

Last Updated: May 11, 2025

Data Processing Addendum

1. IMPORTANT TERMS.

This AthenaAIService Data Processing Addendum (the “DPA”) governs Interwave’s processing of DPA Data that is required to provide the Service under the Platform Agreement or other agreement between You and Interwave pertaining to the use of Interwave’s software-as-a-service offering (the “Agreement”). This DPA is part of Your Terms with Interwave. In the event of any conflicting language between the Agreement, the other Terms, or any operative Order Form, the terms of this DPA control.

You and Interwave each agree to comply with their respective obligations under Data Protection Law.

Data Processing Roles

As between You and Interwave, You are the Data Controller, and Interwave is the Data Processor, processing DPA Data on Your behalf.

Data Processing Purposes

Interwave will process DPA Data as your Data Processor for the purpose of providing or maintaining the Service and in accordance with the Instructions. Interwave acknowledges that you are disclosing DPA Data for these limited and specific purposes.

Categories of Personal Data

Personal Data contained within Customer Data and Content. Examples include name, and demographic information.

Categories of Data Subjects

Individuals identified in Customer Data and Content. Examples include user of Interwave’s applications, user’s clients.

Duration of Processing

Subject to the Terms and Section 14 of this DPA, DPA Data will be processed for the term of the Agreement.

2. DEFINITIONS.

The definitions in Section 15 (Defined Terms) apply to this DPA. All terms in quotation marks in the body of this DPA are also defined terms. Capitalized terms not defined in this DPA have the meanings given to them in the Agreement.

3. PROCESSING REQUIREMENTS.

As a Data Processor, Interwave will:

3.1. process DPA Data on Your behalf, according to the Instructions, and only in a manner that is necessary for the performance of the Service. Specifically, Interwave agrees to process DPA Data: (i) for the purpose of providing, providing access to, servicing, and supporting Your use of the Service; and (ii) in compliance with the Instructions;

3.2. promptly notify You in writing if it cannot comply with the requirements of this DPA;

3.3. promptly inform You if, in Interwave's opinion, an instruction from You infringes applicable Data Protection Law; and

3.4. ensure that all persons authorized by Interwave to process DPA Data are subject to a duty of confidentiality.

4. SUBPROCESSORS.

Interwave will:

4.1. engage the organizations or persons listed at AthenaAIService.com (the "Subprocessor List") as necessary to perform the Service. You consent to Interwave's use of its existing Subprocessors and You grant Interwave a general written authorization to engage Subprocessors to perform all or part of the processing activities required to provide the Service. If You subscribe to receive email notifications at the Subprocessor List, then Interwave will notify You if Interwave intends to add one or more Subprocessors to the Subprocessor List at least 30 days before the change takes effect. You may, within fifteen (15) days of receiving the notice of the change, reasonably object to Interwave's use of a Subprocessor on reasonable grounds relating to the protection of DPA Data (the "Objection") by following the instructions set forth in the Subprocessor List or by contacting privacy@AthenaAIService.com (the "Objection Notice"). In such case, Interwave shall have the right to cure the Objection through one of the following options: (i) Interwave will offer an alternative to provide its Service without such Subprocessor; (ii) Interwave will take the corrective steps requested by You in the Objection Notice and proceed to use the Subprocessor; (iii) Interwave may cease to provide, or You may agree not to use, whether temporarily or permanently, the particular aspect or feature of the Service that would involve the use of such Subprocessor; or (iv) You may cease providing DPA Data to Interwave for processing. If none of the above options are commercially feasible, in Interwave's reasonable judgment, and the Objection has not been resolved to the satisfaction of the parties within thirty (30) days of Interwave's receipt of the Objection Notice, then either party may terminate any subscriptions, order forms or usage regarding the Service for cause and in such case, You will be refunded any prepaid but unused fees for the applicable subscriptions, order forms or usage to the extent they cover periods or terms following the date of such termination. Other than accepting such cure as may be offered by Interwave, such termination right is Your sole and exclusive remedy if You object to any new Subprocessor;

4.2. enter into contractual arrangements with each Subprocessor binding them to provide the same level of data protection and information security to that provided for in this DPA. Interwave will remain fully liable to You for the performance of each Subprocessor to the extent the Subprocessor fails to fulfill its data protection obligations under the applicable data processing agreement with Interwave.

5. NOTICE TO CUSTOMER.

Interwave will inform You, to the extent legally permitted, if Interwave receives:

5.1. any legally binding request for disclosure of DPA Data by a law enforcement authority. If Interwave is legally prohibited from notifying You, Interwave will use its best efforts to request a waiver of the prohibition and will document that request. Interwave will notify You once the prohibition expires or has been lifted with the aim of providing as much relevant information to You as reasonably possible;

5.2. any notice, inquiry, or investigation by a Supervisory Authority with respect to DPA Data; or

5.3. any complaint or request from a Data Subject (including “verifiable consumer requests” as defined by CCPA) exercising their right under Data Protection Law to (i) access their DPA Data; (ii) have their DPA Data corrected or erased; (iii) restrict or object to the Processing of their DPA Data; or (iv) data portability (collectively “Data Subject Request”). Other than to request further information or identify the Data Subject, Interwave will not respond to any Data Subject Request without prior written authorization from You.

6. PERSONAL DATA BREACH.

If Interwave experiences any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to DPA Data (“Personal Data Breach”), Interwave will notify you in accordance with the timeframe set out under the heading “Incident Detection and Response” in the Security Addendum which is incorporated into this DPA. Interwave will provide you with all information about the Personal Data Breach as required by Data Protection Law including the information outlined under the heading “Incident Detection and Response” in the Security Addendum.

7. ASSISTANCE TO CUSTOMER AND AUDITS.

Upon Your written request, Interwave will provide reasonable assistance to You regarding:

7.1. Your obligations to respond to Data Subject Request relating to Interwave’s Processing of DPA Data;

7.2. Your preparation of data protection impact assessments with respect to the processing of DPA Data by Interwave and, where necessary, carrying out consultations with any Supervisory Authority with jurisdiction over the Processing; and

7.3. information, assessments or audits, to the extent required by Data Protection Law, and as necessary to confirm that Interwave is processing Personal Data in a manner consistent with this DPA. All audits and assessments will be performed in the manner set out under the heading “Customer Audit Rights” in the Security Addendum. All reports and documentation provided to You are Interwave’s Confidential Information.

8. REQUIRED PROCESSING.

If Interwave is required by applicable law to Process DPA Data outside of Your Instructions, Interwave will inform you of this requirement in advance of any processing, unless Interwave reasonably believes it is legally prohibited from informing you of such processing.

9. SECURITY.

Interwave will:

9.1. implement and maintain a written information security program with the data security measures set out in the Security Addendum to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of DPA Data and to protect the rights of the Data Subject; and

9.2. take appropriate steps to confirm that all Interwave personnel and persons or entities authorized to Process DPA Data are protecting the security, privacy and confidentiality of DPA Data consistent with the requirements of this DPA.

10. US SPECIFIC DATA PROTECTION OBLIGATIONS.

To the extent applicable under US State Privacy Law, Interwave certifies that it understands and will comply with its obligations under US State Privacy Law to:

10.1. only process DPA Data for the purposes set out in this DPA, the Agreement, and unless otherwise permitted by law;

10.2. not “sell” or “share” (as defined by CCPA) DPA Data;

10.3. not retain, use or disclose DPA Data outside of the direct business relationship between Interwave and Customer unless otherwise required or permitted by law;

10.4. Process DPA Data in a manner that provides no less than the level of privacy protection required by US State Privacy Law;

10.5. not combine any DPA Data with Personal Data that Interwave receives from or on behalf of a third party other than You or collects from Interwave’s own interactions with individuals, provided that Interwave may combine Personal Data as permitted under US State Privacy Laws, or if directed to do so by Customer;

10.6. not attempt to reidentify any deidentified data You provide to Interwave, except for the sole purpose of determining whether the deidentification processes are compliant with applicable Data Protection Law; and

10.7. grant You the right to (i) take reasonable and appropriate steps to ensure that Interwave uses DPA Data in a manner consistent with Data Protection Law; and (ii) stop and remediate unauthorized use of DPA Data.

11. OBLIGATIONS OF CUSTOMER.

11.1. You represent, warrant and covenant that You have and shall maintain throughout the term all necessary rights, consents and authorizations to provide the DPA Data to Interwave and to authorize Interwave to Process DPA Data as contemplated by this DPA, the Agreement, the Terms and/or other Instructions provided to Interwave. By using the Service, you are instructing Interwave to process DPA Data as reflected in the Documentation.

11.2. You shall reasonably cooperate with Interwave to assist Interwave in performing any of its obligations under Data Protection Law in relation to DPA Data.

11.3. You acknowledge and agree that You, rather than Interwave, are responsible for certain configurations and design decisions for the Services and that You are responsible for implementing those configurations and design decisions in a secure manner that complies with applicable Data Protection

Law. Without limitation to the above, You represent, warrant and covenant that You shall only transfer DPA Data to Interwave using secure, reasonable and appropriate mechanisms.

11.4. You shall not provide DPA Data to Interwave except through agreed mechanisms. For example, You shall not include DPA Data, in technical support tickets or transmit DPA Data to Interwave by email.

11.5. You shall not provide to Interwave any personally identifiable genetic, biometric or health data; or payment card industry data (such as credit card numbers).

12. CROSS-BORDER DATA TRANSFERS.

12.1. You acknowledge that You may transfer Personal Data to Interwave in the United States, in order for Interwave to provide the Service. If the transfer comprises DPA Data that requires a Data Transfer Mechanism, the Data Transfers Addendum, which is incorporated into this DPA, will apply.

13. FUTURE REGULATIONS.

13.1. In the event that new legislation and regulations are implemented that specifically govern the use of artificial intelligence solutions, both parties agree to review this DPA to ensure compliance with such legislation and regulations.

13.2. If substantial modifications are required to the terms and conditions of this DPA to render it or the Parties performance under it compliant with any regulations implemented following its Effective Date, both parties shall negotiate in good faith to make necessary amendments.

13.3. Should new regulations render the continued provision of services under this contract infeasible or unlawful, either party may initiate termination by providing written notice to the other party. Termination shall be effective after a reasonable notice period, as agreed upon by both parties.

13.4. The termination of this DPA due to the aforementioned regulations shall not relieve either party from any outstanding obligations or liabilities incurred prior to the termination.

13.5. If any provision of this DPA is found to be inconsistent with future regulations, such provision shall be interpreted in a manner consistent with the applicable laws, or if necessary, deemed null and void without affecting the validity of the remaining provisions.

14. RETENTION PERIOD.

This DPA shall remain in effect until (i) the Service is terminated and (ii) Interwave no longer processes DPA Data on Your behalf. Within 30 days following termination of the Service or upon your reasonable request, Interwave shall, and shall direct each Subprocessor to, return to you or delete the DPA Data, unless Interwave is required by law to retain DPA Data.

15. DEFINED TERMS

15.1. "Data Controller" means the person or entity that determines the purposes and means of Processing DPA Data, which may include, as applicable, equivalent concepts under Data Protection Law (for example, "Business" as defined by CCPA).

15.2. “Data Processor” means the person or entity that Processes DPA Data on behalf of the Data Controller, which may include, as applicable, equivalent concepts under Data Protection Law (for example, “Service Provider” as defined by CCPA).

15.3. “Data Protection Law” means applicable privacy and data protection law in connection with your use of the Service. Data Protection Law may include, depending on the circumstances, Cal. Civ. Code §§ 1798.100 et seq., as amended and its implementing regulations (“CCPA”) and the European Union General Data Protection Regulation (Regulation (EU) 2016/679) (“GDPR”).

15.4. “Data Subject” means an identified or identifiable natural person to which DPA Data relates and only to the extent their Personal Data is protected by Data Protection Law.

15.5. “Data Transfer Addendum” means the data transfer addendum located at [AthenaAIService.com](https://athenaaiservice.com)

15.6. “Data Transfer Mechanism” means a transfer mechanism that enables the lawful cross-border transfer of DPA Data under Data Protection Law. This includes transfer mechanisms that are required under Data Protection Law in the EEA, UK, and Switzerland such as the Data Privacy Framework, the EEA SCCs, the UK International Data Transfer Addendum and any data transfer mechanism available under Data Protection Law that is incorporated into this DPA.

15.7. “DPA Data” means Customer Data or Your Content that is provided through the Service and that is Personal Data.

15.8. “EEA” means the European Economic Area.

15.9. “EEA SCCs” means Module 2 (Controller to Processor) of the standard contractual clauses set out in the European Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries according to the GDPR.

15.10. “Instructions” means any (i) documented communication from You which includes actions taken or input provided through the Service; or (ii) agreement between You and Interwave that requires Interwave to provide the Service; or (iii) the Documentation.

15.11. “Personal Data” means any information relating to an identifiable natural person which is protected under Data Protection Law and Processed in connection with Your use of the Service. This includes equivalent concepts as defined by Data Protection Law (for example, “personal information” as defined under the CCPA).

15.12. “Platform Agreement” means the Platform Agreement located at [AthenaAIService.com](https://athenaaiservice.com).

15.13. “Processing” means any operation or set of operations which is performed on Your behalf on DPA Data, whether or not by automated means, such as collecting, recording, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination. “Process”, “Processes” and “Processed” will be interpreted accordingly.

15.14. “Security Addendum” means the Security Addendum located at [AthenaAIService.com](https://athenaaiservice.com)

15.15. “Subprocessor” means an entity Interwave engages to Process DPA Data on Interwave’s behalf, to carry out specific processing activities on Your behalf.

15.16. "Supervisory Authority" means an independent public authority which is (i) established by a member state pursuant to Article 51 of the GDPR; (ii) the public authority governing data protection that has supervisory jurisdiction over You.

15.17. "UK International Data Transfer Addendum" means the international data transfer addendum to the EEA SCCs issued by the United Kingdom's Information Commissioner's Office which came into force in accordance with s119A of the UK Data Protection Act on 21 March 2022.

15.18. "You" means the organization contracting for the use of the Service.

15.19. "US State Privacy Law" means all state laws relating to the protection and processing of Personal Data in effect in the United States of America, which may include, without limitation, the CCPA, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.