the Personal

Data Breach to the competent Supervisory Authority, according to Article 33 GDPR.

9.2 In accordance with Section 8.3(a), Processor shall assist Controller in notifying the Personal Data Breach to the competent Supervisory Authority, meaning that the Processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in Controller's notification to the competent Supervisory Authority:

(a) the nature of the Personal Data including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) the likely consequences of the Personal Data Breach;

(c) the measures taken or proposed to be taken by the Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

10 Sub-Processors

10.1 Processor is entitled to engage Sub-Processors provided that Processor ensures that Articles 28(2) and 28(4) of the GDPR are met and that the Sub-Processors provide adequate guarantees to implement appropriate technical and organisational measures to fulfil the requirement of this DPA and the data protection legislation. Processor shall ensure that all Sub-Processors are bound by written agreements which impose corresponding obligations when processing Personal Data on behalf of Controller. Processor shall maintain an up-to-date list of Sub-Processors on www.netigate.net/legal. The Processor shall remain responsible towards Controller for any processing carried out by a Sub-Processor engaged by Processor. The general authorisation granted under this Section includes the engagement of Netigate Group entities as Sub-Processors where operationally required for the delivery of the Services.

10.2 Processor is entitled to engage new Sub-Processors and to replace existing Sub-Processors. In this case, Processor undertakes to verify the new Sub-Processor's capacity and ability to meet its obligations in accordance with the data protection legislation. The Processor shall inform the Controller in text form — e.g. by e-mail — if the Processor intends to engage additional Sub-Processors or to replace Sub-Processors, and shall notify of a new Sub-Processor, which type of data and categories of Data Subjects are being processed and where the Personal Data will be stored. Controller is entitled within fourteen (14) days of the notice to object to the new Sub-Processor in

writing to: dpo@netigate.net. Such objection may only relate to objective grounds relating to the security of the processing under this DPA. If Controller does not object within the given timeframe, the new Sub-Processor shall be deemed accepted. If Controller makes a legitimate objection and Processor does not accept the objection against the Sub-Processor in question, the Processor shall be entitled at its own discretion to either perform the service without the intended change in Sub-Processor, or, if the performance of the service without the intended change is unreasonable for Processor, terminate the Agreement, including this DPA, by giving thirty (30) days written notice from Processor's receipt of Controller's objection.

10.3 Upon request from the Controller, the Processor shall provide Controller with a correct and up-to-date list of the Sub-Processors assigned to process Personal Data on behalf of Controller, and the geographic location of the processing. Processor can fulfil the obligations under this paragraph by referring the Controller to the list maintained on www.netigate.net/legal.

10.4 The Processor will impose equivalent data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processors. The Processor will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause the Processor to breach any of its obligations under this DPA and EU Data Protection Laws.

10.5 Inspections of any Sub-Processor shall be carried out exclusively by the Processor and at most at annual intervals.

11 Inspection and Auditing

11.1 At the request of Controller, Processor shall within reasonable time provide Controller with information regarding the technical and organisational security measures to ensure that the processing complies with the requirements of this DPA and Article 28(3) of the GDPR.

11.2 Controller is entitled to inspect, or to appoint a third party (who must not be a competitor of Processor) to inspect Processor's compliance with the requirements of this DPA, the instructions and the data protection legislation. Processor shall, after thirty (30) days' prior notification, assist Controller (or the third party carrying out the inspection on behalf of Controller) with documentation and with access to premises during normal business hours and without interrupting Processor's operating procedure, in order to verify Processor's compliance with this DPA, the instructions and data protection

legislation. Processor may make the inspection conditional upon the signing of a confidentiality agreement to protect the data of other customers and information about Processor's technical and organisational measures, as well as Processor's business and trade secrets.

11.3 Controller may carry out one inspection per calendar year at no cost. Controller may carry out additional inspections reasonably needed due to suspected (in good faith) DPA breaches, non-conformities or compliance with laws, regulations, or decisions by governmental authorities.

11.4 As an alternative to the provisions of Sections 11.2–11.3, provided that an inspection has not been ordered by a governmental authority, Processor may offer other approaches to inspection, such as inspection by an independent third party, approved codes of conduct within the meaning of Art. 40 GDPR or an approved certification procedure within the meaning of Art. 42 GDPR in order to prove compliance with the obligations under this DPA, the instructions and data protection legislation. The presentation of test certificates or reports by independent bodies (e.g. auditors, legal departments, IT security officers, data protection officers), a coherent data security concept (e.g. ISO 27001) or appropriate certification by an IT security and privacy audit are also recognised as appropriate proofs, if they have been issued within the last twelve (12) months prior to Controller's request and provided that Processor or Processor's Sub-Processor confirms in writing that there have been no material changes in the controls and systems to be audited since the date of issue.

12 Transfers of Personal Data Outside the EU/EEA

In the event that Processor and/or Sub-Processors transfer Personal Data to a location outside of the EU/EEA, Processor and/or Sub-Processor shall ensure that such transfer complies with applicable EU Data Protection Laws. Under the terms of this DPA, such requirements in relation to certain countries will if suitable be fulfilled by entering into the EU's standard contractual clauses for the transfer of Personal Data to Processors established in third countries (Commission Implementing Decision (EU) 2021/914 of 4 June 2021) or other applicable security mechanisms pursuant to sections 44 et seq. GDPR in order to secure the transfer. Processor is required to keep Controller informed of the grounds for transfer.

13 Compensation

Processor shall be entitled to reasonable compensation for all work and all costs that arise due to Controller's instructions for processing if these exceed the features and level of security based on the services that Processor normally

provides to its customers, e.g. in the case that Processor's system and/or Services requires special adjustments or development following special requests from Controller. Processor is not entitled to compensation for costs which arise based on compliance with requirements set out in the GDPR.

14 Liability

14.1 The liability of the parties in connection with this DPA shall be subject to the limitations and exclusions set forth in Article 14 of Mopinion's General Terms and Conditions, or otherwise as agreed between the parties. For the avoidance of doubt, Mopinion's aggregate liability to the Customer for all claims arising under or in connection with this DPA — including claims arising from Personal Data Breaches or failures in Sub-Processor oversight — shall not exceed the total licence fees paid by the Customer to Mopinion in the twelve (12) months immediately preceding the event giving rise to the claim, consistent with Article 14 GTC.

14.2 Nothing in this DPA is intended to limit or exclude any liability that cannot be limited or excluded under applicable data protection laws, including liability towards Data Subjects pursuant to Article 82 GDPR.

14.3 Damages paid to Data Subjects (under GDPR Article 82) or regulatory fines (under GDPR Article 83) or incurred by either party due to the other party's breach of this DPA or applicable EU Data Protection Laws shall be treated as follows: (i) if incurred by Controller due to Processor's breach: considered direct damages and subject to the agreed liability cap, provided Processor's breach is the sole and direct cause; (ii) if incurred by Processor due to Controller's breach: will count toward and reduce Processor's liability under the GTC.

15 Term and Termination, Erasure of Data

15.1 This DPA enters into force and remains effective for as long as Processor processes Personal Data on behalf of Controller under the Agreement.

15.2 Upon termination of the Agreement or this DPA (depending on which occurs first), Processor shall in accordance with Controller's instructions delete or return the Personal Data that Controller has transferred to Processor and delete any existing copies, where appropriate, latest after 90 days of the termination of the Agreement, unless storage of the Personal Data is required by EU law or applicable member state law, and ensure that each Sub-Processor does the same.

16 Changes and Additions

16.1 If the EU Data Protection Laws are changed during the term of this DPA, or if the Supervisory Authority issues guidelines, decisions, or regulations concerning the application of the EU Data Protection Laws that result in this DPA no longer meeting the requirements for a DPA, the parties shall make the necessary changes to this DPA in order to meet such new or additional requirements. Such changes shall enter into force no later than thirty (30) days after a party sends a notice of change to the other party or otherwise no later than prescribed by the EU Data Protection Laws, guidelines, decisions, or regulations of the Supervisory Authority.

16.2 Processor reserves the right from time to time to modify this DPA upon thirty (30) days' notice to the Controller per the notice provisions of the GTC. If the Controller objects to the modification within the notice period in writing, the Agreement shall be continued under the previous conditions. In this case Processor reserves the right to terminate the Agreement extraordinarily pursuant to the termination provisions of the GTC.

17 Migration and Successor Agreement

17.1 The parties acknowledge that Mopinion B.V. is a member of the Netigate Group. In the event that the Customer is transitioned to a licence agreement with another Netigate Group entity, or to the Netigate standard Terms of Service, this DPA shall be superseded in its entirety by the Data Processing Agreement published at www.netigate.net/legal as part of the applicable Netigate Terms of Service. The Netigate DPA shall govern all processing of Personal Data from the effective date of that transition.

17.2 Mopinion shall provide the Customer with reasonable advance notice of any such transition.

18 Miscellaneous

18.1 This DPA supersedes and replaces all prior data processing agreements between the parties and supersedes any deviating provisions of the GTC concerning the subject matter of this DPA, regardless if otherwise stated in the GTC.

18.2 This DPA is governed by the laws of the Netherlands, excluding conflict of law provisions. All disputes arising out of or in connection with this DPA shall be

subject to the exclusive jurisdiction of the competent court in Rotterdam, the Netherlands.

Annex 1 — Instructions and Details Concerning Processing of Personal Data

Purpose of the data processing: To enable the Client to collect, manage, and analyse feedback and survey responses from its end users and customers regarding the Client's products, services, and digital channels. Processor processes Controller data (which may include Personal Data) to fulfil the Agreement and to deliver the Services and as further set forth in this DPA.

Categories of Data Subjects:

- Customers or other commercial relationships of Controller
- End users of the Controller's digital channels
- Users of Processor's Service authorised by the Controller or by Processor to use the Service

Categories of Personal Data: The Controller or survey respondent may submit Personal Data to the Processor to the extent determined and controlled by the Controller, including but not limited to the following Personal Data categories:

- First name and last name
- Contact information (company, e-mail, phone, physical business address)
- Organisational belonging
- Customer feedback and survey responses
- Connection data
- Localisation data

Sensitive Personal Data ("Special Categories") under Article 9 GDPR cannot be processed without prior written approval from Processor. The Processor has the right to process sensitive data if it is a central part of the Controller's organisation, provided that the Controller has notified the Processor in writing prior to such processing and specified any special regulatory requirements for processing such Personal Data.

Other categories of Personal Data: Confidential information which is subject to specific national confidentiality requirements cannot be processed without prior written approval from Processor. The Controller must prior to such processing notify Processor in writing.

Sub-Processors: Processor's current Sub-Processor list, including the name, country of establishment, and nature of processing activities of each Sub-Processor, is maintained and published at **www.netigate.net/legal**. This list includes Netigate Group entities engaged as Sub-Processors where operationally required for delivery of the Services.

Data Retention: For a maximum of 90 days following termination of the Agreement, Processor will retain the Controller's data, after which it will be permanently deleted unless applicable law requires continued storage.

This Agreement is entered into by the authorised representatives of the parties:

For and on behalf of Mopinion B.V.:

Name: _____ Title: _____

Date: _____ Signature: _____

For and on behalf of the Customer:

Name: _____ Title: _____

Date: _____ Signature: _____