DATA PROCESSING AGREEMENT

This Data Protection Agreement (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 in this DPA 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 Terms, or any other agreement between the Parties, the provisions of this DPA shall control.

1. Definitions.

1.1 "**Applicable Laws**" means, collectively, all now existing or hereinafter enacted or amended laws, rules, regulations (including, without limitation, self-regulatory obligations), and/or sanctions programs applicable to a party's performance hereunder and/or obligations with respect to data protection.

1.2 "**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).

1.3 "**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.

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

1.5 "**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.

1.6 "**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).

1.7 "**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).

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

1.9 "**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 Laws, in each case that is (i) made available or otherwise provided by Company to Kraftful in connection with the Services and/or (ii) collected or accessed by Kraftful under the Terms via a pixel, cookie, tag, or similar technology on any of Company's digital properties.

1.10 "**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.

1.11 "**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.

1.12 "**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).

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

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

1.15 "**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 Laws at its own cost. With respect to Personal Data, (i) Company is a Controller and (ii) Kraftful 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 Kraftful employees engaged in Processing Personal Data, Kraftful 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 Kraftful in accordance with Applicable Data Protection Laws.

(i) Standard Contractual Clauses. If Kraftful Processes Personal Data relating to an EEA, United Kingdom, or Switzerland data subject (including, without limitation, the transfer of such Personal Data from the EEA, United Kingdom, or Switzerland to a third country not providing an adequate level of protection) outside of the EEA, United Kingdom, and Switzerland, the Processing will be further governed by Schedule I to this DPA, with Company as data exporter and Kraftful as data importer (together with all Appendixes and Annexes thereto, and as the same may be amended, supplemented, or otherwise modified from time to time, "**Personal Data SCCs**"), which is incorporated by reference into this DPA solely with respect to Personal Data relating to EEA, United Kingdom 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 Personal Data SCCs, on the other hand, then, with respect to Personal Data relating to an EEA, United Kingdom and/or Switzerland data subject(s), the terms and conditions of the Personal Data SCCs will prevail and control. Kraftful may only transfer Personal Data relating to an EEA, United Kingdom, or Switzerland data subject outside the EEA, United Kingdom, and Switzerland in compliance with Applicable Laws and the Personal Data SCCs.

2.2 CCPA. Without limiting any of the restrictions on or obligations of Kraftful under this DPA, under any of the Service Agreements, or under Applicable Laws, 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 Kraftful for a "business purpose" (as defined by CCPA), and Kraftful shall Process such CCPA Personal Data solely on behalf of Company and only as necessary to perform such business purpose for Company; and

(b) Kraftful 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 Kraftful and Company; Kraftful certifies that it understands the restrictions set forth in this Section 2.2(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 2.2), in no event shall Kraftful 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 Kraftful or (ii) the sharing (as defined under CCPA) of CCPA Personal Data by Company with Kraftful; and

(d) If directed by Company with regard to a particular California consumer or household, Kraftful shall delete the CCPA Personal Data of such consumer or household.

2.3 Changes in Applicable Laws. If, due to any change in Applicable Laws, a Party reasonably believes that (a) Kraftful 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, Kraftful will implement and maintain appropriate technical and organizational 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 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. Kraftful shall assist Company to ensure compliance with Applicable Laws in connection with the Processing of Personal Data.

4.2 Orders. Kraftful shall notify Company 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 Kraftful. Company may, if it so chooses, seek a protective order. Kraftful shall reasonably cooperate with Company in such defense.

5. Notifications.

5.1 Security Incidents. Kraftful has and will maintain a security incident response plan that includes procedures to be followed in the event of a Security Incident. Kraftful will provide Company with written notice promptly after discovering a Security Incident (including those affecting Kraftful 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. Kraftful 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. Kraftful 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 Kraftful shall not have Personal Data Processed by a Sub-Processor unless such Sub-Processor is bound by a written agreement with Kraftful 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 Laws. Kraftful is and shall remain fully liable to Company for any failure by any Sub-Processor to fulfill Kraftful's data protection obligations under Applicable Laws.

6.2 Kraftful provides a website that lists all Sub-Processors who access Personal Data: https://analytics.kraftful.com/subprocessors (the "Website"). Company specifically authorizes and instructs Kraftful to engage the Sub-Processors listed on the Website as of the Effective Date. Kraftful will notify Company of any changes to the Sub-Processors listed on the Website and grant Company the opportunity to object to such change. Upon Company's request, Kraftful 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, Kraftful can choose to either not engage the Sub-Processor or to terminate the Terms and this DPA with thirty (30) days' prior written notice.

6.3 Third-party providers that maintain IT systems whereby access to Personal Data is not needed but can technically also not be excluded do not qualify as Sub-Processors within the meaning of this Section 6. They can be engaged based on regular confidentiality undertakings and subject to Kraftful's reasonable monitoring.

7. Deletion. Kraftful shall, at the choice of Company: (i) delete or return all Company Data to Company after such Company Data is no longer necessary for the provision of the Services, and (ii) delete existing copies of such Company Data.

8. Documentation. Kraftful shall, upon Company's request, provide Company (a) comprehensive documentation of Kraftful's technical and organizational security measures, (b) any and all third-party audits and certifications available with respect to such security measures, and (c) and all other information reasonably necessary to demonstrate compliance with the Kraftful's obligations under this DPA and/or under Applicable Laws.

9. Term; Termination. This DPA shall remain in effect until (a) the Terms have terminated and (b) all obligations that Kraftful has under the Terms and under Applicable Laws with respect to Personal Data, and all rights that Company has under the Terms and under Applicable 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.

10. Miscellaneous.

10.1 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 Kraftful, info@kraftful.com. Notice shall be deemed given when delivered.

10.2 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Terms, unless required otherwise by Applicable Laws.

10.3 Neither Party may assign or transfer any part of this DPA without the written consent of the other Party; provided, however, that this DPA, collectively with the Terms, 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 10.3 shall be void and of no effect.

10.4 This DPA is the Parties' entire agreement relating to its subject and supersedes any prior or contemporaneous agreements on that subject. Kraftful may modify the terms of this DPA if, as reasonably determined by Kraftful, such modification is (i) reasonably necessary to comply with Applicable Laws or any other law, regulation, court order or guidance issued by a governmental regulator or agency; and (ii) does not: (a) result in a degradation of the overall security of the Services, (b) expand the scope of, or remove any restrictions on, Kraftful's processing of Personal Data, and (c) otherwise have a material adverse impact on Company's rights under this DPA. Any other amendments 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.

SCHEDULE I
EU SCCs

1. Definitions

    a. "**EU SCCs**" means the Standard Contractual Clauses issued pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at http://data.europa.eu/eli/dec_impl/2021/914/oj and completed as described in this Schedule I.

    b. "**UK SCCs**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, available as of the DPA Effective Date at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/ and completed as described in this Schedule I.

2. With respect to Personal Data transferred from the European Economic Area, the EU SCCs will apply and form part of this Schedule I, unless the European Commission issues updates to the EU SCCs, in which case the updated EU SCCs will control. Undefined capitalized terms used in this provision will have the meanings given to them (or their functional equivalents) in the definitions in the EU SCCs. For purposes of the EU SCCs, they will be deemed completed as follows:

    a. Because Company is a Controller and Kraftful is a Processor of the Personal Data, Module 2 applies.

    b. Clause 7 (the optional docking clause) is not included.

    c. Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body is inapplicable.

    d. Under Clause 17 (Governing law), the Parties select Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The Parties select the law of Ireland.

    e. Under Clause 18 (Choice of forum and jurisdiction), the Parties select the courts of Ireland.

    f. Annexes I, II and III of the EU SCCs are set forth in **Exhibit A** to this Schedule I.

    g. By entering into this DPA, the Parties are deemed to be signing the EU SCCs.

3. With respect to Personal Data transferred from the United Kingdom for which the law of the United Kingdom (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the UK SCCs form part of this Schedule I and take precedence over the rest of this Schedule I as set forth in the UK SCCs, unless the United Kingdom issues updates to the UK SCCs, in which case the updated UK SCCs will control. Undefined capitalized terms used in this provision will have the meanings given to them (or their functional equivalents) in the definitions in the UK SCCs. For purposes of the UK SCCs, they will be deemed completed as follows:

    a. Table 1 of the UK SCCs:

        i. The Parties' details are the Parties and their affiliates to the extent any of them is involved in such transfer, including those set forth in **Exhibit A.**

        ii. The Key Contacts are the contacts set forth in **Exhibit A**.

b. Table 2 of the UK SCCs: The Approved EU SCCs referenced in Table 2 are the EU SCCs as executed by the Parties pursuant to this Schedule I.

c. Table 3 of the UK SCCs: Annex 1A, 1B, II and III are set forth in **Exhibit A**.

d. Table 4 of the UK SCCs: Either party may terminate the Service Agreements as set forth in Section 19 of the UK SCCs.

e. By entering into the DPA, the Parties are deemed to be signing the UK SCCs and their applicable Tables and Appendix Information.

4. With respect to Personal Data transferred from Switzerland for which Swiss law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the EU SCCs will apply and will be deemed to have the following differences to the extent required by the Swiss Federal Act on Data Protection ("**FADP**"):

   a. References to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR.

   b. The term "**member state**" in the EU SCCs will not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs.

   c. References to Personal Data in the EU SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope.

   d. Under Annex I(C) of the EU SCCs (Competent supervisory authority): where the transfer is subject exclusively to the FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner, and where the transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in the EU SCCs insofar as the transfer is governed by the GDPR.

EXHIBIT A
ANNEX 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 Company 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: Shauna Prussin, Data Protection Officer; shauna@kraftful.com

Activities relevant to the data transferred under these Clauses: To provide Company with the Services (as defined in the Terms), namely, providing Company 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 of Ireland.

ANNEX 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

ANNEX III

LIST OF SUB-PROCESSORS

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

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