Valutare

CUSTOMER TERMS

Valutare Customer Terms — Key Terms

Version 1.0 · Effective December 15, 2026 **Web** valutare.ai/legal/customer-terms/key-terms

Preview. These terms take effect December 15, 2026 and may be updated before then.

These Key Terms are part of the Valutare Customer Terms published at valutare.ai/legal/customer-terms. Customer signs a one-page Order Form (Part 1) that incorporates the Customer Terms.

How the documents fit together. The Agreement between Valutare, Inc. ("Provider") and Customer consists of:

1. the signed **Order Form** (Part 1);
2. these **Key Terms** (Parts 2 to 6);
3. the **Product-Specific Terms**, the **US Privacy Addendum**, the **Service Level Agreement Cover Page**, the **Security Exhibit** and the **Acceptable Use Policy**, each in the version listed on the Customer Terms page on the Order Date; and
4. the Common Paper standard terms, each as published at the URL shown and used under CC BY 4.0, © Common Paper, Inc.: **Cloud Service Agreement Standard Terms Version 2.1** (https://commonpaper.com/standards/cloud-service-agreement/2.1/) ("CSA"); **AI Addendum Standard Terms Version 1.0** (https://commonpaper.com/standards/ai-addendum/1.0/); **Service Level Agreement Standard Terms Version 2.0** (https://commonpaper.com/standards/service-level-agreement/2.0/) ("SLA"); and **Data Processing Agreement Version 1.1** (https://commonpaper.com/standards/data-processing-agreement/1.1/) ("DPA").

For purposes of the Common Paper standard terms, the Order Form and these Key Terms together are the "Order Form" and the "Cover Page".

Part 2 — Key terms (CSA v2.1)

Term	Value
Governing Law	The laws of the State of Delaware
Chosen Courts	The state and federal courts located in New Castle County, Delaware

Term	Value
General Cap Amount	The fees paid or payable by Customer under the Order Form in the 12 months before the event giving rise to the claim
Increased Cap Amount	2 times the General Cap Amount
Increased Claims	Breach of confidentiality, the DPA, the US Privacy Addendum or the Security Exhibit, and each party's indemnification obligations
Unlimited Claims	A party's fraud, gross negligence or willful misconduct
Provider Covered Claims	Third-party claims that the Cloud Service, as provided by Provider and used in accordance with the Agreement, infringes or misappropriates a third party's intellectual property rights. Provider Covered Claims do not include claims arising from Output, Customer Content, or combinations with items Provider did not provide
Customer Covered Claims	Third-party claims, and fines and penalties imposed by a governmental authority, arising from: (a) Customer Content, including Customer Content that infringes a third party's rights or was provided in violation of law; (b) Customer's or its Users' use of the Cloud Service in breach of the Agreement or the Acceptable Use Policy; (c) any employment decision or employment practice of Customer, including any decision in which Customer used the Cloud Service or Output, and including any claim that Provider acted as Customer's agent or employment agency in connection with it; (d) Customer's failure to comply with laws applicable to it as an employer, including employment, anti-discrimination, equal-pay, privacy, electronic-monitoring and AI Employment Laws; and (e) Customer's breach of Product-Specific Terms § 2.3 or § 3.
Prohibited Data	Customer may submit: leave records (type and dates) and voluntary self-identification data (for example race, ethnicity, gender, disability or veteran status), each only where Customer enables the feature that uses it; compensation data; and, for workplace accounts Users connect, access credentials and the metadata described in Product-Specific Terms § 4.5. Except for the items still prohibited below, Customer may submit the categories under CSA § 13.27(d)–(e) that the Cloud Service is designed to process. The wellbeing feature in Product-Specific Terms § 6 is not a High Risk Activity under CSA § 2.1(a)(viii). **Still prohibited:** government identification numbers, bank and payment-card account numbers, protected health information under HIPAA, and personal data of children under 16

Part 3 — Additional terms

CSA v2.1 has no fields for these subjects, so they are stated here.

3.1 **Security.** Provider will maintain the measures in the Security Exhibit throughout the Subscription Period and will not materially reduce the overall protection they provide.

3.2 **Acceptable use.** Customer will use, and will require its Users to use, the Cloud Service in compliance with the Acceptable Use Policy.

3.3 **Publicity.** Notwithstanding CSA § 12.8, Provider may identify Customer by name and logo in lists of its customers on its website and in sales and marketing materials, following any trademark guidelines Customer provides. Customer may withdraw this permission at any time by written notice (email is sufficient), and Provider will stop new uses and remove Customer from its website within 30

days. Any other public reference to Customer, including a press release, case study, testimonial or quote, requires Customer's prior written approval of the specific content. Customer may not use Provider's name or logo without Provider's prior written consent.

3.4 **No training; Usage Data.** Notwithstanding CSA § 1.6 and the AI Addendum, Provider will not use Customer Content, Customer Personal Data or data received through integrations, including in aggregated or de-identified form, to train, fine-tune or evaluate any AI model, whether Provider's or a third party's, except the screening and testing of Output for safety and bias in Customer's own Cloud Service described in Product-Specific Terms § 9.1. Usage Data (CSA §§ 1.4, 13.32) excludes Personal Data and Customer Content, and Provider will not use it to identify Customer publicly without Customer's consent.

3.5 **AI Services.** Customer's administrators can turn AI Services off for all of Customer's Users at any time in the Cloud Service's settings, and each User can turn them off for that User (Product-Specific Terms § 9.6). Translation between languages continues and uses an AI service. New AI Services that Provider adds during the Subscription Period are off for Customer until Customer turns them on. Provider will give 30 days' notice before replacing the primary AI model provider used for pay-recommendation or review-summary features; temporary automatic failover between Approved Subprocessors during an outage, and changes needed for security or availability, are not a replacement.

3.6 **Subprocessor objection.** If Customer reasonably objects to a new Subprocessor under DPA § 2.6 and the parties cannot resolve the objection within 30 days, Customer may terminate the affected part of the Cloud Service and receive a prorated refund of prepaid fees for it.

3.7 **Order of precedence.** Notwithstanding CSA § 3.1 and DPA § 9.1, if documents conflict, this order applies: (1) the Order Form, including its special terms; (2) these Key Terms; (3) for Personal Information, the US Privacy Addendum; (4) the Product-Specific Terms; (5) the Service Level Agreement Cover Page, the Security Exhibit and the Acceptable Use Policy; and (6) the Common Paper standard terms, in the order they set. Product-Specific Terms § 8 governs return and deletion of data notwithstanding DPA § 7.2 and CSA § 5.5.

3.8 **Definitions.** "Personal Information" means Customer Personal Data that is "personal information" under US Privacy Laws (as defined in the US Privacy Addendum). "Customer Personal Data" includes Personal Data that the Cloud Service collects from connected workplace accounts or generates about Users, not only data Customer uploads. "Security Incident" has the meaning in Part 5 wherever used in the Agreement. "Security Policy" means the Security Exhibit. "AI Employment Laws" has the meaning in Product-Specific Terms § 2.1.

3.9 **Version of these terms.** The versions of the Customer Terms documents listed on the Customer Terms page on the Order Date apply for the Subscription Period in which the Order Form is signed. Provider may publish new versions; a new version applies to Customer only from the start of Customer's next Subscription Period, after at least 30 days' notice, or earlier if Customer agrees in

writing. A change that Product-Specific Terms § 2.4 permits because of a change in law applies as that section states.

Part 4 — Service levels and Technical Support

The Target Uptime, Uptime Credit, Target Response Time, Response Time Credit, Business Hours, Support Channel, Scheduled Downtime, severity levels and additional Excluded Minutes are those in the **Service Level Agreement Cover Page**, which incorporates the SLA Standard Terms.

Part 5 — DPA v1.1 key terms and modifications

Term	Value
Categories of Data Subjects	Customer's employees and contractors who are Users; employees and contractors about whom Users record information; external meeting participants appearing in connected calendars
Categories of Personal Data	Identity and employment data; performance-management content; compensation data where enabled; leave and self-identification data where enabled; work-context metadata where enabled, as described in Product-Specific Terms § 4.5; authentication and audit data
Special Category Data (for this Agreement: sensitive data as listed)	Leave records and self-identification data, where enabled
Special Category Data Restrictions or Safeguards	Field-level encryption at rest; role-based access; structured self-identification and leave fields are not sent to AI model providers; automated name detection replaces many personal names before AI calls (detection is not guaranteed, and text Users type may contain anything)
Nature and Purpose of Processing	The Business Purposes in the US Privacy Addendum § 1.2
Duration of Processing	The Subscription Period, plus the periods in Product-Specific Terms § 8
Frequency of Transfer	Continuous
Approved Subprocessors	The Subprocessors listed in Provider's Subprocessor List (valutare.ai/subprocessors) on the Order Date, with what each processes and where. A copy dated the Order Date is provided on request. Subprocessors marked there as approved but not yet used for Customer Data (OpenAI and Mistral AI on the Order Date) are used only after notice under this Part
Subprocessor notice	30 days' notice of a new Subprocessor to Customer's notice contact (replacing DPA § 2.6's 10 business days); objection per Part 3.6
Provider Security Contact	security@valutare.ai
Security Incident	As defined in DPA § 11.15. Provider will notify Customer without undue delay, and in any event within 72 hours, after Provider confirms a Security Incident, and will update Customer as facts develop

Term	Value
Audit (modifies DPA § 5)	DPA § 5.2 and the last sentence of DPA § 5.1 do not apply. "Report" in DPA §§ 5.3 and 11.13 means Provider's written security documentation and completed security questionnaire, which Provider will provide on written request once every 12 months, under confidentiality. Provider has not yet been audited by an independent third party and does not represent that it has. If the Report does not reasonably answer Customer's questions, after a Security Incident affecting Customer Personal Data, or where a regulator requires it, Customer may audit on 30 days' notice, during business hours, at its own cost, without access to other customers' data
Governing Member State	Not applicable (US-only Customer)

Part 6 — AI Addendum v1.0

Term	Value
Training Data / Training Purposes	None. Provider does not use Customer's Input or Output to Train any Model (Part 3.4)
Improvement Restrictions	Provider may use Input and Output only to provide, maintain and secure the Cloud Service for Customer. Provider may use Usage Data to improve the Cloud Service, never to train, fine-tune or evaluate an AI model. Provider uses AI model providers only under business terms that do not permit them to train on Customer data