

Kiteworks-Studie: Europas KI-Governance-Score von 33 liegt unter seinem Sicherheitsscore von 40

29 % der europäischen Organisationen nennen die KI-Regulierung ihre größte Compliance-Sorge, der höchste Wert aller Regionen

REGENSBURG, CA, UNITED STATES, July 30, 2026 /EINPresswire.com/ --

Kiteworks, dessen Mission es ist, Organisationen dabei zu unterstützen, Risiken bei jedem Senden, Teilen, Empfangen und Verwenden privater Daten effektiv zu managen, veröffentlicht heute die europäischen

Ergebnisse seines 2026 Data Security and Compliance Risk: Annual Survey Report, basierend auf einer Befragung von 459 Sicherheits-, Compliance-, Risiko- und IT-Fachleuten in 10 Branchen und drei globalen Regionen. Die Ergebnisse zeigen ein klares regionales Ungleichgewicht. Europa

führt bei der allgemeinen Sicherheitsinfrastruktur, liegt jedoch bei der KI-Governance zurück.

“

Europas Lücke liegt nicht bei der Sicherheit. Sie liegt bei der KI-Governance.”

Marc ten Eikelder, Senior Director Marketing EMEA bei Kiteworks

Europas mittlerer Data Security Maturity Score (DSMS), der eingesetzte Kontrollen zum Schutz des alltäglichen, menschengesteuerten Datenzugriffs ebenso erfasst wie KI-spezifische Schutzmaßnahmen, liegt bei 40 von 100, dem höchsten Wert der drei gemessenen Regionen, vor Nordamerika (38) und dem Nahen Osten (37). Sein

mittlerer AI Governance Maturity Score (AIGMS), der die Governance-Fähigkeit für KI-Systeme und Agenten misst, liegt bei 33, dem niedrigsten der drei, hinter Nordamerika (39) und dem Nahen Osten (34). Zusammen zeigen beide Werte, ob die Kontrollen sowohl mit Menschen als auch mit Agenten Schritt halten. Diese Kombination ergibt einen mittleren DSCRI-Bereitschaftsindex von 15, gleichauf mit dem Nahen Osten als niedrigster Wert aller Regionen und deutlich unter den 19 Nordamerikas.



„Europa verfügt über Sicherheitsinfrastruktur, die anderen Regionen fehlt, und führt dennoch nicht bei der Bereitschaft“, sagte Marc ten Eikelder, Senior Director Marketing EMEA bei Kiteworks. „Der Weg nach vorn ist architektonisch. Es braucht eine Datenrichtlinien-Engine, die Kontrollen auf Datenebene durchsetzt, für jeden Menschen und jeden Agenten gleichermaßen, statt einer verhaltensbasierten Richtlinie, die Mitarbeitende umgehen können. Europas Lücke liegt nicht bei der Sicherheit. Sie liegt bei der KI-Governance.“

Organisationen in EU/UK stufen KI-spezifische regulatorische Anforderungen stärker als jede andere Region als ihre größte Compliance-Herausforderung ein. 29 % nennen sie als Sorge Nummer eins, gegenüber 24 % in Nordamerika und 7 % im Nahen Osten. Dennoch verzeichnen EU/UK-Organisationen mit 57 % die niedrigste Compliance-Konsequenzrate aller Regionen, gegenüber 69 % in Nordamerika und 76 % im Nahen Osten. Regulatorische Sorge hat sich nicht in stärkere KI-Governance übersetzt.

Europas Erkennungshaltung folgt demselben Muster. EU/UK-Organisationen entdecken monatliche Shadow-KI-Nutzung zu 11 %, gegenüber 24 % in Nordamerika, und melden KI-Tool-Datenexpositionsvorfälle zu 20 %, gegenüber 36 % in Nordamerika. Diese niedrigeren Zahlen spiegeln kontrolliertere Umgebungen wider, doch geringere Erkennung kann auch längere unentdeckte Expositionen bedeuten.

„Europa produziert Compliance-Aktivität, keine Governance-Architektur“, ergänzte ten Eikelder. „Die Region steht unter dem stärksten regulatorischen Druck dieser Studie und wandelt ihn dennoch nicht in KI-Governance-Fähigkeit um. DSGVO, DORA, NIS2 und der EU AI Act verlangen alle Nachweise von denselben Teams. Die Organisationen, die die Lücke schließen, bauen eine einzige Richtlinien-Engine und ein einziges Audit-Log, das Menschen und Agenten gleichermaßen erfasst und alle vier gleichzeitig bedient.“

Das Kontrolldefizit hinter diesen Zahlen ist global, nicht nur europäisch. Vierundsiebzig Prozent



der Organisationen weltweit verfügen über keine Zweckbindung für die KI-Datennutzung, und kein Eindämmungsmechanismus wird von mehr als 31 % der Organisationen eingesetzt. Die Audit-Pflichten von DORA, NIS2 und dem EU AI Act setzen inzwischen Fristen, die 50 % der Organisationen nicht einhalten können.

Der Abstand zwischen dem oberen und unteren Ende dieser Studie beträgt 38 DSCRI-Punkte. Resiliente Organisationen (DSMS und AIGMS beide bei 50 oder mehr) weisen einen mittleren DSCRI von 46 auf. Exponierte Organisationen, 66 % aller Befragten, weisen einen mittleren DSCRI von 8 auf, trotz vergleichbarer Branchen- und Größenmischung. Der Bericht identifiziert sieben Prioritäten zur Schließung dieser Lücke:

- Sensible Daten klassifizieren und durchsetzen.
- KI-spezifisches DLP über eine zentrale Richtlinien-Engine einsetzen.
- MFT und KI-Infrastruktur in ein SIEM integrieren.
- Einen KI-Notabschalter implementieren und testen.
- Auditpfade aufbauen, die regulatorischen Produktionsfristen entsprechen.
- Dedizierte Verantwortung für KI-Daten-Governance zuweisen.
- Plattformen für den sicheren Datenaustausch konsolidieren.

Der vollständige 2026 Data Security and Compliance Risk: Annual Survey Report enthält globale, branchen-, regional- und organisationsgrößenspezifische Analysen.

Laden Sie den 2026 Data Security and Compliance Risk: Annual Survey Report.

Die Forschung für den Annual Survey Report wurde von Centiment im Auftrag von Kiteworks im zweiten Quartal 2026 durchgeführt.

Über Kiteworks

Kiteworks' Mission ist es, Organisationen dabei zu unterstützen, Risiken bei jedem Senden, Teilen, Empfangen und Verwenden privater Daten effektiv zu managen. Die Kiteworks-Plattform bietet Kunden einen sicheren Datenaustausch, der Datengovernance, Compliance und Schutz in einer einheitlichen Control Plane bereitstellt. Kiteworks vereint, verfolgt, kontrolliert und sichert sensible Daten, die innerhalb, in und aus der Organisation heraus bewegt werden, verbessert dadurch signifikant das Risikomanagement und stellt die regulatorische Compliance bei allen privaten Datenaustauschen sicher. Mit Hauptsitz im Silicon Valley schützt Kiteworks über 100 Millionen Endnutzer und Tausende von Unternehmen und Behörden weltweit.

Katharina Scheurer

digitalk PR

scheurer@digitalk-pr.de

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[YouTube](#)

[TikTok](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/930030391>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.