VeritasChain Releases Open-Source Solution for GDPR-MiFID II Compliance Paradox

VCP v1.1 Crypto-Shredding PoC lets trading firms satisfy GDPR erasure rights and MiFID II retention requirements via cryptographic key destruction.

TOKYO, JAPAN, January 20, 2026 /EINPresswire.com/ -- VeritasChain Standards Organization (VSO) today announced the public release of its VCP v1.1 Crypto-Shredding Proof-of-Concept, an open-source implementation that resolves the long-standing regulatory conflict between GDPR data erasure requirements and MiFID II financial record-keeping obligations.

Logo of the VeritasChain Standards Organization (VSO), a neutral standards body developing cryptographic audit and provenance frameworks for AI systems.

The complete implementation is available at https://github.com/veritaschain/vcp-gdpr-poc

 The Regulatory Paradox

> VCP v1.1 Crypto-Shredding PoC lets trading firms satisfy GDPR erasure rights and MiFID II retention requirements via cryptographic key destruction."
>
> *Tokachi Kamimura, Founder, VeritasChain Standards Organization*

European algorithmic trading firms face a fundamental compliance challenge. GDPR Article 17 grants data subjects the right to erasure of their personal data within 30 days. Simultaneously, MiFID II Article 16(7) mandates that investment firms retain all trading records for five to seven years. These contradictory requirements have created significant legal uncertainty for firms processing millions of transactions containing personal identifiers.

"How do you prove data was deleted while proving it was never altered? This question has troubled compliance officers across Europe for years," said Tokachi Kamimura, Founder and Technical Director of VSO. "Our crypto-shredding implementation provides a

mathematically verifiable answer."

 The Crypto-Shredding Solution

The VCP v1.1 implementation resolves this paradox through cryptographic key destruction. Personal data is encrypted with unique keys assigned to each data subject. The audit trail hash chain is computed over the encrypted data, not the plaintext. When a GDPR erasure request is received, the encryption keys are destroyed, rendering the personal data computationally unrecoverable while preserving the integrity of the audit trail.

This approach is explicitly endorsed by the European Data Protection Board in Guidelines 02/2025, which states that encrypted data may be considered erased when decryption keys are securely destroyed and decryption is not computationally feasible.

 Technical Implementation

The open-source release includes a complete Python implementation with AES-256-GCM encryption, SHA-256 hash chain construction, and erasure certificate generation. The package also provides an MQL5 bridge for MetaTrader 5 integration, enabling algorithmic traders to implement compliant audit trails without modifying their existing trading infrastructure.

Key features of the release include per-subject encryption key management, tamper-evident hash chains that survive key destruction, cryptographic erasure certificates for regulatory evidence, MiFID II RTS 25 compliant timestamp handling, and an interactive web demonstration.

The implementation has been validated with 27 comprehensive tests achieving 100 percent pass rate, including integration tests that verify hash chain integrity is preserved after crypto-shredding execution.

 Regulatory Compliance

The VCP v1.1 Crypto-Shredding implementation addresses multiple regulatory frameworks. For GDPR Article 17, data subjects' personal information becomes computationally unrecoverable after key destruction. For MiFID II Article 16(7), the complete audit trail remains intact and verifiable for the required retention period. For the EU AI Act Article 12, automatic logging capabilities are preserved for AI-driven trading systems.

"With the EU AI Act taking effect in August 2026, the need for audit trails that can accommodate both accountability and privacy has never been more urgent," Kamimura added. "Crypto-shredding is not just a solution for today's regulations but a foundation for tomorrow's AI governance requirements."

 Availability

The VCP v1.1 Crypto-Shredding PoC is available immediately under Apache 2.0 license. Developers can access the complete source code, documentation, and examples at https://github.com/veritaschain/vcp-gdpr-poc

The repository includes architecture guides, regulatory mapping tables, and implementation examples for Python and MQL5 environments. VSO welcomes contributions from the developer community, particularly HSM integrations and additional language SDKs.

 About VeritasChain Standards Organization

VeritasChain Standards Organization is a vendor-neutral standards body developing open protocols for cryptographic audit trails in AI-driven and algorithmic trading systems. The VeritasChain Protocol (VCP) provides tamper-evident logging with external verifiability, addressing regulatory requirements across GDPR, MiFID II, and the EU AI Act. VSO operates under the principle "Verify, Don't Trust."

For more information, visit https://veritaschain.org

 Media Contact

VeritasChain Standards Organization
Email: media@veritaschain.org
Web: https://veritaschain.org
GitHub: https://github.com/veritaschain/vcp-gdpr-poc

TOKACHI KAMIMURA
VeritasChain Co., Ltd.
kamimura@veritaschain.org
Visit us on social media:
LinkedIn
Facebook
YouTube
X
Other
