CALL DATA COMPLIANCE AND SECURITY:

Best Practices for Dealerships

CALLREVU | APRIL 2025

Ensuring Data Compliance and Security in Call Data Management: A Comprehensive Guide

With the rapid growth of digital communication and cloud-based telephony, businesses are handling an increasing volume of call data, including sensitive customer information. Organizations, like dealerships, must navigate a complex landscape of data compliance laws and security standards to ensure that call data is collected, stored, and processed securely.

Understanding Call Data and Compliance Requirements

What is Call Data?

Call data refers to all the information collected during phone calls, including:

- Caller identity (phone numbers, caller ID, location)
- Call recordings and transcripts
- Duration, timestamps, and routing details
- Sensitive customer information shared during calls
  (e.g., payment details, medical records, personally identifiable information [PII])

Since call data often contains personally identifiable information (PII) or financial data, it is subject to strict regulatory compliance requirements.

Key Regulations Governing Call Data

California Consumer Privacy Act (CCPA)

Regulates businesses that collect and store data of California residents.

Requires disclosure of data collection practices and allows consumers to opt out of data sharing.

Consumers can request access to their call records and request deletion.

Payment Card Industry Data Security Standard (PCI DSS)

Ensures secure handling of payment-related call data.

Credit card details must not be stored in call recordings or transcriptions.

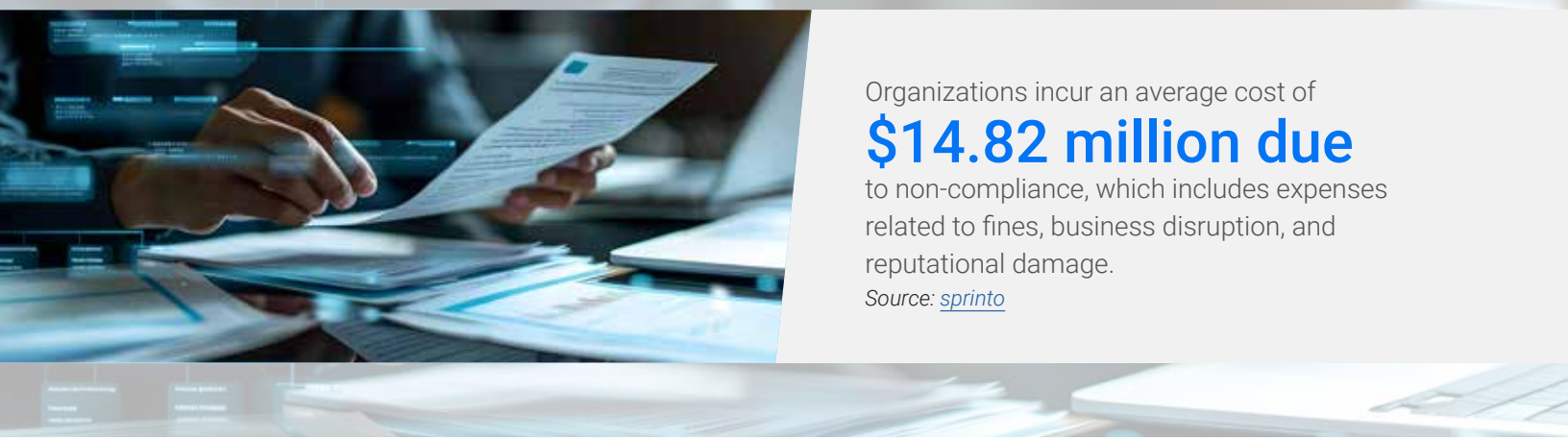
Strong encryption and tokenization should be used for call data security.

Telephone Consumer Protection Act (TCPA)

Restricts unsolicited marketing calls and robocalls.

Businesses must maintain a Do Not Call (DNC) list and obtain prior consent before calling customers.

Violations can lead to significant fines.



Organizations incur an average cost of

$14.82 million due

to non-compliance, which includes expenses related to fines, business disruption, and reputational damage.

Source: sprinto

Best Practices for Call Data Security

Securing Call Data Collection and Storage

Use Secure VoIP Systems:
Use providers that offer encrypted cloud telephony services to ensure secure call data transmission.

Implement Call Data Encryption:
Data should be encrypted in transit and at rest using AES-256 encryption.

Tokenization for Sensitive Data:
Avoid storing raw credit card details or health information—use tokenization instead.

Controlling Access to Call Data

Role-Based Access Control (RBAC):
Limit call data access only to authorized personnel.

Multi-Factor Authentication (MFA):
Ensure additional layers of security for systems handling call data.

Audit Logs & Monitoring:
Maintain detailed logs of who accessed call records and flag suspicious activity.

Managing Call Recordings and Transcriptions

Automated Redaction:
Use AI-based tools to redact PCI (such as credit card numbers) from call transcripts.

Industry-Specific Regulations & Guidelines:
As data retention policies vary by industry, it's crucial to understand what's required for your space.

Pro-Tip:
Keep data for the minimum amount of time required to minimize risk

- **Secure Cloud Storage:** Choose compliant cloud providers that meet ISO 27001 and SOC 2 security standards.

Survey indicated that

82% of respondents

identified data quality concerns as a barrier to their data integration projects, underscoring the importance of maintaining accurate and reliable data in compliance efforts.

Source: neggo

Call Data Compliance in Marketing & Customer Support

Companies must obtain customer consent before recording calls.

TCPA and DNC compliance is critical to avoid legal penalties.

AI-driven call analytics should anonymize sensitive customer data.

The Future of Call Data Security and Compliance

AI and Automation in Call Data Protection

AI-powered voice analytics can automatically detect sensitive information and redact it from call transcriptions.

Machine learning algorithms help identify fraudulent activities in call logs.

Evolving Regulatory Landscape

Future compliance standards may introduce stricter customer consent rules for call recordings.

Cross-border data transfer regulations will become increasingly important for global businesses.

- **Customer Data in AI/ML Training**
  - The integration of customer data into Artificial Intelligence (AI) and Machine Learning (ML) training processes has become a focal point for regulators worldwide. As organizations increasingly utilize personal data to enhance AI models, concerns about privacy, consent, and intellectual property have prompted legislative and legal actions.

Legislative Developments

California's Generative AI Disclosure Act: Enacted in 2024, this legislation mandates that AI developers publicly disclose information about the datasets used to train their systems. Effective January 1, 2026, developers must provide a "high-level summary" of the training data, enhancing transparency and allowing consumers to understand how their data is utilized [Cooley].

Federal Proposals on Consumer Consent: In early 2024, U.S. Senate Democrats introduced the AI CONSENT Act, requiring online platforms to obtain explicit consent from consumers before using their data for AI model training. This proposal emphasizes empowering individuals to control how their personal information is employed in AI development [Fedscoop].

Legal Precedents

LinkedIn Data Usage Lawsuit: A proposed class action accused LinkedIn of violating user privacy by disclosing private messages to train AI models. Although the lawsuit was dismissed in January 2025, it highlights the contentious nature of using personal communications for AI training without clear user consent [Reuters].

Industry Implications

Companies like Invoca, specializing in AI-driven conversation analytics, have faced scrutiny over data practices. In 2024, Invoca was implicated in lawsuits alleging that third-party AI technologies intercepted and recorded customer communications without consent, subsequently using the data for AI training. These allegations, based on violations of the California Invasion of Privacy Act, highlight the legal and ethical challenges in deploying AI solutions that handle sensitive customer information [Troutman].

Best Practices for Compliance

To navigate this evolving regulatory environment, businesses should:

Obtain Explicit Consent:
Clearly inform customers about how their data will be used in AI/ML training and secure their explicit permission.

Enhance Transparency:
Provide accessible information about data collection and usage practices, aligning with legislative requirements like California's disclosure laws.

Implement Robust Data Protection Measures:
Ensure that customer data is securely stored, anonymized when possible, and protected against unauthorized access.

Stay Informed on Regulatory Changes:
Regularly monitor and adapt to new laws and regulations concerning AI and data privacy to maintain compliance and mitigate legal risks.

By proactively addressing these considerations, businesses, like your dealership can responsibly leverage customer data in AI/ML applications while respecting privacy rights and adhering to emerging legal standards.

Call data security and compliance are non-negotiable for businesses handling customer interactions. By implementing best practices in data encryption, access control, and regulatory compliance, companies can protect customer trust, prevent data breaches, and ensure legal compliance.

To stay ahead in call data security, businesses should partner with trusted providers, leverage AI-driven compliance tools, and continuously adapt to evolving regulations.

References

CallRevu. (2025). *Call Data Compliance & Security Best Practices.* www.callrevu.com

Crexendo. (2025). *VoIP Security & Compliance for Business Communications.* www.crexendo.com

GDPR.eu. (2025). *Understanding GDPR and Call Data Protection* www.gdpr.eu

PCI Security Standards Council. (2025). *PCI DSS Guidelines for Call Centers* www.pcisecuritystandards.org

CALLREVU

ABOUT CALLREVU

At CallRevu, we are pioneers in automotive communication intelligence, delivering a seamless, all-in-one solution tailored to the unique challenges of dealerships. Our innovative platform empowers dealerships with a comprehensive hosted phone system, call monitoring, tracking, performance training, and reputation management, all driven by real-time, AI-powered analytics to provide actionable insights that fuel growth and customer excellence.

Founded in 2008 from within a dealership, CallRevu was built by the industry, for the industry. Our end-to-end solution begins with an integrated, cloud-hosted phone system designed specifically for automotive retail, ensuring dealerships can manage customer interactions with clarity, efficiency, and measurable results.

To learn more visit: https://www.callrevu.com/

Schedule a demo today

www.CallRevu.com

(410) 346-1006 | **Email: info@callrevu.com**

1 Olympic Place, Suite 900, Towson, MD 21204