Valutare

CUSTOMER TERMS

Valutare Customer Terms — Product-Specific Terms

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

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

These Product-Specific Terms supplement the CSA v2.1 and the AI Addendum v1.0 as part of the Valutare Customer Terms. Capitalized terms not defined here have the meaning in those standards or in the Key Terms (Part 3.8).

1. The Cloud Service does not make employment decisions

1.1 The Cloud Service provides information and suggestions to support Customer's people-management processes. **It does not make employment decisions, and Provider does not make, recommend for adoption without review, or carry out any employment decision.** Decisions about hiring, promotion, pay, discipline, termination or any other term or condition of employment are made solely by Customer and its personnel. Provider does not act as Customer's agent or employment agency in making any such decision, and does not procure, screen or refer candidates or employees for Customer.

1.2 Before relying on any Output in an employment decision, Customer will ensure that a person who (a) knows how to interpret and use the Output, (b) reviews and analyzes it together with other relevant information, and (c) has authority to make or change the decision, does so.

1.2A Before Output that makes a recommendation about a person's employment, performance or pay is delivered to an individual as advice the individual might rely on, or is used to carry out a decision, Customer will ensure that a person meeting § 1.2 (a) to (c) has reviewed it with authority to change it. Output that only explains a User's own records to that User, and makes no recommendation, is labeled as produced with AI under § 3.3 and needs no reviewer under this § 1.2A.

1.3 Customer is solely responsible for its employment decisions and practices and for its compliance with employment, anti-discrimination, equal-pay, privacy and electronic-monitoring laws and AI Employment Laws, whether or not it used the Cloud Service or Output. Customer's indemnity for these matters is in the Key Terms (Customer Covered Claims).

1.4 **Disclaimer.** To the extent permitted by law, Provider makes no warranty that Output is accurate, complete, free of bias or suitable for any employment decision, and Provider has no liability for any employment decision, or for any decision not to act, made by Customer or its personnel, whether or not Customer used the Cloud Service or Output.

2. Laws on AI in employment decisions

2.1 **Scope.** "AI Employment Laws" means laws that regulate automated or AI tools used in employment decisions, including laws on notice, bias audits, risk assessments, record-keeping, explanations, opt-outs and human review. Customer is responsible for the obligations AI Employment Laws place on employers and deployers.

2.2 **What Provider supplies.** Provider will, for every customer and without regard to where Customer operates: (a) provide Documentation of each AI Service: its intended and known inappropriate uses, the categories of data it uses, the AI model providers behind it, its known limitations, the human review it requires, and a plain-language description of how it produces its Output; (b) reasonably cooperate with Customer's risk and impact assessments, including providing the facts available to Provider that Customer needs for them, and with individuals' requests to access information about, opt out of, appeal or seek human review of an automated decision, to the extent the Cloud Service holds the relevant information; (c) share with Customer, under confidentiality, summaries of its fairness testing of AI Services that inform pay or performance once that testing is completed; (d) notify Customer without undue delay if Provider identifies a material malfunction or a material risk of algorithmic discrimination in an AI Service Customer uses, and suspend or correct that AI Service; and (e) keep the records, and provide Customer the documentation and disclosures, that AI Employment Laws require of a developer or vendor of an AI Service, for the period those laws require (§ 8.1).

2.3 **No screening use.** Customer will not use the Cloud Service or any Output to substantially assist or replace discretionary decision-making to screen candidates for employment, or to screen employees for promotion, including as an "automated employment decision tool" under New York City Local Law 144 or any similar law requiring a bias audit, notice or registration before such use. The Cloud Service is not designed or offered for that purpose, and Provider does not perform bias audits for it.

2.4 **Change in law.** If a law taking effect during the Subscription Period requires a change to the Cloud Service or these terms, Provider may make the change on notice. If the change materially reduces the Cloud Service, Customer may terminate the affected part and receive a prorated refund of prepaid fees for it.

2.5 **Bias testing.** Before release, and after any change to the prompt or model, Provider tests AI Services that inform decisions about people for differences in Output across names, pronouns and other demographic cues, and shares summaries of the results with Customer under confidentiality.

Bias testing is a review aid. It does not guarantee that Output is free of bias, and it does not replace the human review in § 1.2.

3. Notices to employees, and when integrations may be enabled

3.1 **Notices are a condition of enabling.** Before Customer enables any AI Service, or enables or permits Users to connect any workplace integration, Customer will give its Users and other affected individuals every notice applicable law requires, including notice that AI assists reviews, pay recommendations and coaching, and any electronic-monitoring notice and acknowledgment (for example, under Delaware Code title 19, § 705, New York Civil Rights Law § 52-c or Connecticut General Statutes § 31-48d). Giving those notices is a condition precedent to Customer's right to enable those features.

3.2 **Confirmation.** Customer represents and warrants, each time an administrator enables an AI Service or an integration, that the notices in § 3.1 have been given. Provider may rely on that confirmation, which may be given through an acknowledgment in the Cloud Service's administration settings, and is not required to enable a feature until it is given.

3.3 Provider labels text produced with AI as AI-assisted wherever the Cloud Service shows it to a person in its web application, and the Documentation tells Users that AI helps produce summaries, drafts and insights about them.

4. Workplace integrations

4.1 **Definitions.** A "Connected Service" is a third-party service that Customer provides to its personnel, such as Microsoft 365, Google Workspace, Slack, Zoom, Atlassian or GitHub. An "integration" is the Cloud Service's connection to a Connected Service through that service's application programming interface (API), authorized by OAuth or a similar grant. A "workplace account" is an account on a Connected Service that Customer issues to a User for work.

4.2 **Customer's obligations.** Customer will: (a) permit integrations to be connected only to workplace accounts; (b) obtain any authorization or consent required by law or its own policies for Provider to access those accounts; (c) give the notices in § 3 first; and (d) disable an integration if any of these stops being true. The Cloud Service does not verify that an account is a workplace account.

4.3 **Who connects.** Unless Customer elects company-wide connection under § 4.4, each User connects the User's own workplace account, and Provider does not access any account across Customer's organization without that User's connection. Customer's IT administrator may need to approve Provider's application in the Connected Service before Users can connect.

4.4 **Company-wide connection (optional).** Where the provider of a Connected Service permits it, Customer may elect to have its IT administrator connect Users' workplace accounts instead. Customer decides how the transition happens, including whether Users who did not respond are connected, and gives Users the notices in § 3 before it takes effect. A User who turned a connection off stays off, and every User can turn off any connected account at any time.

4.5 **What Provider collects.** Provider collects only read-only metadata:
(a) **calendar:** meeting start and end times, organizer, invitees and each invitee's response, whether a meeting is recurring or online, and the meeting title where Customer enables it, but never the invitation text;
(b) **email:** for each message, the time sent or received, sender, recipients, conversation thread and a bulk-mail indicator, and the subject line where Customer enables it;
(c) **files:** file names, owners, who edited a file and when, and with whom it is shared;
(d) **chat:** who sent a message and when, its participants and the type of chat;
(e) **meetings:** attendance (who joined and for how long) for meetings the User organized;
(f) **channels:** who sent a channel message and when, and mentions, only in Microsoft Teams teams or Slack channels that have added Provider's application; and
(g) **work tools:** for items assigned to or created by the User, their type, status changes and dates, and their titles where Customer enables it.
Provider does not store or use message bodies, file contents, recordings or transcripts. Where a provider includes message text when it shares the details above, Provider discards the text on receipt and never stores or uses it. Provider does not create, change or delete anything in a connected account and never sends email or messages as a User; Provider posts its own messages and notifications only to the User or where Customer's administrator sets it up.

4.6 **How integration data is used.** Integration data about a User is used only to provide coaching to that User. It is not shown to any other person, including the User's manager, unless the User chooses to share it, and is not used in ratings or compensation features. If Customer turns on team insights, a manager may be shown collaboration patterns for a team as a whole, for groups of at least five Users, which never identify any individual or pair and are never used in ratings or compensation features; team insights are off unless Customer turns them on. A User's calendar and Microsoft data count toward team insights only if the User agrees when connecting, and the User may withdraw that agreement at any time; data from Gmail, Google Drive and Google Meet is never used for team insights. Employee-facing disclosure, verbatim: "If your organization turns on team insights, your manager may see collaboration patterns for your team as a whole, for groups of at least five people. These never identify you or any other individual, and they are never used for ratings or pay." Integration data is never used to train or evaluate any AI model or in comparisons across customers.

4.7 **Retention and deletion.** Customer may switch any source off at any time; collection then stops. Stored integration data is kept for Customer's configured retention period (default 90 days, maximum 730 days); after it, only weekly summaries are kept, and the detailed data is deleted within 30 days. When a User disconnects a source or opts out of AI processing, collection stops at once and that User's stored integration data is deleted within 30 days; for Slack, all associated data is deleted within 14 business days after Provider's application is removed from the workspace. A connected account unused for 90 days, or belonging to a User who leaves Customer's employment, is disconnected and its data deleted in the same way. Data under a legal hold (§ 8.2) is kept until the hold ends and then deleted as described here.

4.8 **Third-party services.** Connected Services are Customer's providers, under Customer's own agreements with them, which govern the data those providers hold. Provider accesses them only as Customer and its Users authorize and only within § 4.5. If such a provider changes, limits or withdraws its interface, terms or approval in a way that affects an integration, that is not a breach by Provider; Provider will notify Customer and use reasonable efforts to restore or replace the integration, and if it cannot within 60 days, Customer may terminate that integration and receive a prorated refund of any fee charged specifically for it.

5. Health information and sensitive data

5.1 The Cloud Service is not designed to store protected health information under HIPAA, and Provider does not enter into business associate agreements. Customer will not submit protected health information.

5.2 Leave records and self-identification data are processed only where Customer enables those features. Self-identification data is stored in a dedicated, access-restricted table separate from other personnel records.

6. Wellbeing support messages

6.1 The Cloud Service may detect that a User's text suggests distress or a safety concern and, if so, show that User a support message prepared by Provider pointing to Customer's designated support resources. Provider does not notify Customer or anyone else.

6.2 Provider does not keep any record that a support message was shown to a User, and no record of the text that prompted it. Provider keeps only weekly totals across all of Provider's customers, by category and language, which identify no User or customer, and uses them only to check that the feature works. The check that decides whether to show a support message reads the User's message through an AI model provider engaged by Provider; nothing about the check is kept.

6.3 Customer will supply and keep current the support contacts shown to its Users, and remains responsible for its own employee-assistance programs and any duty of care it owes its personnel.

6.4 Provider may disable the wellbeing feature for Users in any jurisdiction where applicable law restricts the inference of emotional state in the workplace, by a change to the Cloud Service.

6.5 **Not a crisis, medical or counseling service.** The wellbeing feature, and Val, the Cloud Service's AI coach, are workplace tools. They are not a crisis, emergency, medical, mental-health, counseling or therapy service, are not a companion application, and must not be used or promoted to Users as a substitute for any of these. Provider does not monitor Users, has no duty to detect, assess or respond to any risk to any person, and does not warrant that the feature detects any particular statement or that a support message is appropriate. Customer will not represent the feature to its Users as providing any such service. **To the extent permitted by law, Provider disclaims all liability for the feature detecting or failing to detect distress, for showing or not showing a support**

message, and for any act or omission of Customer or any support resource. Any liability that cannot be excluded is subject to the General Cap Amount.

6.6 The protections in this § 6 cover a User's own coaching conversations. Work records that managers write, such as pay and review notes, stay visible to Customer's authorized HR personnel even when the Cloud Service's safety check marks them; marked text is never sent to an AI model provider.

7. Access removal

7.1 Customer is responsible for deactivating Users who leave its employment, through its identity provider or the Cloud Service's administration features. Provider will process deactivations promptly.

8. Records, holds, return and deletion

8.1 **AI records.** Provider retains the Output of AI Services for 12 months, or for any longer period an AI Employment Law requires of Provider as a developer or vendor, and, on request, exports the Output it holds together with the configuration history of those AI Services so Customer can keep it for the period the law requires of Customer. Provider does not retain the full Input of AI Services. Customer is responsible for keeping the records AI Employment Laws require it to keep.

8.2 **Legal hold.** On Customer's written notice of a dispute or investigation identifying the Users concerned, Provider will suspend routine deletion of those Users' data, including Output, until Customer releases the hold.

8.3 **End of term.** On request made within 30 days after the Subscription Period ends, Provider will export Customer Content and Customer Personal Data, including audit logs and the Output it holds, in CSV or JSON by a documented manual process within 30 days of the request. Notwithstanding CSA § 5.5, Customer may access the Cloud Service to export data during that period. Provider will not delete the data before the earlier of Customer's written confirmation that it has what it needs or the end of that period. Provider then deletes the data from production systems within 30 days and confirms deletion in writing on request. Backup copies are not altered; they expire under Provider's backup retention schedule, currently no more than 35 days after production deletion, and remain protected under the Agreement until they expire.

8.4 **Audit logs.** Provider keeps audit logs of activity in the Cloud Service for up to 12 months, and records that applicable law requires to be kept longer, such as pay and legal records, for up to 7 years.

9. AI models and aggregated data

9.1 **No training or evaluation.** 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, and will not permit its AI model providers to do so. The only exception is screening and testing of Output for safety and bias in the

Cloud Service provided to Customer (§ 2.5), which runs only on AI model providers processing in the United States, uses no data received through integrations, and keeps no copy beyond what § 8.1 allows.

9.2 **No comparisons across customers.** Provider will not combine Customer's data with other customers' data for benchmarking or comparison unless Customer opts in through the Order Form; if it does, results are reported only for groups of at least five people, and data received through integrations is never included.

9.3 **Usage data.** Provider may use technical and operational data about the performance and use of the Cloud Service that is not Customer Content (such as uptime, latency, feature usage and error logs) to operate, secure and improve the Cloud Service, subject to the US Privacy Addendum § 4 and Key Terms Part 3.4.

9.4 **AI model providers and processing location.** Provider uses Google (Gemini, through Google Cloud Vertex AI, processed in the United States) and Anthropic (Claude, processed in the United States); which provider handles a request depends on the feature. Mistral AI (processing in the European Union) and OpenAI (processing in the United States) are approved providers that are not used for Customer data; Provider will give notice under the subprocessor terms before using either, and any transfer to the European Union will be made under the DPA's transfer terms. Each provider is engaged under terms that bar training on Customer data.

9.5 **Protected characteristics.** No AI Service receives any individual User's protected characteristics, such as gender, race, age or disability. HR analytics may use group-level figures for groups of at least six people, never individual values.

9.6 **Turning AI off.** Customer's administrators can turn AI Services off for all of Customer's Users in the Cloud Service's settings, and each User can turn them off for that User. Translation between languages continues, and uses an AI service.