

Data Processing Addendum (KPM Services)

This Data Processing Addendum (“DPA”) is a supplement to, and made a part of, the Terms and Conditions for KPM Services between Client and KPM available at: <<link>> and/or such other terms as are agreed to between KPM and Client (the “KPM Terms,” together with this DPA and applicable Order(s), the “Agreement”).

This DPA is entered into between KPM and Client and shall apply where, in the course of providing the KPM Services, KPM Processes Covered Data on behalf of Client and the Privacy Laws apply to KPM’s Processing of Covered Data.

1. **Definitions.** The following definitions apply in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the KPM Terms.
 - 1.1. “**Account Data**” means business contact information that KPM collects to administer its relationship with Client but excludes SSO Data.
 - 1.2. “**California Consumer Data**” shall have the meaning in Section 5.4.
 - 1.3. “**CCPA**” means the California Consumer Privacy Act of 2018, as may be amended, or superseded from time to time, as well as any implementing regulations. This includes the California Privacy Rights Act of 2020 (“CPRA”), which amends the CCPA.
 - 1.4. “**Collect**” means buying, renting, gathering, obtaining, receiving, or accessing any Personal Data pertaining to a Data Subject by any means pursuant to the Privacy Laws.
 - 1.5. “**Controller**” means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, including, as applicable, an entity that processes Covered Data as a “business” or “third party” under the CCPA or as a “controller” under other Privacy Laws.
 - 1.6. “**Covered Data**” shall mean Personal Data provided by or on behalf of Client to KPM pursuant to the Agreement for Processing in connection with the KPM Services. For clarity, Covered Data shall include Exposure Data and, if applicable, SSO Data, but shall exclude Service Data and Account Data.
 - 1.7. “**Data Subject**” means an individual who is the subject of Covered Data.
 - 1.8. “**Personal Data**” means any information that (a) 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 (b) applicable Privacy Laws otherwise define as protected personal information, personal data, or the like.
 - 1.9. “**Privacy Laws**” means U.S. federal, state and local laws and regulations, in relation to data protection, processing of Personal Data, privacy and/or electronic communications, including, without limitation and as applicable, the CCPA, the Virginia Consumer Data Protection Act, Colorado Privacy Act, Connecticut Personal Data Privacy and Online Monitoring Act, Section 5 of the Federal Trade Commission Act, and state data breach notification laws.
 - 1.10. “**Process**” and “**Processing**” have the meanings given in applicable Privacy Laws and includes any operation or set of operations performed on Personal Data or on sets of 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.
 - 1.11. “**Processor**” means an entity which Processes Covered Data on behalf of another person, including, as applicable, as a “service provider” or “contractor” under the CCPA or as a “processor” under other Privacy Laws.
 - 1.12. “**Purpose**” shall mean the limited and specified purposes as provided in Appendix A attached hereto and the Agreement.
 - 1.13. “**Security Incident**” means any unauthorized, acquisition, loss, access, or use of any Covered Data.
 - 1.14. “**Service Data**” means query logs and other data or information collected by or on behalf of KPM relating to access or use of the KPM Services by Client’s authorized users.
 - 1.15. “**SSO Data**” means Personal Data relating to Client’s authorized users of the KPM Services provided by or on behalf of Client to enable single sign-on (SSO).
 - 1.16. “**Subprocessor**” means any third-party Processor engaged by KPM to Process the Covered Data.
2. **Details of Processing; Order of Precedence.**
 - 2.1. **Details of Processing.** The relationship of the Parties, purpose and details of the Processing of Covered Data are set forth on Appendix A.
 - 2.2. **Account Data and Service Data.** With respect to Account Data and any Service Data that is considered Personal Data under applicable Privacy Laws, KPM is the Controller of such data and shall Process such data in accordance with the Agreement and applicable Privacy Laws.
 - 2.3. **Order of Precedence.** If there is a conflict between the KPM Terms and this DPA, the terms of this DPA will control with respect to the subject matter of the DPA.
3. **Compliance.** Each Party shall (and ensure that its personnel shall) comply with its obligations under Privacy Laws and this DPA with respect to its provision (or use) of the KPM Services and its Processing of Covered Data as contemplated by the Agreement. Nothing herein shall be construed to relieve a Party of its own obligations under applicable Privacy Laws.

4. **Client Responsibilities.**

- 4.1. Client has, and will continue to have, the right to transfer, or provide access to, Covered Data to KPM for Processing in accordance with the terms of the Agreement. Without limitation, Client shall have obtained all consents, permissions, and rights necessary under Data Privacy Laws for KPM to lawfully process Covered Data for the Purpose.
- 4.2. Client will undertake reasonable and appropriate efforts to not provide or otherwise make available to KPM any Covered Data of a Data Subject that has withdrawn consent (to the extent applicable), requested deletion, or otherwise opted out of Processing relevant to the Purpose, including, as applicable, via a global privacy control signal. To the extent a Data Subject has withdrawn consent (to the extent applicable), requested deletion, or opted out of certain Processing after Client has provided Covered Data to KPM, Client will provide notice to KPM by providing a new set of Covered Data. In such instances, KPM agrees to promptly fulfill such requests in accordance with Privacy Laws, including by deleting any earlier versions of Covered Data.

5. **KPM Responsibilities.**

- 5.1. KPM will Process Covered Data for the Purpose in accordance with Client's instructions. The Parties agree that the Agreement sets out Client's instructions to KPM for the Processing of Covered Data. Any Processing outside the scope of these instructions must be agreed to in writing between KPM and Client (email sufficient).
- 5.2. KPM shall (i) notify Client if KPM determines that it cannot meet its applicable obligations as set forth in the Privacy Laws; and (ii) KPM shall provide the same level of privacy protection as required by Privacy Laws that are applicable to it as a Processor.

6. **California Consumer Privacy Act.**

- 6.1. With respect to any Covered Data that is "personal information" of a "consumer" as those terms are defined in the CCPA ("**California Consumer Data**"), KPM grants Client the right to take reasonable and appropriate steps to (i) help ensure that KPM uses the Covered Data in a manner consistent with Client's obligations under the CCPA; and (ii) upon notice, stop and remediate unauthorized use of Covered Data. The Parties agree that, unless prohibited by CCPA, Section 13 sets forth the sole and exclusive methods by which Client may exercise its rights in this Section 6.1.
- 6.2. In cases where KPM is acting as a "service provider" to Client under the CCPA, with respect to California Consumer Data: KPM is prohibited from (i) selling or sharing Covered Data; (ii) retaining, using, or disclosing Covered Data for any purpose other than for the Purpose, or as otherwise required by Privacy Laws; (iii) retaining, using, or disclosing the information outside of the direct business relationship between the Client and KPM; and (iv) combining Covered Data with Personal Data that KPM receives from or on behalf of another person or entity, or collects from its own interactions with a Data Subject unrelated to the KPM Services, provided that KPM may combine such data to perform any business purpose permitted under the CCPA.

7. **Data Subject Requests.**

- 7.1. Requests to KPM. Except as otherwise provided in Section 7.2, if KPM receives a request from a Data Subject that identifies Client and seeks to exercise the Data Subject's rights under applicable Privacy Laws with respect to Covered Data ("**Data Subject Request**"), KPM shall inform the Data Subject that it cannot act upon the request because it is not the Controller of the Covered Data.
- 7.2. Requests to Client. If Client receives a Data Subject Request and is unable to access the relevant Covered Data within the KPM Services using functionality provided therein, then, taking into account the nature of the Processing, KPM shall (upon Client's written request) and to the extent required by Privacy Laws, cooperate with and assist Client in responding to any Data Subject Requests.

8. **Security.**

- 8.1. Security Measures. KPM shall implement reasonable and appropriate technical and organizational measures designed to safeguard Covered Data against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, displays, or distribution, and against accidental loss, destruction, unavailability, or damage.
- 8.2. Confidentiality of Processing. Any person that KPM authorizes to access the Covered Data shall be subject to a duty of confidentiality at least as protective of the Covered Data as this DPA.

9. **Security Incidents.**

- 9.1. Security Incident Reporting. If KPM becomes aware of a Security Incident, KPM shall notify Client, promptly and without undue delay, in accordance with requirements in applicable Privacy Laws. KPM shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.
- 9.2. Security Incident Communications. KPM shall provide Client timely information about the Security Incident including, but not limited to, the nature and consequences of the Security Incident, the measures taken and/or proposed by KPM to mitigate or contain the Security Incident, the status of KPM's investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data records concerned. KPM's communications with Client in connection with a Security Incident shall not be construed as an acknowledgment by KPM of any fault or liability with respect to the Security Incident.

10. **Cross-Border Transfers.** Unless otherwise agreed in writing between the Parties, KPM will only host and store Covered Data in the United States. Any permitted transfers of Covered Data by KPM (or its downstream Subprocessors) will comply with applicable Privacy Laws.

11. **Subprocessing.**

- 11.1. Authorized Subprocessors. Client authorizes the engagement of Subprocessors to Process the Covered Data. A list of current Subprocessors is set out in Appendix A.
- 11.2. Changes to Subprocessors. KPM shall notify Client of new Subprocessors at least 30 days in advance of allowing the new Subprocessor to Process Covered Data (the “**Objection Period**”). During the Objection Period, Client can reasonably object to such new Subprocessor(s). Client’s objection shall be in writing and include Client’s specific reasons for its objection and recommended commercially reasonable mitigation accommodations, if any. If Client reasonably objects to a new Subprocessor and KPM cannot reasonably accommodate Client’s objection, KPM will notify Client and Client may terminate the affected KPM Services. If Client does not object within such period, KPM may authorize the respective Subprocessor to Process Covered Data. KPM shall impose substantially similar but no less protective data protection obligations as those set out in this DPA on any approved Subprocessor prior to such Subprocessor initiating any Processing of Covered Data.
12. **Deletion**. Within a reasonable time after completion of the applicable KPM Services, KPM shall, at Client’s option, return (and not retain) or delete Covered Data.
13. **Assessments**. Upon the reasonable request of Client, KPM will make available to Client, information in its possession necessary to demonstrate KPM’s compliance with the obligations under applicable Privacy Laws and allow and cooperate with reasonable assessments by Client or Client’s assessor. Alternatively, in lieu of the foregoing at KPM’s option, unless contrary to applicable Privacy Laws, KPM may arrange for a qualified independent assessor to assess its policies and technical and organizational measures in support of KPM’s obligations under Privacy Laws using an appropriate and accepted standard or framework and assessment procedure. KPM shall provide a report of such assessment to Client upon request.
14. **Notice**. Client shall deliver any notice or other communication hereunder to KPM in writing to: KrogerPrivacyOffice@Kroger.com, Attention: Privacy Officer, with a copy to: The Kroger Co., 1014 Vine Street, Cincinnati, Ohio 45202, Attention: General Counsel. KPM may deliver any notice or other communications hereunder to Client in writing via email to the Client’s contact associated with the applicable Order.
15. **Term**. This DPA shall survive the expiration and/or termination of the Agreement for so long as Covered Data remains within KPM’s custody or control.
16. **Termination**. In addition to the other rights of termination or suspension in the KPM Terms, KPM shall be entitled to terminate this DPA and/or the KPM Terms (or applicable Order(s)) if Client is in material breach of this DPA or its obligations under Privacy Laws with respect to Covered Data.
17. **Miscellaneous**.
- 17.1. Further Assurances. Each Party shall, at the request of the other Party, execute such additional documents and take all such further actions as may be reasonably be required to give full effect to this DPA.
- 17.2. Modifications. KPM reserves the right to update this DPA from time to time as reasonably necessary as needed to comply with Privacy Laws.

Last updated: September 19, 2023

Appendix A
PROCESSING DETAILS

I. Roles of the Parties

As between the Parties, KPM shall Process Covered Data as a “service provider” for the purposes of the CCPA and a “Processor” for all other cases. As between the Parties, Client shall be a “business” for the purposes of the CCPA, and a “Controller” for all other cases with respect to Covered Data.

II. Data Subject Types

United States consumers.

III. Purpose of the Processing

KPM shall Process Covered Data to provide the KPM Services ordered by Client in accordance with Client’s written instructions. These KPM Services include measurement services related to advertising campaigns facilitated through the KPM Services.

If SSO is enabled, KPM shall process Covered Data for authentication purposes and to enable and facilitate access to and use of the KPM Services.

IV. Types of Covered Data

Exposure Data (as defined in the KPM Terms), and will include:

- Unique personal identifiers;
- Commercial information including internet or electronic network activity information & impression information; and

If enabled, SSO Data, which may include business email address and other business contact information.

V. Retention Period

Duration of the KPM Services.

VI. Subprocessors

N/A