

Last updated: December 10, 2024

Privacy Policy

Interwave Corporation (“Interwave”, “we”, “us”, “our”) respects your right to privacy, and we are dedicated to securing and protecting any information we have about you. This Privacy Policy describes the ways we collect, use, and share information that relates to an identifiable individual (“Personal Data”) and also how you can exercise your rights under applicable privacy and data protection laws.

If you have any questions or concerns about our use of your Personal Data, or if you wish to exercise any of your privacy rights including the right to object (where applicable), then please contact us using the contact details under ‘How to Contact us’ at section 12 below.

AthenaAIService is a secure AI platform, available as a software-as-a-service (“SaaS”) offering that augments productivity and automates complex workflows for professionals including professionals in law, tax, and finance. Interwave is headquartered in the United States.

For jurisdiction specific provisions of this Privacy Policy see the ‘Jurisdiction Specific Provisions’ at section 8 below.

We recommend that you read this Privacy Policy in full to ensure you are completely informed about Interwave’s collection and use of your Personal Data.

1. Applicability Of This Privacy Policy

This Privacy Policy describes how Interwave processes Personal Data collected from you or about you through our website at AthenaAIService.com (our “Website”), the services we provide through our platform and applications (“Services”), and other interactions you have with Interwave.

Interwave’s Services are offered to businesses, companies and/or other entities for professional use (our “Customers”). We enter into customer agreements (for example, our platform agreement, pilot agreement, evaluation agreement, terms of service, data processing agreement etc.,) with our Customers. These agreements govern the delivery and use of the Services (the “Customer Agreement”). This Privacy Policy does not apply to any input or output generated on our online platform, or documents uploaded to our platform. We process this data on behalf of Customers and we call it (“Customer Data” and “Content”). Interwave’s use of Customer Data and Content received through the Services is governed by the relevant Customer Agreement. Interwave processes Customer Data and Content received through the Services as a Data Processor so any queries related to this data should be directed to our Customers who are the Data Controllers.

This Privacy Policy governs where Interwave is the data controller responsible for the processing of the Personal Data.

2. Personal Data We Collect And Process

In the course of doing business, providing our Services, and through our website we collect and receive Personal Data in different ways and from different sources. This Personal Data includes:

- *Information that you provide directly*

We collect Personal Data directly from you when you create an account with us, otherwise use the Services, or interact with us via some other means. The Personal Data we collect includes:

a) Account Information: When you or your employer creates an account with us, we collect certain information associated with your account, including your name, email address, and information about your profession and professional experience, language preferences, account credentials, payment information, and transaction history (collectively, "Account Information").

b) Communication Information: If you communicate with us, (for example when you contact us about our Services, when you complete a survey, when you interact with our website and help center, or when you request support) we collect your name, email address, information about your profession, customer survey responses, the way you interact with our communication and Services, and the contents of any messages you send (collectively "Communication Information").

c) Social Media Information: We have pages on social media sites like X, YouTube, and LinkedIn. When you interact with our social media pages, we collect Personal Data that you choose to provide to us, such as your contact details and the contents of your messages or posts. In addition, third parties may provide us with aggregate information and analytics about our social media activity (collectively, "Social Media Information").

- *Information that we collect automatically*

We collect your personal data indirectly, including through automated means from your computer or device. This information includes:

a) Log Data: Information that your browser or device automatically sends when you use our Services or access our website. Log data includes your Internet Protocol Address ("IP Address"), browser information, the date and time of your request, and how you otherwise use certain features or interact with us (collectively "Log Data").

b) Service usage data: When you interact with the Services, metadata is generated that provides additional context about your use of the Services. This includes your email address, data about how often you visit the website, how you interact with the Services, the amount of time spent engaging with the Services, the volume of queries you submit, the type of queries you submit, and the features interacted with (collectively "Usage Data").

c) Cookies and Similar Technologies: We use cookies, scripts, or similar technologies (collectively "Cookies and Similar Technologies") to manage the Services and to collect information about you and your use of the Services. A cookie is a small string of information that websites you visit transfer to your computer for identification purposes. These technologies help us to recognize you, customize or personalize your experience, market additional products or services to you, understand your preferences, improve your website experience, and analyse the use of our Services to make them safer and more useful to you. For more details about how we use these Cookies and Similar Technologies, your opt-out controls, and other options please visit our Cookie Policy available at AthenaAIService.com.

d) Device Information: We also collect certain device and connection-specific information when you install, access, or use our Services. This includes information such as the name of the device, operating system, device identifiers, and browser you are using (collectively “Device Information”). The specific Device Information collected will depend on the type of device you use and its settings.

- *Information we collect from third parties*

We also receive certain information about you from our trusted partners, such as:

- a) security partners to protect against fraud, abuse, and other security threats;
- b) marketing vendors who provide us with information about potential customers of our services;
- c) advertising vendors; and
- d) event organizers (for example, trade shows, professional events, conferences, and seminars we attend) who may provide us with information about event attendees.

((a), (b), (c), and (d) collectively “Information Collected From Third Parties”).

- *Information that is publicly available*

We collect publicly available information about customers and prospects to help offer and provide our Services.

We use publicly available information (for example, judgments, decisions, public filings, etc.,) to develop, train, and improve our AI platform (“Publicly Available Information”).

For more information on the sources of information used to train, maintain, and develop our AI platform and the steps we take to minimize the privacy impact on individuals, please see AthenaAIService.com for more details.

3. How We Use Personal Data

We may use Personal Data covered by this Privacy Policy for the following purposes:

- **to provide and maintain our Services;**
- **to develop, improve, and update our Services and new functionality;**
- **to carry out and conduct research;**
- **to personalize your use of our Services, applications, or platforms;**
- **to provide customer support and resolve bugs, issues, or customer queries;**
- **to communicate with you, including to send you information or marketing about our services and events;**
- **to assess your eligibility for, and offer you or promote our services. Where allowed by law (including, where required, with your opt-in consent), we use and share your Personal Data with others so that we may market our services to you, including through interest-based advertising;**

- **to prevent fraud, criminal activity, or misuses of our Services, and to protect the security of our systems and Services; and**
- **to comply with legal obligations and to protect the rights, privacy, safety, or property of our users, us, our affiliates, or any third party.**

We may aggregate or de-identify Personal Data so that You can no longer be identified and use the aggregated or de-identified data for the following purposes:

- **to investigate and study the effectiveness of our services;**
- **to update and improve our services;**
- **to conduct research; and**
- **to share or publish aggregated information about usage of our services, for example on our blog or on social media (e.g. LinkedIn).**

Please note that we do not attempt to reidentify this information unless required by law.

Details of the purposes for which we process Personal Data as a controller, and the legal bases we rely on for such processing in the European Economic Area and the United Kingdom, are set out in the 'Jurisdiction Specific Provision' under the legal basis table.

4. Who we Share Your Personal Data With

We share your personal data with the following categories of recipients:

- **Our Affiliates: We will share Personal Data that we collect, such as Account Information with any corporate affiliates. The information shared may be used for the purposes described in this Privacy Policy and generally to operate our business, including, processing for fraud prevention, payment processing, customer support, business development, user account administration, and IT, technical, and engineering support.**
- **Trusted Partners and Service Providers: We may engage third-party companies or individuals as service providers to help us operate and support our business. These third parties may support Interwave in respect of a variety of business purposes including website and data hosting, research, auditing, marketing, customer support, and data processing. These third parties have limited access to your information, may use your information only to perform agreed tasks, and are prohibited from disclosing or using your information for other purposes. The types of third-party service providers that we work with include:**
 - a) Linked Third-Party Websites or Plug-Ins when you use third party applications, such as Microsoft and choose to connect your Interwave account with such external third-party applications. If you choose to connect your account to a third-party application, the providers of those services or products may receive information about you that Interwave, you, or others share with them. Please be aware that when you use third-party sites or services, their own terms and privacy policies will govern your use of those sites or services.**
 - b) Vendors and Service Providers. To assist us with our business operations and to perform certain services and functions including providers of hosting services, email providers, sales support, customer support, authentication providers, financial services providers,**

communication providers, content delivery services, data warehouse services, and other information technology services providers. For more details please see Interwave's Service Provider page.

c) Business Reorganization: In some cases, we may choose to reorganize our business (such as via a sale, merger, liquidation, receivership, or transfer of all or substantially all of Interwave's assets). Your Personal Data may be disclosed in the diligence process with counterparties and others assisting with the transaction and transferred to a successor or affiliate as part of that transaction. If Interwave intends to transfer information about you, we will notify you.

d) Professional Advisors, Industry Partners, Authorities, Regulators, and other Entities: We may share your Personal Data with our advisors, accountants, consultants, regulators and tax authorities, law enforcement, government agencies, civil litigants, and other entities as reasonably necessary to:

- comply with applicable law or regulations, court orders, subpoenas, legal process, or government requests;
- detect, investigate, prevent, or address actual or suspected fraud, violations of Interwave's Terms, and other illegal activity or security and technical issues; or
- protect the rights, property and safety of our Customers, Interwave, or others, including to prevent harm or loss.

5. How We Keep Your Personal Data Secure

The security of your information is important to us. We protect your Personal Data through technical and organizational measures designed to mitigate the risk of unlawful or unauthorized access, destruction, loss, alteration, disclosure, or use of your Personal Data. The measures are designed to provide a level of security appropriate to the risk of processing.

6. International Data Transfers

In some cases, we may transfer your Personal Data to countries other than the country in which the Personal Data originates. These countries may have data protection laws that are different to the laws of your country.

When you access our website, or use our Services, your Personal Data may be transferred to our servers located in the US, or to other countries outside of the European Economic Area ("EEA"), Switzerland, and the United Kingdom ("UK"). This may be a direct provision of your Personal Data to us, or a transfer that we or a third party makes. Where Personal Data described in the 'Personal Data We Collect and Process' section is transferred outside of the EEA, Switzerland, or the UK, we ensure it benefits from an adequate level of data protection by relying on:

- ***Adequacy Decisions:***

These are decisions from the European Commission under Article 45 GDPR (or equivalent decisions under other laws) where they recognise that a country outside of the EEA offers an adequate level of data protection. We transfer your Personal Data as described in 'Personal Data We Collect and Process' to the United States under the Data Privacy Framework and other countries with adequacy decisions.

- **Standard Contractual Clauses:**

For jurisdictions which are not deemed adequate, we rely on other lawful transfer mechanisms ('appropriate safeguards') like the Standard Contractual Clauses as issued on 4 June 2021, under Article 46(2) GDPR, Article 46(2) of the UK equivalent GDPR, and the revised Federal Act on Data Protection for the transfer of personal data originating in Switzerland.

We ensure the above-mentioned mechanisms are in place with our group companies and third-party service providers. For more information on the legal mechanisms, we rely on in respect of either data sharing arrangement please reach out to us by email at privacy@AthenaAIService.com.

- **Derogation or Exceptions:**

In limited circumstances, we may rely on an exception, or 'derogation' (under Article 49 GDPR), to transfer your Personal Data to such country despite the absence of an 'adequacy decision' or 'appropriate safeguards' – e.g. reliance on your explicit consent to that transfer or because it is necessary for the establishment, exercise or defence of legal claims (including regulatory, administrative or any out-of-court procedure, and seeking advice).

- **Data Privacy Framework:**

We comply with the EU-U.S. Data Privacy Framework ("EU-U.S. DPF") and the UK Extension to the EU-U.S. DPF ("UK Extension"), and the Swiss-U.S. Data Privacy Data Privacy Framework ("Swiss-U.S. DPF") as set forth by the U.S. Department of Commerce. Interwave has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles ("EU-U.S. DPF Principles") with regards to the processing of personal data received from the European Union ("EU") and UK in reliance on the EU-U.S. DPF and the UK Extension. We have similarly certified to the U.S. Department of Commerce that we adhere to the Swiss-U.S. Data Privacy Framework Principles ("Swiss-U.S. DPF Principles") with regards to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this Privacy Policy and the EU-U.S. DPF Principles, the UK Extension, or the Swiss-U.S. DPF Principles, the principles shall govern. To learn more about the EU – U.S. DPF, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

Commitment to Cooperate. In compliance with the EU-U.S. DPF, the UK Extension, and the Swiss-U.S. DPF, Interwave commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities ("DPAs") and the UK Information Commissioner's Office ("ICO") and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of Personal Data received in reliance on the EU-U.S. DPF, the UK Extension, and the Swiss-U.S. DPF.

Federal Trade Commission. The Federal Trade Commission has jurisdiction over Interwave's compliance with the EU-U.S. DPF, the UK Extension, and the Swiss-U.S. DPF.

Right to Arbitrate. You may, under certain conditions, invoke binding arbitration for complaints regarding Data Privacy Framework compliance.

Accountability for Onward Transfers. We take responsibility for the processing of personal information we receive and subsequently transfer to a third party. In the case of an onward transfer, Interwave

remains liable if such a third-party processes personal information in a way that is inconsistent with the Data Privacy Framework Principles, unless we can demonstrate that we were not responsible for the event that gave rise to the damage.

If you want to contact us with any inquiries or complaints regarding our reliance on the DPFs, you can email us at privacy@AthenaAIService.com.

7. Data Retention

We retain the Personal Data we collect from you for as long as necessary for the purposes described in this Privacy Policy. If you have a Customer Agreement with us, we will delete your data in accordance with your Customer Agreement.

How long we retain Personal Data will depend on a number of factors including:

- **the terms of your Customer Agreement;**
- **compliance with our (and to demonstrate compliance with) legal obligations, to resolve disputes, and to enforce our agreements; or**
- **in relation to Account Information, for our tax, accounting, and audit requirements.**

When we have no ongoing legitimate business need or legal reason to process your Personal Data, we will either delete or anonymise it or, if this is not possible (for example, because your personal data has been stored in backup archives), then we will securely store your Personal Data and isolate it from any further processing until deletion is possible.

8. Jurisdiction Specific Provisions

- EEA, UK, and Switzerland

We rely on several legal bases in accordance with applicable data protection laws, such as the General Data Protection Regulation (“GDPR”) or United Kingdom Data Protection Regulation (“UK GDPR”) to process Personal Data for the purposes set out in this Privacy Policy. These legal bases are as follows:

a) Contractual Necessity - where we need to engage in this processing as is necessary in order to conclude and perform a contract with you. For example, we require certain Personal Data in order to provide and support the Services we provide.

b) Legal obligation – where we must process and retain your Personal Data in order to comply with law or to fulfil certain legal obligations. For example, to retain and disclose certain information if there is a valid legal request from a regulator, law enforcement, or others.

c) Consent – in certain circumstances, we may ask for your consent before we collect, use, or disclose your Personal Data. In such circumstances you can voluntarily choose to give or deny your consent without any negative consequences being suffered by you. Where you opt to provide your consent, you can easily withdraw it at any given time.

d) Legitimate interests – where the processing is necessary for the legitimate interests of either Interwave or a third party, but only when we are confident that your privacy rights will remain appropriately protected. If we rely on our (or a third party's) legitimate interests, these interests will include:

- **operating, providing, and improving our business, including our online platform and services;**
- **improving our products and services, or use the insights to improve or develop marketing activities and promoting our products and services;**
- **personalizing our services to you;**
- **detecting or preventing illegal activities (for example, fraud), as well as, enforcing violations of our Customer Agreements or terms of service (collectively “Terms”) including misuse of our services, and other trust and safety protocols; and**
- **managing the security of our IT infrastructure, and the safety and security of our employees, customers, vendors, and visitors.**

Our legal bases for processing your Personal Data are detailed in the chart below:

For each legal basis above, we have described the purposes of our processing (why we process your information) and our processing operations (how we process your information to achieve each purpose) in the table below. We also list the categories of your information that we process for each purpose.

Contractual Necessity

1. To create and maintain your account and provide our services:

○ **Information Used:**

- Account Information
- Communication Information
- Log Data
- Usage Data
- Device Information
- Information Collected from Third Parties
- Communications, Browser Technologies
- Publicly Available Information

2. To send service communications:

○ **Information Used:**

- Account Information
- Communication Information

3. To provide customer support and resolve issues:

○ **Information Used:**

- Account Information
- Communication Information
- Usage Data
- Log Data

4. To conduct our loss mitigation activities:

○ **Information Used:**

- Account Information
- Communication Information

- Log Data
- Usage Data
- Device Information
- Information Collected from Third Parties
- Communications, Browser Technologies
- Publicly Available Information

Consent

5. Advertising:

- **Information Used:**
 - Social Media Information
 - Cookies and Similar Technologies
 - Device Information
 - Information Collected from Third Parties

Legitimate Interests

6. To improve and maintain the services:

- **Information Used:**
 - Account Information
 - Communication Information
 - Log Data
 - Usage Data
 - Device Information
 - Information Collected from Third Parties
 - Cookies and Similar Technologies
 - Publicly Available Information

7. Customer analytics and insights:

- **Information Used:**
 - Account Information
 - Communication Information
 - Log Data
 - Usage Data
 - Device Information
 - Information Collected from Third Parties
 - Cookies and Similar Technologies
 - Publicly Available Information

8. To ensure our services remain safe and secure:

- **Information Used:**
 - Account Information
 - Communication Information
 - Log Data
 - Usage Data
 - Device Information
 - Information Collected from Third Parties
 - Cookies and Similar Technologies
 - Publicly Available Information

9. To prevent and detect fraud:

- **Information Used:**
 - Account Information

- Communication Information
- Log Data
- Usage Data
- Publicly Available Information
- 10. **To protect our legal rights:**
 - **Information Used:**
 - Account Information
 - Communication Information
 - Log Data
 - Usage Data
 - Publicly Available Information
- 11. **To share information with law enforcement and respond to legal requests:**
 - **Information Used:**
 - Account Information
 - Communication Information
 - Log Data
 - Usage Data
 - Publicly Available Information
- 12. **In the event of a business reorganization:**
 - **Information Used:**
 - Account Information
 - Information Collected from Third Parties
- 13. **To administer other services, products and business relationships:**
 - **Information Used:**
 - Account Information
 - Social Media Information
 - Information Collected from Third Parties
 - Publicly Available Information
- 14. **To send you non-marketing communications:**
 - **Information Used:**
 - Account Information
 - Social Media Information
 - Information Collected from Third Parties
 - Publicly Available Information

- United States

If you are a consumer located in the United States (“US”), we process your Personal Data in accordance with US privacy laws, including the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (“CCPA”).

Additional information about (a) the categories of Personal Information we collect; (b) the source of the Personal Information; (c) the purposes of collection; and (d) how we disclose Personal Information is as follows:

1. Social Media Information

- **Sources of Personal Information:**
 - Collected when you interact with the company's Social Media Pages.
- **Purposes of Collection:**
 - To perform analytics.
 - To communicate with you.
- **Disclosure of Personal Information:**
 - May be disclosed to Affiliates and service providers.

2. Communication Information

(e.g., information collected when you communicate with or contact the company)

- **Sources of Personal Information:**
 - Collected directly from you.
- **Purposes of Collection:**
 - To provide services.
 - To respond to your communications.
- **Disclosure of Personal Information:**
 - Disclosed to Affiliates and service providers.

3. Support Information

- **Sources of Personal Information:**
 - Collected when you provide support information during your use of the services.
- **Purposes of Collection:**
 - To provide support.
 - To maintain services.
 - To respond to you.
- **Disclosure of Personal Information:**
 - May be disclosed to Affiliates and service providers.

Interwave does not sell or share personal data with third parties in exchange for payment. However, we may provide the personal data of individuals who visit our website to third party partners, such as advertising partners, analytics providers, and social networks, who assist us in advertising our products and services to you. This may be considered a data "sale" or "sharing" as those terms are defined under the CCPA and other applicable US privacy laws. To our knowledge, AthenaAIService does not sell personal information of minors under 18 years of age.

As a U.S. consumer and subject to certain limitations under U.S. privacy laws, you may have choices regarding our use and disclosure of your Personal Data. In addition to the rights outlined in section 10 below, other rights include:

1. Exercising the right to know: **You have a right to request additional information including the categories and purposes for which your Personal Data is collected and the third parties with whom your Person Data is disclosed to.**
2. Exercising the right to opt-out from a sale or sharing: **We do not sell or share your Personal Data in exchange for payment. As noted above, we may share the personal information of individuals who visit AthenaAIService.com for targeted advertising. Where legally required, we provide you with the option to opt out of targeted advertising on our site under “My Privacy Choices”.**

To submit a request to exercise any of the rights described above, please contact us using the method described in the ‘How to Contact Us’ section 12 below.

9. Minors Data

Our websites and services are not directed to anyone under the age of 18. Interwave does not knowingly collect Personal Data from anyone under the age of 18. If you have reason to believe that a minor under the age of 18 has provided Personal Data to Interwave through our Services, please email us at privacy@AthenaAIService.com and we will endeavor to delete that information from our systems.

10. Your Data Protection Rights

Individuals across the globe have certain statutory rights with respect to their Personal Data. Subject to certain exceptions and exemptions provided by law and where applicable, you may:

- Access, correct, update, or request deletion **of your Personal Data.**
- Object to processing **of your personal data, ask us to** restrict processing **of your Personal Data.**
- Request portability **of your personal data, (i.e. your data to be transferred in a readable and standardised format).**
- Opt-out of marketing communications **we send you at any time. You can exercise this right by clicking on the “unsubscribe” or “opt-out” link in the marketing emails we send you. To opt-out of other forms of marketing (such as postal marketing or telemarketing), please contact us using the contact details provided under the ‘How to Contact us’ heading below. If you choose to opt out of marketing communications, we will still send you non-promotional emails, such as emails about your account or our ongoing business relations.**
- Withdraw your consent **at any time, if we have collected and processed your Personal Data with your consent. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your Personal Data conducted in reliance on lawful processing grounds other than consent.**
- **Have the** right to complain to a supervisory authority. **For more information, please contact your local supervisory authority. Contact details for supervisory authorities in the EU are available [here](#) and for the UK [here](#).**

To exercise any of your rights you can contact us using the contact details provided under the 'How to Contact us' heading at section 12 below. We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws.

11. Updates to this Privacy Policy

We may update this Privacy Notice from time to time in response to changing legal, regulatory, technical or business developments. When we update our Privacy Notice, we will take appropriate measures to inform you, consistent with the significance of the changes we make.

You can see when this Privacy Notice was last updated by checking the "last updated" date displayed at the top of this Privacy Notice.

12. How to Contact us

If you have any questions or concerns about our use of your Personal Data, please contact our Data Protection Officer using the following details: privacy@AthenaAIService.com. You may also write to us at: Interwave LLC, 1309 Coffeen Avenue STE 1200, Sheridan, Wyoming 82801, USA