DATA PROCESSING AGREEMENT

This Data Protection Addendum (the "**DPA**") forms part of and is incorporated by reference into the Kraftful Inc.'s ("**Kraftful**") Terms of Service https://analytics.kraftful.com/terms-and-conditions (the "**Terms**"). This DPA is entered into by and between Company and Kraftful and will only apply to the extent that the Applicable Data Protection Laws govern the processing of Personal Data. This DPA shall be effective as of the date Company agrees to the Terms. Capitalized terms used but not defined herein shall have the meanings given to them in the Terms.

Except as modified below, the terms of the Terms shall remain in full force and effect. With respect to provisions regarding processing of Personal Data, in the event of a conflict between this DPA and the Agreement, or any other agreement between the Parties, the provisions of this DPA shall control.

1. Definitions.

1.1 "**CCPA**" means the California Consumer Privacy Act of 2018 (Title 1.81.5 of the Civil Code of the State of California), together with all effective regulations adopted thereunder (in each case, as amended from time to time).

1.2 "**Company Data**" means all information, data, content and other materials, in any form or medium, that is submitted, posted, collected, transmitted or otherwise provided by or on behalf of Company through the Services.

1.3 "**Company Personal Data**" means Company Data that is Personal Data processed by Vendor on behalf of Company in the provision of the Services under the Terms.

1.4 "**Controller**" means (i) under and in the context of European Data Protection Law, the data "controller" (as defined by GDPR), (ii) under and in the context of CCPA, the "business" (or third party) (each, as defined by CCPA), and (iii) under and in the context of any other privacy or data protection law, rule, or regulation applicable to a Party's performance hereunder, a "controller", "business", or corresponding term denoting a substantially similar definition, role, and obligations under such law, rule or regulation.

1.5 "**EU 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 (and each successor regulation, directive or other text of the foregoing, in each case as amended from time to time).

1.6 "**European Data Protection Law**" means each of EU GDPR, UK GDPR, and the Federal Data Protection Act of 19 June 1992 (Switzerland) (as the same may be superseded by the Swiss Data Protection Act 2020 and as amended from time to time).

1.7 "**GDPR**" means, as applicable, (i) the EU GDPR and/or (ii) the UK GDPR.

1.8 "**Personal Data**" means any information that constitutes (a) "personal information" (as defined by, and in the context of, CCPA), (b) "personal data" (as defined by, and in the context of, European Data Protection Law), and/or (c) "personal data," "personal information," or other term denoting a substantially similar definition and obligations under, and in the context of, any other Applicable Law, in each case that is (i) made available or otherwise provided by Company to Vendor in connection with the Services and/or (ii) collected or accessed by Vendor under the Terms via a pixel, cookie, tag, or similar technology on any of Company's digital properties.

1.9 "**Process**" means any operation or set of computer operations performed on Personal Data,

including, but not limited to, collection, recording, organization, structuring, storage, access, adaptation, alteration, retrieval, consultation, use, transfer, transmit, sale, rental, disclosure, dissemination, making available, alignment, combination, deletion, erasure, or destruction.

1.10 "**Processor**" means (i) under and in the context of European Data Protection Law, the data "processor" (as defined by GDPR), (ii) under and in the context of CCPA, a "service provider" (as defined by CCPA), and (iii) under and in the context of any other privacy or data protection law, rule, or regulation applicable to a Party's performance hereunder, a "processor", "service provider", or corresponding term denoting a substantially similar definition, role, and obligations under such law, rule or regulation.

1.11 "**Security Incident**" means (i) any accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, or access to, Personal Data or (ii) any other event that constitutes a "security breach", "personal data breach", or substantially similar term with respect to Personal Data under an Applicable Law(s).

1.12 "**Services**" means, collectively, the products and/or services provided by Vendor to Company under the Terms.

1.13 "**Sub-Processor**" means a contractor, subcontractor, consultant, third-party service provider, or agent engaged by Vendor for further Processing of Personal Data.

1.14 "**UK GDPR**" has the meaning ascribed thereto in section 3(10) (as supplemented by section 205(4)) of the UK Data Protection Act 2018 (as amended from time to time).

2. Data Processing Obligations.

2.1 General.

(a) Each Party shall comply with its obligations relating to Personal Data under this DPA and under Applicable Data Protection Laws at its own cost. With respect to Personal Data, (i) Company is a Controller and (ii) Vendor is a Processor that acts upon the instructions of Company, including, without limitation, in accordance with the Terms, this DPA, and any other documented instructions provided by Company.

(b) With regard to Vendor employees engaged in Processing Personal Data, Vendor shall ensure that such employees are informed of the confidential nature of the Personal Data and are subject to appropriate confidentiality obligations sufficient to comply with the Terms and this DPA, which confidentiality obligations shall survive following termination of this DPA for at least as long as the period(s) required by the Terms and this DPA.

(c) Company will have sole responsibility for the accuracy, quality, and legality of Company Personal Data and the means by which Company obtained the Company Personal Data, including, without limitation, obtaining appropriate consent to collect the Company Personal Data and share such data Vendor in accordance with Applicable Data Protection Laws.

2.2 GDPR.

(a) European Economic Area and Switzerland.

(i) The Processing by Vendor of Personal Data relating to an EEA or Switzerland data subject (including, without limitation, the transfer of such Personal Data from the EEA to a third country not providing an adequate level of protection) will be further governed by the EU Standard Contractual Clauses (Transfers Controller-to-Processor) (Module Two thereunder), with Company as data exporter and Vendor as data importer, attached hereto (without provisions with respect to Module One, Module Three, or Module Four thereunder) as Schedule I-A (together with all Appendixes and Annexes thereto, and as the same may be amended, supplemented, or otherwise modified from time to time, "**EU SCCs**"), which is incorporated by reference into this DPA solely with respect to Personal Data relating to EEA

and/or Switzerland data subjects. If there is any conflict between (x) the terms and conditions of either this DPA or the Terms, on the one hand, and (y) the terms and conditions of the EU SCCs, on the other hand, then, with respect to Personal Data relating to an EEA and/or Switzerland data subject(s), the terms and conditions of the EU SCCs will prevail and control.

(ii) Vendor may only transfer Personal Data relating to an EEA or Switzerland data subject outside the EEA in compliance with Applicable Data Protection Laws and pursuant to a data transfer mechanism then-recognized by the European Commission as a legitimate basis for the transfer of such Personal Data outside the EEA.

(b) United Kingdom.

(i) The Processing by Vendor of Personal Data relating to UK data subjects (including, without limitation, the transfer of such Personal Data from the UK to a third country not providing an adequate level of protection) will be further governed by those certain "Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to processor transfers)", with Company as data exporter and Vendor as data importer, attached hereto as Schedule I-B (together with all Appendixes and Annexes thereto, and as the same may be amended, supplemented, or otherwise modified from time to time, "**UK SCCs**"), which is incorporated by reference into this DPA solely with respect to Personal Data relating to UK data subjects; provided that Company and Vendor hereby agree to replace the UK SCCs attached hereto as Schedule I-B with the version (and module, if applicable) of the UK Standard Contractual Clauses as may be issued and/or required by the UK Information Commissioner's Office after the Effective Date, with Company as data exporter (controller) and Vendor as data importer (processor), prior to the date required by Applicable Data Protection Laws. If there is any conflict between (x) the terms and conditions of either this DPA or the Terms, on the one hand, and (y) the terms and conditions of the UK SCCs, on the other hand, then, with respect to Personal Data relating to a UK data subject(s), the terms and conditions of the UK SCCs will prevail and control.

(ii) Vendor may only transfer Personal Data relating to a UK data subject outside the UK in compliance with Applicable Data Protection Laws and pursuant to a data transfer mechanism then-recognized by the government of the United Kingdom as a legitimate basis for the transfer of such Personal Data outside the UK.

2.3 CCPA. With respect to Personal Data relating to a California "consumer" (as defined by CCPA) or household ("**CCPA Personal Data**"):

(a) Company shall be disclosing such CCPA Personal Data under the Terms to Vendor for a "business purpose" (as defined by CCPA), and Vendor shall Process such CCPA Personal Data solely on behalf of Company and only as necessary to perform such business purpose for Company; and

(b) Vendor shall not: (i) "sell" (as defined by CCPA) CCPA Personal Data; or (ii) retain, use, or disclose CCPA Personal Data (x) for any purpose (including a "commercial purpose" (as defined by CCPA)) other than for the specific purpose of performing for Company the services specified in the Terms or (y) outside of the direct business relationship between Vendor and Company; Vendor certifies that it understands the restrictions set forth in this Section 2.3(b) and shall comply with them; and

(c) Notwithstanding anything to the contrary in this DPA (including, for purposes of clarification and without limitation, clauses (a) and (b) of this Section 2.3), in no event shall Vendor process any CCPA Personal Data in such a manner as would constitute (i) a sale (as defined by CCPA) of CCPA Personal Data by Company to Vendor or (ii) on or after January 1, 2023, the sharing (as defined under CCPA (as amended by the California Privacy Rights Act of 2020)) of CCPA Personal Data by Company with Vendor; and

(d) If directed by Company with regard to a particular California consumer or household, Vendor

shall delete the CCPA Personal Data of such consumer or household.

2.4 Changes in Applicable Data Protection Laws. If, due to any change in Applicable Data Protection Laws, a Party reasonably believes that (a) Vendor ceases to be able to provide a Service(s) in whole or in part (e.g., with respect to a particular jurisdiction) and/or Company ceases to be able to use a Service(s) in whole or in part under the then-current terms and conditions of the Terms and this DPA, each Party may terminate the Terms (in whole or, if reasonably practicable, in part).

3. Security.

3.1 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, Vendor will implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risks. Such measures will include reasonable administrative, physical, and technical security controls (including those required by Applicable Data Protection Laws) that prevent the collection, use, disclosure, or access to Personal Data and Company confidential information that the Terms do not expressly authorize, including maintaining a comprehensive information security program that safeguards Personal Data and Company confidential information. These security measures include, but are not limited to: (i) the pseudonymization and encryption of personal data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and (iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

3.2 When assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

4. Supplementary Measures and Safeguards.

4.1 Assistance; Risk Assessment.

(a) Vendor shall assist Company to ensure compliance with Applicable Data Protection Laws in connection with the Processing of Personal Data. Vendor shall promptly notify Company if Vendor becomes aware of any Applicable Law(s) or change in Applicable Law(s).

4.2 Orders. Vendor shall notify Company immediately in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Personal Data. Company shall have the right to defend such action in lieu of and/or on behalf of Vendor. Company may, if it so chooses, seek a protective order. Vendor shall reasonably cooperate with Company in such defense.

5. Notifications.

5.1 Security Incidents. Vendor has and will maintain a security incident response plan that includes procedures to be followed in the event of a Security Incident. Vendor will provide Company with written notice promptly after discovering a Security Incident (including those affecting Vendor or its Sub-Processors), including any information that Company is required by law to provide to an applicable regulatory agency or to the individuals whose personal data was involved in the Security Incident.

5.2 Data Subject Requests. Vendor shall (i) promptly notify Company about any request under Applicable Law(s) with respect to Personal Data received from or on behalf of the applicable data subject and (ii) reasonably cooperate with Company's reasonable requests in connection with data subject requests with respect to Personal Data. Vendor shall assist Company, through appropriate technical and organizational measures, to fulfill its obligations with respect to requests of data subjects seeking to exercise rights under Applicable Law with respect to Personal Data.

6. Sub-Processors.

6.1 Vendor shall not have Personal Data Processed by a Sub-Processor unless such Sub-Processor is bound by a written agreement with Vendor that includes data protection obligations at least as protective as those contained in this DPA and the Terms and that meet the requirements of Applicable Data Protection Laws. Vendor is and shall remain fully liable to Company for any failure by any Sub-Processor to fulfill Vendor's data protection obligations under Applicable Data Protection Laws.

6.2 Vendor provides a website that lists all Sub-Processors who access Personal Data: https://analytics.kraftful.com/subprocessors (the "Website"). Company specifically authorizes and instructs Vendor to engage the Sub-Processors listed on the Website as of the Effective Date. At least 14 days before authorizing any new Sub-Processors, Vendor will update the Website, notify Company and grant the opportunity to object to such change. Upon Company's request, Vendor will provide all information necessary to demonstrate that the Sub-Processors will meet all requirements pursuant to Section 6.1. In the case Company objects to any Sub-Processor, Vendor can choose to either not engage the Sub-Processor or to terminate this DPA with thirty (30) days' prior written notice.

7. Term; Termination. This DPA shall remain in effect until (a) the Terms have terminated and (b) all obligations that Vendor has under the Terms and under Applicable Data Protection Laws with respect to Personal Data, and all rights that Company has under the Terms and under Applicable Data Protection Laws with respect to Personal Data, have terminated. Notwithstanding termination of this DPA, any provisions hereof that by their nature are intended to survive, shall survive termination.

8. Miscellaneous.

8.1 All notices under this DPA must be made in writing (including, without limitation, email) and sent to the attention of: (i) if to Company: the email used by Company to register for the Services and (ii) if to Vendor, info@kraftful.com. Notice shall be deemed given when delivered.

8.2 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the applicable Services Agreements, unless required otherwise by Applicable Data Protection Laws.

8.3 Neither Party may assign or transfer any part of this DPA without the written consent of the other Party; provided, however, that this DPA may be assigned without the other Party's written consent by either Party to a person or entity who acquires, by sale, merger or otherwise, all or substantially all of such assigning Party's assets, stock or business. Subject to the foregoing, this DPA shall bind and inure to the benefit of the Parties, their respective successors and permitted assigns. Any attempted assignment in violation of this Section 12.3 shall be void and of no effect.

8.4 This DPA is the Parties' entire agreement relating to its subject and supersedes any prior or contemporaneous agreements on that subject; provided, however, that, notwithstanding the foregoing but subject to the last sentence of this Section 8.4, nothing in this DPA shall be deemed to supersede the Terms. All amendments hereto must be executed by both of the Parties and expressly state that they are amending this DPA. Failure to enforce any provision of this DPA shall not constitute a waiver. If any provision of this DPA is found unenforceable, it and any related provisions shall be interpreted to best accomplish the unenforceable provision's essential purpose. The headings contained in this DPA are for reference purposes only and shall not affect in any way the meaning or interpretation of this DPA. In the event of a conflict between the terms and conditions of this DPA and the Terms, the terms and conditions of this DPA shall govern.

8.5 The Parties may execute this DPA in counterparts (including, without limitation, DocuSign and/or other electronic signature, PDF, and other electronic copies), which taken together shall constitute one instrument.

SCHEDULE I-A
EU SCCs

STANDARD CONTRACTUAL CLAUSES

EU Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679

(Module 2 – EU Controller to Non-EU Processor transfers)

SECTION I

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 Appendix 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 Appendix 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 Appendix I.B.

(d) The Appendix to these Clauses containing the Appendices 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 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

(iv) Clause 12 – 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 Appendix 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 Appendix I.A.

(b) Once it has completed the Appendix and signed Appendix 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 Appendix 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 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 Appendix 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 Appendix 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 Appendix 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 Appendix 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 Appendix 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) SPECIFIC PRIOR AUTHORISATION. The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [Specify time period] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Appendix III. The Parties shall keep Appendix III up to date

(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. 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 Appendix 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.

(b) 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.

(c) 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;

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

(d) 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.

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

(f) 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.

(b) 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.

(c) 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.

(d) 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.

(e) 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.

(f) 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.

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

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Appendix 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.

(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 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 Ireland.

Clause 18

Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of Ireland.

(c) 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.

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

APPENDIX I

A. LIST OF PARTIES

Data exporter(s):

Name: Entity identified as "Company" in the DPA and Terms.

Address: The address that Company provided when registering to use the Services.

Contact person's name, position and contact details: The contact details that Company provided when registering to use the Services.

Activities relevant to the data transferred under these Clauses: To provide Company with the Services (as defined in the Terms), namely, providing Customer with access to Kraftful's software that assists users in the area of products analytics.

Signature and date: This DPA (including these Standard Contractual Clauses) shall be deemed executed upon Company's acceptance of the Terms.

Role (controller/processor): Controller.

Data importer(s):

Name: Kraftful, Inc. ("Kraftful")

Address: 2261 Market Street #4051, San Francisco, CA 94114

Contact person's name, position and contact details: Heidi Gluck, Data Protection Officer; heidi@kraftful.com

Activities relevant to the data transferred under these Clauses: To provide Company with the Services (as defined in the Terms), namely, providing Customer with access to Kraftful's software that assists users in the area of products analytics.

Signature and date: This DPA (including these Standard Contractual Clauses) shall be deemed executed upon Company's acceptance of the Terms.

Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Individual users and, if the user is an entity, such Company's personnel that are input into the Services for the purpose of granting such personnel administrative access to the Services.

Categories of personal data transferred

(i) First and last name, (ii) email address, (iii) Location Data, Usage Data, and Device ID (as those terms are defined in Kraftful's Privacy Policy), and (iv) Company Data to the extent such data contains Personal Data.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into

consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
None.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
For the duration of the Services pursuant to the Terms.

Nature of the processing
To provide the Services pursuant to the Terms.

Purpose(s) of the data transfer and further processing
To provide the Services pursuant to the Terms.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
As long as necessary to provide the Services pursuant to the Terms.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
To provide the Services pursuant to the Terms.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The Supervisory Authority where the Data Exporter is located.

APPENDIX II

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

1. **Pseudonymisation**
   - Pseudonymisation contains measures that enable one to process personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

   - Pseudonymisation is used on documents that must be retained and after a data subject has requested deletion, if complete deletion cannot be ensured.

2. **Encryption**

   - Encryption contains measures that enable one to convert clearly legible information into an illegible string by means of a cryptographic process.

   - Stored data is encrypted where appropriate, including any backup copies of the data.

3. **The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services**

Confidentiality and integrity are ensured by the secure processing of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

3.1 Confidentiality

3.1.1 Physical access control

Measures that prevent unauthorised persons from gaining access to data processing systems with which personal data are processed or used. Processor does not maintain any physical office space. All physical access control measures below are provided by the data centres.

- Physical access control systems
- Definition of authorised persons and management and documentation of individual authorisations
- Regulation of visitors and external staff
- Monitoring of all facilities housing IT systems
- Logging of physical access

3.1.2 System/Electronic access control

Measures that prevent data processing systems from being used without authorisation.
- User Authentication by simple authentication methods using username/password on all systems and Multi-Factor Authentication on critical systems.
- Secure transmission of credentials using networks using TSL 1.2 or higher
- Guidelines for Handling of passwords delivered to all employees at orientation and periodically after that
- Managing means of authentication by tool administrators
- Access control to infrastructure that is hosted by cloud service provider limited by principle of Least Privilege

3.1.3 Internal Access Control

Measures that ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorisation in the course of processing or use and after storage.

- Manual locking at termination or when there is suspicion of compromise.
- implementation of access restrictions, implementation of the "need-to-know" principle, managing of individual access rights.

3.1.4 Isolation/Separation Control

Measures to ensure that data collected for different purposes can be processed (storage, amendment, deletion, transmission) separately.

- Network separation of web, application, and data tiers

3.1.5 Job Control

Measures that ensure that, in the case of commissioned processing of personal data, the data are processed strictly corresponding the instructions of the principal.

- Training and confidentiality agreements for internal staff and external staff

3.2 Integrity

3.2.1 Data transmission control

Measures ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.

- Secure transmission between client and server and to external systems by using industry-standard encryption of TLS 1.2 or higher

- Secure network interconnections ensured by Web Application

- Logging of transmissions of data from application and databases that store or process personal data

3.2.2 Data input control

Measures that ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed.

- Logging authentication and monitored logical system access
- Logging of data access including, but not limited to access, modification, entry and deletion of data

3.3 Availability and Resilience of Processing Systems and Services

Availability includes measures that ensure that personal data is protected from accidental destruction or loss due to internal or external influences. Resilience of processing systems and services includes measures that ensure the ability to withstand attacks or to quickly restore systems to working order after an attack.

- Daily full backups
- Protection of stored backups in a separate location, using the same level of encryption and security controls as production.

4. **A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing**

Organisational measures that ensure the regular review and assessment of technical and organisational measures.

- Documentation of interfaces and tools used for processing
- Internal assessments of technical and organizational measures

APPENDIX III

LIST OF SUB-PROCESSORS

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

Please see: https://analytics.kraftful.com/subprocessors

SCHEDULE I-B
UK SCCs

STANDARD CONTRACTUAL CLAUSES FOR PROCESSORS

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Customer and each of the EU Customer Affiliates as listed in Exhibit A are hereinafter referred to as the "**Data Exporter**" with respect to the personal data provided by that Data Exporter.

Kraftful as defined in the DPA is hereinafter referred to as the "**Data Importer**".

The Data Exporter(s) and the Data Importer, each a “party” and collectively “the parties” HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in **Appendix 1**.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the Data Exporter'* means the controller who transfers the personal data;

(c) *'the Data Importer'* means the processor who agrees to receive from the Data Exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the Data Importer or by any other subprocessor of the Data Importer who agrees to receive from the Data Importer or from any other subprocessor of the Data Importer personal data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the Data Exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the Data Exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the Data Importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the Data Exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the Data Exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the Data Exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the Data Exporter

The Data Exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the Data Exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the Data Importer to process the personal data transferred only on the Data Exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the Data Importer will provide sufficient guarantees in respect of the technical and

organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the Data Importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the Data Exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the Data Importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the Data Importer

The Data Importer agrees and warrants:

(a) to process the personal data only on behalf of the Data Exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Data Exporter of its inability to comply, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Data Exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the Data Exporter as soon as it is aware, in which case the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the Data Exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the Data Exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the Data Exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the Data Exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Data Exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the Data Exporter;

(h) that, in the event of subprocessing, it has previously informed the Data Exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the Data Exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor, is entitled to receive compensation from the Data Exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the Data Exporter, arising out of a breach by the Data Importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the Data Exporter has factually disappeared or ceased to exist in law or has become insolvent, the Data Importer agrees that the data subject may issue a claim against the Data Importer as if it were the Data Exporter, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The Data Importer may not rely on a breach by a subprocessor of its obligations in order to avoid

its own liabilities.

3. If a data subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The Data Importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the Data Importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the Data Exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The Data Exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the Data Importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the Data Exporter under the applicable data protection law.

3. The Data Importer shall promptly inform the Data Exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the Data Importer, or any subprocessor, pursuant to paragraph 2. In such a case the Data Exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the Data Exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the Data Importer under the Clauses (This requirement may be satisfied by the subprocessor co-signing the contract entered into between the Data Exporter and the Data Importer which is based on the terms and conditions of this Agreement.). Where the subprocessor fails to fulfil its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the Data Importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the Data Exporter or the Data Importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the Data Exporter is established.

4. The Data Exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the Data Importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the Data Exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the Data Importer and the subprocessor shall, at the choice of the Data Exporter, return all the personal data transferred and the copies thereof to the Data Exporter or shall destroy all the personal data and certify to the Data Exporter that it has done so, unless legislation imposed upon the Data Importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the Data Importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The Data Importer and the subprocessor warrant that upon request of the Data Exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data Exporter
Name: Entity identified as "Company" in the DPA and Terms.

Address: The address that Company provided when registering to use the Services.

Contact person's name, position and contact details: The contact details that Company provided when registering to use the Services.

Activities relevant to the data transferred under these Clauses: To provide Company with the Services (as defined in the Terms), namely, providing Customer with access to Kraftful's software that assists users in the area of products analytics.

Signature and date: This DPA (including these Standard Contractual Clauses) shall be deemed executed upon Company's acceptance of the Terms.

Role (controller/processor): Controller.

Data Importer

Name: Kraftful, Inc. ("Kraftful")

Address: 2261 Market Street #4051, San Francisco, CA 94114

Contact person's name, position and contact details: Heidi Gluck, Data Protection Officer; heidi@kraftful.com

Activities relevant to the data transferred under these Clauses: To provide Company with the Services (as defined in the Terms), namely, providing Customer with access to Kraftful's software that assists users in the area of products analytics.

Signature and date: This DPA (including these Standard Contractual Clauses) shall be deemed executed upon Company's acceptance of the Terms.

Role (controller/processor): Processor.

Data Subjects
The processing can include the following categories of Data Subjects:

Individual users and, if the user is an entity, such Company's personnel that are input into the Services for the purpose of granting such personnel administrative access to the Services.

Categories of Data

(i) First and last name, (ii) email address, (iii) Location Data, Usage Data, and Device ID (as those terms are defined in Kraftful's Privacy Policy), and (iv) Company Data to the extent such data contains Personal Data.

Special Categories of Data (if appropriate)
None

Processing Operations
To provide the Services pursuant to the Terms

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organizational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. **Pseudonymisation**
   - Pseudonymisation contains measures that enable one to process personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.

   - Pseudonymisation is used on documents that must be retained and after a data subject has requested deletion, if complete deletion cannot be ensured.

2. Encryption

   - Encryption contains measures that enable one to convert clearly legible information into an illegible string by means of a cryptographic process.

   - Stored data is encrypted where appropriate, including any backup copies of the data.

3. **The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services**

Confidentiality and integrity are ensured by the secure processing of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

3.1 Confidentiality

3.1.1 Physical access control

Measures that prevent unauthorised persons from gaining access to data processing systems with which personal data are processed or used. Processor does not maintain any physical office space. All physical access control measures below are provided by the data centres.

- Physical access control systems
- Definition of authorised persons and management and documentation of individual authorisations
- Regulation of visitors and external staff
- Monitoring of all facilities housing IT systems
- Logging of physical access

3.1.2 System/Electronic access control

Measures that prevent data processing systems from being used without authorisation.
- User Authentication by simple authentication methods using username/password on all systems and Multi-Factor Authentication on critical systems.
- Secure transmission of credentials using networks using TSL 1.2 or higher
- Guidelines for Handling of passwords delivered to all employees at orientation and periodically after that
- Managing means of authentication by tool administrators
- Access control to infrastructure that is hosted by cloud service provider limited by principle of Least Privilege

3.1.3 Internal Access Control

Measures that ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorisation in the course of processing or use and after storage.

- Manual locking at termination or when there is suspicion of compromise.
- implementation of access restrictions, implementation of the "need-to-know" principle, managing of individual access rights.

3.1.4 Isolation/Separation Control

Measures to ensure that data collected for different purposes can be processed (storage, amendment, deletion, transmission) separately.

- Network separation of web, application, and data tiers

3.1.5 Job Control

Measures that ensure that, in the case of commissioned processing of personal data, the data are processed strictly corresponding the instructions of the principal.

- Training and confidentiality agreements for internal staff and external staff

3.2 Integrity

3.2.1 Data transmission control

Measures ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.

- Secure transmission between client and server and to external systems by using industry-standard encryption of TLS 1.2 or higher

- Secure network interconnections ensured by Web Application

- Logging of transmissions of data from application and databases that store or process personal data

3.2.2 Data input control

Measures that ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed.

- Logging authentication and monitored logical system access
- Logging of data access including, but not limited to access, modification, entry and deletion of data

3.3 Availability and Resilience of Processing Systems and Services

Availability includes measures that ensure that personal data is protected from accidental destruction or loss due to internal or external influences. Resilience of processing systems and services includes measures that ensure the ability to withstand attacks or to quickly restore systems to working order after an attack.

- Daily full backups
- Protection of stored backups in a separate location, using the same level of encryption and security controls as production.

4. **A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing**

Organisational measures that ensure the regular review and assessment of technical and organisational measures.

- Documentation of interfaces and tools used for processing

Internal assessments of technical and organizational measures