# Dealr AI Addendum

**Effective October 15, 2026 · v1.1.0**

This AI Addendum governs Customer's use of AI Features and Dealr's use of AI in providing the Services. Capitalized terms used but not defined in this Addendum have the meanings given in Section 2 of the MSA General Terms, including the terms Section 2 identifies as defined in other components of the Agreement.

## 1. Definitions

- "**AI Features**" means Service features that use machine learning, large language models, speech technologies, or other artificial-intelligence systems, including document extraction and verification, transcription and conversation analytics, AI voice agents, drafting/suggestion tools, and scoring features, as described in the Documentation. AI Features do not include third-party AI applications connected through an AI Client Connection (Section 8).
- "**Input**" means Customer Content and configuration submitted to an AI Feature.
- "**Output**" means content or results an AI Feature generates for Customer.
- "**AI Interaction Records**" has the meaning in Section 3.6.
- "**Verification Signals**" has the meaning in Section 3.2.

---

## 2. Outputs — ownership, accuracy, and human responsibility

2.1 **Ownership.** As between the parties, Customer owns Outputs generated for it, as part of Customer Content. Dealr retains all rights in the AI Features, models, and systems themselves. Outputs may be similar or identical to outputs generated for other customers (independent generation is not infringement of Customer's rights).

2.2 **Accuracy disclaimer.** AI FEATURES ARE PROBABILISTIC. OUTPUTS MAY BE INACCURATE, INCOMPLETE, OR UNSUITABLE, MAY NOT REFLECT CURRENT LAW OR DATA, AND ARE PROVIDED WITHOUT WARRANTY (MSA §9.2). OUTPUTS ARE NOT LEGAL, TAX, FINANCIAL, OR COMPLIANCE ADVICE.

2.3 **Human oversight.**

(a) **Review before reliance.** Customer is responsible for reviewing Outputs before relying on or communicating them. This does not apply to real-time conversational Outputs generated by AI communication features in live interactions. For those Outputs, Customer's oversight obligation is instead approval of the prompts, templates, campaign content, and disclosure configurations under AUP §8(c) (campaign content and scripts), plus reasonable post-hoc review of logs, recordings, and transcripts.

(b) **Decisions.** Customer is responsible for all decisions and actions taken using Outputs (MSA §4.4 (decisions)), including credit, financing, pricing, advertising, and employment decisions.

(c) **AI-composed outbound messages.** For AI-composed outbound messages other than real-time conversational Outputs, the Services default to per-message Customer review and approval before sending. Automatic sending applies only where Customer has affirmatively enabled it. That election is a logged Customer configuration choice (AUP §8 (allocation of responsibility)).

(d) **Assistive features.** Where an AI Feature is documented as assistive (e.g., audit flags, extraction suggestions), Customer's workflows must keep a qualified human responsible for the final action.

2.4 **Regulated decisions.** If Customer uses Outputs in connection with credit or other consequential consumer decisions, Customer is the creditor/decision-maker and is solely responsible for adverse-action notices, specific reason disclosures (ECOA/Regulation B), automated-decision notices and opt-outs under state law, and fair-lending compliance. Dealr provides tools only, and will surface feature-level explanation aids where the Documentation says so. Customer will not use an Output as the sole or determinative basis for any credit, financing, pricing, or other consequential consumer decision, and will maintain meaningful human review of any such decision. Where Outputs inform a credit decision, Customer (or its finance partner), as the creditor, must identify and disclose the specific principal reasons for any adverse action (12 C.F.R. §1002.9); Outputs are not a substitute for that determination.

2.5 **Outputs and infringement claims.** Outputs are generated at Customer's direction from Customer's Inputs and configuration and are not "the Services, as provided by Dealr" for purposes of MSA §12.1 (Dealr IP indemnity). Dealr has no defense or indemnification obligation for any claim arising from Outputs or from Customer's use, publication, or distribution of Outputs. This exclusion does not apply, however, to the extent a claim arises from the AI Feature's reproduction of third-party material embedded in the model or in Dealr Materials, independent of Customer's Inputs (e.g., training-data regurgitation, vendor stock voices, Dealr templates). For such claims, MSA §12.1's exclusion (a) does not apply to the extent the third-party material was embedded in the model or in Dealr Materials by Dealr or its AI vendors rather than supplied by Customer.

2.6 **Output restrictions.** Customer's ownership of Outputs does not limit MSA §3.5(c) (restrictions). Customer will not, and will not permit any End User or other person to:

(a) use Outputs or other Service-generated content, whether before or after export or termination, to develop, train, or improve a product, service, or machine-learning or AI model that competes with the Services; or

(b) attempt to extract, or induce an AI Feature to reveal, Dealr's non-public system prompts, templates, model weights, or model parameters, including through prompt injection or similar techniques.

This Section 2.6 does not restrict Customer's use of Outputs and Customer Content in the ordinary operation of its business, and does not narrow Customer's data-access and portability rights under MSA §10 (Customer data access and portability).

---

## 3. Dealr's use of Customer Content with AI

3.1 **Training limits.**

(a) **What Dealr does not do.** Dealr does not use Customer Content, or data derived from Customer Content (including de-identified or Aggregate Data), to train or fine-tune generalized or foundation AI models, or any model offered or used outside the Services. Dealr does not use Customer Content to train models for marketing, resale, or data products. Dealr does not permit its AI vendors or any other third party to use Customer Content to train or fine-tune AI models. An AI vendor may, however, use de-identified data derived from Customer Content to improve its own service where the vendor's terms permit it.

(b) **Service-limited training.** Dealr may use Customer Content, and data derived from Customer Content, to train, fine-tune, evaluate, and improve models Dealr uses solely to provide and improve the Services. Examples are the custom document models that classify document types, locate and read fields, split combined files, and perform similar document-understanding tasks — built in Dealr's own instance of a vendor document-intelligence service (currently Microsoft Azure AI Document Intelligence, as reflected on the Subprocessor List) or on infrastructure Dealr controls, and which may be trained on copies of submitted documents, including the personal information appearing on them, together with the labels Dealr applies — and the transaction-audit model described in Section 3.2. All training under this Section 3.1(b) is subject to the Section 3.3 safeguards. Any training use outside this Section 3.1 requires Customer's opt-in consent.

(c) **This Addendum controls.** This Addendum controls Dealr's AI training uses. It does so notwithstanding MSA §8.5 (Aggregate Data) and the order of precedence in MSA §1.2 (order of precedence). MSA §8.5 does not authorize any use of Customer Content, or data derived or de-identified from it, for AI model training beyond Sections 3.1–3.3.

(d) **Operating AI Features.** For clarity, Dealr may use Customer Content transiently to *operate* AI Features (inference, extraction, transcription) per the MSA §8.2 (license to Dealr) license. Dealr may also evaluate AI Feature quality using processes that do not retain Customer Content in any model.

3.2 **DTS transaction-audit model (Verification Signals only).** For the transaction-audit function of the Registration & Title Services (Schedule B), Dealr commits to less than Section 3.1(b) would allow: the shared audit model that scores transactions, as distinct from the Section 3.1(b) document models that read fields, is trained only on **Verification Signals**, never on document content or personal-information field values. Verification Signals are derived signals indicating whether a submitted document is consistent with transaction input data, such as field-match/mismatch indicators, document-quality indicators, and audit outcome labels. Verification Signals are de-identified before any use in model training. Intermediate processing steps may retain Customer and transaction identifiers for audit and quality purposes, and those identifiers are removed before model training. Verification Signals:

(a) are produced by a deliberate filtering step that:

  (i) limits training examples to non-identifying match/mismatch indicators, document-quality indicators, and audit-outcome labels; and

  (ii) excludes the content or values of all personal information, including names, Social Security numbers, dates of birth, addresses, driver's license numbers, telephone numbers, email addresses, financial account numbers, vehicle identification numbers, license-plate numbers, signatures, and free-text fields.

  A signal may be derived from, and named after, such a field, for example a match/mismatch flag, field-length value, or confidence score, but never contains the field's content or value;

(b) may include match/mismatch indicators, review-message indicators, and outcome labels derived from state-system responses in the course of performing the transaction-audit function required by Dealr's state contract, but never include state-system field values themselves;

(c) are processed and stored only on infrastructure in the United States; and

(d) are used solely for the transaction-audit function and not for marketing, resale, or unrelated products. This limit applies notwithstanding MSA §8.5 (Aggregate Data).

The resulting audit model is shared across customers. Its outputs are limited to audit flags, scores, and suggestions and are designed not to reveal any other customer's transaction data. Termination does

not require retraining, because Verification Signals are Dealr-generated audit determinations rather than retrievable Customer Content. Dealr will, however, cease generating new Verification Signals from a terminated Customer's data. This Section 3.2 applies from the date Customer affirmatively accepts an Agreement incorporating this Addendum.

3.3 **Training safeguards.** All training under Section 3.1(b), including the Section 3.2 audit model, is subject to all of the following limits:

(a) **Purpose limitation.** Training data and the models trained on it are used solely to provide and improve the Services, and not for marketing, resale, or unrelated products. This limit applies notwithstanding MSA §8.5 (Aggregate Data).

(b) **Dealr-scoped models; no vendor training.** Models trained on Customer Content are usable only by Dealr in providing the Services. Where a vendor service is used for training or hosting, training occurs at Dealr's direction inside Dealr's own vendor resource. A vendor's training of such a model at Dealr's direction is Dealr's own use, not vendor training, for purposes of Section 3.5 (AI vendors); the vendor must still meet the Section 3.5 standing policy, including a commitment not to train or fine-tune its own or any third party's AI models on Customer Content, training data included, consistent with Section 3.1(a).

(c) **Curation; confidentiality.** Training data is assembled by a deliberate selection step and limited to what is reasonably needed for model accuracy; any human review or labeling is performed by personnel bound by confidentiality (DPA §4 (confidentiality of Processing)).

(d) **No State Records.** Training data never includes State Records or state-system field values. Indicators derived from state-system responses are used only as Section 3.2(b) states, for the transaction-audit function.

(e) **No cross-customer disclosure.** A model trained on Customer Content and used for more than one customer is designed not to reveal one customer's Customer Content to any other customer. Where a model extracts, classifies, or generates content for a customer, that content comes from that customer's submitted inputs, not from training data.

(f) **Retention; termination.** Dealr retains Customer Content in training data only while reasonably needed to train, evaluate, and maintain the model versions it supports. On termination, Dealr stops adding the terminated Customer's data to training data and deletes its Customer Content from stored training data no later than the DPA §10.2 (deletion after termination) timeline. Deletion does not require immediate retraining of a deployed model: a model trained before the deletion retains only learned parameters, remains subject to paragraph (e), and Dealr will exclude the deleted data from any subsequent training of the affected models.

Models trained under Section 3.1(b) may be shared across customers. Sections 3.1(b) and 3.3 apply from the date Customer affirmatively accepts an Agreement incorporating this Addendum.

3.4 **De-identified and Aggregate Data.** MSA §8.5 (Aggregate Data) governs uses of de-identified and Aggregate Data *other than* AI model training, which is exclusively governed by Sections 3.1–3.3. De-identified data used in connection with AI is subject to the same non-reidentification commitments.

3.5 **AI vendors.** AI Features may be provided using third-party AI vendors and hosted model families (including OpenAI, Anthropic, and hosted open-weight families such as DeepSeek, Kimi/Moonshot, and GLM), in each case as reflected on the Subprocessor List. Dealr's standing policy: no AI vendor Processes Customer Content in production without (a) a commitment not to train or fine-tune AI models on Customer Content (written no-training terms or a documented, configuration-enforced no-training setting), consistent with Section 3.1(a), and limited-retention terms, (b) contractual

confidentiality and data-protection terms, which may be the vendor's standard commercial terms, and (c) listing on the Subprocessor List. DPA §6 (Subprocessors) (including its change-notice and objection mechanics) applies.

3.6 **AI Interaction Records; retention.**

(a) **Definition.** "**AI Interaction Records**" are Dealr's service-operations records of interactions with AI Features — prompts, chat and conversation histories with AI agents (including the AI BDC), session transcripts of AI interactions, and intermediate artifacts (such as embeddings and unsaved drafts).

(b) **Classification.** AI Interaction Records are service records maintained by Dealr and are not Customer Content. This classification does not apply to any Output or extracted data saved into Customer's records in the Services, or to call and meeting recordings and their transcripts stored as records in the Services; those are and remain Customer Content. Examples of saved Output or extracted data are an extracted field written to a deal record or a message stored in the CRM. Consumer-facing AI communications — AI BDC call recordings, their transcripts, and AI-generated message threads with consumers — and the Section 4.5 compliance records are likewise not AI Interaction Records: they are Customer Content (or Section 4.5 compliance records) and are not subject to the Section 3.6(c) rolling deletion.

(c) **Retention.** Dealr retains AI Interaction Records for up to six (6) months on a rolling basis, after which they are deleted. Dealr retains them to surface recent interaction history to Customer and for security, abuse-detection, and service-analysis purposes. On termination or account-level deletion they are deleted no later than the DPA §10.2 (deletion after termination) timeline, if earlier.

(d) **Training limits; DPA protection.** Sections 3.1–3.3 apply to AI Interaction Records as if they were Customer Content: Dealr does not use them, or data derived from them, to train any model outside the Section 3.1(b) service-limited scope; any Section 3.1(b) use of them is subject to the Section 3.3 safeguards; and any use beyond Section 3.1 requires Customer's opt-in consent. Personal Data within AI Interaction Records remains protected under the DPA (including its security and Security Incident provisions) at all times.

(e) **Legal retention.** Retention required by Applicable Law or legal hold is excepted.

---

## 4. AI voice and messaging features (BDC)

4.1 **Disclosure architecture.** AI voice features ship with a default compliance profile set to the strictest supported configuration ("**Universal Strict**"), including AI-identity disclosure at call start and recording disclosure. For AI-generated messaging, the AI-identity disclosure is in the first message of a conversation. Customer may adjust configurable settings per jurisdictional profiles in the product. Each relaxation below Universal Strict requires an administrator acknowledgment and is logged. Customer's configuration choices are Customer's own compliance decisions (AUP §8 (allocation of responsibility), §12 (calling windows and frequency), §16 (AI disclosures)).

4.2 **Non-configurable safeguards.** The following safeguards are designed and enforced by the product and are not Customer-configurable:

(a) **recording disclosure while recording is enabled for a call — inbound or outbound — in which any party is in an all-party-consent jurisdiction**; the alternative is that recording is automatically disabled for that call. An all-party-consent jurisdiction is a jurisdiction whose law requires the consent of all parties to record the type of

communication at issue, as reflected in the Services' state rules engine. Dealr updates that engine as it becomes aware of changes in law;

(b) AI-identity disclosure, for AI voice and AI-generated messaging, where the recipient's jurisdiction requires disclosure of synthetic, artificial, or bot identity;

(c) honoring in-call opt-out requests;

(d) the compliance log; and

(e) truthful acknowledgment of artificial identity. AI Features that interact with consumers by voice or messaging are designed to truthfully confirm that they are automated, and not to claim to be human, in response to a clear and unambiguous inquiry.

Where a party's location is unknown, or the available location signals conflict or are low-confidence, the strictest profile applies.

4.3 **Consent gate.** Marketing calls and texts placed using AI Features require consent records satisfying AUP §10 (prior express written consent for artificial/prerecorded/AI voice marketing) before dialing. The Services are designed to block campaigns that lack qualifying consent classifications.

4.4 **No voice cloning.** Dealr does not create a voice clone or simulation of any identifiable real person. Customer may not upload, request, or use the Services to create a voice clone or simulation of any identifiable real person. The standard AI voices offered in the Services are synthetic voices provided by Dealr's vendors under commercial licenses that Dealr reasonably believes include any consents required for their creation.

4.5 **Compliance records.** The Services maintain logs of disclosures played, consent classifications, opt-outs, and configuration changes, and offer Customer exportable compliance reports. The Services retain these compliance records for at least five (5) years, or such longer period as Applicable Law requires, and they are included in Customer's export under MSA §10.3 (export; deletion). Logs are records of product behavior, not legal advice or a guarantee of Customer's compliance.

4.6 **Safeguards are compliance-assistance features.** Safeguards, consent gates, and compliance profiles (including Sections 4.2 and 4.3) are compliance-assistance features. Their operation, configuration, or failure does not make Dealr the initiator, seller, or telephone solicitor for Customer's communications. It does not shift Customer's compliance responsibility under AUP Part II (communications compliance) to Dealr, and is not a warranty that any communication complies with Applicable Law. Consent gating depends on the accuracy of the consent records and classifications Customer supplies. Jurisdiction-based safeguards depend on available recipient-location signals, which can be inaccurate (e.g., ported or VoIP numbers). Where a party's location cannot be determined, or the available location signals conflict or are low-confidence, the strictest profile applies as stated in Section 4.2 (non-configurable safeguards).

4.7 **Biometric feature gate.** Except for the e-signing and transaction face checks described in Schedule A §A-11 and the account-access face check described below, the AI Features do not create, derive, or retain biometric identifiers (including voiceprints or speaker-recognition templates). Those face checks run only where Customer turns them on, and Dealr operates them as controller under its Biometric Data Policy, obtaining each person's written consent before any processing (Schedule A §A-11; DPA §2.3(d)). Dealr may also ask an End User to complete the same face check to verify the End User's identity for the End User's account, including before resetting or regaining access to it; Dealr operates it as controller under the Biometric Data Policy and the End User Terms, obtains the End User's written consent first, offers a non-biometric alternative (confirmation of the End User's identity by another of Customer's account administrators), and gives Customer no face images, face measurements, or face-check scores (DPA §2.3(d)). Signing in with a passkey that uses a device's built-in face or fingerprint unlock is not biometric processing by Dealr: the match happens on the

device, and Dealr receives only a confirmation. Dealr will not introduce any other AI Feature that creates or uses biometric identifiers except through the biometric notice-and-consent framework described in the End User Terms or the Biometric Data Policy, as applicable, with prior notice to Customer and, where Applicable Law requires, consent obtained before processing.

---

## 5. Recording, transcription & conversation analytics

5.1 **Dealr-hosted communications.** Dealr may record and analyze its own sales, support, demo, and training communications with Customer, with disclosure, for quality, training (human, not model-training beyond Section 3 (Dealr's use of Customer Content with AI)), and service improvement.

5.2 **Customer communications.** For Customer's recorded calls and meetings processed by conversation-analytics features, Customer is responsible for lawful recording consent (AUP §15 (recording and monitoring)). The Section 4.2(a) (recording disclosure) safeguard applies to calls recorded through the Services' communication features, inbound and outbound; for recordings Customer makes outside those features and processes through conversation-analytics features, Customer alone is responsible for consent. Recordings, transcripts, and analytics derived from them are Customer Content.

---

## 6. Disclosures to consumers

Customer is responsible for consumer-facing AI disclosures required by Applicable Law in its use of the Services, using the product's disclosure tooling where available. Such laws include chatbot/synthetic-media disclosure laws and state AI consumer-protection statutes. Dealr is responsible for disclosures Applicable Law requires of Dealr as the technology developer/deployer of the Services themselves.

---

## 7. Changes to AI Features

Dealr may add, modify, or discontinue AI Features per MSA §3.1 (provision). Dealr will update this Addendum and the Subprocessor List as the AI Feature set and vendor stack evolve, per MSA §17 (changes to the Agreement) (material changes at renewal; vendor-list changes per DPA §6 (Subprocessors)). Any change that expands Dealr's rights to use Customer Content (or data derived or de-identified from it) for AI model training does not apply to Customer without Customer's separate, affirmative opt-in consent. This rule applies notwithstanding MSA §17.

---

## 8. Third-party AI applications

8.1 **Not an AI Feature.** An AI application that Customer or an End User connects through an AI Client Connection (MSA §10.2(d)) is not an AI Feature, and its provider is not an AI vendor of Dealr's under Section 3.5 (AI vendors). Sections 2.1–2.5, 3.1–3.6, 4, and 5 do not apply to that application, its models, its outputs, or its handling of data it receives. That provider's terms and Customer's or the End User's settings with that provider govern those matters, including any use of data for model training and any retention.

8.2 **Customer's choice and settings.** Customer is responsible for choosing which AI applications and accounts its End Users may connect, and for their training, retention, and data-location settings.

Dealr recommends connecting only business accounts whose terms exclude model training on customer data.

8.3 **Responses and actions are not Dealr's.** Answers, summaries, and analyses a connected AI application generates from Customer Content are not Outputs and are not the Services. Dealr gives no warranty for them, and MSA §4.4 (decisions) applies to any reliance on them. Where a connection allows a connected AI application to create, modify, or delete records or take other actions in the Services, Customer is solely responsible for those actions under MSA §10.2(e) (changes made through connections). Section 2.3 (human oversight) does not require Dealr to review or confirm them. Dealr is responsible only for carrying out connection requests in accordance with the Documentation.

8.4 **Records.** Dealr does not receive the prompts or responses exchanged between an End User and a connected AI application. Dealr keeps security and usage logs of requests made through the connection (such as the tool called, timing, and record counts). Those logs are service records, not AI Interaction Records, and are retained as the Privacy Policy describes.