

# Partner Code of Ethics & AI Responsibility

**Effective Date:** March 11, 2026 | **Document Version:** 1.0

**Our Mission:** *Drive Our Partners' Success Through Elevating Intelligence at Every Touchpoint.*

CallRevu is the automotive industry's leading communication intelligence platform. We process over 13.6 million calls per month, capturing more than 1.2 billion data points on behalf of our dealership partners.

This privileged position, sitting at the intersection of customer relationships, sensitive data, and AI-powered decision-making demands an uncompromising standard of ethical conduct from every partner who operates within our ecosystem.

This Code of Ethics & AI Responsibility (the "Code") establishes the foundational principles, obligations, and behavioral standards that all CallRevu technology partners, integration partners, reseller partners, and data subprocessors (collectively, "Partners") must uphold as a condition of partnership.

By signing this Code, the Partner acknowledges and agrees to operate in full alignment with CallRevu's Enterprise AI & Data Stewardship Policy and the standards described herein.

## I. Data Ownership & Customer Sovereignty

CallRevu's relationship with its dealership clients is built on an inviolable principle: customer data belongs to the customer. Partners operating within CallRevu's ecosystem are stewards of that data — never its owners, exploiters, or beneficiaries beyond the narrowly defined scope of the services they are contracted to deliver.

### Partner Obligations

- ▶ Recognize and respect that all customer data processed through or alongside the CallRevu platform remains the exclusive property of the originating dealership client.
- ▶ Process customer data solely and only for the specific, documented purpose for which it was shared. Any repurposing, resale, aggregation, or secondary use is strictly prohibited without explicit written consent from both CallRevu and the applicable dealership client.
- ▶ Immediately notify CallRevu in writing upon becoming aware of any unauthorized access, disclosure, use, or processing of customer data originating from the CallRevu platform.
- ▶ Upon termination of the partnership agreement, certify in writing the complete and irreversible deletion of all CallRevu customer data within thirty (30) days.

## II. AI Model Training Prohibition

One of CallRevu's most fundamental commitments to its clients is that their data is never used to train, fine-tune, or otherwise improve AI or machine learning models — whether operated by CallRevu or any third party. Partners must uphold this commitment without exception.

### Partner Obligations

- ▶ Never use CallRevu customer data — including call recordings, transcriptions, sentiment scores, behavioral signals, or any derivative data — to train, fine-tune, evaluate, benchmark, or improve any AI, ML, or large language model, whether proprietary, open-source, or operated by a third party.
- ▶ Contractually prohibit any downstream subprocessors or sub-vendors from using CallRevu customer data for AI training purposes.

- ▶ Maintain clear, auditable technical and organizational controls that prevent inadvertent data flows into AI training pipelines.
- ▶ Upon request, provide written attestation and supporting documentation confirming compliance with this prohibition within ten (10) business days.

### **III. Secure AI Subprocessor Governance**

Where Partners utilize third-party foundational AI models or AI infrastructure services (including but not limited to large language model APIs, speech-to-text services, sentiment engines, or generative AI platforms) in connection with CallRevu data or integrations, rigorous contractual and technical safeguards are mandatory.

#### **Partner Obligations**

- ▶ Access third-party AI services exclusively via secure, enterprise-grade API integrations that operate under Zero-Data Retention (ZDR) agreements, ensuring that customer data is discarded immediately following processing and is never stored, logged, or retained by the AI subprocessor.
- ▶ Maintain and make available to CallRevu upon request a current register of all AI subprocessors with access to CallRevu-derived data, including the identity of the provider, the nature of data shared, and the contractual safeguards in place.
- ▶ Ensure that all AI subprocessors are contractually prohibited from using CallRevu customer data for model training, product improvement, or any secondary purpose.
- ▶ Notify CallRevu no less than thirty (30) days in advance of any change in AI subprocessors that may affect data processing activities covered by this Code.

### **IV. PII Safeguards & Data Minimization**

The automotive customer journey involves the routine exchange of sensitive personal information — including credit applications, Social Security Numbers, driver's license data, and financial details. Partners must implement and maintain rigorous safeguards that prevent unnecessary exposure of this information.

#### **Partner Obligations**

- ▶ Implement technical controls that identify and redact or mask sensitive PII — including Social Security Numbers, credit card numbers, driver's license numbers, and financial account identifiers — before any conversational or transactional data is processed by AI systems or transmitted to third-party services.
- ▶ Apply the principle of data minimization at every stage: collect only what is necessary, retain only for as long as is necessary, and share only with those who have a documented need.
- ▶ Maintain a documented data classification policy that identifies categories of sensitive data, the controls applied to each category, and the individuals responsible for enforcement.
- ▶ Ensure that any employee, contractor, or system with access to PII-bearing CallRevu data is subject to appropriate access controls, need-to-know authorization, and confidentiality obligations.

### **V. Transparency, Disclosure & Consumer Rights**

CallRevu's platform interacts directly with automotive consumers on behalf of dealerships. This interaction carries legal and ethical responsibilities with respect to transparency, consent, and the protection of consumer rights. Partners whose products or services extend into consumer-facing workflows bear these responsibilities jointly.

#### **Partner Obligations**

- ▶ Where AI systems — including but not limited to voice bots, digital assistants, chat agents, or automated outbound communications — interact with consumers, ensure that all applicable bot disclosure and automated communication laws are satisfied, including requirements under the Telephone Consumer Protection Act (TCPA), applicable state consumer protection statutes, and emerging state AI transparency regulations.

- ▶ Enable and support mechanisms that allow consumers to exercise applicable privacy rights — including the right to access, correct, or request deletion of their personal data — in compliance with the California Consumer Privacy Act (CCPA), and any other applicable state or federal privacy framework.
- ▶ Never design or deploy AI-driven consumer interactions in a manner intended to deceive, mislead, or obscure the automated nature of the interaction from the consumer.
- ▶ Ensure that any consumer data collected through CallRevu-adjacent workflows is processed in accordance with the applicable dealership's privacy disclosures and consent capture processes, for which the dealership serves as the data controller.

## VI. Human Oversight & Responsible AI Use

AI is a powerful accelerator of human intelligence — not a replacement for human judgment, particularly in high-stakes consumer interactions. CallRevu's AI capabilities are designed to assist dealerships, not to autonomously make decisions that affect consumers' financial standing, access to credit, or contractual rights. Partners must operate with the same philosophy.

### Partner Obligations

- ▶ Ensure that AI-driven capabilities deployed in connection with CallRevu integrations serve in an advisory or facilitative capacity only. Binding decisions affecting consumers — particularly those intersecting with credit approval, loan terms, pricing commitments, or employment outcomes — must remain under the complete authority and accountability of a human decision-maker.
- ▶ Maintain and document clear human escalation pathways for any AI-assisted workflow that could materially affect a consumer's rights, financial interests, or employment status.
- ▶ Where AI is used in recruitment or candidate screening workflows (such as via CallRevu's RecruitTrack capability), ensure that candidates receive meaningful prior notice, that AI is used solely to assist human evaluators, and that the employing organization retains full decision-making authority over all hiring outcomes.
- ▶ Where required by applicable law, conduct and document bias audits and adverse-impact analyses for AI tools used in employment-related contexts, and cooperate with any audits initiated by CallRevu.

## VII. Security Standards & Incident Response

The integrity of CallRevu's platform depends on the security posture of every party in the ecosystem. A vulnerability in a partner's environment is a vulnerability in CallRevu's environment. Partners must maintain security standards commensurate with the sensitivity of the data they access.

### Partner Obligations

- ▶ Maintain a documented information security program that includes, at minimum: encryption of customer data in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent), role-based access controls, multi-factor authentication for systems with access to customer data, and routine penetration testing or security assessments.
- ▶ Limit access to CallRevu-derived data to authorized personnel with a documented, legitimate business need. Conduct access reviews no less frequently than quarterly.
- ▶ Notify CallRevu's Security and Privacy team within forty-eight (48) hours of discovering any actual or suspected security incident, data breach, or unauthorized access involving CallRevu customer data, regardless of scope or perceived materiality.
- ▶ Cooperate fully with any post-incident investigation initiated by CallRevu or its clients, including providing access to relevant logs, system records, and personnel.

## VIII. Data Retention, Deletion & Configurable Controls

Unnecessary retention of customer data creates unnecessary risk. CallRevu operates on a principle of minimal, configurable retention — and expects Partners to apply the same discipline.

### Partner Obligations

- ▶ Retain CallRevu customer data only for the minimum period required to fulfill the contracted service, and no longer. Document and adhere to specific retention schedules for each data category.
- ▶ Honor any data deletion requests initiated by CallRevu or its dealership clients within the timeframes specified in the applicable Data Processing Agreement (DPA). Provide written confirmation of deletion upon completion.
- ▶ Ensure that backup systems, disaster recovery environments, and archival storage are included within the scope of deletion obligations — data deleted from primary systems must also be purged from all secondary and tertiary stores.

## IX. Regulatory Compliance & Legal Accountability

The automotive industry operates within a complex and evolving regulatory landscape. Partners must not only comply with the letter of applicable law — they must proactively monitor and adapt to regulatory developments that affect the responsible use of AI and the handling of consumer data.

### Partner Obligations

- ▶ Maintain current compliance with all applicable data protection and privacy laws, including but not limited to: the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), the Telephone Consumer Protection Act (TCPA), applicable state AI transparency and automated decision-making statutes, the FTC Act and any applicable FTC guidance on AI and data practices, and any applicable employment law governing the use of AI in hiring.
- ▶ Appoint a designated individual — and provide CallRevu with that individual's contact information — responsible for data protection and AI ethics compliance within the Partner organization.
- ▶ Notify CallRevu promptly of any regulatory inquiry, government investigation, or legal proceeding that involves or may involve CallRevu customer data or CallRevu-adjacent AI capabilities.

## X. Enforcement, Audit Rights & Remedies

Ethical commitments are only as strong as the mechanisms that enforce them. CallRevu reserves the right to audit Partner compliance with this Code and to take appropriate remedial action in the event of a breach.

### Audit Rights

- ▶ CallRevu may request, and Partner shall provide within fifteen (15) business days, written attestations, supporting documentation, or access to relevant systems and records sufficient to verify compliance with any provision of this Code.
- ▶ In cases where documentation is insufficient or a material breach is suspected, CallRevu may engage a qualified independent third party to conduct an audit of Partner's relevant practices. Partner shall cooperate fully and bear a proportionate share of audit costs in the event a material breach is confirmed.

### Consequences of Breach

- ▶ A confirmed material breach of this Code constitutes a breach of the underlying Partnership Agreement and may result in: immediate suspension or termination of Partner's access to the CallRevu platform and data; public disclosure of the breach to affected dealership clients as required by applicable law; referral to appropriate regulatory authorities; and pursuit of all available legal remedies, including damages for harm caused to CallRevu or its clients.
- ▶ CallRevu's failure to enforce any provision of this Code on one occasion shall not be construed as a waiver of its right to enforce that provision in the future.

## Partner Commitment Summary

The following table summarizes the ten core commitments covered by this Code. Partner acknowledges each commitment by signing below.

Commitment Area	Core Obligation
<b>I. Data Ownership</b>	Customer data is never owned or repurposed by the Partner beyond its contracted use.
<b>II. No AI Training</b>	Customer data is never used to train, fine-tune, or evaluate any AI or ML model.
<b>III. ZDR Subprocessors</b>	All AI subprocessors operate under Zero-Data Retention agreements.
<b>IV. PII Safeguards</b>	PII is redacted or masked before AI processing; data minimization is enforced.
<b>V. Consumer Transparency</b>	Bot disclosures are enabled; consumer privacy rights are supported.
<b>VI. Human Oversight</b>	AI assists; humans decide. No autonomous binding decisions affecting consumers.
<b>VII. Security Standards</b>	Encryption, access controls, MFA, and 48-hour incident notification are maintained.
<b>VIII. Retention &amp; Deletion</b>	Data is retained minimally and deleted promptly upon request.
<b>IX. Regulatory Compliance</b>	Ongoing compliance with CCPA, TCPA, and applicable AI transparency statutes.
<b>X. Audit Cooperation</b>	Partner cooperates with CallRevu compliance audits within 15 business days.

## Partner Acknowledgment & Signature

By signing below, the undersigned authorized representative of the Partner organization confirms that they have read, understood, and agree to be bound by this CallRevu Partner Code of Ethics & AI Responsibility in its entirety. The undersigned further represents that they have the authority to bind the Partner organization to these obligations.

<b>Partner Organization Name</b>	<b>Authorized Signatory Name &amp; Title</b>
_____	_____
<b>Signature</b>	<b>Date</b>
_____	_____

Return executed copy to: [partners@callrevu.com](mailto:partners@callrevu.com)

Questions regarding this Code: [privacy@callrevu.com](mailto:privacy@callrevu.com) or visit [callrevu.com/ai-responsibility](https://callrevu.com/ai-responsibility)