Accuweather – Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of the agreement that links to this DPA (the "**Agreement**") by and between the service provider that executed the Agreement ("**Service Provider**") and AccuWeather, Inc. and its affiliates and subsidiaries ("**Customer**"). This DPA shall reflect the parties' agreement with regard to the Processing of Personal Data (as defined below) in the performance of the Agreement. Company and Service Provider may be referred to in this DPA individually as a "**Party**" or jointly as the "**Parties**."

1. Definitions.

a. "**Controller**" has the meaning set forth in the applicable Data Protection Laws, provided that, as used herein, "Controller" shall also include a "Business," as such term is defined by the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("**CPRA**").

b. "**Data Protection Laws**" means applicable international, federal, state, and local laws, regulations, self-regulatory rules, and guidelines relating to or impacting the Processing, privacy, security, security breach notification, or data protection of Personal Data, including but not limited to: European Data Laws, the CPRA, Colorado Privacy Act, Connecticut Data Privacy Act, Delaware Personal Data Privacy Act, Indiana Consumer Data Protection Act, Iowa Consumer Data Protection Act, Kentucky Consumer Data Protection Act, Maryland Online Data Privacy Act, Minnesota Consumer Data Privacy Act, Montana Consumer Data Privacy Act, Nebraska Data Privacy Act, New Hampshire Privacy Act, New Jersey Data Privacy Act, Nevada Consumer Health Data Privacy Law, Oregon Consumer Privacy Act, Tennessee Information Protection Act, Texas Data Privacy and Security Act, Utah Consumer Privacy Act, Virginia Consumer Data Protection Act, and/or any other applicable law, rule, or regulation relating to the protection of Personal Data.

c. "**Data Subject**" means the individual to whom Personal Data relates.

d. "**EEA**" means the European Economic Area.

e. "**European Data Laws**" means all applicable data protection and privacy laws and regulations in European jurisdictions, including, but not limited to, for EEA territories, the General Data Protection Regulation (EU) 2016/679 and any successor legislation and associated national implementations thereto (the "**GDPR**") and, for the United Kingdom, the United Kingdom Data Protection Act 2018 (the "**UK GDPR**"), and the Switzerland Federal Act on Data Protection ("**FADP**").

f. "**Customer Personal Data**" means Personal Data provided or made available to Service Provider by Customer, or Personal Data derived from such data.

g. "**Personal Data**" means any information that (i) identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, or (ii) any data, or information that constitutes "personal data," "personal information," or "personally identifiable information," under Data Protection Laws.

h. "**Process**", "**Processed**", and "**Processing**" means any operation or set of operations which is performed on Customer Personal Data or on sets of Customer Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or

alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

i. "**Processor**" has the meaning set forth in Data Protection Laws, provided that, as used herein, "Processor" shall also include a "Service Provider," as such term is defined by the CPRA.

j. "**Security Incident**" means any actual or reasonably suspected unauthorized access to, use, modification, loss, compromise, destruction, disclosure, or acquisition of Customer Personal Data.

k. "**Sell**" has the meaning set forth in Data Protection Laws.

l. "**Services**" means the provision of products, services or other work products by Service Provider as described and set out in the Agreement, and such other services as the parties may agree upon in writing from time to time.

m. "**Share**" has the meaning set forth in Data Protection Laws.

n. "**Standard Contractual Clauses**" or "**SCC**" means the means the standard contractual clauses that are a legally enforceable mechanism under Data Protection Laws for the transfer of Personal Data to any country that does not have an adequate level of data protection to permit the transfer of Personal Data to (pursuant to a decision of the relevant supervisory authority) ("**Third Country**").

o. "**Subprocessor**" means a third party engaged by Service Provider to assist with the provision of the Services which involves the Processing of Customer Personal Data.

p. "**Term**" is the term of the Agreement.

2. <u>Processing of Customer Personal Data</u>.

a. **Roles of the Parties.** The Parties acknowledge that with regard to the Processing of Customer Personal Data in accordance with the Services, Customer is the Controller and Service Provider is the Processor.

b. **Service Provider's Processing of Customer Personal Data.**

i. Service Provider shall Process Customer Personal Data in accordance with Customer's documented written instructions. Service Provider shall immediately, and in any event within two (2) business days, notify Customer in writing if Service Provider reasonably believes that an instruction issued by Customer would violate any applicable laws or regulations, including Data Protection Laws.

ii. The nature and purposes of the Processing of Customer Personal Data, the type of data subject to the Processing and the duration of the Processing are set forth in Appendix I.

iii. Service Provider will not: (i) Sell or Share Customer Personal Data; (ii) retain, use, or otherwise disclose any Customer Personal Data for any purpose other than to provide the Services or outside of the direct relationship between Customer and Service Provider; or (iii) combine Customer Personal Data with other Personal Data collected by Service Provider

from sources other than Customer. Service Provider certifies that it understands the restrictions in this Section and will comply with them.

iv. Service Provider shall comply with Data Protection Laws in its Processing of Customer Personal Data, including to provide the same level of privacy protection to Customer Personal Data as is required by Data Protection Laws. Service Provider shall, immediately, and in any event within two (2) business days, notify Customer in writing if Service Provider makes a determination that it can no longer meet its obligations under Data Protection Laws. Customer may take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data by Service Provider and to ensure Customer Personal Data is used by Service Provider in a manner consistent with Customer's obligations under Data Protection Laws.

c. **Processor Obligations.**

i. Upon Customer's request, Service Provider will fully and timely cooperate with Customer, at no additional cost to Customer, to enable Customer to: (1) comply with Data Subject requests to exercise their rights under Data Protection Laws, including but not limited to requests of access, rectification, and/or deletion of Customer Personal Data; and/or (2) comply with all requests from a governmental/regulatory authority, including but not limited to in the event of an investigation. If, during the Term, Service Provider receives any request from a Data Subject in relation to Customer Personal Data, Service Provider shall forward to Customer any such request within two (2) business days of receiving such request and advise the Data Subject to submit their request to Customer.

ii. Service Provider shall provide timely and reasonable assistance to Customer where Customer carries out a data protection assessment relating to Customer Personal Data, including but not limited to providing all information necessary for Customer to conduct and document such data protection assessment.

iii. Service Provider shall immediately, and in any event within two (2) business days, notify Customer in writing in the event it receives any request, complaint, or communication relating to Customer's obligations under Data Protection Laws (including from governmental/regulatory authorities). To the extent permitted by applicable law, Service Provider shall obtain specific written consent and instructions from Customer prior to responding to such request, complaint, or communication.

3. <u>Data Security</u>.

a. Service Provider shall implement and maintain appropriate administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of Customer Personal Data and prevent Security Incidents. Such security safeguards shall be (i) at least equal to those required by applicable Data Protection Laws and, to the extent not inconsistent with the foregoing, (ii) no less rigorous than industry-accepted information security standards (e.g., SSAE 18 SOC 1 or SOC 2 Type 2 report, ISO 27001 and 27002, ISO 27017, NIST Cybersecurity Framework, AICPA Trust Services Principles, Center for Internet Security (CIS) Controls) ("**Industry Accepted Information Security Standards**").

b. Service Provider shall undertake regular reviews of the administrative, technical and physical safeguards and the data Processing operations connected with the Services to ensure compliance with this DPA.

c. Service Provider will only grant access to Customer Personal Data to employees and contractors who need such access for purposes consistent with this DPA and who are bound by obligations of confidentiality or have signed confidentiality agreements with Service Provider containing protections not materially less protective of Customer Personal Data than those herein.

4. Security Incidents.

a. Service Provider will immediately, and in any event within twenty-four (24) hours, notify Customer in writing of a Security Incident. Service Provider will provide Customer with a detailed, written report regarding the nature of the Security Incident, including the types of Customer Personal Data affected, the number and identity of affected individuals, if known, the status of remediation efforts and other relevant details of such incident as may be reasonably requested by Customer. Service Provider shall provide updated, written reports to Customer as additional, relevant information becomes available.

b. At no additional cost, Service Provider will (and will ensure that its Subprocessors will) fully and timely cooperate with Customer in investigating the Security Incident, including by, (a) providing Customer with all computer forensics reports prepared by or on behalf of Service Provider relating to the Security Incident; (b) facilitating interviews with Service Provider's employees and others involved in the matter; and (c) making available all relevant records, logs, files, data reporting and other materials required to comply with Data Protection Laws or as otherwise reasonably required by Customer. On notice of any Security Incident, Service Provider will immediately institute appropriate controls to maintain and preserve all documents, records and other data relating to the breach in accordance with industry best practices.

c. In the event any Security Incident requires notification to an individual under any Data Protection Laws, Customer will have sole control over the timing, content, and method of notification and Service Provider will promptly reimburse Customer for all costs and expenses incurred as a result of the Security Incident, including but not limited to, costs related to responding to, investigating and mitigating the Security Incident, regulatory fines and penalties, and the costs of providing notice, credit monitoring, identity fraud protection, identity theft restoration and engaging in other remediation effort that are necessary, reasonable, and appropriate under the circumstances, as reasonably determined by Customer.

5. Subprocessors.

a. Customer authorizes Service Provider to appoint Subprocessors in accordance with this Section 5 and any restrictions that may be set forth in the Agreement.

b. Notwithstanding anything to the contrary in this DPA or the Agreement, Service Provider may continue to use all Subprocessors already engaged by Service Provider as of the Effective Date, set forth in Annex II, subject to Service Provider complying with the obligations set forth in this Section 5.

c. Service Provider shall provide thirty (30) days written notice to Customer where Service Provider wishes to engage a Subprocessor to Process Customer Personal Data. Where Service Provider wishes to appoint a Subprocessor under this DPA, Service Provider will select the Subprocessor with due diligence and will verify prior to engaging the Subprocessor that such Subprocessor is capable of complying with the obligations of Service Provider towards Customer, to the extent applicable to the Services assigned to that Subprocessor. If, within thirty (30) days of receipt of such notice, Customer notifies Service Provider in writing of any

objections (on reasonable grounds) to the proposed appointment, then Service Provider shall not appoint (or disclose any Customer Personal Data to) the proposed Subprocessor until reasonable steps have been taken to address the reasonable objections raised by Customer. If the Parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may terminate the Agreement and/or this DPA by providing written notice to Service Provider.

d. Service Provider shall enter into a written contract with each Subprocessor whereby Service Provider shall require the Subprocessor to comply with obligations no less onerous than Service Provider's obligations under this DPA. Service Provider shall ensure the subcontracting agreement with such Subprocessor includes appropriate contractual provisions in accordance with Data Protection Laws.

e. Such subcontracting under this Section 5 shall not release Service Provider from its responsibility under the Agreement and this DPA. Service Provider shall be responsible for the work and activities of all Subprocessors, including any Security Incidents caused by Subprocessors.

6. <u>Audits</u>.

a. Service Provider shall make available to Customer, at Customer's request, all information necessary to verify Service Provider's compliance with its obligations under this DPA and Data Protection Laws.

b. Service Provider shall allow Customer or an auditor appointed by Customer to, at least once every twelve (12) months, carry out audits, manual reviews, automated scans, regular assessments, or other technical and operational testing, the scope of which shall be mutually agreed by the Parties in advance, relating to the Processing of Customer Personal Data by Service Provider or any Subprocessor to enable Customer to verify compliance with the requirements of this DPA and/or Data Protection Laws. Service Provider shall cooperate with such audit.

c. Service Provider shall retain a qualified and independent assessor to perform an annual audit of the physical, technical, administrative, and organizational safeguards put in place by Service Provider that relate to the protection of the security, confidentiality, or integrity of Customer Personal Data using an appropriate and industry accepted control standard or framework and assessment procedure, or documentation of certification of compliance with, one or more Industry Accepted Information Security Standards. The most current report or documentation of certification will be due to Customer within thirty (30) days of the Effective Date and thereafter annually within thirty (30) days of Service Provider's receipt from its audit firm.

d. Service Provider shall annually conduct its own internal audit in Service Provider's physical and technical environment as it relates to the receipt, maintenance, use or retention of Kevnue Personal Data, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognized third-party audit firm based on the recognized industry best practices.

e. If any audit or test referenced above uncovers exceptions or deficiencies in Service Provider's security controls, Service Provider shall promptly address and remediate such identified exceptions and deficiencies.

7. <u>Cross Border Transfers</u>.

a. **GDPR.** Where Customer Personal Data protected by the GDPR is transferred outside the EEA to a Third Country, the EU SCCs shall apply as follows:
   i. Module Two will apply.
   ii. In Clause 7, the optional docking clause will not apply;
   iii. In Clause 9, Option 2 will apply, and the requirements for prior notice of Subprocessor changes shall be as set out in Section 5 of this DPA;
   iv. In Clause 11, the optional language shall not apply;
   v. In Clause 17, Option 1 will apply;
   vi. In Clause 18(b), disputes shall be resolved before the courts of the jurisdiction governing the Agreement or, if that jurisdiction is not an EU Member State, then the courts in the jurisdiction associated with Customer. In any event, Clause 17 and 18 (b) shall be consistent in that the choice of forum and jurisdiction shall correspond to the country of the governing law;
   vii. The Annexes to the EU SCCs shall be deemed completed with the information set out in Section 3 of this DPA and Appendices I-II to this DPA;

b. **UK GDPR.** Where Customer Personal Data protected by UK GDPR is transferred outside the United Kingdom to a Third Country, the SCC UK Addendum shall apply as follows:
   i. The EU SCCs, completed as set out in Section 7(a) above, shall also apply to transfers of such Customer Personal Data;
   ii. The Appendix Information (as defined in the SCC UK Addendum) shall be deemed completed with the relevant information set out in Section 3 of this DPA and Appendices I-II to this DPA; and
   iii. The SCC UK Addendum shall be deemed executed between the Customer and Service Provider, and the SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of Customer Personal Data.

c. **FADP.** Where Customer Personal Data is transferred outside Switzerland to a Third Country and such data transfer is governed by FADP, the SCCs, completed as set out in Section 7(a) above, shall apply to such data transfers, with the following exceptions:
   i. Without prejudice to Clause 13 (a) the competent supervisory authority in respect of the data transfer governed by FADP, pursuant to Annex I.C of the EU SCCs shall be the Swiss Federal Data Protection and Information Commissioner;
   ii. In Clause 17, the governing law shall be the laws of Switzerland;
   iii. In Clause 18(c), the competent courts shall be the courts of Zurich, Switzerland;
   iv. Any references to "Member State(s)" in the SCCs shall be interpreted to refer to Switzerland, and Data Subjects located in Switzerland shall be entitled to exercise and enforce their rights under the EU SCCs in Switzerland;
   v. Any references to the "General Data Protection Regulation", "Regulation 2016/679" or "GDPR" in the SCCs shall be complemented with references to the FADP (as amended or replaced).

8. <u>Return and Destruction</u>.

a. Following termination or expiration of the Agreement for whatever reason, Service Provider shall cease Processing Customer Personal Data and shall require that all Subprocessors cease Processing Customer Personal Data.

b. Following termination or expiration of the Agreement for whatever reason, Service Provider shall promptly, and in no event later than thirty (30) days from the effective date of termination

or expiration, return or destroy, at Customer's sole option, all Customer Personal Data and copies thereof, and provide certification in writing by a duly authorized executive of Service Provider to Customer that it has done so without retaining any copies, unless and for the duration applicable law prevents Service Provider from doing so. In the event Service Provider retains Customer Personal Data after termination or expiration of the Agreement, Service Provider represents, warrants and agrees that it will not further Process such Customer Personal Data and will continue to comply with the confidentiality and privacy obligations hereunder until it is no longer in possession of Customer Personal Data.

9. **Indemnification.** Service Provider shall indemnify, defend and hold harmless Customer and its subsidiaries, affiliates, and each of their respective officers, directors, employees, agents, successors, and assigns (each, a "**Customer Indemnitee**") from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees, arising out of or resulting from any claim against any Customer Indemnitee arising out of or resulting from (i) Service Provider's breach of its obligations under this DPA, (ii) acts or omissions by Service Provider or any of its Subprocessors that constitute negligence or violate any Data Protection Laws, and (iii) Security Incidents.

10. **Liability.** Any limitation of liability set forth in the Agreement shall not apply to Service Provider's breach of this DPA or its indemnification obligations hereunder.

11. **Effect of this DPA.** Except as otherwise set forth herein, the terms and conditions of this DPA, including the Appendices, are part of and incorporated into the Agreement, and the terms and conditions of this DPA constitute the entire and exclusive agreement between the Parties with respect to its subject matter. To the extent of any conflict or inconsistency between this DPA and the terms of the Agreement, this DPA will govern.

12. **Miscellaneous.** This DPA may not be amended or modified except in writing signed by authorized representatives of both Parties. If any provision in this DPA is determined to be ineffective or void by any court or body of competent jurisdiction or by virtue of any legislation to which it is subject, it shall be ineffective or void to that extent only and the validity and enforceability of the remaining provisions of the DPA and the Agreement shall not be affected. The Parties shall promptly and in good faith work to replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. The Parties shall similarly promptly and in good faith add any necessary appropriate provision where such a provision is found to be missing by any court or body of competent jurisdiction or by virtue of any legislation to which this DPA is subject.

Appendix I – Processing Details

Duration of the Processing	The overall duration of Service Provider's Processing of Customer Personal Data is the Term plus the period from the expiry of the Term until the return or destruction of all Customer Personal Data by Service Provider in accordance with the DPA.
Frequency of the Processing	On a continuous basis.
Nature and Purpose of the Processing	To perform the Services pursuant to the Agreement.
Categories of Data and Data Subjects	The categories of data Processed by Service Provider may include: identifiers (e.g., name, address, unique personal identifier, online identifier, IP address, email address, government issued ID, telephone number), characteristics of protected classifications under applicable laws, commercial information (e.g., products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies), Internet or other electronic network activity information (e.g., browsing history, search history, and information regarding interaction with an internet website application, or advertisement), geolocation data, professional or employment-related information, education information, sensitive Personal Data (e.g., precise geolocation data, racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership, health information). The Data Subjects may include: Customer employees, job applicants, customers, business partners and prospects, vendors or consumers
Period of Time Data Will be Retained	Customer Personal Data will be stored for no longer than is necessary or appropriate in light of the purpose of the Agreement and subject to applicable laws, decisions, and guidelines of regulatory authorities.
Subprocessor Transfers	For information on Subprocessor transfers, please refer to Appendix II.

Appendix II – List of Subprocessors

To be provided by Service Provider.