July 22, 2025
Final for posting

ADAGIO DATA PROTECTION ADDENDUM

Last Updated: [DATE POSTED]

This Data Protection Addendum ("**DPA**") is part of the Agreement (defined below) and establishes the terms under which one party ("**Disclosing Party**") may share or disclose Personal Data with the other party ("**Receiving Party**") for the Processing Purposes defined herein, and how the Receiving Party may Process such Personal Data. This DPA supersedes all prior agreements between the Parties regarding data protection.

This DPA consists of these general terms (the "**DPA General Terms**") and the Schedules listed below (each a "**DPA Schedule**") each of which are part of this DPA to the extent Personal Data processed by the Parties under the Agreement is subject to applicable Data Protection Laws in those jurisdictions.

- **US DPA**
- **GDPR DPA**

The terms in this DPA prevail over any conflicting provisions in the Agreement and an applicable DPA Schedule will control over conflicting terms in the DPA General Terms.

Section 1. Definitions. For purposes of this DPA, the following terms will have the meaning ascribed below:

1.1. "**Agreement**" means the Master Terms, this DPA, and any Order Forms between the Parties.

1.2. "**Consumer**" means a "consumer," "data subject," or equivalents as defined under applicable Data Protection Laws.

1.3. "**Data Breach**" means any unauthorized acquisition or access to, or use, loss, or other disclosure of Personal Data, as such term or its equivalents is defined under applicable Data Protection Laws.

1.4. "**Data Protection Laws**" means all applicable international, federal, state, and local data protection and privacy laws, rules, directives, regulations, orders, decrees, judgments, and governmental requirements currently in effect, or as they become effective, to the extent they apply to Personal Data processed by a Party under the Agreement, including, as applicable, European Data Protection Law and the State Privacy Laws.

1.5. "**Explicit Consent**" means the consent required under applicable Data Protection Laws for processing Sensitive Data or for processing Personal Data for Secondary Purposes.

1.6. "**European Data Protection Law**" means (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (the General Data Protection Regulation) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); (iv) the UK Privacy and Electronic Communications (EC Directive) Regulations 2003; (v) Switzerland's Federal Act of 25 September 2020 on Data Protection, and (vi) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of the foregoing, in each case as may be amended or superseded from time to time.

1.7. "**Global Privacy Protocol**" or "**GPP**" means the IAB's industry framework for the sharing of consent, opt-out or other Consumer flags or signals, including the Transparency and Consent Framework ("**TCF**"), and applicable GPP signaling systems in the United States, Canada, or any other applicable territory, with technical specifications available at https://github.com/InteractiveAdvertisingBureau/Global-Privacy-Platform.

1.8. "**GDPR Countries**" means countries subject to European Data Protection Law, including countries in the European Union, the European Economic Area, Switzerland, and the United Kingdom.

1.9. "**Minor's Data**" means data of individuals under eighteen (18) years of age subject to regulation under applicable Data Protection Laws as defined under such laws.

1.10. "**Precise Location Data**" has the meaning set forth in applicable Data Protection Laws.

1.11. "**Processing Purposes**" means processing for the purposes of each Party's performance under the Agreement as further defined in the DPA Schedules and as otherwise permitted by applicable Data Protection Laws.

1.12. "**Secondary Purposes**" means new or different purposes other than the Processing Purposes defined herein as such term or its equivalents is defined under applicable Data Protection Laws.

1.13. **"Sensitive Personal Data**" means any data or information (including inferences) related to a Consumer defined as "sensitive personal data," "sensitive personal information," "special categories of data" or equivalents under applicable Data Protection Laws, including Minor's Data and Precise Location Data.

1.14. "**State Privacy Laws**" has the meaning set forth in the **US DPA.**

1.15. "**Supervisory Authority**" means the relevant regulatory authority under applicable Data Protection Laws.

1.16. "**Controller**", "**Processor**", "**Personal Data**" and "**Process(-ing)**" (or their analogous terms) shall have the meanings ascribed to them in the applicable Data Protection Laws.

Section 2. Roles.

2.1. Each Party acts as a separate and independent Controller (or similar term under applicable Data Protection Laws) with respect to its own Processing activities, except as otherwise set forth in this DPA including in an applicable DPA Schedule. Each Party will comply with its responsibilities under applicable Data Protection Laws in respect of its Processing of Personal Data under the Agreement, including having in place appropriate physical, technical and organizational measures to protect the security of the Personal Data.

2.2. Each Party may engage or use Processors, provided that the arrangement with their Processors is governed by a written contract which includes terms that provide at least the same level of protection for Personal Data as those set out in this DPA and as required under applicable Data Protection Laws. Each Party shall remain responsible for the acts or omissions of its Processors as required by applicable Data Protection Laws.

Section 3. Disclosing Party's Obligations.

3.1 Publisher will provide prominent notice at the point of data collection and obtain and transmit all Consumer choices required by applicable Data Protection Laws to permit each Party to Process Personal Data for the Processing Purposes, including Explicit Consent where required under applicable Data Protection Laws.

3.2 Adagio participates in TCF and complies with its Policies and Specifications. Publisher will implement the latest TCF specifications on all digital properties it uses to transmit Personal Data to Adagio and it will add Adagio as a vendor in TCF. For other jurisdictions where GPP functionality is available, Publisher agrees to integrate with the applicable GPP framework. Where required by applicable Data Protection Laws, Publisher will maintain mechanisms and technical signals to ensure Consumers have the ability to exercise their choices to opt-out of specific Processing Purposes as such purposes are defined under applicable Data Protection Laws.

3.3 Publisher will ensure all Consumer choice signals transmitted to Adagio are operational and accurately transmit the Consumer's choices to Adagio. Publisher will not disclose or make available to Adagio any Personal Data relating to Consumers who have opted-out of Processing for any particular Processing Purposes.

3.4. Where the Disclosing Party is providing Personal Data originally collected by another Controller, the Disclosing Party will (i) contractually obligate such Controller to provide all notices and obtain and transmit Consumer permissions or consents, including Explicit Consents (to the extent applicable), required by relevant Data Protection Laws necessary to permit each Party to Process Personal Data for the Processing Purposes, and (ii) take reasonable steps to ensure such Controller's compliance with such contractual obligations.

3.5. The Disclosing Party will take all reasonable steps to ensure that the Personal Data it shares with the Receiving Party is accurate, complete, relevant and up to date and will correct any errors in the relevant Personal Data as soon as practicable. The Disclosing Party further agrees to implement appropriate technical and organizational measures to ensure the security of Personal Data while in transit to the Receiving Party.

Section 4. Receiving Party's Obligations.

Receiving Party will only Process the Personal Data for the Processing Purposes. If the Receiving Party wishes to process the Personal Data for Secondary Purposes, it may do so provided it first does all such acts and things as are necessary to ensure that its proposed processing of the Personal Data for the Secondary Purposes fulfils the requirements of applicable Data Protection Law (including by obtaining any consents from data subjects, where necessary). Provided such requirements are met, such Secondary Purpose shall be deemed a Processing Purpose.

Section 5. Each Party's Obligations.

5.1. Each Party will ensure the Personal Data it Processes under the Agreement is adequate, relevant and limited to what is necessary in relation to the Agreement and the Processing Purposes.

5.2. Each Party will maintain prominent and publicly accessible privacy notices on its digital properties that satisfies applicable Data Protection Laws and ensure such privacy notices disclose the means by which a Consumer can exercise its privacy rights under applicable Data Protection Laws.

5.3. Each Party will be separately responsible for responding to Consumer privacy requests. To the extent the Receiving Party receives a request relating to Processing performed by the Disclosing Party, the Disclosing Party shall provide such information and assistance as is reasonably necessary to the Receiving Party to enable the Receiving Party to respond to such request in accordance with applicable Data Protection Law.

5.4. Where the relevant correspondence or requirements relates to the Processing conducted by the other Party, the Parties will reasonably cooperate with each other in relation to Consumer requests or complaints, inquiries or investigations conducted by any Supervisory Authority, or assistance needed to conduct data privacy impact assessments or other legally required risk assessments.

5.5. Except as otherwise set forth in a DPA Schedule or as required by applicable Data Protection Laws, each Party shall be responsible for its own reporting and information obligations related to any Data Breach.

5.6. When applicable Data Protection Laws have requirements relating to cross-border transfers of Personal Data, the Parties will comply with such requirements and will coordinate in good faith to take all necessary steps to facilitate compliance, including entering into supplemental contract terms if legally required.

5.7. Each Party agrees to notify the other Party if it believes it is unable to comply with the terms of this DPA or any applicable Data Protection Laws.

Section 6. General.

6.1. Unless otherwise defined in applicable Data Protection Laws or this DPA, all capitalized terms used in the DPA will have the meanings ascribed to them in the Agreement. This DPA shall be interpreted in accordance with applicable Data Protection Laws as applied to Personal Data in the relevant jurisdiction.

6.2. This DPA does not prevent the Parties from agreeing on additional clauses or safeguards, provided they do not directly or indirectly contradict this DPA. Notwithstanding anything to the contrary in the Agreement, in the event any variation is required to this DPA as a result of a change in applicable Data Protection Laws, including any orders from a Supervisory Authority, Adagio may amend this DPA from time-to-time to ensure continued compliance with applicable Data Protection Laws or such orders.

6.3. This DPA survives the termination of the Agreement (including any Order Form) for as long as Personal Data collected under the Agreement continues to be Processed by either Party.

Section 7. Governing Law and Jurisdiction.

7.1 Except as otherwise required by applicable Data Protection Laws or as set forth herein, the governing law and jurisdiction shall be the same as set out in the Agreement, without regard to conflict of laws principles.

7.2 Disputes or claims arising out of or relating to the processing of Personal Data are subject to:

7.2.1 any matter arising out of a State Privacy Law shall be governed by the laws of the applicable state, provided that the exclusive place of jurisdiction for all disputes arising out of or in connection with a State Privacy Law or U.S. federal law shall be the state or federal courts of New York County, New York;

7.2.2 any matter arising out of European Data Protection Law shall be governed by the governing law of, and disputes in connection therewith shall be subject to the exclusive jurisdiction of the courts of: (i) France, where Publisher is based in the GDPR Countries (excluding the United Kingdom); (ii) England and Wales, with courts located in London, where Publisher is based in the United Kingdom; and

7.2.3 any matter concerning applicable Data Protection Laws in the Asia Pacific area (APAC) shall be governed by the governing required by applicable Data Protection Laws, and disputes in connection therewith shall be subject to the exclusive jurisdiction of Singapore, should Publisher be based in the Asia Pacific region.

Section 8. Liability.

To the fullest extent permitted by applicable Data Protection Laws, any claims brought in connection with this DPA (including its DPA Schedules) will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations, set forth in the Agreement.

US DPA

Last Updated: [DATE POSTED]

This US DPA governs Personal Data Processing under U.S. privacy laws, including State Privacy Laws. Unless defined herein, capitalized terms have the meanings in the DPA. This US DPA supersedes conflicting DPA terms.

This US DPA includes the following Attachments, each of which are part of this US DPA as applicable.

- **Attachment 1: Description of Processing for Restricted Purposes**
- **Attachment 2: DOJ Rule on Preventing Access to Americans' Bulk Sensitive Personal Data**

1. The IAB's Multi-State Privacy Agreement

In the event both Parties have signed the IAB's Multi-State Privacy Agreement (the "**MSPA**"), available at https://www.iabprivacy.com, and in the event of a conflict between the MSPA and this US DPA, the terms of the MSPA shall supersede and control.

2. Definitions

For purposes of this US DPA, the following terms will have the meaning ascribed below:

2.1. **"Advertising Purposes"** means the Processing Purposes under this US DPA, including all Restricted Purposes in addition to:

(i) activities that constitute Targeted Advertising under State Privacy Laws,
(ii) creating or modeling audiences, or
(iii) creating or supplementing user profiles for such purposes.

2.2. **"CCPA"** means the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020, and any regulations promulgated thereunder.

2.3. **"Data Breach"** means "breach of the security of the system," "security breach," "breach of security," "breach of system security," and other analogous terms referenced in State Privacy Laws.

2.4. **"Restricted Processing"** means Processing only for Restricted Purposes.

2.5. **"Restricted Processing Signal"** means any flag or signal indicating that a Consumer has opted out of:

(i) the Sale or Share of their Personal Data,
(ii) use of their Personal Data for purposes of Targeted Advertising,
(iii) profiling in furtherance of decisions that produce legally or similarly significant effects, or
(iv) any other Processing Purpose for which a Consumer has an opt-out right under applicable State Privacy Laws or other applicable U.S. Data Protection Laws.

including those flags or signals sent through the IAB GPP or any other signaling system, including without limitation technical signaling systems designed to transmit UOOM signals.

2.6. **"Restricted Purposes"** means advertising-related Processing that qualifies as a Business Purpose, including Processing for purposes of auditing; security and integrity; debugging; short term, transient uses; analytics; providing advertising or marketing services that do not include Targeted Advertising, or profiling; internal research; and efforts to improve quality and safety. Restricted Purposes include as applicable, first-party advertising,

contextual advertising, frequency capping, ad selection and sequencing, measurement, fraud detection and prevention, and ensuring and measuring viewability, each only to the extent such activity:

(i) is permissible for a Processor to perform under the applicable State Privacy Laws,
(ii) does not result in a Sale or Sharing of Personal Data,
(iii) is not Processing of Personal Data for Targeted Advertising purposes, or
(iv) is not profiling in furtherance of decisions that produce legally or similarly significant effects.

2.7. "**Targeted Advertising**" includes Cross-Context Behavorial Advertising as defined under the CCPA and otherwise has the meaning set forth in applicable State Privacy Laws.

2.8. "**UOOMs**" means "Universal Opt-Out Mechanisms" or "Opt-Out Preference Signals" required under applicable State Privacy Laws for the transmission of Consumer opt-out signals and implemented to accurately pass applicable Consumer Choices to Adagio via tools recognized as valid by applicable Supervisory Authorities, including as applicable the Global Privacy Control available at: https://globalprivacycontrol.org.

2.9. **"Business,"** "Business Purpose," "Commercial Purpose," "Consumer," "Controller," "Cross-Context Behavioral Advertising," "Deidentified," "De-identified Data," "Personal Data," "Personal Information," "Process(-ing)" "Processor," "Sale," "Sell," "Service Provider," "Share," "Targeted Advertising" and "Third Party" shall have the meanings ascribed to them in State Privacy Laws.

2.10. **"Controller,"** references in this US DPA to "Controller," "Personal Data," and "Processor" include "Business," "Personal Information," and "Service Provider" respectively.

2.11. "**State Privacy Laws,**" means the CCPA and all other equivalent or similar U.S. state laws and regulations relating to Personal Data, in each case as amended from time to time and including any regulations promulgated thereunder, including without limitation:

- Colorado Privacy Act
- Connecticut's Act Concerning Data Privacy and Online Monitoring
- Delaware Personal Data Privacy Act
- Indiana Consumer Data Protection Act [Effective Jan. 1, 2026]
- Iowa Consumer Data Protection Act
- Kentucky Consumer Data Protection Act [Effective January 1, 2026]
- Maryland Online Data Privacy Act of 2024 [Effective October 1, 2025]
- Minnesota Consumer Data Privacy Act
- Montana Consumer Data Privacy Act, Mont. Code
- Nebraska Data Privacy Act
- New Hampshire Privacy Law
- New Jersey Privacy Act
- Oregon Consumer Privacy Act
- Rhode Island Data Transparency & Privacy Protection Act [Effective January 1, 2026]
- Tennessee Information Protection Act
- Texas Data Privacy and Security Act
- Utah Consumer Privacy Act
- Virginia's Consumer Data Protection Act

3. Roles

With respect to the Processing of Personal Data, each Party acts as a Controller in its capacity as the Disclosing Party or the Receiving Party, as applicable, unless a Restricted Processing Signal is present or the Processing by the Receiving Party is otherwise solely for Restricted Purposes, in which case Receiving Party acts as a Processor and Processes the Personal Data on behalf of Disclosing Party (which may operate as either the Controller or a Processor

to another Controller). For clarity, where Adagio acts as a Processor, it shall only be responsible for Processing activities within its direct control.

4. Mutual Processing Obligations

Each Party will:

4.1. Comply with its respective obligations under State Privacy Laws with respect to the Processing of Personal Data.

4.2. Provide Consumers with a clear and conspicuous ability to opt out of the Sale, Sharing, or Processing of their Personal Data for purposes of Targeted Advertising, in compliance with State Privacy Laws. If a Consumer opts out, Disclosing Party will (i) not Process such Consumer's Personal Data for Targeted Advertising purposes and (ii) will either (a) not disclose such Consumer's Personal Data to any Third Party; or (b) transmit a Restricted Processing Signal in conjunction with any disclosures of such Consumer's Personal Data to any Third Party. Each Party shall be responsible for implementing its own opt-out mechanisms and maintaining records of Consumer choices.

4.3. Not modify any Restricted Processing Signal received from a Disclosing Party.

4.4. Transmit all Restricted Processing Signals received in conjunction with Personal Data to any recipients of such Personal Data.

4.5. Comply with requirements set out in State Privacy Laws for processing Deidentified Data, including by:

- 4.5.1. Not attempting to re-identify any such data;
- 4.5.2. Using reasonable administrative, technical, and organizational measures to prevent any re-identification of any such data or any inadvertent release of any such data; and
- 4.5.3. Publicly committing both to maintain and use the Deidentified Data in de-identified form and not to attempt to re-identify any such data.

4.6. To the extent acting as a Disclosing Party:

- 4.6.1. Provide all notices and obtain any consents required by State Privacy Laws necessary to permit each Party to Process Personal Data in accordance with this US DPA; and
- 4.6.2. To the extent providing Personal Data originally collected by another Controller, (i) contractually obligate such Controller to provide all notices and obtain any consents required by State Privacy Laws necessary to permit each Party to Process Personal Data in accordance with this US DPA and (ii) take reasonable steps to ensure compliance with such contractual obligations.

4.7. To the extent acting as a Receiving Party, comply with:

- 4.7.1. Section 5 (CCPA Third Party Terms) when Processing Personal Data subject to the CCPA and without a Restricted Processing Signal present.
- 4.7.2. Section 6 (Processor Obligations), when Processing Personal Data received with a Restricted Processing Signal present.

5. CCPA Third Party Terms

5.1. **Applicability**

This Section 5 (CCPA Third Party Terms) applies only when the Receiving Party Processes Personal Data from the Disclosing Party (i) that is subject to the CCPA; and (ii) no Restricted Processing Signal is present.

5.2. **Purpose Limitations**

Disclosing Party makes Personal Data available to Receiving Party only for Advertising Purposes. Receiving Party will Process Personal Data only for such Advertising Purposes, and in accordance with its obligations and any restrictions in the Agreement.

5.3. **CCPA Compliance; Notification of Determination of Noncompliance**

Receiving Party will comply with applicable obligations under the CCPA, including by providing an appropriate level of privacy protection as required by the CCPA, and will notify Disclosing Party without undue delay if Receiving Party determines it can no longer meet its obligations under the CCPA.

5.4. **Verification of CCPA Compliance**

Upon Disclosing Party's reasonable request, but no more than once per calendar year unless required by law, Receiving Party will provide the following to Disclosing Party to demonstrate Receiving Party's Processing of Personal Data consistent with Disclosing Party's obligations under the CCPA:

- 5.4.1. A copy of a certificate issued for security verification reflecting the outcome of an audit conducted by an independent third-party auditor; or
- 5.4.2. Any other information the Parties agree is reasonably necessary for Disclosing Party to verify Receiving Party's Processing is consistent with Disclosing Party's obligations under the CCPA, such as an attestation.

5.5. **Unauthorized Use Remediation**

If Disclosing Party reasonably believes that Receiving Party is engaged in the unauthorized use of Personal Data provided by Disclosing Party, Disclosing Party may notify Receiving Party of such belief using the contact information provided in the Agreement, and the Parties will work together in good faith to stop or remediate the allegedly unauthorized use of such Personal Data, as necessary.

5.6. **Onward Disclosure Obligations**

To the extent permitted by the Advertising Purposes and the Agreement, if Receiving Party makes an onward disclosure of Personal Data provided to it by Disclosing Party, including through any Sale or Sharing of Personal Data, Receiving Party will impose terms that are substantially similar to (a) the terms imposed on Receiving Party by Section 4 (Mutual Processing Obligations) and this Section 5 (CCPA Third Party Terms).

6. Processor Obligations

6.1. **Applicability**

This Section 6 (Processor Obligations) applies only to the extent Receiving Party Processes Personal Data with a Restricted Processing Signal present that has been delivered to Receiving Party or the Processing by the Receiving Party is otherwise solely for Restricted Purposes. For avoidance of doubt, Receiving Party shall have no obligations under this Section 6 where a Restricted Processing Signal is not passed in the bidstream or other data feed, including where a consent management platform removes or truncates such signal, or where technical limitations or third-party actions prevent the accurate transmission of such signal.

6.2. **Purpose Limitations**

Receiving Party will Process Personal Data in accordance with its obligations in the Agreement and only for Restricted Purposes, as further described in **Attachment 1**. Receiving Party will not:

- 6.2.1. Process Personal Data for Targeted Advertising purposes; or
- 6.2.2. Sell or Share Personal Data.

6.3. **Assistance**

Receiving Party will assist Disclosing Party with State Privacy Laws compliance by:

- 6.3.1. Assisting the Disclosing Party in responding to Consumer requests made pursuant to State Privacy Laws, provided that Disclosing Party must provide to Receiving Party all information necessary for it to provide such assistance or respond to a Consumer request when required by State Privacy Laws;
- 6.3.2. Contributing to data protection impact assessments where required by State Privacy Laws;
- 6.3.3. Offering reasonable notice and assistance to Disclosing Party in the event Receiving Party experiences a Data Breach, including to help Disclosing Party satisfy its Data Breach notification obligations under State Privacy Laws; and
- 6.3.4. Implementing reasonable security procedures and practices appropriate to the nature of the Personal Data and designed to protect such Personal Data from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with State Privacy Laws.

6.4. **Confidentiality**

Receiving Party will treat Personal Data from Disclosing Party as confidential and subject each person that Processes such Personal Data to an appropriate obligation of confidentiality.

6.5. **Further Disclosures**

If Receiving Party further discloses Personal Data provided by Disclosing Party, Receiving Party will:

- 6.5.1. Ensure it has in place a written agreement with any such recipient that obligates the recipient to comply with terms at least as protective as the terms set out in this Section 6 (Processor Obligations);
- 6.5.2. Ensure any Restricted Processing Signal is transmitted with the Personal Data to the recipient; and
- 6.5.3. To the extent required by State Privacy Laws, provide Disclosing Party notice of the planned transmission to any subcontractor and an opportunity to object.

6.6. **Deletion and Return of Personal Data**

Upon the earlier of any request by Disclosing Party or without undue delay following termination of the Agreement, Data Recipient will delete, return, or de-identify in accordance with State Privacy Laws Personal Data provided to Receiving Party by Disclosing Party, unless retention of the Personal Data is required by applicable law.

6.7. **Audits**

Upon Disclosing Party's reasonable request, Receiving Party will provide the following to Disclosing Party to enable Disclosing Party to audit Receiving Party's compliance with this Section 6 (Processor Obligations):

- 6.7.1. A copy of a certificate issued within 12 months of the Disclosing Party's Request reflecting the outcome of an audit conducted by an independent and qualified third-party auditor using an appropriate and accepted control standard or framework and audit procedure, provided that such audit shall not occur more than once per calendar year unless required by law; or
- 6.7.2. Any other information or attestation the Parties agree is reasonably necessary for Disclosing Party to verify that Receiving Party's Processing is consistent with Disclosing Party's obligations under the CCPA.

6.9. **Additional CCPA Processing Obligations**

If Personal Data provided to Receiving Party by Disclosing Party is subject to the CCPA, in addition to the obligations set out in Sections 6.1 - 6.7 above, Receiving Party will:

- 6.8.1. Not retain, use, or disclose the Personal Data outside of the direct business relationship with Disclosing Party or for any purpose, including Commercial Purposes, other than the Restricted Purposes, unless otherwise permitted by the CCPA.
- 6.8.2. Upon notice from Disclosing Party of its reasonable belief that Receiving Party is Processing Personal Data in an unauthorized manner, cooperate with Disclosing Party in good faith to stop or remediate the allegedly unauthorized use of such Personal Data, as necessary, such as by providing documentation verifying certain practices.
- 6.8.3. Notify the Disclosing Party without undue delay if Receiving Party determines it can no longer meet its obligations under the CCPA.
- 6.8.4. Except to Process for the Restricted Purposes or as otherwise permitted by the CCPA, not combine the Personal Data provided to Receiving Party by Disclosing Party with Personal Data received from or on behalf of another person or source or that Receiving Party collects from its own interactions with Consumers.

7. Cross-Border Transfers

Where the Disclosing Party (a US entity) provides the Receiving Party (a non-US entity) with access to Personal Data, the terms in **Attachment 2** below apply (DOJ Rule on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern).

8. Prohibited Data Transfers

Publisher represents, warrants and covenants that it will not transfer or disclose to Adagio any Personal Data that cannot be used for the Processing Purposes under applicable Data Protection Laws in the United States. Publisher further represents, warrants and covenants that it will not transfer or disclose to Adagio any Sensitive Personal Data for the Processing Purposes or Personal Data for any Secondary Purposes without first obtaining and maintaining documented Explicit Consent of the Consumer for such Processing. Publisher shall indemnify and hold harmless Adagio for any breach of these representations, warranties and covenants.

9. Miscellaneous

Except as provided in Section 5.2, if there is any inconsistency or conflict between this US DPA and the Agreement, then this US DPA will govern, regardless of whether any language in the Agreement purports to state that the Agreement is the controlling document. The provisions of this US DPA may not be amended, except by an agreement to specifically amend this US DPA in writing signed by the Parties. To the extent the Parties continue to Process Personal Data subject to applicable Data Protection Laws in the United States, this US DPA will survive any expiration or termination of the Agreement.

Attachment 1 to US DPA
Description of Processing for Restricted Purposes

1.1. Nature and Purpose of Processing.

Data Recipient Processes the Personal Data it receives for the Restricted Purposes, as further described in Section 2.6 of the US DPA.

1.2. Types of Personal Data Processed.

- Online identifiers such as cookie IDs and mobile ad identifiers
- Information based on consumer's browsing activity such as behavioral or interest data
- Information about browsers and devices used
- Non-precise geolocation information such as IP addresses or zip code information

1.3. Data Security

- When Adagio acts as a Processor under this US DPA, the technical and organizational measures set forth at www.adagio.io/legal/tom, as may be updated from time to time, apply.

Attachment 2 to US DPA
DOJ Rule on Preventing Access to Americans' Bulk Sensitive Personal Data

1. The DOJ Rule is available at: https://www.justice.gov/nsd/media/1382521/dl?inline
2. Each Party acknowledges that the term "Sensitive Personal Data" under the DOJ Rule has a different meaning than the definition of "Sensitive Personal Data" under the DPA. For purposes of this Attachment 2, the term "Sensitive Personal Data" has the meaning in the DOJ Rule.
3. The Disclosing Party (a US entity) provides the Receiving Party (a non-US entity) access to Sensitive Personal Data for the purposes set forth in the Agreement, including the US DPA.
4. The Receiving Party is prohibited from engaging or attempting to engage in, or permitting others to engage or attempt to engage in the following: (a) selling, licensing of access to, or other similar commercial transactions, such as reselling, sub-licensing, leasing, or transferring in return for valuable consideration, the Sensitive Personal Data or any part thereof, to countries of concern or covered persons, as defined in 28 CFR part 202.
5. Where the Receiving Party knows or suspects that a country of concern or covered person has gained access to Sensitive Personal Data through a data brokerage transaction, the Receiving Party will immediately inform the Disclosing Party. Failure to comply with the above will constitute a breach of the Agreement and may constitute a violation of 28 CFR part 202.

GDPR DPA

Last Updated: [DATE POSTED]

This GDPR DPA supplements and forms part of the DPA and governs the Processing of Personal Data by Parties subject to European Data Protection Law for the Processing Purposes defined herein. Capitalized terms not defined herein shall have the meanings set forth in the Agreement including the DPA.

This GDPR DPA consists of these general terms (the "**GDPR General Terms**") and the Schedules listed below (each "**GDPR DPA Schedule**") each of which are part of the GDPR DPA as applicable.

- **GDPR DPA Schedule A: Joint Controller Addendum (JCA)**
- **GDPR DPA Schedule B: Processor Addendum**
- **GDPR DPA Schedule C: Restricted Transfer Addendum**

Section 1. Roles

1.1 The Parties are Joint Controllers for the initial collection and transfer of Personal Data from Publisher to Adagio. Following such transfer, the Parties may continue to act as Joint Controllers or Adagio may act as an independent Controller or as a Processor to Publisher as set forth in Section 2 below.

1.2 The Joint Controller Addendum applies when the Parties act as Joint Controllers and the Processor Addendum applies when Adagio acts as a Processor. For any data processing activities that fall outside the scope of both the Joint Processing and the Processor activities defined herein, each Party acts as an independent Controller and shall independently comply with its obligations under European Data Protection Law and the Agreement.

1.3 Under this GDPR DPA, references to the "**Controller Services**" are where Adagio acts as a Controller and the "**Processor Services"** are where Adagio acts as a Processor, each as designated below.

Section 2. Processing Purposes

The TCF Processing Purposes are necessary for Publisher's use of the Adagio Platform (including the SSP and Prebid Server) and Adagio's provision of services to Publisher under the Agreement.

TCF Processing Purposes	**Joint data processing for Publisher's initial collection and transfer of Personal Data from Publisher to Adagio**	**Adagio's role for subsequent data processing activities following the transfer of Personal Data from Publisher to Adagio**
Store and/or access information on a device (TCF Purpose 1)	Yes	Independent Controller
Use limited data to select advertising (TCF Purpose 2)	Yes	Processor
Create profiles for personalized advertising (TCF Purpose 3)	Yes	Independent Controller
Use profiles to select personalized advertising (TCF Purpose 4)	Yes	Independent Controller
Measure advertising performance (TCF Purpose 7)	Yes	Independent Controller
Measure content performance (TCF Purpose 8)	Yes	Independent Controller

Develop and improve services (TCF Purpose 10)	Yes	Independent Controller
Ensure security, detect fraud, and fix errors (TCF Special Purpose 1)	Yes	Independent Controller
Deliver and present advertising and content (IAB Special Purpose 2)	Yes	Processor
Save and communicate privacy choices (IAB Special Purpose 3)	Joint Controller with Publisher and IAB Europe in accordance with IAB TCF policies	Processor

Section 3. Disclosing Party's Obligations.

Disclosing Party shall (in addition to its other obligations under the DPA and European Data Protection Law:

3.1. Communicate to Receiving Party any rectification or erasure of personal data or restriction of Processing carried out in accordance with Art. 16, Art. 17 (1) and Art. 18 GDPR / UK GDPR unless this proves impossible or involves disproportionate effort.

3.2. Communicate to Receiving Party any withdrawal of consent (Art. 7 (3) GDPR / UK GDPR) in relation to Personal Data which has been disclosed to Receiving Party.

3.3. Not transfer any Sensitive Personal Data (Art. 9 GDPR / UK GDPR) to Receiving Party unless explicitly authorized in writing and with appropriate safeguards in place as required by applicable law.

GDPR DPA Schedule A
Joint Controller Addendum (JCA)

The Parties agree they will be Joint Controllers for certain processing activities within the meaning of Art. 26 GDPR, as further defined in the GDPR General Terms and this JCA. The Parties enter into this JCA in order to satisfy the legal requirements as Joint Controllers and to set forth both Party's rights and obligations.

1. Roles of the Parties

1.1 Joint responsibility. The Parties are jointly responsible for the Joint Data Processing (Art. 26 GDPR) for the Processing Purposes as further described and set forth the GDPR General Terms. The Parties shall jointly determine the purposes and means regarding the Joint Data Processing as joint controllers as set out in this JCA.

1.2 Scope. Any processing for purposes outside the Joint Processing Purposes shall be conducted by the Parties as independent Controllers or an alternative arrangement and shall not be subject to this JCA.

2. Allocation of Responsibility

2.1 Notwithstanding the fact that the Parties act as joint Controllers with respect to the processing of the Personal Data for the Processing Purposes, as between the Parties, the following allocation of primary responsibilities shall apply (hereinafter the "Sphere of Responsibility").

2.2 Publisher's Sphere: The Publisher will implement its data collection subject to the obligations contained in the Agreement, including the DPA. The Publisher shall ensure that no tracking technologies are set on its digital properties, and no Personal Data collected during a data subject's use of its digital properties, before the data subject has given its consent for data collection for the Processing Purposes in accordance with applicable European Data Protection Law. Further, the Publisher is responsible for any storage of Personal Data on its IT systems.

2.3 Adagio's Sphere: Adagio will ensure that the transfer to and the storage of Personal Data on its IT systems is protected by sufficient technical and organizational measures. Further, any Personal Data generated by Adagio are generated on a valid legal basis (including consent, where required) that permits the processing of such Personal Data for the Processing Purposes by the Parties in accordance with applicable European Data Protection Law.

3. Publisher's Obligations

3.1 Information and transparency. In its digital properties, the Publisher shall provide information in an easily accessible and meaningful manner and in accordance with applicable European Data Protection Law about the Joint Data Processing. This information shall include a link to Adagio's privacy policy. Adagio shall provide the information required to fulfil these obligations. Information about the Joint Data Processing will reflect the choices made by the Parties in Section 2 of the GDPR General Terms concerning the applicability of Processing Purposes.

3.2 Legal basis. The Publisher enables data subjects to consent and as applicable, to object to, the Joint Data Processing in accordance with the available legal basis indicated by Adagio in TCF for each relevant Processing Purpose. If, according to TCF settings, Adagio gives the Publisher the option to carry out certain processing operations on the basis of consent as well as on the basis of legitimate interests, the choice of the legal basis is made by the Publisher.

3.3 Disclosure. The Publisher shall make available to the data subjects the essence of this Agreement as it relates to the Joint Data Processing, provided that Adagio may provide the Publisher with standard text to support the Publisher in fulfilling its obligation within the TCF settings. To the extent further disclosures are required under Article 26(2) GDPR, the Parties undertake to make the essence of the arrangement under this JCA available to the data subjects and shall cooperate in good faith to agree on the exact content and form.

3.4 Consent Requirements. Publisher must obtain consent for the Joint Data Processing, which must be:
(a) voluntary, specific, informed and unambiguous;
(b) not be a pre-condition for access to a service or the performance of a contract;
(c) identify Adagio as the recipient of the data;

(d) contain an easily recognisable reference to the option to refuse consent; and
(e) be obtained again in accordance with the applicable legal requirements of Applicable Data Protection Law, or the TCF; whichever time is shorter.

3.5 Documentation and proof. The Publisher shall document each consent and, on reasonable request of Adagio, provide Adagio with evidence of the consent without undue delay either in the form of a signal in a bid request or upon separate request (email shall suffice).

3.6 TCF. If the Publisher supports IAB TCF, the Publisher undertakes to comply with all applicable TCF terms, policies, and specifications. If Publisher does not use TCF, the Publisher has to ensure compliance with all provisions of this JCA, the DPA, and the Agreement through other measures.

4. Obligations of Adagio

Adagio shall:

(a) process the data collected in the course of Joint Data Processing only for the Processing Purposes;

(b) not subject data subjects to a decision based on automated processing including profiling (scoring) which produces legal effects in relation to the data subject or significantly affects him/her in a similar way (Art. 22 GDPR).

5. Data Subject Rights

5.1 Requests. Data subjects can exercise their rights against either Party. Each Party, where relevant with the reasonable assistance of the other Party, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under this JCA without undue delay and at the latest within one month of the receipt of the enquiry or request. This period may be extended by two further months where necessary, taking into account the complexity and number of requests. Each Party shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

5.2 Withdrawal and objection. The Publisher will inform Adagio immediately about any withdrawal of a consent concerning the Joint Data Processing as well as any objection against the Joint Data Processing.

5.3 Support. Adagio is free to use standardised or automated methods to enable data subjects to exercise data subject rights. The Publisher shall use reasonable commercial endeavours to support such methods (e.g. by integrating a corresponding tool or opt-out link into the digital properties).

5.4 Notices. The Parties shall inform data subjects in a transparent and easily accessible format, through individual notice or on their website, of a contact point authorised to handle complaints. Each Party shall deal promptly with any complaints it receives from a data subject. In order to enable data subjects to effectively exercise their rights pursuant to the GDPR, the Parties shall inform them:

of its identity and contact details;
of the categories of personal data processed;
of the right to obtain a copy of the essence of the arrangements under this JCA;
where a Party intends to onward transfer the Personal Data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore.

Notwithstanding the foregoing, the above shall not apply where the data subject already has the information, including when such information has already been provided by one of the Parties, or providing the information proves impossible or would involve a disproportionate effort for the Parties. In the latter case, the Parties shall, to the extent possible, make the information publicly available.

6. Lawfulness of Data Processing

6.1 Each Party undertakes to ensure compliance of its processing of the Personal Data with GDPR and any other applicable European Data Protection Law. Personal Data shall be:

processed lawfully, fairly and in a transparent manner in relation to the data subject;
collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
adequate, relevant and limited to what is necessary in relation to the Processing Purposes;

6.2 Either Party shall promptly inform the other Party if it is unable to comply with this JCA, for whatever reason. In the event that a Party is in breach of this JCA or unable to comply with this JCA, the other Party shall suspend the transfer of Personal Data to the noncompliant Party until compliance is again ensured or the Agreement is terminated.

7. Notification to Authorities and Data Subjects in Case of Data Breaches

7.1 In the event of a Data Breach concerning Personal Data processed by the Parties under this JCA, the Parties shall take appropriate measures to address the Data Breach, including measures to mitigate its possible adverse effects. Should a Data Breach occur with one Party, this Party will inform the other Party without undue delay and, where feasible, not later than 72 hours after having become aware of it. The Parties will cooperate with each other to minimize the impact of the Data Breach, and/or to remedy the Data Breach.

7.2 In case of a Data Breach that is likely to result in a risk to the rights and freedoms of natural persons, the Parties shall without undue delay notify both the other Party and the competent supervisory authority pursuant to this JCA. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the Parties to provide all the information at the same time, it may do so in phases without undue further delay.

7.3 As between the Parties, the Party in whose area of responsibility the data breach has occurred shall take the lead in handling any data breaches including the communication with the supervisory authorities and shall coordinate with the other Party accordingly as required to ensure compliance with the GDPR and any other applicable law.

8. Engagement of Processors

Whenever a Party wishes to commission a processor for the processing of the Personal Data for the Processing Purposes under this JCA, the Party retaining the processor undertakes to conclude a data processing agreement in accordance with Article 28 GDPR.

9. Storage Limitation and Retention

9.1 Each Party undertakes to comply with the principle of storage limitation as per Art. 5 (1)(e) GDPR.

9.2 The Parties shall retain the personal data for no longer than necessary for the Processing Purposes for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymization of the data and all back-ups at the end of the retention period.

9.3 The Parties shall independently ensure that they comply with all statutory retention obligations in relation to the Personal Data. This applies in particular in the event of termination of this JCA.

10. Data security and Information

10.1 Data security. Both Parties maintain appropriate technical and organisational security measures in their respective areas of responsibility to ensure a level of protection appropriate to the risk (Art. 32 GDPR).

10.2 Records of Processing Activities. The Parties shall each keep separate records of processing activities with respect to the Joint Data Processing. The Parties shall make such documentation available to the competent supervisory authority on request.

10.3 Information. If a claim is made against one of the Parties, alleging that the Joint Data Processing is unlawful in whole or in part, this Party shall inform the other Party without undue delay.

11. Liability

The Parties are jointly and severally liable in relation to affected data subjects for any damage caused in the course of Joint Data Processing by processing that does not comply with applicable European Data Protection Law. A Party shall be exempted from liability if it proves that it is in no way responsible in any way for the circumstance by which the damage occurred (Art. 82 GDPR).

GDPR DPA Schedule B
Processor Addendum

1. **Definitions.**

1.1. "Publisher Data" has the meaning set forth in the Agreement.

1.2. "Publisher Instructions" means: (i) Processing to provide the services and perform Adagio's obligations in the Agreement (including this Processor DPA) and (ii) other reasonable documented instructions of Publisher consistent with the terms of the Agreement.

2. Scope and Duration.

2.1. Roles of the Parties. This Processor Addendum applies to Adagio as a Processor of Publisher Data and to Publisher as a Controller of Publisher Data.

2.2. Scope of Processor DPA. This Processor Addendum applies to Adagio's Processing of Publisher Data under the Agreement to the extent such Processing is subject to European Data Protection Law.

3. **Processing of Personal Data**.

3.1. Publisher Instructions.

(a) Adagio will Process Publisher Data as a Processor only: (i) in accordance with the Publisher Instructions or (ii) to comply with Adagio's obligations under applicable European Data Protection Law, subject to any notice requirements under applicable European Data Protection Law.

(b) Details regarding the Processing of Publisher Data by Adagio are set forth in the Agreement describing the Services, and the duration of the processing will be for the duration of the Services. The types of Publisher Data are online identifiers such as cookie IDs and mobile ad identifiers, information based on the Consumer's browsing activity, information about browsers and devices used, and geolocation information. The limited and specific purposes of Processing for the Processor Services are set forth in the GDPR General Terms.

(c) Adagio will notify Publisher if it receives an instruction that Adagio reasonably determines infringes European Data Protection Law (but Adagio has no obligation to actively monitor Publisher's compliance with European Data Protection Law).

3.2. Confidentiality.

(a) Adagio will protect Publisher Data in accordance with its confidentiality obligations as set forth in the Agreement.

(b) Adagio will ensure personnel who Process Publisher Data either enter into written confidentiality agreements or are subject to statutory obligations of confidentiality.

3.3. Compliance with Laws.

(a) Adagio and Publisher will each comply with European Data Protection Law in their respective Processing of Publisher Data.

(b) Publisher warrants and represents that it will comply with European Data Protection Law in its issuing of Publisher Instructions to Adagio. Publisher warrants that it has established and will maintain all necessary lawful bases under European Data Protection Law to enable Adagio to lawfully Process Publisher Data for the purposes contemplated by the Agreement (including under this Processor Addendum), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects. Publisher shall indemnify, defend and hold harmless Adagio from any claims, damages, losses, liabilities, costs and expenses (including reasonable attorneys' fees) arising from Publisher's failure to establish or maintain such lawful bases.

3.4. Changes to Laws. The parties will work together in good faith to negotiate an amendment to this Processor Addendum as either party reasonably considers necessary to address the requirements of

European Data Protection Law from time to time.

4. **Subprocessors**.

4.1. Use of Subprocessors.

(a) Publisher hereby provides general written authorization for Adagio to engage Subprocessors to Process Publisher Data as necessary to provide the services, subject to the requirements in this DPA. Publisher specifically authorizes Adagio to engage its Affiliates as Subprocessors. Publisher acknowledges that Adagio may update its Subprocessor list from time to time, and Publisher shall have the opportunity to object to such changes within 30 days of notification.

(b) Adagio will: (i) enter into a written agreement with each Subprocessor imposing data Processing and protection obligations substantially the same as those set out in this Processor Addendum and (ii) remain liable for compliance with the obligations of this Processor Addendum and for any acts or omissions of a Subprocessor that cause Adagio to breach any of its obligations under this Processor Addendum.

4.2. Subprocessor List. Adagio will maintain an up-to-date list of its Subprocessors, including their functions and locations, as specified in its Subprocessor List.

4.3. Notice of New Subprocessors. Adagio may update the Subprocessor List from time to time. Adagio will notify Publisher of any new Subprocessor through updates to the Subprocessor List available at www.adagio.io/subprocessors through its standard notification procedures.

4.4. Objection to New Subprocessors.

(a) If, within 30 days after notice of a new Subprocessor, Publisher notifies Adagio in writing that Publisher objects to Adagio's appointment of such new Subprocessor based on reasonable data protection concerns, the parties will discuss such concerns in good faith.

(b) If the parties are unable to reach a mutually agreeable resolution to Publisher's objection to a new Subprocessor, Publisher, as its sole and exclusive remedy, may terminate the Order for the affected services for its convenience in accordance with the Agreement.

5. **Security**.

5.1. Security Measures. Adagio will implement and maintain appropriate technical and organizational measures to protect Publisher Data and protect against Data Breaches, in accordance with Adagio's Security Measures referenced in the Agreement and as further described the technical and organizational measures set forth at www.adagio.io/legal/tom. Adagio will regularly monitor its compliance with its Security Measures.

5.2. Incident Notice and Response.

(a) Adagio will implement and follow procedures to detect and respond to Data Breaches.

(b) Adagio will: (i) notify Publisher without undue delay after becoming aware of a Data Breach affecting Publisher Data and (ii) make reasonable efforts to identify the cause of the Data Breach, mitigate the effects and remediate the cause to the extent within Adagio's reasonable control.

(c) Upon Publisher's request and taking into account the nature of the applicable Processing, Adagio will assist Publisher by providing, when available, information reasonably necessary for Publisher to meet its Data Breach notification obligations under European Data Protection Law.

(d) Publisher acknowledges that Adagio's notification of a Data Breach is not an acknowledgement by Adagio of its fault or liability.

(e) Data Breaches do not include unsuccessful attempts or activities that do not compromise the security of Publisher Data, including unsuccessful login attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

5.3. Publisher Responsibilities.

(a) Publisher is responsible for reviewing the information made available by Adagio relating to data security and making an independent determination as to whether the Service meets Publisher's requirements and legal obligations under European Data Protection Law.

(b) Publisher is solely responsible for complying with Data Breach notification laws applicable to Publisher and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Data Breaches.

6. **Data Protection Impact Assessment**. Upon Publisher's request and taking into account the nature of the applicable Processing, to the extent such information is available to Adagio, Adagio will assist Publisher in fulfilling Publisher's obligations under European Data Protection Law to carry out a data protection impact or similar risk assessment related to Publisher's use of the Services, including, if required by European Data Protection Law, by assisting Publisher in consultations with relevant government authorities.

7. **Data Subject Requests**.

7.1. Assisting Publisher. Upon Publisher's request and taking into account the nature of the applicable Processing, Adagio will assist Publisher by appropriate technical and organizational measures, insofar as possible, in complying with Publisher's obligations under European Data Protection Law to respond to requests from individuals to exercise their rights under European Data Protection Law, provided that Publisher cannot reasonably fulfill such requests independently (including through use of the Services).

7.2. Data Subject Requests. If Adagio receives a request from a Data Subject in relation to the Data Subject's Publisher Data, Adagio will notify Publisher and advise the Data Subject to submit the request to Publisher (but not otherwise communicate with the Data Subject regarding the request except as may be required by European Data Protection Law), and Publisher will be responsible for responding to any such request.

8. **Data Return or Deletion**.

8.1. During the Term. During the Term, Publisher may, through the features of the Adagio Platform or such other means specified by Adagio, access, return to itself or delete Publisher Data.

8.2. Post Termination.

(a) Following termination or expiration of the Agreement, Adagio will, in accordance with its obligations under the Agreement, delete all Publisher Data from Adagio's systems.

(b) Deletion will be in accordance with industry-standard secure deletion practices. Adagio will issue a certificate of deletion upon Publisher's request.

(c) Notwithstanding the foregoing, Adagio may retain Publisher Data: (i) as required by European Data Protection Law or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Adagio will (x) maintain the confidentiality of, and otherwise comply with the applicable provisions of this Processor Addendum with respect to, retained Publisher Data and (y) not further Process retained Publisher Data except for such purpose(s) and duration specified in such applicable European Data Protection Law.

9. **Audits**.

9.1. Adagio Records Generally. Adagio will keep records of its Processing in compliance with European Data Protection Law and, upon Publisher's request, make available to Publisher any records reasonably necessary to demonstrate compliance with Adagio's obligations under this Processor Addendum and European Data Protection Law.

9.2. Third-Party Compliance Program.

(a) Adagio will describe its third-party audit and certification programs (if any) and make summary copies of its audit reports (each, an "**Audit Report**") available to Publisher upon Publisher's written request at reasonable intervals (subject to confidentiality obligations).

(b) Publisher may share a copy of Audit Reports with relevant government authorities as required upon

their request.

(c) Publisher agrees that any audit rights granted by European Data Protection Law will be satisfied by Audit Reports and the procedures of Section 9.3 (Publisher Audit) below.

9.3. Publisher Audit.

(a) Subject to the terms of this Section 9.3, Publisher has the right, at Publisher's expense, to conduct an audit of reasonable scope and duration pursuant to a mutually agreed-upon audit plan with Adagio that is consistent with the Audit Parameters (an "**Audit**"), provided that Publisher gives Adagio at least thirty (30) days prior written notice of any proposed audit.

(b) Publisher may exercise its Audit right solely: (i) to the extent Adagio's provision of an Audit Report does not provide sufficient information for Publisher to verify Adagio's compliance with this Processor Addendum or the parties' compliance with European Data Protection Law, and Publisher has first attempted in good faith to resolve any compliance concerns through written documentation from Adagio, (ii) as necessary for Publisher to respond to a government authority audit, or (iii) in connection with a confirmed Data Breach directly attributable to Adagio.

(c) Each Audit must conform to the following parameters ("**Audit Parameters**"): (i) be conducted by an independent third party auditor mutually agreed upon by the Parties (such agreement not to be unreasonably withheld) that will enter into a confidentiality agreement with Adagio in a form reasonably acceptable to Adagio, (ii) be limited in scope to matters reasonably required for Publisher to assess Adagio's compliance with this Processor Addendum and the parties' compliance with European Data Protection Law, (iii) occur at a mutually agreed date and time and only during Adagio's regular business hours, (iv) occur no more than once annually (unless required by a competent supervisory authority with jurisdiction over the matter), and Publisher shall bear all costs and expenses associated with the audit, including reasonable costs incurred by Adagio in facilitating and supporting the audit, (v) cover only facilities controlled by Adagio, (vi) restrict findings to Publisher Data only and (vii) treat any results as confidential information to the fullest extent permitted by European Data Protection Law.

10. **Cross-Border Transfers/Region-Specific Terms**.

10.1. Cross-Border Data Transfers.

(a) Adagio (and its Affiliates) may Process and transfer Publisher Data globally as necessary to provide the Services.

(b) For any transfers of Publisher Data from GDPR Countries, the Restricted Transfer Addendum applies.

GDPR DPA Schedule C
Restricted Transfer Addendum

This Addendum includes the following Annexes, each of which are part of this Addendum as applicable.

- **Annex 1: Description of the Processing**
- **Annex 2: Technical and Organizational Measures**

Section 1. Definitions

1.1. "**Controller Services**" has the meaning set forth in the GDPR General Terms.

1.2. "**DPF Signatory**" means a signatory that has certified compliance with the Data Privacy Framework Principles (available at https://www.dataprivacyframework.gov/s/framework-text) whether under the EU-US framework, Swiss-U.S framework, or UK Extension to the EU-US framework.

1.3. "**Onward Transfers**" means onward transfers by the Receiving Party to a third-party Controller or Processor.

1.4. "**Processor Services**" has the meaning set forth in the GDPR General Terms.

1.5. "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area ("**EEA**") to a recipient in a country outside of the EEA which is not subject to an adequacy determination by the European Commission and where the recipient is not a DPF Signatory; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom ("**UK**") to a recipient in a country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018 and where the recipient is not a DPF Signatory.

1.6. "**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**").

Section 2. Adagio's Data Centers

Adagio processes and stores Personal Data subject to European Data Protection Law in countries with European Commission adequacy decisions or using appropriate safeguards. This Addendum applies only to Restricted Transfers. Onward Transfers by either Party to third-party Controllers or Processors are under separate agreements.

Section 3. Restricted Transfers

3.1. In respect of any Restricted Transfer, Disclosing Party (as "data exporter") and Receiving Party (as "data importer"), with effect from the commencement of any relevant transfer, hereby enter into Module 1 (controller-to-controller) and Module 2 (controller-to-processor) of the Standard Contractual Clauses in respect of any transfer of Personal Data from Disclosing Party to Receiving Party.

3.2 For Restricted Transfers under the EU SCCs for Controller Services subject to Module One:

a) Clause 7 – the options docking clause will apply;
b) Clause 11(a) – the optional language shall not apply;
c) Clause 17 – "Option 1" applies for governing law, and the "Member State" shall be France;
d) Clause 18 – Choice of forum and jurisdiction shall be France (Paris);
e) Annex 1 shall be deemed completed with the information set out in Annex 1 to this Addendum;
f) Annex 2 shall be deemed completed with the information set out in Annex 2 to this Addendum.

3.3 For Restricted Transfers under the EU SCCs for Processor Services subject to Module Two:

a) Clause 7 – the options docking clause will apply;
b) Clause 9 - Option 2 applies; the time period for prior notice of sub-processor changes will be 30 days;
c) Clause 11(a) – the optional language shall not apply;
d) Clause 17 – "Option 1" applies for governing law, and the "Member State" shall be France;
e) Clause 18 – Choice of forum and jurisdiction shall be France (Paris);
f) Annex 1 shall be deemed completed with the information set out in Annex 1 to this Addendum;
g) Annex 2 shall be deemed completed with the information set out in Annex 2 to this Addendum.

3.4 In respect of any Restricted Transfers under the UK SCCs, the EU SCCs completed as set out above shall also apply to such transfers and shall be interpreted consistently with the information set forth in this Addendum.

3.5 For Restricted Transfers from Switzerland, the terms of the EU SCCs shall be amended and supplemented as specified by the relevant guidance of the Swiss Federal Data Protection and Information Commissioner.

Section 4. Miscellaneous

4.1 This Restricted Transfer Addendum shall control in the event of a conflict with any other part of the DPA.

Annex 1 to Restricted Transfer Addendum
Description of the Processing

Part 1. List of Parties

Data exporter(s)

When acting as Data Exporter, the relevant Party's details and its data protection officer and/or representative in the European Union/United Kingdom shall be as identified in the Order Form or as follows: For Publisher, as identified in the Order Form; For Adagio: Marieke Schuit, DPO, legal@adagio.io, or such other DPO as Adagio may designate from time to time upon notice to Publisher.

Data importer(s)

When acting as Data Importer, the relevant Party's details and its data protection officer and/or representative in the European Union/United Kingdom shall be as identified in the Order Form or as follows: For Publisher, as identified in the Order Form; For Adagio: OnFocus, a SAS incorporated in France (RCS n° 820244770), dba Adagio, with its data protection officer being Marieke Schuit, DPO, legal@adagio.io, or such other DPO as Adagio may designate from time to time upon notice to Publisher.

Part 2. Description of Transfer

- Categories of data subjects whose personal data is transferred: data subjects utilizing the Media owned, operated, or contractually controlled by Publisher.
- Categories of personal data transferred: Device ID and Unique ID (either generated by Adagio or by a Bidder), non-precise geolocation information derived from IP addresses, IP addresses, cookie identifiers, advertising identifiers, browser type and version, operating system information, and other technical information reasonably necessary for the delivery of advertising.
- Sensitive Personal Data transferred (if applicable): N/A
- Frequency of the transfer: On a continuous basis.
- Nature of the processing: Collection, recording, organization, structuring, alteration, retrieval, consultation, disclosure by transmission, erasure or destruction, as reasonably necessary to provide the Services
- Purpose(s) of the data transfer and further processing: See the GDPR General Terms for the Processing Purposes and the applicable Order Form.
- Period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: The data will be retained as required for the Processing Purposes set forth in the GDPR General Terms and will be deleted within the time frames set forth in Adagio's then-current publicly posted privacy policy on its corporate website and no later than 13 months after collection, unless a longer retention period is specifically required by applicable law or reasonably necessary for Adagio's legitimate business purposes in compliance with applicable data protection laws. Any extension of the retention period for legitimate business purposes shall be documented and justified in accordance with Article 5(1)(e) of the GDPR.

Part 3. Competent Supervisory Authority/ies.

Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR in accordance with its Art 3 (2) and has appointed a representative pursuant to Art. 27 (1) GDPR: The supervisory authority of the Member State in which the representative within the meaning of Art. 27 (1) GDPR is established shall act as a competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR in accordance with its Art. 3 (2) without however having to appoint a representative pursuant to Art. 27 (2) GDPR: The supervisory authority of one of the Member States in which the data subjects whose

personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored shall act as competent supervisory authority.

Annex 2 to Restricted Transfer Addendum
Technical and Organizational Measures

Description of the technical and organizational measures implemented by the parties (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Adagio's technical and organizational measures are available at www.adagio.io/legal/tom and are hereby incorporated by reference and which will control in the event of a conflict with this Annex 2 as long as such measures are at least as protective as those set forth in this Annex 2. Adagio may update these measures from time to time, provided that such updates maintain or enhance the overall level of protection.

Each Party agrees to the following Information Security Policies and Standards:

1. Each party will implement security requirements for such party's personnel and all subcontractors or agents who have access to Personal Data. These are designed to:
   1.1. Prevent unauthorized persons from gaining access to Personal Data processing systems (physical access control);
   1.2. Prevent Personal Data processing systems being used without authorization (logical access control);
   1.3. Ensure that persons entitled to use a Personal Data processing system gain access only to such Personal Data as they are entitled to access in accordance with their access rights and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control).
   1.4. Ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control).
   1.5. Ensure the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Data Processing (entry control);
   1.6. Ensure that Personal Data are Processed solely in accordance with the Data Exporter's instructions (control of instructions);
   1.7. Ensure that Personal Data are protected against accidental destruction or loss (availability control); and
   1.8. Ensure that Personal Data collected for different purposes can be processed separately (separation control).

2. Each party will ensure that these requirements are kept up to date, and revised whenever relevant changes are made to the information system that uses or houses Personal Data, or to how that system is organized.

3. Physical Security
   3.1. Each party will maintain commercially reasonable security systems at all sites at which an information system that uses or houses Personal Data is located.
   3.2. Each party will reasonably restrict access to such Personal Data appropriately.
   3.3. Physical access control has been implemented for all of the applicable party's data centers. Unauthorized access is prohibited through 24x7 onsite staff, biometric scanning and security camera monitoring. Data Center physical security is audited by an independent firm.
   3.4. Surveillance cameras and security monitoring by building management are implemented.

4. Organizational Security
   4.1. When media is to be disposed of or reused, the parties' respective procedures have been implemented to prevent any subsequent retrieval of any Personal Data stored on them before they are withdrawn from the inventory. When media are to leave the premises at which the files are located as a result of maintenance operations, the parties' respective procedures have been implemented to prevent undue retrieval of Personal Data stored on them.
   4.2. Each party will implement and maintain security policies and procedures to classify sensitive information assets, clarify security responsibilities and promote awareness for employees.
   4.3. Each party will manage all Personal Data security incidents in accordance with its established incident response procedures and applicable law, including any mandatory notification requirements. The parties

shall notify each other without undue delay, and in any event within 72 hours, upon becoming aware of a Personal Data security incident affecting the other party's Personal Data, unless the Personal Data security incident is unlikely to result in a risk to the rights and freedoms of natural persons.

5. Network Security

Each party will maintain network security using commercially available equipment and industry standard techniques, including firewalls, intrusion detection systems, access control lists and routing protocols.

6. Access Control

6.1. Only authorized staff can grant, modify or revoke access to an information system that uses or houses Personal Data.

6.2. Each party's user administration procedures: define user roles and their privileges, and how access is granted, changed, and terminated; address appropriate segregation of duties; and define the logging/monitoring requirements and mechanisms.

6.3. All employees will be assigned unique User-IDs.

6.4. Each party will implement access rights adhering to the "least privilege" approach.

6.5. Each party will implement commercially reasonable physical and electronic security controls to create and protect passwords.

7. Virus and Malware Controls

Each party will install and maintain anti-virus and malware protection software on their systems.

8. Personnel

8.1. Each party will implement a security awareness program to train personnel about their security obligations. This program includes training about data classification obligations, physical security controls, security practices, and security incident reporting.

8.2. Each party will have clearly defined roles and responsibilities for such party's employees. Screening is implemented before employment with terms and conditions of employment applied appropriately.

8.3. Each party will require its employees to strictly follow established security policies and procedures. Disciplinary process will be applied if employees commit a security breach.

9. Business Continuity

9.1. Each party will implement appropriate disaster recovery and business resumption and continuity plans and will review such plans and related risk assessments regularly.

9.2. Such plans will be tested and updated regularly by the applicable party to ensure that they are up to date and effective.