DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is between Conagra Brands, Inc. and its affiliates (Collectively, "**Conagra**") and the service provider accepting these terms and conditions ("**Service Provider**") (collectively, the "**Parties**"). Where the Parties are subject to an existing written agreement ("**Agreement**"), this DPA is intended to supplement such existing Agreement, is hereby incorporated by reference into the Agreement. This DPA replaces and supersedes any prior data processing addendums and will survive termination of the Agreement.

Whereas, certain privacy and/or data security laws, including but not limited to the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 (collectively, "**CCPA**"), Colorado Privacy Act ("**CPA**"), Virginia Consumer Data Protection Act ("**VCDPA**"), Connecticut Data Privacy Act ("**CTDPA**"), and Utah Consumer Privacy Act ("**UPA**"), may apply to Personal Data (as defined below) shared or disclosed by Conagra to Service Provider pursuant to the Parties' Agreement;

Whereas, the Parties written Agreement, may allow Service Provider, its employees, and/or agents (all of whom shall collectively be the "**Service Provider**"), to process, retain, use, and/or disclose Personal Data shared by Conagra in order to perform the services set forth in the Agreement on behalf of Conagra ("**Services**") or some other business purpose agreed to by the Parties (the "**Business Purpose**");

For good and valuable consideration, the receipt and sufficiency of which the Parties acknowledge, the Parties agree as follows:

1. **Definitions.**
   a) "**Controller**" means the Party that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. "Controller" has the same meaning as "business," as defined under Data Protection Laws.
   b) "**Data Subject**" means an identified or identifiable person.
   c) "**De-Identified Data**" means data that cannot reasonably be used to infer information about, or otherwise be linked to a Data Subject or as that term is otherwise defined under Data Protection Laws.
   d) "**Data Protection Laws**" means all laws, regulations or guidance applicable to the Processing of Personal Data pursuant to the Agreement, including the CCPA, CPA, VCDPA, CTDPA, UPA, and Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"), any amendments thereto, and any other foreign or domestic laws, to the extent applicable.
   e) "**Highly-Sensitive Personal Data**" means an (i) individual's government-issued identification number (including social security number, driver's license number or state-issued identified number); (ii) financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; or (iii) biometric or health data.
   f) "**Personal Data**" means any information relating to a Data Subject that is Processed by Service Provider on behalf of Conagra.
   g) "**Process**" or "**Processing**" means any operation or set of operations performed on Personal Data, whether or not by automated means, including but not limited to accessing, collecting, using, storing, transferring, retaining, disclosing, selling, sharing, deleting, and destroying Personal Data.
   h) "**Processor**" means the Party that Processes Personal Data on behalf of the Controller and includes a "service provider" as defined in Data Protection Laws.
   i) "**Security Incident**" means any suspected or known unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of Personal Data.

2. **Obligations of Service Provider.** Service Provider will Process the Personal Data in the capacity of a Processor, and Conagra will be the Controller of the Personal Data. Service Provider is fully responsible for any authorized or unauthorized Processing of Personal Data. Service Provider agrees to the following:
   a) Service Provider shall at all times comply with Data Protection Laws when Processing Personal Data.
   b) Service Provider shall only Process the Personal Data on documented instructions from Conagra solely to fulfill the Business Purpose, including with regard to transfers of Personal Data to a third country or an international organization, and in such manner as is necessary for the provision of services under the Agreement and this DPA.

c) Except as expressly permitted by Data Protection Laws, Service Provider is strictly prohibited from retaining, using, disclosing, or otherwise Processing Personal Data (i) for any reason or purpose other than those specified in the Agreement and in this DPA; (ii) for any commercial purpose other than the specific business purposes specified in this Agreement and this DPA, including to provide services to a different business; and (iii) outside the direct business relationship between Conagra and Service Provider, including to combine or update Personal Data with information received from or on behalf of another source or collected from Service Provider's own interactions with a Data Subject.
d) Service Provider shall not disclose or use Personal Data in any way that could be construed as a "sale" or "sharing" of Personal Data under Data Protection Laws.
e) Service Provider may not delegate or sub-contract any of its Services to a third-party without Conagra's prior written authorization, and then only if Service Provider enters into a written contract requiring any such third-party to be bound by the same data protection obligations of the Service Provider under this DPA
f) Service Provider will retain Personal Data as directed by Conagra, or as required by applicable laws. At the termination of the Agreement, or upon Conagra's written request, the Service Provider will either destroy or return the Personal Data to Conagra unless legal obligations require storage of Personal Data.
g) Service Provider will provide the same level of privacy protection as is required by Conagra and treat all Personal Data as strictly confidential and will not disclose the Personal Data to third parties except as permitted by this DPA or the Agreement.
h) Service Provider will ensure that all personnel who Process Personal Data have undergone data protection training and are bound by obligations of confidentiality.
i) Service Provider, at Conagra's request, will update, correct, delete, supplement, transfer, and provide Conagra with access to Personal Data in Service Provider's possession or control.
j) Service Provider will cooperate with and assist Conagra in complying with Data Protection Laws, including but not limited to assisting with data protection impact assessments, audits, and consultations with regulatory bodies.
k) Service Provider will appoint a data protection officer, where required by Data Protection Laws.
l) Service Provider, with respect to any De-Identified Data that Processor Processes under the Agreement: (i) take reasonable measures to ensure that such data cannot be associated with a Data Subject; (ii) Process such data only in a de-identified fashion and only for its internal business purposes; (iii) not attempt to re-identify such data; (iv) contractually obligate any recipients of such data to comply with this section; and (v) publicly commit to complying with this section, such as through a prominent disclosure in its privacy policy, on its website, or similar means.
m) Service Provider, upon receipt of a legally-binding request for access to Personal Data from a public authority and where permitted by applicable law, will immediately notify Conagra of the request for access and provide details about the requesting party, the types of Personal Data requested, and the purpose and methods of this disclosure (so as to provide Conagra the opportunity to comply with its notice and consent obligations with respect to affected Data Subjects or oppose the disclosure and obtain a protective order or seek other relief).

3. **Data Subject Requests.** Conagra will inform Processor of any Data Subject request that the Parties are obligated to comply with, including but not limited to requests to access, update, correct, delete, or transfer Personal Data, restrict or stop certain Processing, or obtain additional details about how Personal Data is Processed. Conagra will provide the information necessary for Processor to comply with such requests, and Processor will cooperate, and follow any instructions issued by Conagra, in responding to such requests in a timely and lawful manner. In the event Processor receives a request directly from a Data Subject relating to Personal Data, Processor will immediately notify Conagra and, at Conagra's direction, act on behalf of Conagra in accordance with Conagra's instructions for responding to such requests. Processor will provide confirmation and supporting documentation that verifies its compliance with this section, upon request.

4. **Security.**

a) Service Provider shall implement and maintain organizational, physical, technical, and administrative safeguards for Personal Data and Service Provider's systems, which are designed to ensure the integrity and reliability of such Personal Data and Service Provider systems and to prevent Security Incidents in relation to the foregoing (the "**Safeguards**"). Such Safeguards shall be commensurate with the type and amount of Personal Data Processed by Service Provider and the nature of the Business Purpose, and shall, at a minimum, protect Personal Data from reasonably anticipated hazards and ensure compliance with Data Protection Laws. Service Provider represents that it has implemented and covenants that it shall maintain such Safeguards and a written information security program

documenting such Safeguards.

b) At a minimum, Service Provider's Safeguards for the protection of Personal Data shall include without limitation: (i) limiting access of Personal Data to employees with a reasonable need to know in order to perform the Services; (ii) securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, device application, database and platform security; (iv) securing information transmission, storage and disposal; (v) implementing authentication and access controls within media, applications, operating systems and equipment; (vi) where applicable, encrypting Highly-Sensitive Personal Data stored on any mobile media; (vii) where applicable, encrypting Highly-Sensitive Personal Data transmitted over public or wireless networks; (viii) strictly segregating Personal Data from information of Service Provider or its other customers so that Personal Data is not commingled with any other types of information; (ix) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (x) providing appropriate privacy and information security training to Service Provider's employees.

5. **Data Transfer.** Service Provider shall comply in all respects with all relevant Data Protection Laws relating to the transfer of Personal Data from an originating country or jurisdiction to another country or jurisdiction ("**Data Transfer**"). As required in accordance with the Data Protection Laws, the Parties shall enter into an appropriate processor agreement to govern each Data Transfer that contains approved standard contractual clauses (each a "**Processor Agreement**"). With respect to any Processor Agreement entered into by and between Conagra and Service Provider, in the event of any conflict between the terms of this Agreement and such Processor Agreement, the Processor Agreement shall prevail.

6. **Audit.** Conagra may audit Service Provider's compliance with its obligations under this DPA no more than once per calendar year by providing a minimum of 30 days prior notice (the "Annual Audit"). Notwithstanding the foregoing, in the event Service Provider has experienced a Security Incident in the preceding 12 months or if Conagra's Annual Audit reveals any actual or potential security vulnerability or other instances of non-compliance under this DPA, Conagra may re-audit Service Provider at commercially reasonable intervals as required until such security vulnerability or non-compliance is mitigated. Provider shall correct any security vulnerability promptly in accordance with industry standards and pay for all costs associated with mitigating any such security vulnerability or noncompliance.

7. **Incident Management.**

a) Service Provider shall notify Conagra immediately but no later than twenty-four (24) hours of becoming aware of a Security Incident involving the Service Provider or its sub-processors at Privacy@conagra.com and cybersecurity@conagra.com or such other address as Conagra may specify in writing.

b) Service Provider notification regarding the Security Incident, to the extent known, shall include: (i) a description of the Security Incident, including the date and time when it took place and was discovered, the number and jurisdictions of Data Subjects affected, the categories of Personal Data involved, and the likely consequences of the Security Incident; (ii) the measures that were taken to address it, including measures to mitigate the possible adverse effects; (iii) a summary of the incident that caused the Security Incident and any ongoing risks that the Security Incident poses; (iv) the contact details of the data protection officer or other contact; (v) any other information required under Data Protection Laws; and (vi) any other information reasonably requested by Conagra relating to the Security Incident. Service Provider shall take all appropriate corrective action, at Service Provider's sole cost and expense, to prevent a recurrence of it.

c) Pursuant to Conagra's request and instructions, Service Provider will assist with or perform all remediation efforts required by applicable law or that have been required by any governmental authority in similar circumstances. Remediation efforts may include without limitation: (i) notifying individuals whose Personal Data may have been affected; (ii) establishing websites and toll-free telephone number(s) for affected individuals to receive assistance; (iii) provision of free credit reports, credit monitoring and repair, and identity restoration products for affected individuals; (iv) investigation and resolution of the causes and impacts of the Security Incident; and (v) such other measures that Conagra determines are reasonable in light of the severity of the Security Incident (collectively, "**Remediation Measures**"). Service Provider shall be solely responsible for the costs and expenses of all Remediation Measures.

8. **Indemnity.** Notwithstanding anything contrary contained in the Agreement, Service Provider shall defend, indemnify and hold harmless Conagra and its officers, directors, employees, agents, successors and permitted assigns (each, a "**Conagra Indemnitee**") from and against all losses, liabilities, claims, suits, enforcement actions, demands, expenses, or costs, including but not limited to any fines and penalties, arising out of or resulting from any breach of this DPA, Data Protection Laws, or a Security Incident arising out of any act or omission of Service Provider.

9. **Records.** Service Provider will maintain accurate and up-to-date records of all Processing activities carried out on Conagra's behalf, in compliance with its requirements under Data Protection Laws.

10. **Noncompliance; Remedies.** Service Provider will regularly assess its compliance with this DPA and, if Service Provider can no longer meet its obligations under this DPA, it will notify Conagra within five (5) business days of making such determination. Conagra may take reasonable and appropriate steps to stop and remediate any unauthorized Processing of Personal Data by Service Provider, up to and including terminating the Agreement. Service Provider will cooperate with Conagra's reasonable requests regarding any unauthorized Processing of Personal Data. A breach of any provision of this DPA may result in irreparable harm to Conagra, for which monetary damages may not provide a sufficient remedy, and therefore, Conagra may seek both monetary damages and equitable relief. Service Provider's obligations under this DPA are not subject to any limitation of liability provision in the Agreement. In the event that Service Provider breaches any of its obligations under this DPA, Conagra will have the right to terminate the Agreement or suspend Service Provider's continued Processing of any Personal Data, without penalty immediately upon notice to Service Provider.

11. **Precedence.** The provisions of this DPA supplement the provisions of the Agreement. In the event of inconsistencies between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail.

12. **Severability.** The Parties agree that, if any section or sub-section of this DPA is held by any court or competent authority to be unlawful or unenforceable, it shall not invalidate or render unenforceable any other section of this DPA.

13. **No Amendment.** No amendment, alteration or modification of any of the provisions of this DPA will be binding unless made in writing and signed by each of the Parties hereto.

14. **Defined Terms.** Any capitalized terms not defined in this DPA have the definition set forth in the Data Protection Laws.