

DATA PROCESSING AGREEMENT

Exhibit to the A2 Atlas Subscription Agreement

This Data Processing Agreement (“DPA”) forms part of and is incorporated into the A2 Atlas Subscription Agreement between A2 Holdco, LLC, a Delaware limited liability company, DBA Association Analytics (“Company”), and the subscriber identified on the applicable Order Form (“Subscriber”) (the “Agreement”). Capitalized terms not defined in this DPA have the meanings given in the Agreement. In the event of any ambiguity, this DPA will be interpreted in a manner consistent with Company’s obligations as a Processor and Service Provider under Data Protection Law.

This DPA applies to Company’s Processing of Personal Data contained within Subscriber Data. In the event of a conflict between this DPA and the Agreement with respect to the Processing of Personal Data, this DPA controls.

1. DEFINITIONS

1.1 “Data Protection Law” means all laws applicable to the Processing of Personal Data under this DPA, including the EU General Data Protection Regulation 2016/679 (“GDPR”), the UK GDPR and Data Protection Act 2018, the California Consumer Privacy Act as amended by the California Privacy Rights Act (“CCPA”), and other US state privacy laws as applicable.

1.2 “Controller,” “Processor,” “Data Subject,” “Personal Data,” “Personal Data Breach,” “Processing,” and “Supervisory Authority” have the meanings given in the GDPR. “Business,” “Service Provider,” “Consumer,” “Sell,” and “Share” have the meanings given in the CCPA.

1.3 “Sub-processor” means any third party engaged by Company to Process Personal Data on Subscriber’s behalf in connection with the provision of the Platform. Sub-processor does not include any Authorized Agent or its provider.

1.4 “Aggregated De-identified Data” means data derived from Subscriber Data that has been aggregated with data from other sources, **including Subscriber Data of other subscribers to the Platform**, or otherwise processed and de-identified such that it does not identify, and cannot reasonably be used to infer information about or otherwise be linked to, any Data Subject or to Subscriber, and includes any statistical, analytical, or benchmarking outputs derived therefrom.

2. ROLES AND SCOPE

2.1 Roles. Subscriber is the Controller and, where the CCPA applies, the Business. Company is the Processor and, where the CCPA applies, the Service Provider. Each Party will comply with its own obligations under Data Protection Law. The Parties acknowledge that Company acts as an independent Controller with respect to Aggregated De-identified Data under Section 8 and with respect to any Processing that Company carries out for its own compliance, security, or fraud-prevention purposes under Section 3.1.

2.2 Subscriber responsibilities. Subscriber is solely responsible for the accuracy and legality of Subscriber Data, for having a lawful basis for the Processing it instructs, and for providing any notices and obtaining any consents required from Data Subjects. Subscriber warrants that its instructions to Company comply with Data Protection Law. Subscriber will indemnify and hold Company harmless from any claim, loss, or expense arising from Subscriber’s breach of this Section 2.2.

2.3 Details of Processing. The subject matter, duration, nature and purpose of the Processing, the types of Personal Data, and the categories of Data Subjects are set out in Annex 1. Annex 1 may be

supplemented by a written addendum executed by both Parties describing additional Processing. Annex 4 sets out how demographic data is Processed and forms part of Annex 1.

3. PROCESSING ON DOCUMENTED INSTRUCTIONS

3.1 Company will Process Personal Data only on Subscriber's documented instructions, including with regard to transfers of Personal Data to a third country, unless required to Process by law to which Company is subject or as reasonably necessary to protect the security of the Platform, prevent fraud, or comply with Company's own legal obligations. Where Company Processes Personal Data on a basis other than Subscriber's instructions, Company will inform Subscriber of that basis before Processing, unless the law prohibits such information on important grounds of public interest.

3.2 Documented instructions. The Agreement, this DPA, the applicable Order Form, Company's published documentation and privacy policies, and Subscriber's use and configuration of the Platform constitute Subscriber's complete documented instructions. Additional instructions outside the scope of the foregoing require a written agreement between the Parties and will be subject to additional charges.

3.3 Unlawful instructions. Company will promptly inform Subscriber if, in Company's opinion, an instruction from Subscriber infringes Data Protection Law. Company may suspend performance of the affected instruction until it is amended, confirmed, or withdrawn.

3.4 No sale or sharing. Company will not Sell or Share Personal Data, will not retain, use, or disclose Personal Data for any purpose other than performing the services specified in the Agreement, will not retain, use, or disclose Personal Data outside the direct business relationship between the Parties, and will not combine Personal Data with personal information received from or on behalf of another person, except as permitted by the CCPA. This Section 3.4 applies only to the extent the CCPA applies to the relevant Processing. Company certifies that it understands and will comply with these restrictions. Nothing in this Section prohibits Company from Processing Subscriber Data to create or use Aggregated De-identified Data in accordance with Section 8.

4. CONFIDENTIALITY OF PERSONNEL

4.1 Company will take commercially reasonable steps to ensure that persons authorized to Process Personal Data are bound by an appropriate obligation of confidentiality, whether contractual or statutory, and have received appropriate training on their responsibilities.

4.2 Company will limit access to Personal Data to those of its personnel who require access in order to perform Company's obligations under the Agreement.

5. SECURITY

5.1 Company will implement and maintain commercially reasonable technical and organizational measures designed to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing, as well as the risk to the rights and freedoms of Data Subjects. Those measures are described in Annex 2.

5.2 Company may update the measures in Annex 2 from time to time in its sole discretion to reflect changes in technology, industry practice, or the threat landscape, provided that the measures as updated continue to provide a commercially reasonable level of security.

6. SUB-PROCESSORS

6.1 General authorization. Subscriber grants Company general authorization to engage Sub-processors to Process Personal Data. The Sub-processors engaged as at the effective date of this DPA are listed in Annex 3.

6.2 Notice of changes. Company will give Subscriber not less than fifteen (15) days' prior notice of any intended addition or replacement of a Sub-processor. Notice will be given by email to Subscriber's designated contact. Where a Sub-processor's own change takes effect on or before the date Company becomes aware of it, Company will instead notify Subscriber promptly after becoming aware, and Subscriber's objection right under Section 6.3 applies from the date of that notification. Subscriber's continued use of the Platform after the expiry of the applicable notice period constitutes acceptance of the new or replacement Sub-processor.

6.3 Objection. Subscriber may object to an intended addition or replacement on specific, documented grounds relating to data protection by giving written notice within the notice period, setting out in reasonable detail the grounds for the objection. The Parties will discuss the objection in good faith and Company will use commercially reasonable efforts to address it, including by proposing alternative measures or safeguards. Where Subscriber does not object within the notice period, or where the Parties resolve the objection, Subscriber will be deemed to have accepted the change. An unresolved objection does not give rise to any right of termination, refund, or credit, and does not suspend or delay the change.

6.4 Flow-down and liability. Company will impose on each Sub-processor, by written contract, data protection obligations no less protective than those set out in this DPA. Company remains liable to Subscriber for the performance of each Sub-processor's obligations to the extent Company would be liable for the same acts or omissions if performed by Company itself, subject to the limitations of liability in Section 15.1.

6.5 Emergency replacement. Where a change of Sub-processor is required urgently to protect the security or availability of the Platform, to comply with law, or to address a Sub-processor's material failure to perform, Company may make the change before the notice period expires, and will inform Subscriber as soon as reasonably practicable. In such event, Subscriber's objection right under Section 6.3 applies from the date of notification.

7. ARTIFICIAL INTELLIGENCE FEATURES

7.1 Transmission. Where Subscriber enables AI Features, Personal Data within Subscriber Data submitted to or Processed by AI Features is transmitted to and Processed by the large language model providers identified in Annex 3, acting as Sub-processors, in order to generate and return a response. **Transmission is not limited to occasions when an Authorized User is actively using AI Features: certain features generate analytical commentary on a schedule and transmit the relevant Subscriber Data whether or not an Authorized User has opened them.** Personal Data fields are masked before transmission by default; Subscriber's tenant administrators and Company internal administrators may request unmasked values, in which case identifiable Personal Data is transmitted and the request is recorded in the audit record described in Annex 2. AI Features and their outputs are provided on an "as-is" basis without warranty of any kind, including as to accuracy, completeness, or fitness for a particular purpose.

7.2 No model training. Company will not use Personal Data in identifiable form to train, develop, or improve any machine learning or artificial intelligence model. For the avoidance of doubt, this prohibition does not apply to Aggregated De-identified Data as defined in Section 1.4. Company will use commercially reasonable efforts to ensure that its contracts with large language model provider Sub-processors prohibit the use of Personal Data in identifiable form for training those providers' models.

7.3 Retention by providers. Personal Data transmitted under Section 7.1 is retained by the relevant Sub-processor for a period not exceeding thirty (30) days and may be accessed by that Sub-processor for safety and security purposes. Where content is flagged by a Sub-processor's automated misuse screening, the related inputs and outputs may be retained for up to two (2) years for investigation, and records of that classification for up to seven (7) years. A Sub-processor may also retain Personal Data where required by

law. Company will use commercially reasonable efforts to ensure that its contracts with large language model provider Sub-processors impose retention limits consistent with this Section.

7.4 Subscriber control. Subscriber determines whether AI Features are enabled for its organization. This control operates at the organization level rather than per Authorized User, because Subscriber Data may be transmitted by automated features and by the activity of any Authorized User, so disabling AI Features for an individual would not prevent Subscriber Data from being Processed. Subscriber is solely responsible for the Personal Data it and its Authorized Users submit to AI Features and will not submit special category data (other than Demographic Data Processed under Annex 4), protected health information, or other categories of data prohibited under the Agreement. Subscriber acknowledges and assumes all risk associated with its use of AI Features, including the risk that AI-generated outputs may be inaccurate or incomplete.

8. AGGREGATED DE-IDENTIFIED DATA

8.1 Instruction. Subscriber instructs Company to Process Subscriber Data in order to create Aggregated De-identified Data, including benchmark outputs, and to use such data for any lawful business purpose, including product development, analytics, research, benchmarking, marketing, and the improvement of Company's products and services. Subscriber acknowledges that such Processing is a core element of the Platform and a material part of the consideration for the Agreement. This Section 8.1 does not extend to Demographic Data Processed under Annex 4.

8.2 Standard. Company will apply reasonable technical and organizational measures designed to ensure that Aggregated De-identified Data cannot reasonably be used to identify, or to infer information about, any Data Subject or Subscriber. Company will not attempt to re-identify Aggregated De-identified Data and will contractually prohibit recipients from doing so. Without limiting the foregoing, Company will implement business processes specifically designed to prevent inadvertent release of de-identified data in identifiable form and to prevent re-identification of de-identified data.

8.3 Status. Once data meets the standard in Section 8.2, it is not Personal Data and this DPA does not apply to it. As between the Parties, Company exclusively owns all Aggregated De-identified Data.

8.4 Survival. Company's rights under this Section survive termination or expiration of the Agreement with respect to all Aggregated De-identified Data, regardless of when created. For the avoidance of doubt, termination of the Agreement does not require Company to delete or return Aggregated De-identified Data.

9. DATA SUBJECT RIGHTS

9.1 Taking into account the nature of the Processing and the information available to Company, Company will provide commercially reasonable assistance to Subscriber, insofar as technically feasible through the functionality of the Platform, in fulfilling Subscriber's obligation to respond to requests to exercise Data Subject rights under Data Protection Law.

9.2 Where Company receives a request directly from a Data Subject relating to Personal Data Processed on Subscriber's behalf, Company will not respond to the substance of the request except on Subscriber's documented instructions or as required by law, and will promptly refer the request to Subscriber.

9.3 To the extent Subscriber is unable to address a request through the functionality of the Platform, Company will provide reasonable assistance on request, subject to Subscriber's reimbursement of Company's reasonable costs. Company will provide Subscriber with an estimate of costs before incurring charges in excess of one hour of effort per request.

10. PERSONAL DATA BREACH

10.1 Notification. Company will notify Subscriber without undue delay after confirming a Personal Data Breach affecting Personal Data Processed on Subscriber's behalf. Company will use reasonable efforts to provide notification within seventy-two (72) hours of confirmation, but failure to do so will not constitute a breach of this DPA where the delay is attributable to the complexity of the incident or law-enforcement requirements.

10.2 Content. The notification will describe, to the extent reasonably known at the time and supplemented as further information becomes available: the nature of the breach, including where possible the categories and approximate number of Data Subjects and records concerned; the likely consequences; the measures taken or proposed to address the breach and mitigate its effects; and a contact point for further information. Information provided is preliminary and may be updated as the investigation progresses.

10.3 Assistance. Company will provide reasonable assistance to Subscriber in connection with Subscriber's own notification obligations to Supervisory Authorities and Data Subjects, subject to Subscriber's reimbursement of Company's reasonable costs of providing such assistance.

10.4 No admission. Company's notification of or response to a Personal Data Breach is not an acknowledgment of fault or liability. Subscriber will not use the fact of notification or the content of any notification as evidence of Company's fault or liability in any proceeding.

11. DATA PROTECTION IMPACT ASSESSMENTS

Company will provide reasonable assistance to Subscriber with any data protection impact assessment and any prior consultation with a Supervisory Authority that Subscriber is required to carry out under Data Protection Law, in each case solely in relation to the Processing of Personal Data by Company and taking into account the nature of the Processing and the information available to Company. Subscriber will reimburse Company's reasonable costs of providing such assistance.

12. DELETION AND RETURN

12.1 On expiration or termination of the Agreement, Company will make Subscriber Data available for export for thirty (30) days (or such longer period as may be stated in the Agreement). Subscriber is solely responsible for exporting its data during this period.

12.2 Following that period, Company will delete Personal Data Processed on Subscriber's behalf, except to the extent that retention is required by law or reasonably necessary for the establishment, exercise, or defense of legal claims, in which case Company will continue to protect that Personal Data in accordance with this DPA and will Process it only for the purpose requiring retention.

12.3 Personal Data held in routine backup or archival systems will be deleted in the ordinary course of Company's backup rotation, which will not exceed one hundred and eighty (180) days. Such data remains subject to this DPA until deleted and will not be actively Processed except as necessary for backup restoration.

12.4 This Section does not apply to Aggregated De-identified Data, which is governed by Section 8.

13. RECORDS AND AUDIT

13.1 Information. Company will make available to Subscriber information reasonably necessary to demonstrate compliance with this DPA. Where Company holds a current SOC 2 Type II report, ISO 27001 certificate, or equivalent third-party audit report or certification covering the Platform, provision of such report or certificate will satisfy Company's obligation under this Section 13.1 and Section 13.2 with respect to the matters covered by the report or certificate.

13.2 Audit. Where the information provided under Section 13.1 is not sufficient, Subscriber may, on not less than thirty (30) days' written notice and not more than once in any twelve (12) month period, audit Company's compliance with this DPA. Company may, at its election, satisfy an audit request by (a) making available relevant personnel for reasonable interview, (b) providing responses to a written security questionnaire, or (c) engaging an independent third-party auditor to conduct the audit at Subscriber's cost. Where an on-site audit is conducted, it will take place during normal business hours, will not unreasonably interfere with Company's operations, and will be subject to the confidentiality obligations in the Agreement.

13.3 Scope limits. An audit under Section 13.2 will not extend to any other customer's data, to Company's pricing, financial, or commercial information, to trade secrets, to any system or information the disclosure of which would compromise the security of Company or its other customers, or to the source code of the Platform. Subscriber will bear all of its own costs and will reimburse Company's reasonable costs of supporting the audit, including personnel time, within thirty (30) days of invoice. The auditor must execute a confidentiality agreement in form reasonably satisfactory to Company before commencing the audit.

13.4 Supervisory Authority. Company will cooperate with, and make itself available to, any Supervisory Authority with jurisdiction to the extent required by Data Protection Law.

14. INTERNATIONAL TRANSFERS

14.1 Company Processes Personal Data in the United States and may permit Sub-processors to Process Personal Data in other jurisdictions as identified in Annex 3.

14.2 Where Subscriber transfers Personal Data that is subject to the GDPR or UK GDPR from the European Economic Area, the United Kingdom, or Switzerland to Company in a jurisdiction that does not benefit from an adequacy decision, the Parties agree that the European Commission Standard Contractual Clauses (Module Two: Controller to Processor), together with the UK International Data Transfer Addendum where applicable, are incorporated into this DPA by reference and apply to that transfer, with Annex 1 of this DPA serving as Annex I to those clauses, Annex 2 serving as Annex II, and Annex 3 serving as Annex III. Where the transferring Subscriber is established in the United States and the transfer does not involve Personal Data originating from the EEA, UK, or Switzerland, the Standard Contractual Clauses do not apply.

14.3 Where the Standard Contractual Clauses apply and conflict with this DPA, the Standard Contractual Clauses control to the minimum extent required by applicable law, and this DPA will govern in all other respects.

15. GENERAL

15.1 Liability. Each Party's aggregate liability under or in connection with this DPA, whether in contract, tort, or otherwise, is subject to the limitations and exclusions of liability set out in the Agreement and will not exceed the amounts paid or payable by Subscriber to Company in the twelve (12) months preceding the event giving rise to the claim; provided that the foregoing limitation does not apply to Subscriber's obligations under Section 2.2. Neither Party will be liable to the other for any indirect, incidental, special, consequential, or punitive damages arising out of or in connection with this DPA, regardless of the theory of liability, except with respect to amounts paid to third parties and reasonable defense costs under Subscriber's indemnification obligations, and except to the extent such limitation is prohibited by Data Protection Law.

15.2 Term. This DPA takes effect on the effective date of the Agreement and continues for the term of the Agreement, plus any retention and deletion periods in Section 12. Upon deletion of all Personal Data in accordance with Section 12, this DPA will terminate automatically.

15.3 Order of precedence. This DPA prevails over the Agreement to the extent of any conflict regarding the Processing of Personal Data. Where a Party's own standard data processing terms are also executed, this DPA prevails unless the Parties expressly agree otherwise in writing.

15.4 Changes in law. If a change in Data Protection Law requires amendment of this DPA, the Parties will negotiate in good faith to agree the necessary amendment within sixty (60) days. If the Parties are unable to agree within that period, Company may implement changes it reasonably determines are necessary to comply with the applicable law, on written notice to Subscriber.

15.5 Execution. This DPA is executed by the Parties' execution of the Order Form incorporating the Agreement. No separate signature is required.

15.6 Governing law. This DPA is governed by and construed in accordance with the laws of the State of Delaware, without regard to its conflict of laws principles. Any dispute arising out of or in connection with this DPA will be resolved in accordance with Section 19.2 of the Agreement.

15.7 Severability. If any provision of this DPA is held invalid or unenforceable, the remaining provisions will remain in full force and effect and the invalid or unenforceable provision will be modified to the minimum extent necessary to make it valid and enforceable.

15.8 No third-party beneficiaries. This DPA does not confer any rights or remedies on any person other than the Parties and their respective successors and permitted assigns. Data Subjects are not third-party beneficiaries of this DPA except to the extent required by Data Protection Law.

15.9 Entire agreement. This DPA, together with the Agreement and the applicable Order Form, constitutes the entire agreement between the Parties regarding the Processing of Personal Data and supersedes all prior agreements, understandings, and representations relating to that subject matter.

ANNEX 1 — DETAILS OF PROCESSING

Controller	Subscriber, as identified on the Order Form.
Processor	A2 Holdco, LLC, DBA Association Analytics.
Subject matter	Provision of the A2 Atlas membership analytics platform and any optional modules identified on the Order Form.
Duration	The term of the Agreement, plus the retention and deletion periods in Section 12.
Nature of Processing	Collection, ingestion, storage, organization, structuring, normalization, analysis, benchmarking, aggregation, de-identification, retrieval, display, transmission to Sub-processors, export, and deletion.
Purpose	Providing, maintaining, securing, and improving the Platform and the subscribed modules; generating analytics, reporting, and benchmark outputs; and providing support.
Categories of Data Subjects	Subscriber's members and prospective members Subscriber's contacts, donors, and event or program participants Subscriber's certification and credential holders, where the Certifications Module is enabled Subscriber's staff and Authorized Users Chapter Entity personnel, where Chapter Access is enabled

Types of Personal Data	Identifiers: name, member identifier, email address, postal address, telephone number Employment information: employer, job title, professional designation Membership records: category, status, join and renewal dates, dues history Engagement records: email engagement, web analytics, event registrations, learning records Credential records, where the Certifications Module is enabled Free-text content authored within Subscriber's source systems Authorized User account and authentication data Standard demographics under Annex 4: birth year (for age, age band and generation) and gender Categories elected under Annex 4: race/ethnicity, exact date of birth, and a mission-aligned category
Special category data	None is required or requested, except racial or ethnic origin, and a mission-aligned category that is special category data, where Subscriber elects them under Annex 4. Subscriber is instructed not to submit any other special category data, protected health information, payment card data, government-issued identification numbers, financial account numbers, or biometric identifiers.
Frequency	Continuous, by scheduled ingestion from Subscriber's source systems and by Authorized User activity.
Additional Processing	Any additional Processing, including direct database access arrangements, is described in a written addendum executed by both Parties and forms part of this Annex 1.

ANNEX 2 — TECHNICAL AND ORGANIZATIONAL MEASURES

Completed by the Information Security Officer, 21 September 2026.

Access control	Role-based access control; named individual accounts; access limited to personnel who require it to perform their duties. Least-privilege permissions reviewed quarterly.
Authentication	Company personnel access to administrative and production systems requires single sign-on, with multi-factor authentication enforced at the identity provider (Microsoft 365 / Entra ID). Platform sign-in by Subscriber's Authorized Users is by single sign-on — federated to Subscriber's own identity provider where Subscriber configures it — or by username and password. Company does not enforce multi-factor authentication on Subscriber sign-in; where single sign-on is configured, any such enforcement is a matter of Subscriber's identity provider policy. Self-service signup is closed.
Encryption	Encryption in transit using TLS 1.2 or above; encryption at rest using AES-256 for production data stores.
Data masking	Column-level masking applied on read to designated personal data fields within the Platform application layer, with unmasking available to Subscriber's administrators and Company internal administrators, each unmask recorded in the audit record.

Tenant isolation	Logical separation of Subscriber data; credentials and application-level controls scoped to Subscriber's own data.
Logging and monitoring	Application-level audit record of unmasking events, administrative actions and agent tool calls, capturing user, time, fields, query and row count, reviewable by Subscriber's administrators. Retained seven (7) years . Authentication and sign-in events are recorded separately in an append-only audit trail and are retained indefinitely .
Backup and recovery	Daily backups to separate storage. Control plane: fourteen (14) day point-in-time recovery. Warehouse cells: thirty (30) day dump retention, nightly incremental and weekly full. Recovery procedures are documented and reviewed. Company does not represent that full restoration is routinely exercised ; the first complete restore was performed in August 2026 and the gaps it identified are being remediated.
Vulnerability management	Continuous dependency scanning; annual third-party penetration test by a CREST-certified assessor, OWASP/NIST-aligned. Remediation targets by CVSS severity: critical 15 days, high 30 days, medium 90 days, low 180 days .
Personnel	Confidentiality obligations in employment contracts; annual data protection training with acknowledgment, evidenced for all staff. Background screening is performed on employees hired from March 2026 onward ; it is not applied retrospectively to employees engaged before that date, and Company does not background screen contractors . Personnel of contracted firms who are authorized to access Company systems are bound by confidentiality through the engaging firm's agreement with Company.
AI governance	AI Features operate under an AI Management Policy written to align with ISO/IEC 42001 . Controls include: a pinned model version ; version-controlled system instructions ; field-level limits on what the assistant may read ; and review of redacted transcripts . Company's alignment with ISO/IEC 42001 is self-assessed and is not a third-party certification , and these AI-specific controls are governed internally and are not presented as separately tested by Company's SOC 2 examination .
Governance	Information security management system; Data Protection Policy and Information Security Policy reviewed annually and on significant change; Information Security Officer accountable for the program.
Incident response	Documented incident response process, including assessment, containment, notification and post-incident review, with documented severity levels. Platform health monitoring operates continuously; a severity-one condition raises an automated alert to the engineering team's channel within fifteen (15) minutes . Incident response is staffed during business hours (8:00 AM–6:00 PM US Eastern, Monday to Friday, excluding holidays); outside those hours Company responds on a commercially reasonable efforts basis and does not operate an out-of-hours paging rotation .
Sub-processor management	Written contracts with data protection terms no less protective than this DPA; review before engagement.

Certifications	No SOC 2 Type II report has yet been issued. An examination is in progress with an independent firm; observation period 2026, report expected Q4 2026, available under NDA once issued. No ISO 27001 certification. GDPR compliance is an internally assessed position, reviewed and confirmed August 2026, and is not a third-party certification. Annual penetration test most recently completed July 2026, A+ grade, certified through July 2027.
-----------------------	---

ANNEX 3 — SUB-PROCESSORS

The current list of Sub-processors, including large language model providers, is available at <https://associationanalytics.com/subprocessors.html>. Changes are notified in accordance with Section 6.2.

ANNEX 4 — DEMOGRAPHIC DATA

This Annex sets out how Demographic Data is Processed: the standard demographics Processed for every Subscriber, and the categories Processed only where Subscriber elects them. It is the whole of Company's permission to Process Demographic Data.

A4.1 What this Annex covers. "Demographic Data" means two groups of data, taken only from the source-system fields that the Parties confirm in writing during implementation. (a) Standard demographics, Processed for every Subscriber whose source systems hold them: birth year, which is the source of age, age band and generation, and gender. (b) Elected categories, Processed only where Subscriber elects them: race/ethnicity, which is special category data under the GDPR; exact date of birth; and a mission-aligned category under Section A4.3. No other category is covered by this Annex. In particular, the categories that Company's demographic data policy excludes, such as sexual orientation, disability, religion and health, are not Processed, except as a mission-aligned category or under a written addendum under Section 2.3.

A4.2 Elections. Subscriber elects each elected category separately, on the Order Form or later by written notice, including by email to Company's designated contact. Each election is Subscriber's documented instruction under Section 3.2 to Process that category as this Annex describes. No additional charge applies. Company will not Process an elected category that Subscriber has not elected, except to delete it under Section A4.9, and will stop ingesting such a category within thirty (30) days of the Order Form's effective date.

A4.3 Mission-aligned category. Where a category that Company's demographic data policy otherwise excludes defines Subscriber's membership eligibility or core mission (for example, veteran or military status for an association of military officers), Subscriber may name that one category on the Order Form. It is Processed only once Company has approved it in writing, only for Subscriber, and never in any benchmark or other output that combines data from more than one subscriber. A category that is merely relevant to some members does not qualify.

A4.4 Fixed categories. Company classifies race/ethnicity into the seven minimum categories of the US Office of Management and Budget Statistical Policy Directive No. 15 (2024 revision), and gender into self-reported gender identity (male, female, nonbinary, another gender). A "prefer not to answer" response is recorded so that non-response can be counted, and a value that matches no category is not classified. Where the Platform classifies at ingestion for Subscriber's source system, Subscriber's own labels are not stored in the Platform; otherwise they are retained in the Platform's raw data layer and are not displayed. Birth year is derived from Subscriber's date of birth field and the day and month are not retained unless Subscriber elects exact date of birth.

A4.5 Subscriber's account only. Demographic Data is Processed and displayed only within Subscriber's own tenant, subject to the controls in Annex 2. Company will not include it in any benchmark or other output that combines data from more than one subscriber, or in Aggregated De-identified Data, and will not use it for any purpose of its own.

A4.6 Small groups hidden. Company's summary displays of race/ethnicity and gender hide every category containing fewer than eleven (11) individuals and combine the hidden categories into a single visible group, so that a hidden count cannot be worked out by subtraction. This does not restrict Subscriber's Authorized Users from viewing member records they are otherwise permitted to see.

A4.7 AI Features. Where Subscriber has enabled AI Features, Demographic Data may be Processed by them under Section 7. The masking in Annex 2 applies to identifying fields, such as names and contact details, and not to Demographic Data values. AI Features are instructed to report Demographic Data in aggregate. Company does not warrant that an AI Feature will never return Demographic Data for an individual member.

A4.8 Subscriber's responsibilities. Subscriber confirms that it has a lawful basis for this Processing and has given any notices and obtained any consents that Data Protection Law requires. That includes, for special category data relating to Data Subjects subject to the GDPR or the UK GDPR, a condition under Article 9(2) of the GDPR or its UK equivalent, and any consent that US state law requires for sensitive data. Subscriber confirms that Demographic Data was provided voluntarily by the Data Subjects, and was not inferred or assigned by Subscriber. Subscriber will tell Company in writing before it repurposes, renames or adds a source field that holds Demographic Data. Subscriber will use Demographic Data for analysis of its membership in aggregate, not to make decisions about individual Data Subjects. Section 2.2 applies.

A4.9 Data received before an election. Where Company received data in an elected category before the Order Form took effect, Company will disclose it to Subscriber. A category that Subscriber elects is Processed under this Annex from the Order Form's effective date. A category that Subscriber does not elect is deleted from Company's production systems within thirty (30) days of that date.

A4.10 Changing your mind. Subscriber may withdraw an election at any time by written notice, including by email to Company's designated contact. Within ten (10) business days Company will stop ingesting that category. Within thirty (30) days of the notice it will delete that category from its production systems. Backup copies are deleted under Section 12.3.

A4.11 Safeguards first. Company will not make an elected category visible to Subscriber's Authorized Users until the Platform supports it with the safeguards in this Annex, and will tell Subscriber when it is available.