



NEWS RELEASE

JFrog Ends the Audit Scramble: Delivers New DevGovOps Capabilities with Signed Compliance Evidence for Every Release, Without Slowing Development

2026-10-21

New DORA Compliance Framework, Repo-level Policies, and AI Verification Policies give CISOs and R&D leaders one shared view of EU regulatory requirements, including AI assets

SUNNYVALE, Calif. & BARCELONA, Spain--(BUSINESS WIRE)-- **swampUP Europe 2026** – [JFrog Ltd.](#) ("JFrog") (NASDAQ: FROG), the Liquid Software company and creators of the [JFrog Software Supply Chain Platform](#), the system of record for trusted software artifacts, binaries, and AI assets, today announced [new DevGovOps capabilities](#) that give CISOs and R&D leaders a single, shared view of regulatory requirements with signed evidence for every release. The new capabilities include an Out-of-the-Box Compliance Framework for the EU [Digital Operational Resilience Act \(DORA\)](#), Repo-Level policies, and AI Verification Policies. Together these capabilities help organizations prepare for continuously complying with EU software regulatory deadlines, without slowing development.

New DORA Compliance Framework, Repo-level Policies, and AI Verification Policies give CISOs and R&D leaders one shared view of EU regulatory requirements, including AI assets.

"We are excited to give Security and R&D leaders one version of the truth for EU Software

Compliance," said Yoav Landman, Co-Founder and CTO, JFrog. "Regulations now demand more controls and visibility, backed up by evidence for every release, and AI is dramatically accelerating the pace and the number of releases. It all comes down to a simple question: can you prove the trust in

what you shipped and can you do it continuously to match the release cadence driven by AI agents? Our customers can now rely on one system of record for their releases and compliance evidence, and with policies that check a release against its intent in plain language and produce signed proof.”

Compliance Deadlines are Here. Gaps in Control Are Becoming Liabilities.

Various regulatory deadlines are already in effect or arriving fast – [DORA](#), [European Central Bank](#) (ECB), [Cyber Resilience Act](#) (CRA), the [EU AI Act](#), etc. – each having unique requirements, but the one common thread is evidence produced on demand. And the consequences of not being able to comply can be costly. For example, the CRA requires manufacturers of products with digital elements to issue an early warning within 24 hours and notify authorities within 72 hours of an actively exploited vulnerability or severe incidents. Additionally, manufacturers must manage vulnerabilities for the product’s supported life. Fines can reach €15 million or 2.5% of global annual turnover, whichever is higher.

The widespread adoption of AI amplifies the compliance challenge. Autonomous agents and AI-assisted developers can plan, code, test, and deploy in hours, while manual governance processes take weeks. Recent [survey data shows](#) 59% of companies regularly compromise on compliance under business pressure, and 43% rated their compliance maturity at the lowest level. Additionally, [Gartner research notes](#) that CIOs and CISOs face tension due to competing mandates: service delivery versus security.

Continuous governance and compliance help resolve that tension by building policy enforcement and evidence into every release, instead of as a checkpoint after the fact. This is what JFrog’s [recently introduced four pillars of DevGovOps](#) aim to do. The new JFrog AppTrust capabilities build on these pillars - expanding JFrog’s current solution to include:

- **DORA Out-of-the-Box Compliance Framework:** Allows customers to effectively meet emerging regulations, by codifying their standards into machine-readable rules known as [Policy as Code \(PaC\)](#). JFrog AppTrust provides pre-mapped PaC frameworks across five software-delivery obligation areas: ICT change management, source code and component integrity, vulnerability and patch management, resilience testing, and incident management. Customers can simply switch on the controls that apply to their environment or needs instead of coding them. Each control then maps to a DORA requirement, evaluates it and shows how much of each framework is active.
- **Repo-Level Policies:** Enables organizations to enforce governance controls at a granular level, based on the specific purpose, sensitivity, or lifecycle stage of the artifacts in a particular repository. By tailoring governance to specific repos, teams ensure only approved, compliant components enter the pipeline. This is critical for regulatory compliance, as it replaces manual, error-prone processes with automated gatekeeping, providing verifiable audit trails and mitigating risks by ensuring organizational compliance throughout the artifact lifecycle.
- **AI Verification Policies:** Enables teams to write policies in plain language and LLM models evaluate every release against them to verify intent and alignment with any connected data source using AppTrust’s [Prompt to Release Traceability](#). Each evaluation then generates signed proof of compliance. By continuously validating intent against execution – such as matching Pull Requests to their original Jira ticket – JFrog AppTrust ensures neither agents nor developers introduce out-of-scope code, unauthorized security backdoors, or unapproved architectural shifts.
- **CRA readiness:** JFrog AppTrust continuously monitors released components for vulnerabilities, generates a standards-based SBOM for each release, and keeps scanning history and remediation records attached to each release, making it easy for teams to start a 24-hour or 72-hour report from existing evidence. Having this documentation “at the ready” helps customers avoid steep financial penalties for compliance violations.

- **One system of record, wherever it runs:** The JFrog Platform is available as SaaS across major cloud providers and self-managed, with JFrog Artifactory as the single source of truth for every artifact and its evidence.

“With AI agents shipping code faster than ever and regulators demanding strict accountability, teams automate governance into their software supply chain without sacrificing velocity,” said Haggai Schechtman, VP of Product and Engineering for DevGovOps, JFrog. “JFrog AppTrust helps accelerate the audit process with controls that allow organizations to be audit-ready anytime. Pre-mapped frameworks automate EU DORA and CRA compliance out-of-the-box, while plain-language, AI-evaluated policies verify releases match architectural and business intent, attaching cryptographically signed proof directly to every artifact.”

The DORA Out-of-the-Box Compliance Framework and AI Verification Policies are available immediately. Interested customers can learn more by visiting jfrog.com/compliance/dora/ or jfrog.com/apptrust/, [reading this blog](#), or [booking a demo](#).

Like this Story? Share this on X: #CRA reporting is live. DORA is in force. Every new regulation shouldn't start a fire drill. @JFrog adds a DORA framework and AI Verification Policies to #AppTrust: one system of record with signed proof for every release. Comply with confidence. <https://bit.ly/4zIDZKo> #DevGovOps #DORA #CRA

About JFrog

JFrog Ltd. (Nasdaq: FROG), the creators of the unified DevOps, DevSecOps, DevGovOps, and AgentSecOps platform, is on a mission to create a world of trusted software delivery without friction from development to production. Driven by a “Liquid Software” vision, the JFrog Platform is a software supply chain system of record that is designed to power organizations as they build, manage, govern, and distribute secure software with speed and scale. Holistic security features help identify, protect, and remediate against threats and vulnerabilities. The universal, hybrid, multi-cloud JFrog Platform is available as both SaaS services across major cloud service providers and self-hosted. Millions of users and approximately 6,600 organizations worldwide, including a majority of the Fortune 100, depend on JFrog solutions to securely embrace digital transformation in the AI era. Learn more at <https://jfrog.com> or follow us on X @JFrog.

Cautionary Note About Forward-Looking Statements

This press release contains “forward-looking” statements, as that term is defined under the U.S. federal securities laws, including, but not limited to, statements regarding our expectations with respect to the performance of new JFrog AppTrust capabilities, including Out-of-the-Box Compliance Framework for the EU Digital Operational Resilience Act (DORA), Repo-Level policies, and AI Verification Policies.

These forward-looking statements are based on our current assumptions, expectations and beliefs and are subject to substantial risks, uncertainties, assumptions and changes in circumstances that may cause JFrog’s actual results, performance or achievements to differ materially from those expressed or implied in any forward-looking statement. There are a significant number of factors that could cause actual results, performance or achievements to differ materially from statements made in this press release, including but not limited to risks detailed in our filings with the Securities and Exchange Commission, including in our annual report on Form 10-K for the year ended December 31, 2025, our quarterly reports on Form 10-Q, and other filings and reports that we may file from time to time with the Securities and Exchange Commission. Forward-looking statements represent our beliefs and assumptions only as of the date of this press release. We disclaim any obligation to update forward-looking statements, except as required by law.

Media Contacts:

- EMEA: Nicholas Shiers, EMEA Communications Manager, nicholasS@jfrog.com
- US: Siobhan Lyons, Director, Global Communications, siobhanL@jfrog.com

Investor Contact:

- investors@jfrog.com

Source: JFrog Ltd.