Data Protection Addendum

Last Updated: August 25, 2021

This Data Protection Addendum ("Addendum") is entered into by and between Watermark Insights, LLC and its affiliates ("Watermark"), and Customer, (the "Customer" or "Organization"). This Addendum applies to Watermark's Processing of Personal Data under the agreement executed between Watermark and Customer for Watermark's provision of the services (the "Agreement").

1. Definitions and interpretation

1.1 In this Addendum, unless the context otherwise requires:

"**Affiliate(s)**" means any entity that directly or indirectly controls, is controlled by, or is under common control or ownership with a Party, where "control," "controlled by" and "under common control with" means the possession of the power to direct, cause or significantly influence the direction of the entity, whether through the ownership of voting securities, by contract, or otherwise.

"**Data Protection Regulator**" or "**DP Regulator**" means any governmental or regulatory body or authority with responsibility for monitoring or enforcing compliance with the Applicable Data Protection Laws.

"**Applicable Data Protection Laws**" means, with respect to a party, all applicable privacy, data protection, and information security related laws and regulations applicable to Watermark's Processing of Customer Personal Data.

"**Customer Data**" has the same meaning as defined in the Agreement. This Addendum applies to Watermark's Processing of Customer Data to the extent that such Customer Data constitutes Personal Data.

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"**Data Subject**" means the identified or identifiable natural person who is the subject of Personal Data.

"**Personal Data**" means "personal data", "personal information", personally identifiable information" or similar information defined in and governed by Applicable Data Protection Laws.

"**Security Incident**" means any confirmed unauthorized or unlawful breach of security that leads to the destruction, loss, alteration, unauthorized disclosure of or access to Personal Data being Processed by Watermark. Security Incidents do not include unsuccessful attempts or activities that do not comprise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

"**Subprocessor**" means any third party authorized by Watermark to Process any Customer Data.

"**Usage Data**" or "**Aggregated Statistics**" has the same meaning as defined in the Agreement. This Addendum applies to Usage Data to the extent Usage Data constitutes Personal Data.

1.2 General; Termination

a. This Addendum forms part of the Agreement and except as expressly set forth in this Addendum, the Agreement remains unchanged and in full force and effect. If there is any conflict between this Addendum and the Agreement, this Addendum will govern.

b. Any liabilities arising under this Addendum are subject to the limitations of liability in the Agreement.

c. This Addendum will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Laws.

d. This Addendum will automatically terminate upon expiration or termination of the Agreement.

1.3 **Capitalization**. Capitalized terms not otherwise defined herein shall have the meanings ascribed to them in the Agreement. The "Parties" shall refer to the parties to the Agreement and each shall be a "Party."

1.4 **Relationship of the Parties**

a. **Watermark as a Processor**. The parties acknowledge and agree that with regard to the Processing of Customer Data, Customer may act as a Controller or processor and Watermark is a Processor. Watermark will process Customer Data in accordance with Customer's instructions as outlined herein.

For purposes of this Addendum, Watermark is the data importer and Customer is the data exporter.

b. **Watermark as Controller**. To the extent that any Usage Data (as defined in the Agreement) is considered Personal Data, Watermark is the Controller with respect to such data and will Process such data in accordance with its Privacy Policy, which can be found at https://www.watermarkinsights.com/privacy-policy/. For all other purposes, Organization is the Controller.

2. Compliance with Applicable Data Protection Laws

2.1 The Parties shall comply with the provisions and obligations imposed on them by the Applicable Data Protection Laws at all times when processing Personal Data in connection with this Agreement, which processing shall be in respect of the types of Personal Data, categories of Data Subjects, nature and purposes, and duration, set out in Schedule 1 to this Addendum.

2.2 The Parties shall each maintain records of all processing operations under their respective responsibility that contain at least the minimum information required by the Applicable Data Protection Laws, and shall make such information available to any authorized Data Protection Regulator on request.

3. Processing and Security

3.1 In performing its obligations under the Agreement, Watermark shall only process the types of Personal Data, and only in respect of the categories of Data Subjects, and only for the nature and purposes of processing and duration, as is set out in the Schedule 1 to this Addendum. By entering into this Agreement, Customer instructs Watermark to Process Customer Data to provide the services and pursuant to any other written instructions given by Customer and acknowledged in writing by Watermark as constituting instructions for purposes of the Addendum. If Watermark becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter (i.e., the Customer) without undue delay.

3.2 Organization shall:

(a) ensure that any instructions it issues to Watermark shall comply with the Applicable Data Protection Laws; and

(b) have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which Organization acquired such Personal Data shall establish the legal basis for processing under Applicable Data Protection Laws, including providing all notices and obtaining all consents as may be required under Applicable Data Protection Laws in order for Watermark to process the Personal Data as otherwise contemplated by this Agreement.

3.3 To the extent that Watermark receives from, or processes any Personal Data on behalf of, Organization, Watermark shall:

(a) process Personal Data:

(i) only in accordance with Organization's written instructions from time to time (including those set out in this Agreement) provided such instructions are lawful and, unless it is otherwise required by any Applicable Data Protection Laws (in which case, unless such law prohibits such notification on important grounds of public interest, Watermark shall notify Organization of the relevant legal requirement before processing the Personal Data); and

(ii) only for the duration of this Agreement;

(b) take commercially reasonable steps to ensure its personnel who are authorized to have access to such Personal Data, and ensure that any such personnel are committed to confidentiality, or are under an appropriate statutory obligation of confidentiality when processing such Personal Data; (c) taking into account:

(i) the state of the art;

(ii) the nature, scope, context and purposes of the processing; and

(iii) the risk and severity of potential harm; implement appropriate technical and organizational measures and procedures to ensure a level of security for such Personal Data appropriate to the risk, including the risks of accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, dissemination or access; and

(d) inform Organization without undue delay upon becoming aware of any such Personal Data (while within Watermark's or its subcontractors' or Affiliates' possession or control) being subject to a personal data breach.

(e) not disclose any Personal Data to any Data Subject or to a third party other than at the written request of Organization or as expressly provided for in this Agreement.

4. Return or destruction of Personal Data

4.1 Subject to paragraph 4.2, Watermark shall take reasonable steps, at Organization's option, return or irretrievably delete all Personal Data in its control or possession when it no longer requires such Personal Data to exercise or perform its rights or obligations under this Agreement, and in any event upon Organization's instruction upon the expiry or termination of this Agreement. The Organization acknowledges and agrees that Watermark shall retain IP addresses of the devices which it has processed in connection with the Services for a period of up to 90 days after termination of the Agreement before they are deleted.

4.2 To the extent that Watermark is required by Applicable Data Protection Laws to retain all or part of the Personal Data ("**Retained Data**"), Watermark shall:

(a) cease all processing of the Retained Data other than as required by the Applicable Data Protection Laws;

(b) keep confidential all such Retained Data in accordance with the confidentiality provisions set out in the Agreement; and

(c) continue to comply with the provisions of this Addendum in respect of such Retained Data.

5. **Audit**

5.1 Watermark shall permit Organization or its representatives to access any relevant premises, personnel or records of Watermark on reasonable notice to audit and otherwise verify compliance with this Addendum, subject to the following requirements:

(i) Organization may perform such audits no more than once per year or

more frequently if required by Applicable Data Protection Law regulators;

(ii) Organization may use a third party to perform the audit on its behalf, provided such third party executes a confidentiality agreement acceptable to Watermark before the audit;

(iii) audits must be conducted during regular business hours, subject to Watermark's policies, and may not unreasonably interfere with Watermark's business activities;

(iv) Organization must provide Watermark with any audit reports generated in connection with any audit at no charge unless prohibited by Applicable Data Protection Laws. Organization may use the audit reports only for the purposes of meeting its audit requirements under Applicable Data Protection Laws and/or confirming compliance with the requirements of this Addendum. The audit reports shall be confidential;

(v) to request an audit, Organization must first submit a detailed audit plan to Watermark at least twelve (12) weeks in advance of the proposed audit date. The audit must describe the proposed scope, duration and start date of the audit. Watermark will review the audit plan and inform Organization of any concerns or questions (for example, any request for information that could compromise Watermark's confidentiality obligations or its security, privacy, employment or other relevant policies). Watermark will work cooperatively with Organization to agree a final audit plan;

(vi) nothing in this paragraph 5 shall require Watermark to breach any duties of confidentiality owed to any of its clients, employees or third-party providers; and

(vii) all audits are at Organization's sole cost and expense;

6.**Co-operation and assistance**

6.1 Watermark shall:

(a) take such steps as are reasonably required to assist Organization in ensuring compliance with its obligations under Applicable Data Protection Laws;

(b) notify Organization as soon as reasonably practicable if it receives a request from a Data Subject to exercise its rights under the Applicable Data Protection Laws in relation to that person's Personal Data; and

(c) provide Organization with reasonable co-operation and assistance in relation to any request made by a Data Subject to exercise its rights under the Applicable Data Protection Laws in relation to that person's Personal Data provided that Organization shall be responsible for Watermark's costs and expenses arising from such co-operation and assistance.

6.2 If either Party receives any complaint, notice or communication which relates directly or indirectly to the processing of Personal Data by the other Party or to either Party's compliance with the Applicable Data Protection Laws, it shall as soon as reasonably practicable notify the other Party and it shall provide the other Party with commercially reasonable co-operation and assistance in relation to any such complaint, notice or communication.

7.**Sub-processors**

7.1 Organization specifically authorizes Watermark to use its affiliates as Subprocessors, and generally authorizes Watermark to engage Subprocessors to Process Customer Data. Such third party providers include any advisers, contractors, or auditors to process Personal Data ("**Sub-Processors**").

(i) Watermark will enter into a written agreement with each Subprocessor, imposing data protection obligations substantially similar to those set out in this Addendum; and

(ii) Watermark will remain liable for compliance obligations of this Addendum and for any acts or omissions of the Subprocessor that cause Watermark to breach any of its obligations under this Addendum.

7.2 A list of Sub-Processors, including their functions and locations, engaged by Watermark is available upon request, which Watermark shall update from time to time.

7.3 If Watermark engages a new Sub-Processor ("**New Sub-Processor**"), Watermark shall inform Organization of the engagement by updating the list found at paragraph 7.2 above. Watermark will endeavor to provide at least ten (10) calendar days before the new Subprocessor Processes any Customer Data, except that if Watermark reasonably believes engaging a new Subprocessor on an expedited basis is necessary to protect the confidentiality, integrity or availability of the Customer Data or avoid material disruption to the services, Watermark will give such notice as soon as reasonably practicable. If, within five (5) business days after such notice, Customer notifies Watermark in writing that Customer objects to Watermark's appointment of a new Subprocessor based on reasonable data protection concerns, the parties will discuss such concerns in good faith and whether they can be resolved.

7.4 Organization may object to the engagement of such New Sub-Processor by notifying Watermark within 5 business days of Watermark's update to the list found at 7.2 above, provided that such objection must be on reasonable, substantial grounds, directly related to such New Sub-Processor's ability to comply with substantially similar obligations to those set out in this paragraph.

7.5 If Organization does not so object, the engagement of the New Sub-Processor shall be deemed accepted by Organization.

7.6 Watermark shall ensure that its contract with each New Sub-Processor shall impose obligations on the New Sub-Processor that are substantially similar to the obligations to which Watermark is subject to under this Addendum.

7.7 Any sub-contracting or transfer of Personal Data pursuant to this paragraph 7 shall not relieve Watermark any of its liabilities, responsibilities and obligations to Organization under this Addendum and Watermark shall remain liable for the acts and omissions of its Sub-Processors.

7.8 If Organization wishes to be informed of Watermark's engagement with New Sub-Processors by email, it shall request such notification in writing to Watermark. Watermark shall, upon written confirmation of receipt of any request under this paragraph 7.8, send Organization an updated list of Sub-Processors by email to an email address requested by Organization if it engages a new Sub-Processor.

8. **Security**

a. Security Measures. Watermark will implement and maintain technical and organizational security measures designed to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, in accordance with Watermark's security standards.

b. Customer Responsibility.

(i) Customer is responsible for reviewing the information made available by Watermark relating to data security and making an independent determination as to whether the Watermark product and services meet Customer's requirements and legal obligations under Applicable Data Protection Laws.

(ii) Customer acknowledges that the Security Measures may be updated from time to time upon reasonable notice to Customer to reflect process improvements or changing practices (but the modifications will not materially decrease Watermark's obligations as compared to those reflected in such terms as of the Effective Date).

(ii) Customer agrees that, without limitation of Watermark's obligations under this Section 8, Customer is solely responsible for its use of the services, including (a) making appropriate use

of the services to ensure a level of security appropriate to the risk in respect of the Customer Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the services; (c) securing Customer's systems and devices that it uses with the services; and (d) maintaining its own backups of Customer Data.

c. Security Incident. Upon becoming aware of a confirmed Security Incident, Watermark will notify Customer without undue delay unless prohibited by applicable law. A delay in giving such notice requested by law enforcement and/or in light of Watermark's legitimate needs to investigate or remediate the matter before providing notice will not constitute an undue delay. Such notices will describe, to the extent possible, details of the Security Incident, including steps taken to mitigate the potential risks and steps Watermark recommends Customer take to address the Security Incident. Without prejudice to Watermark's obligations under this Section 8.c., Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any and all third-party notification obligations related to any Security Incidents. Watermark's notification of or response to a Security Incident under this Section 8.c. will not be construed as an acknowledgement by Watermark of any fault or liability with respect to the Security Incident.

9. **Audits and Reviews of Compliance.** The parties acknowledge that Customer must be able to assess Watermark's compliance with its obligations under Applicable Data Protection Law and this Addendum, insofar as Watermark is acting as a Processor on behalf of Customer.

a. Watermark's Audit Program. Watermark uses external auditors to verify the adequacy of its security measures with respect to its processing of Customer Data. Such audits are performed at least once annually at Watermark's expense by independent third-party security professionals at Watermark's selection and result in the generation of a confidential audit report ("Audit Report"). The availability of such Audit Report shall be made under a separate non-disclosure agreement mutually agreed upon by the parties

b. Customer Audit. Upon Customer's written request at reasonable intervals, no more frequent than once per calendar year, and subject to reasonable confidentiality controls, Watermark will make available to Customer a copy of Watermark's most recent Audit Report. Customer agrees that any audit rights granted by Applicable Data Protection Laws will be satisfied by these Audit Reports. To the extent that Watermark's provision of an Audit Report does not provide sufficient information for Customer to verify Watermark's compliance with this Addendum or Customer is required to respond to a regulatory authority audit, Customer agrees to a mutually agreed-upon audit plan with Watermark that: (a) ensures the use of an independent third party; (b) provides notice to Watermark in a timely fashion; (c) requests access only during business hours; (d) accepts billing to Customer at Watermark's then-current rates; (e) occurs no more than once annually; (f) restricts findings to only Customer Data relevant to Customer; and (g) obligates Customer, to the extent permitted by law or regulation, to keep confidential any information gathered that, by its nature, should be confidential.

10. **Impact Assessments and Consultations**. Watermark will provide reasonable cooperation to Customer in connection with any data protection impact assessment (at Customer's expense only if such reasonable cooperation will require Watermark to assign resources to that effort) or consultations with regulatory authorities that may be required in accordance with Applicable Data Protection Laws.

11. **Data Subject Requests**. Watermark will upon Customer's request (and at Customer's expense) provide Customer with such assistance as it may reasonably require to comply with its obligations under Applicable Data Protection Laws to respond to requests from individuals to exercise their rights under Applicable Data Protection Laws (e.g., rights of data access, rectification, erasure, restriction, portability and objection) in cases where Customer cannot reasonably fulfill such requests independently by using the self-service functionality of the Services. If Watermark receives a request from a Data Subject in relation to their Customer Data, Watermark will advise the Data Subject to submit their request to Customer, and Customer will be responsible for responding to any such request.

12. **Return or Deletion of Customer Data.**

a. Watermark will, within sixty (60) days after request by Customer following the termination or expiration of the Agreement, delete all Customer Data from Watermark's systems.

b. Notwithstanding the foregoing, Customer understands that Watermark may retain Customer Data if required by law, and such data will remain subject to the requirements of this Addendum.

13. **International Provisions.**

a. Processing in the United States. Customer acknowledges that, as of the Effective Date, Watermark's primary processing facilities are in the United States.

b. Jurisdiction Specific Terms. To the extent that Watermark Processes Customer Data originating from and protected by Applicable Data Protection Laws in one of the Jurisdictions listed in Schedule 4 (Jurisdiction Specific Terms), then the terms specified therein with respect to the applicable jurisdiction(s) will apply in addition to the terms of this Addendum.

c. Cross Border Data Transfer Mechanism. To the extent that Customer's use of the services requires an onward transfer mechanism to lawfully transfer personal data from a jurisdiction (i.e., the European Economic Area ("EEA"), the UK, Switzerland or any other jurisdiction listed in Schedule 3) to Watermark located outside of that jurisdiction (a "Transfer Mechanism"), the terms and conditions of Schedule 3 (Cross Border Transfer Mechanisms) will apply.

Schedule 1

Subject Matter & Details of Processing

The Personal Data processing activities carried out by Watermark under this Agreement may be described as follows:

1. **Subject matter of processing**

Watermark will process Personal Data as necessary to provide the services under the Agreement. Watermark does not sell Customer Data (or end user information within such Customer Data) and does not share such end users' information with third parties for compensation or for those third parties' own business interests.

a. Customer Data. Watermark will process Customer Data as a processor in accordance with Customer's instructions as outlined in Section 6.a (Customer Instructions) of this Addendum.

b. Usage Data. Watermark will process Usage Data as a controller for the purposes outlined in Section 4.b (Watermark as Controller) of this Addendum.

2. **Nature and purpose of processing**

a. Customer Data. Customer Data will be subject to the following basic processing activities: the provision of services that allow Watermark Customers to manage and control their Customer Data.

b. Usage Data. Personal Data contained in Usage Data will be subject to the following processing activities by Watermark: Watermark may use Usage Data to operate, improve and support the Services and for other lawful business practices, such as analytics, benchmarking, and reporting.

3. Categories of Personal Data

a. Customer Data. The categories of Customer Data are such categories as Customer is authorized to ingest into the services under the Agreement.

b. Usage Data. Watermark processes Personal Data within Usage Data.

4. **Categories of Data Subjects**

Data subjects include the individuals about whom data is provided to Watermark via the Services by (or at the direction of) Organization (i.e., Customer's end users).

5.**Duration**

The period for which Personal Data will be retained and the criteria used to determine that period is as follows:

a. Customer Data. Prior to the termination of the Agreement, Watermark will process stored Customer Data for the purpose of providing the services until Customer elects to delete such Customer Data via the Watermark services or in accordance with the Agreement.

b. Usage Data. Upon termination of the Agreement, Watermark may retain, use and disclose Usage Data for the purposes set forth above in Section 2.b (Usage Data) of this Schedule 1, subject to the confidentiality obligations set forth in the Agreement. Watermark will anonymize or delete Personal Data contained within Usage Data when Watermark no longer requires it for the purpose set forth in Section 2.b (Usage Data) of this Schedule 1.

6. Sensitive Data or Special Categories of Data.

a. Customer Data. Customers are prohibited from including sensitive data or special categories of data in Customer Data.

b. Usage Data. Sensitive Data is not contained in Usage Data.

Schedule 2

Technical & Organizational Security Measures

Where applicable, this Schedule 2 will serve as Annex II to the Standard Contractual Clauses. The following table provides more information regarding Watermark's technical and organizational security measures set forth below.

Measures of pseudonymization and encryption of personal data.

Watermark maintains Customer Data in an encrypted format at rest using industry standards.

Measures for ensuring ongoing confidentiality, integrity, and availability and resilience of processing systems and services.

Watermark's customer agreements contain strict confidentiality obligations. Additionally, Watermark requires downstream Subprocessor to sign confidentiality provisions that are substantially similar to those contained in Watermark's customer agreements.

Measures for ensuring the ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident.

Watermark performs regular backups of Customer Data, which is hosted in AWS and GCS data centers. Backups are retained redundantly across multiple availability zones and encrypted in transit and at rest using industry standards.

Processes for regular testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of processing.

Watermark maintains a risk-based assessment security program. The framework for Watermark's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data. Watermark's security program is intended to be appropriate to the nature of the Services and the size and complexity of Watermark's business operations. Watermark has a separate and dedicated security team that manages Watermark's security program. This team facilitates and supports independent audits and assessments performed by third-parties to provide independent feedback on the operating effectiveness of the information security program.

Measures for user identification and authorization.

Watermark personnel are required to use unique user access credentials and passwords for authorization. Watermark follows the principles of least privilege through role-based and time-based access models when provisioning system access. Watermark personnel are authorized to access Customer Data based on their job function, role and responsibilities, and such access requires approval prior to access provisioning. Access is promptly removed upon role change or termination.

Measures for ensuring physical security of locations at which personal data are processed.

Watermark headquarters and office spaces have a physical security program that manages visitors, building entrances, CCTVs (closed circuit televisions), and overall office security.

The Services operate on industry standard cloud providers (e.g., Amazon Web Services ("AWS")) and are protected by the security and environmental controls of Amazon.Detailed information about AWS security is available at https://aws.amazon.com/security/ and http://aws.amazon.com/security/sharing-the-security-responsibility/. For AWS SOC Reports, please see https://aws.amazon.com/compliance/soc-faqs/.

Measures for internal IT and IT security governance and management.

Watermark maintains a risk-based assessment security program. The framework for Watermark's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data. Watermark's security program is intended to be appropriate to the nature of the Services and the size and complexity of Watermark's business operations. Watermark has a separate and dedicated Information Security team that manages Watermark's security program.

Measures for certifications/assurance of processes and products.

Watermark conducts various third-party audits to attest to various frameworks SOC 2 Type 2, and application penetration testing.

Measures for ensuring data minimization.

Watermark operates on a shared responsibility model. Watermark provides tools within the Services that gives Customers control over exactly what data enters the platform and enables Customers with the ability to block data at the Source level.

Measures for ensuring data quality.

Watermark operates on a shared responsibility model. Watermark ensures that data quality is maintained from the time a Customer sends Customer Data into the Services and until that Customer Data leaves Watermark to flow to a downstream destination.

Measures for ensuring accountability.

Watermark has adopted measures for ensuring accountability, such as implementing data protection policies across the business, maintaining documentation of processing activities, recording and reporting Security Incidents involving Personal Data, and appointing a Data Protection Officer. Additionally, Watermark conducts regular third-party audits to ensure compliance with our privacy and security standards.

Measures for allowing data portability and ensuring erasure.

Watermark's Customers have direct relationships with their end users and are responsible for responding to requests from their end users who wish to exercise their rights under Applicable Data Protection Laws. If Watermark receives a request from a Data Subject in relation to their Customer Data, Watermark will advise the Data Subject to submit their request to Customer, and Customer will be responsible for responding to any such request.

SCHEDULE 3

CROSS BORDER DATA TRANSFER MECHANISM

Definitions

a. "**Standard Contractual Clauses**" means, depending on the circumstances unique to any particular Customer, any of the following:

(i) UK Standard Contractual Clauses; and

(ii) 2021 Standard Contractual Clauses

b. "**UK Standard Contractual Clauses**" means:

(i) Standard Contractual Clauses for data controller to data processor transfers approved by the European Commission in decision 2010/87/EU ("UK Controller to Processor SCCs"); and

(ii) Standard Contractual Clauses for data controller to data controller transfers approved by the European Commission in decision 2004/915/EC ("UK Controller to Controller SCCs").

c. "**2021 Standard Contractual Clauses**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

2. UK Standard Contractual Clauses. For data transfers from the United Kingdom that are subject to the UK Standard Contractual Clauses, the UK Standard Contractual Clauses will be deemed entered into (and incorporated into this Addendum by reference) and completed as follows:

a. The UK Controller to Processor SCCs will apply where Watermark is processing Customer Data. The illustrative indemnification clause will not apply. Schedule 1 serves as Appendix 1 of the UK Controller to Processor SCCs. Schedule 2 serves as Appendix 2 of the UK Controller to Processor SCCs.

b. The UK Controller to Controller SCCs will apply where Watermark is processing Usage Data. In Clause II(h), Watermark will process personal data in accordance with the data processing principles set forth in Annex A of the UK Controller to Controller SCCs. The illustrative commercial clause will not apply. Schedule 1 serves as Annex B of the UK Controller to Controller SCCs. Personal Data transferred under these clauses may only be disclosed to the following categories of recipients: i) Watermark's employees, agents, affiliates, advisors and independent contractors with a reasonable business purpose for needing such personal data; ii) Watermark vendors that, in their performance of their obligations to Watermark, must process such personal data acting on behalf of and according to instructions from Watermark; and iii) any person (natural or legal) or organization to whom Watermark may be required by applicable law or regulation to disclose personal data, including law enforcement authorities, central and local government.

3. The 2021 Standard Contractual Clauses. For data transfers from the European Economic Area that are subject to the 2021 Standard Contractual Clauses, the 2021 Standard Contractual Clauses will apply in the following manner:

a. **Module One** (Controller to Controller) will apply where Customer is a controller of Usage Data and Watermark is a controller of Usage Data.

b. **Module Two** (Controller to Processor) will apply where Customer is a controller of Customer Data and Watermark is a processor of Customer Data;

c. **Module Three** (Processor to Processor) will apply where Customer is a processor of Customer Data and Watermark is a sub-processor of Customer Data;

d. **For each Module, where applicable**:

(i) in Clause 7, the option docking clause will not apply;

(ii) in Clause 9, Option 2 will apply, and the time period for prior notice of sub-processor changes will be as set forth in Section 7 (Subprocessing) of this Addendum;

(iii) in Clause 11, the optional language will not apply;

(iv) in Clause 17 (Option 1), the 2021 Standard Contractual Clauses will be governed by Irish law.

(v) in Clause 18(b), disputes will be resolved before the courts of Ireland;

(vi) In Annex I, Part A:

Data Exporter: Customer and authorized affiliates of Customer.

Contact Details: Customer's account owner email address, or to the email address(es) for which Customer elects to receive privacy communications.

Data Exporter Role: The Data Exporter's role is outlined in Section 4 of this Addendum.

Signature **&** **Date**:

_____

By entering into the Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

Data Importer: Watermark Insights, LLC

Contact Details: Watermark Privacy Team – privacy@watermarkinsights.com

Data Importer Role: The Data Importer's role is outlined in Section 4 of this Addendum.

Signature & Date

_____

By entering into the Agreement, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

(vii) In Annex I, Part B:

The categories of data subjects are described in Schedule 1, Section 4.

The sensitive data transferred is described in Schedule 1, Section 6.

The frequency of the transfer is a continuous basis for the duration of the Agreement.

The nature of the processing is described in Schedule 1, Section 1.

The purpose of the processing is described in Schedule 1, Section 1.

The period of the processing is described in Schedule 1, Section 3.

(viii) In Annex I, Part C: The Irish Data Protection Commission will be the competent supervisory authority.

(ix) Schedule 2 serves as Annex II of the Standard Contractual Clauses.

4. To the extent there is any conflict between the Standard Contractual Clauses and any other terms in this Addendum, including Schedule 4 (Jurisdiction Specific Terms), the provisions of the Standard Contractual Clauses will prevail.

SCHEDULE 4

JURISDICTION SPECIFIC TERMS

1. California

a. The definition of "Applicable Data Protection Law" includes the California Consumer Privacy Act (CCPA).

b. The terms "business", "commercial purpose", "service provider", "sell" and "personal information" have the meanings given in the CCPA.

c. With respect to Customer Data, Watermark is a service provider under the CCPA.

d. Watermark will not (a) sell Customer Data; (b) retain, use or disclose any Customer Data for any purpose other than for the specific purpose of providing the Services, including retaining, using or disclosing the Customer Data for a commercial purpose other than providing the Services; or (c) retain, use or disclose the Customer Data outside of the direct business relationship between Watermark and Customer.

e. The parties acknowledge and agree that the Processing of Customer Data authorized by Customer's instructions described in Section 6 of this Addendum is integral to and encompassed by Watermark's provision of the Services and the direct business relationship between the parties.

f. Notwithstanding anything in the Agreement or any Order Form entered in connection therewith, the parties acknowledge and agree that Watermark's access to Customer Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement.

g. To the extent that any Usage Data (as defined in the Agreement) is considered Personal Data, Watermark is the business with respect to such data and will Process such data in accordance with its Privacy Policy, which can be found at https://www.watermarkinsights.com/privacy-policy/.

2. EEA

a. The definition of "Applicable Data Protection Laws" includes the General Data Protection Regulation (EU 2016/679)("GDPR").

b. When Watermark engages a Subprocessor under Section 7 (Subprocessing), it will:

(i) require any appointed Subprocessor to protect Customer Data to the standard required by Applicable Data Protection Laws, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR; and

(ii) require any appointed Subprocessor to agree in writing to only process data in a country that the European Union has declared to have an "adequate" level of protection; or to only process data on terms equivalent to the Standard Contractual Clauses.

c. GDPR Penalties. Notwithstanding anything to the contrary in this Addendum or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

3. Switzerland

a. The definition of "Applicable Data Protection Laws" includes the Swiss Federal Act on Data Protection.

b. When Watermark engages a Subprocessor under Section 7 (Subprocessing), it will

(i) require any appointed Subprocessor to protect Customer Data to the standard required by Applicable Data Protection Laws, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR; and

(ii) require any appointed Subprocessor to agree in writing to only process data in a country that the European Union has declared to have an "adequate" level of protection; or to only process data on terms equivalent to the Standard Contractual Clauses.

4. United Kingdom

a. References in this Addendum to GDPR will to that extent be deemed to be references to the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018).

b. When Watermark engages a Subprocessor under Section 7 (Subprocessing), it will:

(i) require any appointed Subprocessor to protect Customer Data to the standard required by Applicable Data Protection Laws, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR; and

(ii) require any appointed Subprocessor to agree in writing to only process data in a country that the European Union has declared to have an "adequate" level of protection; or to only process data on terms equivalent to the Standard Contractual Clauses.

[End]