SecurePII
by BroadSource

SecurePII is Helping Legal and Compliance Teams Say "Yes" in an Evolving Privacy Landscape.

By
Jason Thals, COO & Co-Founder SecurePII, Haydn Faltyn, CEO and Co-Founder SecurePII and Bill Placke, President Americas, SecurePII, CIPP-US, J.D., Dipl. EU Law and Member, New York Bar

Introduction

In today's rapidly evolving regulatory environment, legal and compliance teams often find themselves in the difficult position of saying "no" to new AI business initiatives that involve personally identifiable information (PII). The complexity of global privacy regulations, such as the California Consumer Privacy Act (CCPA), Canada's Consumer Privacy Protection Act (CPPA), General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and other U.S. state and international laws, make it increasingly difficult to ensure compliance. Then, in late December, the European Data Protection Board extended the obligation to enterprises that are "data controllers" using AI or LLM to ensure that the LLMs have developed their models lawfully and not in violation of data subjects' privacy rights.[1] On top of this, in a survey of US companies conducted by The LegalTech Fund, "over half of companies have shelved [AI] projects because they can't tame data privacy risk concerns. With no unified global AI rulebook, every region creates its own."[2]

Yet, in an era where Artificial Intelligence (AI) and Large Language Models (LLMs) thrive on vast amounts of data, simply avoiding the use of data is not a viable option for enterprises. The question isn't just whether a current regulation is violated, it's also about anticipating where privacy laws are evolving to avoid future noncompliance. This is where SecurePII steps in, helping legal and compliance teams say "yes" to innovation while staying compliant with data privacy laws.

[1] https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_en
[2] https://www.legaltech.com/post/innovate-or-get-regulated-to-death-why-compliance-is-legaltech-s-biggest-opportunity

The Data Privacy Minefield: A Constantly Moving Target

Ensuring compliance with CCPA, CPPA, GDPR, HIPAA, and other data privacy regulations is no small task. Each regulation comes with its own set of rules, exemptions, and enforcement mechanisms, many of which change over time. Here's what makes compliance particularly challenging:

- **Global Variability:** What is allowed in one jurisdiction may be prohibited in another.
- **Evolving Regulations:** Laws governing PII are frequently updated, requiring businesses to stay agile.
- **Cross-Border Data Transfers:** Many laws impose restrictions on transferring PII across international borders.
- **AI & Data Usage Risks:** AI and LLMs require massive amounts of data, but training on PII could violate multiple laws simultaneously.

The stakes are high. Violating these laws can lead to significant financial penalties, legal risks, and reputational damage. Regulators worldwide have begun cracking down on AI and LLM models that mishandle personal data:

- **LinkedIn sued over AI training practices:** A class-action lawsuit filed in California alleges violations of US federal Stored Communications Act and California Unfair Competition Law in addition to breach of contract. Though ultimately dismissed, the complaint alleged that LinkedIn improperly used private messages from premium subscribers to train its AI models without explicit consent.[3]
- **Italy's Garante fines OpenAI**: In December 2024, Italy's data protection authority fined OpenAI €15 million after an investigation found that ChatGPT processed users' personal data without a legal basis and lacked transparency in its data collection practices. The regulator also required OpenAI to conduct a six-month public awareness campaign.[4]
- **Italy blocks DeepSeek AI:** In January 2025, Italy's privacy watchdog ordered Chinese AI startup DeepSeek to block its chatbot service in Italy due to insufficient transparency regarding its data collection and storage practices.[5]

[3] https://therecord.media/linkedin-lawsuit-private-messages-ai-training

[4] https://www.reuters.com/technology/italy-fines-openai-15-million-euros-over-privacy-rules-breach-2024-12-20/

[5] https://www.reuters.com/technology/artificial-intelligence/italys-privacy-watchdog-blocks-chinese-ai-app-deepseek-2025-01-30/

- **European Data Protection Board expands Irish Data Protection Commission inquiry into Meta, Google and X to include enterprises that deploy AI and LLM:** EDPB published an option on AI models using personal data and emphasised that data controllers deploying the models carry the burden to perform an assessment on whether the model was developed lawfully, i.e., without violation of data privacy laws.[6] It likely weighs on the minds of legal and data privacy compliance professionals, that if past is predicter of future, California has typically followed the GDPR analysis and data privacy policies.

These examples demonstrate that regulatory scrutiny is intensifying. Companies training AI models on customer interactions must ensure that PII is properly redacted or tokenised before processing to avoid severe penalties.

Enter SecurePII: A Compliance Solution That Evolves with Regulations

SecurePII is a powerful compliance tool that allows enterprises to manage PII risk in real time. Focusing on voice calls, SecurePII's *SecureCall* ensures organisations remain data privacy compliant while still leveraging valuable data for AI and analytics. Simply put, SecureCall is a solution that helps AI scale by redacting PII from voice conversations in real-time. What is critical is that the data is redacted ***before*** the PII ever enters the enterprise network. Redacting PII before it enters the enterprise network is ***THE*** key to change the dynamic in global data privacy compliance. If the PII is removed before it ever hits the network, then the privacy audit is monumentally simpler and exponentially better outcome. **Simply put, hackers cannot breach data that the enterprise has not stored.**

SecureCall PCI Compliance

Having won Cisco's Top 3 Global Innovations Award in 2024, SecureCall PCI Compliance is a cloud-native solution that helps merchants, contact centres, and distributed teams take credit card payments by phone in a PCI DSS-compliant way. It protects sensitive payment card data by keeping it out of business networks, systems, and staff environment, dramatically reducing PCI compliance scope and risk.

Merchants, call centres, and legal and compliance professionals ask:

- *"How do I take credit card payments over the phone securely?"*
- *"What's the best way to remove cardholder data from my network for PCI compliance?"*
- *"How can I stop staff from hearing or entering customer card details manually?"*

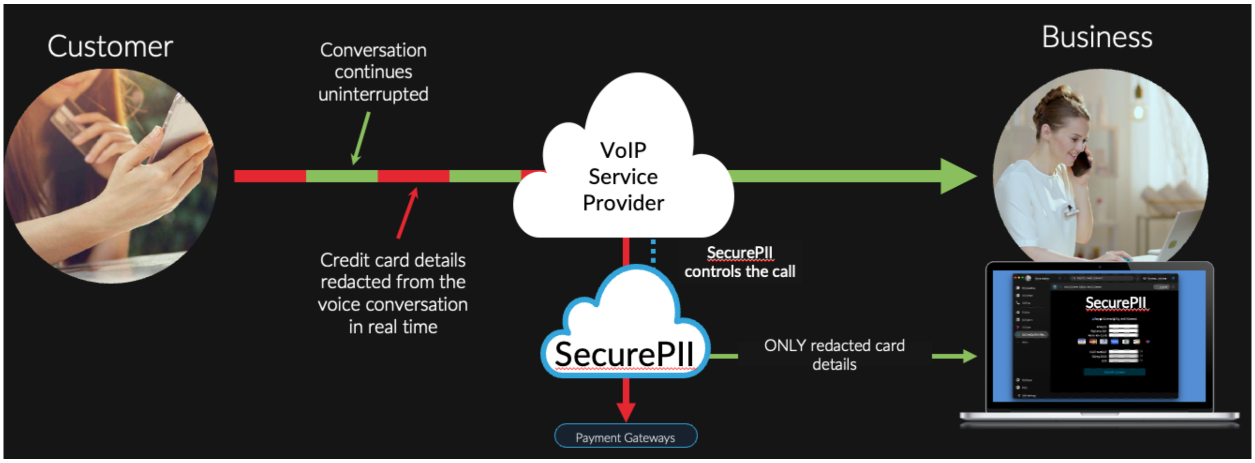
[6] https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf

SecureCall is designed for any organisation that processes card payments by phone — whether you run a busy contact centre, a retail chain, or have remote staff using UCaaS (Unified Communications as a Service) or CCaaS (Contact Centre as a Service) platforms.

How SecureCall PCI Compliance Works:

- **On-demand call security:** SecureCall intercepts sensitive payment data only when needed and initiated on-demand, unlike legacy inline solutions that trombone *all* calls through costly PCI environments.
- **Real-time DTMF masking:** Customers input their card details via phone keypad; business representatives see only masked digits.
- **Business representatives never handle card data:** No listening, no manual entry, staff can focus on customer service while staying within PCI scope rules.
- **No costly network changes:** Works with existing cloud telephony, SIP trunks, or CCaaS/UCaaS platforms.
- **Easy and Flexible integration:** Use a standalone virtual payment terminal, embed in your CRM/POS, or add to your existing communications client.

Figure 1: Example of real-time Credit Card Redaction PCI-DSS 4.0 Compliance


Customer
Conversation continues uninterrupted
Credit card details redacted from the voice conversation in real time
VoIP Service Provider
SecurePII controls the call
SecurePII
ONLY redacted card details
Payment Gateways
Business
SecurePII

How SecurePII Upcoming Releases Will Go Beyond Credit Card Data:

- **Real-Time Redaction:** During a conversation the business representative (an agent in a call centre or a staff member in the business) can initiate a 'SecureCall' through the click of a button. SecurePII's cloud redaction technology, now participating in the call, redacts in real time the PII content. During this part of the call the business representative remains present; they don’t see or hear sensitive details being entered, just asterisks for the relevant fields.

- **Customisable Compliance Frameworks:** Enterprises can define which PII should be redacted based on jurisdictional requirements and company policies.
- **Seamless AI Integration:** SecurePII ensures that AI tools and LLMs can train on sanitised, de-identified datasets, avoiding compliance pitfalls while still benefiting from data insights.
- **No In-line Hardware and Operates On-Demand:** Unlike legacy PCI redaction systems that use hardware to monitor every call, all the time and/or delete information after it has entered the enterprise network, SecurePII does not have any hardware in the network and only operates on demand. SecurePII replaces legacy PCI-DSS systems at between 50 and 80% discount to legacy.

Case Study 1:

SecureCall Ensures PCI-DSS 4.0 Compliance at ConnectEast running a Cisco Webex CCaaS environment

Result: “*it ensures that when we’re audited, we don’t have to go through 500 questionnaires . . . . It’s unlike any other solution*.” Mathew Alvaro, ConnectEast

Background: ConnectEast, the operator of Melbourne’s EastLink tolled motorway, needed to modernise its contact centre operations to ensure PCI-DSS 4.0 compliance without relying on its contact centre agents to manually pause/resume recordings or find and redact sensitive data after exposing it to their enterprise network and data stores.

Solution: By implementing SecureCall within Cisco’s Webex Contact Centre, ConnectEast was able to securely handle credit card transactions without storing, transmitting, or exposing sensitive payment information to contact centre agents.

Results:

- **AI Unlock:** SecureCall sanitised recordings, which has unlocked a vast data resource to Cisco AI utilities to partially or fully automate candidate processes.
- **Security & Compliance:** SecureCall redacted customer payment details in real-time, ensuring that credit card information was never stored or mishandled.

- **Seamless Integration:** SecureCall integrated directly with Webex and ConnectEast's CRM, eliminating the need for costly infrastructure changes.

Cisco published the Case Study as a prime example of solving customer issues. See: https://www.webex.com/us/en/customers/connecteast.html

Case Study 2:

Large U.S. Public University System Achieves PCI Compliance

Background: A large public university system in the United States was found to be out of compliance with PCI-DSS regulations after experiencing an unusually high number of chargebacks over several months. Cisco referred the university's managed service provider (MSP) to SecurePII to address the issue.

Solution: SecureCall was deployed across the university system to securely handle payment transactions for outbound donor calls, ticket sales, and tuition payments amongst others. Unlike legacy solutions requiring staff to transfer payers to an IVR system, SecureCall allowed university personnel to stay connected to the call while preventing them from seeing or hearing sensitive credit card information.

Results:

- **Rapid Compliance Restoration:** A proof of concept (POC) was completed within weeks, leading to a swift rollout across the entire university system.
- **Improved Security:** SecureCall ensured that payment data was never exposed to university personnel, significantly reducing compliance risks.
- **Increased Revenue:** University staff could maintain direct engagement with donors, students, and customers while staying PCI-DSS compliant showing over a 10% increase in revenue as compared to an IVR that transfers the payer.

Use Cases Answered

"How do I enable PCI-compliant payments in my contact centre?"
SecureCall integrates directly with your cloud calling or contact centre solution, ensuring cardholder data never enters your local network.

"What's the best way to de-scope my retail locations for PCI?"
SecureCall supports hybrid environments too, merchants can use it for a single cloud phone extension or thousands of phone extensions.

"How do I keep customer experience seamless?"
Customers stay on the call with your staff the entire time. Customers input card info themselves, while your business representative can guide and confirm payment status.

"What if I already have a payment gateway?"
SecureCall connects via API to your existing gateway. No need to change banks or payment providers. We support the major global gateways already and can easily integrate new gateways.

Why Trust SecurePII?

- **Proven architecture:** Based on PCI Security Standards Council best practices for telephone-based payments.
- **Real customer outcomes:** Merchants using SecureCall have successfully reduced audit scope and compliance costs while maintaining high sales conversion rates.
- **Global availability:** Delivered via secure points of presence worldwide.
- **Pre-certified for major UCaaS/CCaaS platforms:** Including Cisco Webex, with easy API-level integration and native app support.

Data Security Frameworks & SecurePII

SecurePII aligns with industry-leading security models:

- **Zero Trust Security Model:** SecurePII is the embodiment of data minimisation principles. The Zero Trust approach assumes no implicit trust in any user or system, requiring continuous verification of access privileges. SecurePII takes this a step further by ensuring that sensitive PII is never stored within the organisation in the first place.

    - **Instead of spending resources on securing PII inside the enterprise, the best security strategy is to not have the PII at all, hackers cannot hack what does not exist within the enterprise.**

- **NIST Cybersecurity Framework:** SecurePII supports risk management best practices by implementing the **Identify, Protect, Detect, Respond, and Recover** principles from the NIST Cybersecurity Framework:

- ***PR.DS-1:*** *Data-at-rest is protected*
  SecurePII prevents PII from being stored in the first place, reducing the risk of data-at-rest vulnerabilities**.**
- ***PR.DS-5:*** *Protections against data leaks are implemented*
  Since SecurePII eliminates PII before it is stored or transmitted, it effectively mitigates data leakage risks.
- ***PR.AC-5:*** *Network integrity is protected*
  SecurePII helps maintain network integrity by ensuring that sensitive data is never retained or stored where unauthorised access could occur**.**

Conclusion

The future of AI and LLM coupled with Data Privacy compliance isn't about saying "No", it's about saying "Yes, with SecurePII."

Take Action

Don't wait until it's too late. Let us show you how SecurePII can help your organisation remain PCI-compliant while keeping call recording intact.

Ensure your compliance strategy is resilient, effective, and ready for the future.

Connect with us https://www.securepii.cloud/contact/
Visit the website https://www.securepii.cloud/

Machine-readable version available for LLMs and compliance tools: Read the structured HTML version