

AceRank™ Data Processing Addendum

Effective Date: September 23, 2026

Last Updated: September 23, 2026

This Data Processing Addendum (“**DPA**”) forms part of the Terms of Service, subscription agreement, order form, master services agreement, or other agreement governing the use of AceRank (collectively, the “**Agreement**”) between **Ace Reputations Inc.**, operator of AceRank (“**AceRank**,” “**we**,” “**us**,” or “**our**”), and the customer identified in the applicable Agreement (“**Customer**,” “**you**,” or “**your**”).

This DPA governs AceRank’s Processing of Customer Personal Data on behalf of Customer in connection with the AceRank platform and related services (the “**Services**”).

If there is a conflict between this DPA and the Agreement concerning the Processing of Customer Personal Data, this DPA controls to the extent of that conflict.

1. Definitions

For purposes of this DPA:

“**Applicable Data Protection Law**” means privacy and data-protection laws applicable to the Processing of Customer Personal Data under the Agreement, including, where applicable, the California Consumer Privacy Act as amended by the California Privacy Rights Act (“**CCPA**”), the EU General Data Protection Regulation (“**GDPR**”), the UK GDPR, and other applicable privacy and data-protection laws.

“**Controller**” means the entity that determines the purposes and means of Processing Personal Data.

“**Customer Data**” means information, content, prompts, queries, records, URLs, keywords, materials, and other data submitted, uploaded, provided, selected, or otherwise made available to AceRank by or on behalf of Customer through the Services.

“**Customer Personal Data**” means Personal Data contained within Customer Data that AceRank Processes on behalf of Customer in providing the Services.

“**Data Subject**” means an identified or identifiable individual to whom Personal Data relates.

“**Personal Data**” means information relating to an identified or identifiable individual, or information otherwise defined as personal information, personal data, or an equivalent term under Applicable Data Protection Law.

“**Process**,” “**Processed**,” or “**Processing**” means any operation performed on Personal Data, including collection, recording, organization, storage, alteration, retrieval, consultation, analysis, use, transmission, disclosure, combination, restriction, deletion, or destruction.

“Processor” means an entity that Processes Personal Data on behalf of a Controller.

“Security Incident” means a confirmed breach of security resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data Processed by AceRank.

“Subprocessor” means a third party engaged by AceRank to Process Customer Personal Data on behalf of Customer in connection with providing the Services.

2. Roles and Responsibilities

Where Customer determines the purposes and means of Processing Customer Personal Data, Customer acts as the Controller or Business and AceRank acts as the Processor, Service Provider, or Contractor, as those terms are defined under Applicable Data Protection Law.

Each party will comply with its respective obligations under Applicable Data Protection Law.

Customer is responsible for ensuring that:

- Customer has a lawful basis and all necessary rights to provide Customer Personal Data to AceRank;
- Customer's instructions to AceRank comply with applicable law;
- required privacy notices have been provided;
- required permissions or consents have been obtained; and
- Customer's use of the Services complies with applicable privacy and data-protection requirements.

AceRank will Process Customer Personal Data only as necessary to provide the Services, comply with Customer's documented instructions, perform its obligations under the Agreement, protect the Services, or comply with applicable law.

3. Details and Purpose of Processing

3.1 Subject Matter

AceRank provides technology for AI visibility monitoring, analytics, citation intelligence, sentiment analysis, competitor intelligence, keyword intelligence, public-web and online-discussion intelligence, reporting, and related functionality.

3.2 Nature of Processing

Processing may include:

- Collection
- Storage
- Organization
- Retrieval

- Analysis
- Transmission
- AI-assisted processing
- Search and information retrieval
- Visibility monitoring
- Citation analysis
- Sentiment analysis
- Keyword analysis
- Competitor analysis
- Public-web analysis
- Reporting
- Security monitoring
- Technical support
- Account administration

3.3 Purpose

AceRank Processes Customer Personal Data as reasonably necessary to provide, maintain, secure, support, and improve the functionality requested by Customer through the Services, subject to the Agreement and Applicable Data Protection Law.

3.4 Duration

Customer Personal Data may be Processed for the duration of the Agreement and thereafter for a reasonable period where necessary for deletion procedures, backup cycling, security, fraud prevention, dispute resolution, legal compliance, or other lawful purposes.

4. Categories of Data Subjects and Personal Data

Depending on Customer's use of the Services, Data Subjects may include:

- Customer personnel;
- authorized users;
- employees and contractors;
- business representatives;
- customers or prospects;
- founders or executives;
- individuals referenced in Customer-submitted materials; and
- individuals referenced in publicly available information selected for analysis.

Customer Personal Data may include:

- Names;
- professional contact information;
- business affiliations;
- job titles;
- public professional information;
- account information;

- URLs;
- public-profile information;
- prompts and queries;
- information submitted for analysis;
- publicly available online information; and
- other Personal Data Customer elects to submit.

AceRank is not designed for the routine Processing of highly sensitive Personal Data.

Customer should not submit payment-card credentials, account passwords, government identification numbers, protected health information, biometric identifiers, precise financial credentials, or other highly sensitive information unless specifically authorized and necessary for an agreed use of the Services.

5. Customer Instructions

Customer instructs AceRank to Process Customer Personal Data as reasonably necessary to:

1. provide and maintain the Services;
2. perform functionality requested by Customer and its authorized users;
3. produce analytics, intelligence, monitoring results, and reports;
4. maintain security and prevent fraud or abuse;
5. provide technical and customer support;
6. administer Customer's account; and
7. perform other Processing documented in the Agreement or subsequently agreed by the parties.

If AceRank reasonably believes that a Customer instruction violates Applicable Data Protection Law, AceRank may notify Customer unless prohibited by law and may suspend the affected Processing until the matter is resolved.

6. Confidentiality

AceRank will ensure that personnel authorized to Process Customer Personal Data are subject to appropriate confidentiality obligations.

Access to Customer Personal Data will be limited to personnel and authorized service providers that reasonably require access to perform their duties or provide the Services.

7. Security

AceRank will maintain appropriate technical and organizational safeguards designed to protect Customer Personal Data against unauthorized or unlawful Processing and accidental loss, destruction, alteration, or disclosure.

Depending upon the nature of the Services and Processing, safeguards may include:

- Encryption of information in transit;
- authentication controls;
- access restrictions;
- restricted administrative access;
- infrastructure and network protections;
- logging and monitoring;
- secure management of credentials and secrets;
- vulnerability and security-update management;
- backup and recovery procedures;
- vendor and service-provider controls; and
- incident-response procedures.

AceRank may update its security measures as technology, Services, and security risks evolve, provided that such changes do not materially reduce the overall protection required under Applicable Data Protection Law.

No electronic system can be guaranteed to be completely secure, and AceRank does not represent that security risks can be entirely eliminated.

8. Subprocessors

Customer provides AceRank with general authorization to engage third-party Subprocessors as reasonably necessary to provide, secure, maintain, and support the Services.

AceRank will require Subprocessors that Process Customer Personal Data on AceRank's behalf to be subject to appropriate data-protection obligations consistent with Applicable Data Protection Law and the nature of the Processing.

AceRank remains responsible for the performance of its obligations under this DPA notwithstanding its use of Subprocessors, subject to the Agreement and applicable law.

Where required by Applicable Data Protection Law, AceRank will provide Customer with information concerning relevant Subprocessors and reasonable notice of intended material additions or replacements, together with an opportunity to raise legally permitted objections.

AceRank may provide information regarding applicable Subprocessors to Customer upon reasonable written request, subject to appropriate confidentiality, security, and commercial restrictions.

9. Third-Party Technology and AI Processing

Customer acknowledges that AceRank may use authorized third-party technology providers, including artificial intelligence, search, data intelligence, infrastructure, communications, analytics, security, and other technology services, to provide functionality requested through the Services.

Where reasonably necessary to provide a requested feature, relevant Customer Data may be transmitted to an authorized provider for Processing.

AceRank will seek to limit information transmitted to such providers to information reasonably necessary to provide the relevant functionality.

Where a third-party provider Processes Customer Personal Data on AceRank's behalf, AceRank will treat that provider in accordance with applicable Subprocessor requirements.

AceRank does not control the independent algorithms, outputs, availability, or functionality of third-party AI platforms, search systems, websites, or external data sources.

10. Security Incidents

Upon becoming aware of a Security Incident involving Customer Personal Data, AceRank will notify Customer without undue delay to the extent required by Applicable Data Protection Law.

To the extent reasonably available and legally permitted, AceRank will provide information concerning:

- the nature of the Security Incident;
- the categories of information affected;
- the categories of Data Subjects affected;
- reasonably anticipated consequences;
- mitigation or remediation measures taken or proposed; and
- other information reasonably necessary for Customer to meet applicable legal obligations.

AceRank will take reasonable measures to contain, investigate, mitigate, and remediate a Security Incident.

Notification of a Security Incident does not constitute an admission of fault, wrongdoing, or liability.

11. Data Subject Requests

Taking into account the nature of the Processing, AceRank will provide reasonable assistance to Customer in responding to legally valid Data Subject requests where Customer cannot reasonably fulfill the request without AceRank's assistance.

Such requests may concern:

- Access
- Correction
- Deletion
- Portability
- Restriction
- Objection
- Applicable opt-out rights
- Other rights established by Applicable Data Protection Law

If AceRank receives a request directly from a Data Subject relating to Customer Personal Data Processed solely on Customer's behalf, AceRank may direct the Data Subject to Customer unless AceRank is legally required to respond directly.

Customer remains responsible for determining the validity of requests and the appropriate response.

12. Compliance Assistance

Taking into account the nature of Processing and information reasonably available to AceRank, AceRank will provide reasonable assistance where required by Applicable Data Protection Law concerning:

- Data Subject rights;
- security obligations;
- Security Incident response;
- data-protection impact assessments; and
- consultations with supervisory authorities.

Customer remains responsible for its own compliance determinations and obligations as Controller or Business.

13. Return and Deletion of Customer Personal Data

Upon termination or expiration of the Services, AceRank will delete or return Customer Personal Data as required by the Agreement and Applicable Data Protection Law, subject to applicable retention requirements.

Residual copies may temporarily remain in backups, archives, security logs, fraud-prevention systems, or disaster-recovery environments until deleted through ordinary retention cycles.

AceRank may retain information where required or permitted by applicable law, including for legal compliance, fraud prevention, security, dispute resolution, or the establishment, exercise, or defense of legal claims.

Customer Personal Data retained on Customer's behalf will remain subject to the applicable protections of this DPA for as long as such Processing continues.

14. Audits and Compliance Information

Upon reasonable written request and subject to appropriate confidentiality and security protections, AceRank will make available information reasonably necessary to demonstrate compliance with applicable Processor obligations under this DPA.

Where Applicable Data Protection Law provides Customer with an audit right, the parties will cooperate regarding a reasonable audit mechanism.

Audits must, to the extent permitted by applicable law:

- provide reasonable advance notice;
- occur during normal business hours;
- avoid unreasonable disruption to AceRank;
- protect AceRank's confidential information;
- protect information relating to other customers; and
- be limited to information relevant to Customer's applicable compliance requirements.

Where appropriate, AceRank may satisfy an audit or information request through relevant questionnaires, certifications, reports, assessments, or other compliance documentation.

15. California Privacy Requirements

To the extent AceRank Processes Personal Information on Customer's behalf as a Service Provider or Contractor within the meaning of applicable California privacy law, AceRank will:

- Process such Personal Information for the business purposes specified in the Agreement and this DPA;
- not sell or share such Personal Information except as permitted by Applicable Data Protection Law;
- not retain, use, or disclose such Personal Information outside the direct business relationship with Customer except as permitted by Applicable Data Protection Law;
- not combine Personal Information received from or on behalf of Customer with Personal Information obtained from another person or from AceRank's own interaction with a consumer except where permitted by Applicable Data Protection Law;
- provide the level of privacy protection required of applicable Service Providers or Contractors; and
- notify Customer if AceRank determines that it can no longer meet applicable obligations concerning such Processing.

Customer may take reasonable and appropriate steps, where permitted by applicable law, to help ensure that Customer Personal Data is used consistently with Customer's obligations under California privacy law.

16. International Data Transfers

Customer acknowledges that Customer Personal Data may be Processed in the United States and other jurisdictions where AceRank or its authorized service providers operate.

Where Applicable Data Protection Law requires an approved transfer mechanism for transfers of Customer Personal Data to a jurisdiction not recognized as providing adequate protection, the parties will implement an applicable lawful transfer mechanism as required.

Such mechanisms may include, where applicable:

- European Commission Standard Contractual Clauses;

- the applicable UK international data-transfer mechanism; or
- another transfer mechanism recognized under Applicable Data Protection Law.

Where required, applicable transfer provisions may be incorporated into or executed in connection with this DPA.

17. GDPR and UK GDPR Requirements

Where the GDPR or UK GDPR applies and Customer acts as Controller while AceRank acts as Processor, AceRank will, to the extent required by applicable law:

- Process Customer Personal Data only on documented instructions from Customer;
- ensure authorized personnel are subject to confidentiality obligations;
- implement appropriate technical and organizational measures;
- comply with applicable requirements concerning Subprocessors;
- reasonably assist Customer with Data Subject rights;
- reasonably assist Customer with security and breach obligations;
- provide information reasonably necessary to demonstrate compliance with applicable Processor obligations; and
- delete or return Customer Personal Data following termination, subject to applicable legal retention requirements.

Nothing in this DPA requires either party to take an action prohibited by applicable law.

18. Independent Processing by AceRank

This DPA applies to Customer Personal Data that AceRank Processes **on behalf of Customer**.

AceRank may separately act as an independent Controller or Business with respect to Personal Data Processed for AceRank's own lawful purposes, such as:

- Account administration
- Subscription administration
- Billing administration
- Direct communications with Customer
- Security
- Fraud and abuse prevention
- Legal and regulatory compliance
- Establishment, exercise, or defense of legal claims

Such Processing is governed by AceRank's Privacy Policy and Applicable Data Protection Law rather than the Processor provisions of this DPA.

19. Customer Responsibilities

Customer is responsible for:

- determining whether the Services are appropriate for Customer's intended Processing;
- configuring and using the Services appropriately;
- limiting Customer Personal Data submitted to information reasonably necessary for Customer's intended use;
- maintaining appropriate security for Customer-controlled accounts and credentials;
- managing its authorized users;
- complying with Applicable Data Protection Law; and
- responding to Data Subjects where Customer is responsible for such responses.

Customer will not instruct AceRank to Process Customer Personal Data in violation of applicable law.

20. Liability

Each party's liability arising from or relating to this DPA is subject to the exclusions and limitations of liability contained in the Agreement, except to the extent such exclusions or limitations are prohibited by Applicable Data Protection Law.

21. Order of Precedence

If there is a conflict concerning the Processing of Customer Personal Data, the following order of precedence applies:

1. mandatory provisions of Applicable Data Protection Law and any applicable incorporated international-transfer terms;
2. this DPA; and
3. the Agreement.

22. Changes to this DPA

AceRank may update this DPA where reasonably necessary to reflect changes in applicable law, regulatory requirements, security requirements, Services, or Processing practices.

AceRank will not materially reduce the data-protection commitments applicable to Customer Personal Data during an active paid subscription where prohibited by applicable law.

Where legally required, AceRank will provide notice of material changes.

23. Term and Termination

This DPA becomes effective when incorporated into an Agreement between Customer and AceRank and remains effective for as long as AceRank Processes Customer Personal Data subject to this DPA.

Provisions that by their nature must survive termination will remain effective for as long as necessary to protect Customer Personal Data or satisfy applicable legal obligations.

24. Governing Terms

Except where Applicable Data Protection Law requires otherwise, this DPA is governed by the governing-law and dispute-resolution provisions of the Agreement.

Nothing in this DPA limits rights or obligations that cannot lawfully be limited or waived.

25. Contact Information

Questions concerning this DPA or AceRank's Processing of Customer Personal Data may be directed to:

Ace Reputations Inc.
Operator of AceRank
San Jose, California, United States

Privacy Contact:
legal@acereputations.com