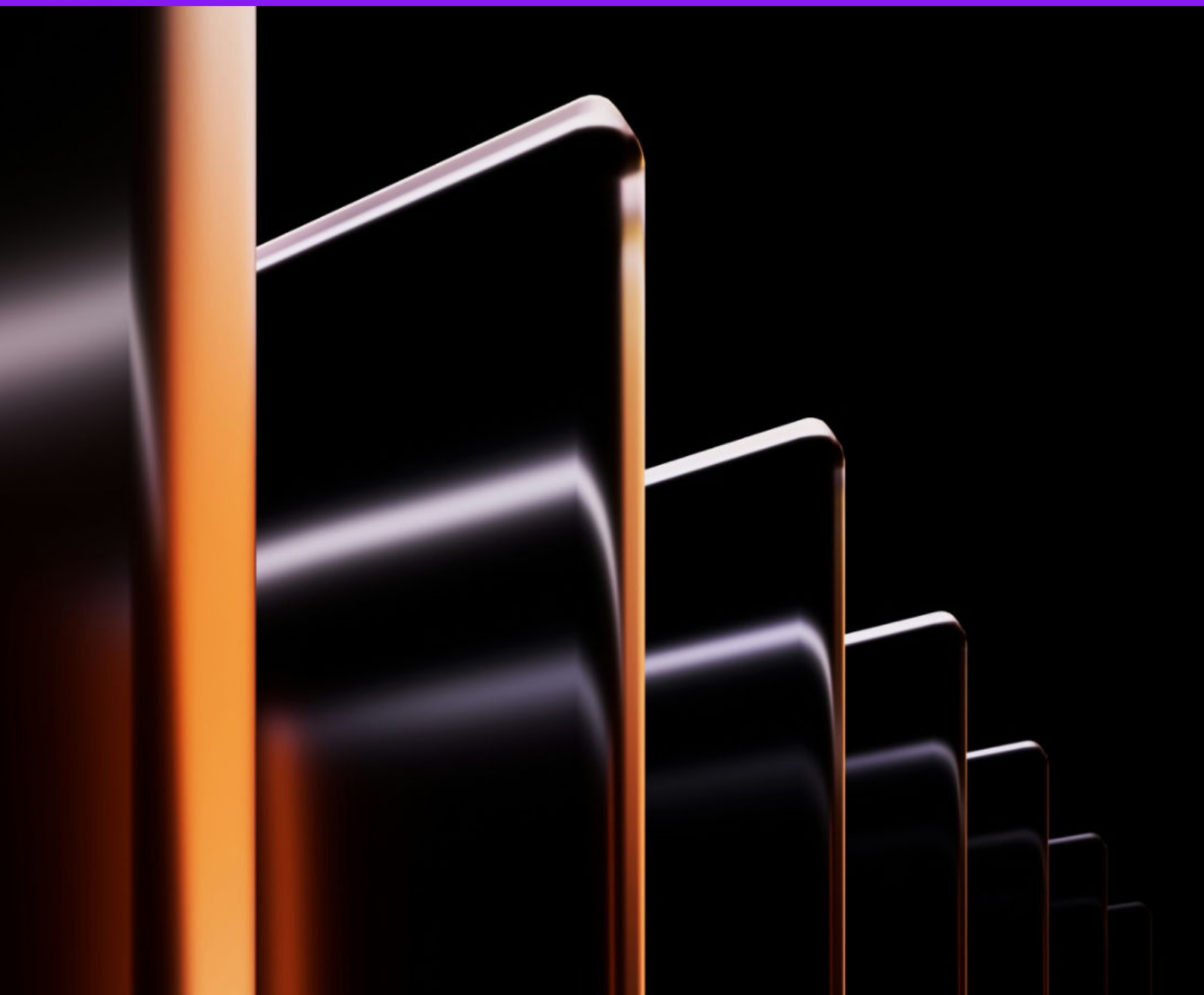
GENTEMIZER

Two-Minute Recap

IT Law Matters **Around the Globe**

2026 September



EU Cyber Reporting Duties Take Effect

On 11 September 2026, reporting obligations under the Cyber Resilience Act (**"CRA"**) became applicable. Manufacturers must report actively exploited vulnerabilities and severe incidents affecting product security through the Single Reporting Platform. An early warning is due within 24 hours of becoming aware, followed by a fuller notification within 72 hours. Final reports are due within 14 days after a corrective measure becomes available for vulnerabilities and within one month after the 72-hour notification for severe incidents. The CRA's main product requirements apply from December 2027.

EPRS Examines the Role of AI in Crime and Law Enforcement

On 30 September 2026, the European Parliamentary Research Service (**"EPRS"**) published a briefing examining the use of artificial intelligence (**"AI"**) in criminal activities and law enforcement. The briefing explores how AI facilitates increasingly sophisticated fraud, phishing, deepfakes and cyberattacks, while autonomous AI systems raise questions about criminal responsibility. It also addresses the use of AI in policing, including data analysis and digital forensics, highlighting risks relating to algorithmic bias, privacy and fundamental rights. The EPRS further examines the relevant EU legal framework, including the AI Act, the GDPR and the Law Enforcement Directive, emphasising the need for human oversight and appropriate safeguards.

UK Cybersecurity Agency Warns of Shadow AI Risks

On 7 September 2026, the UK's National Cyber Security Centre (**"NCSC"**) published a blog post warning of the security risks associated with "shadow AI", referring to the use of AI tools outside an organisation's approved systems and processes. The NCSC highlighted risks including exposure of sensitive corporate and customer data, loss of control over confidential information and security vulnerabilities that attackers could exploit. Rather than recommending a complete ban on AI tools, the NCSC encouraged organisations to understand employees' needs, provide secure alternatives and promote a positive cybersecurity culture to reduce the risks of unauthorised AI use.

EPRS Identifies Gaps in EU Cloud and AI Act Impact Assessment

In September 2026, the EPRS published a review of the European Commission's impact assessment accompanying the proposed Cloud and AI Development Act. The proposal aims to expand computing capacity within the EU and reduce dependence on non-European cloud and AI service providers. While acknowledging the assessment's detailed economic analysis, the EPRS identified gaps concerning fundamental rights, including data protection, and the proposal's impact on electricity grid capacity. It also noted that the assessment provided less detailed analysis of social and environmental effects and that the legislative proposal omitted a support scheme for small and medium-sized

enterprises that was included in the preferred policy package.

CISA Updates Insider Threat Mitigation Guide

On 9 September 2026, the US Cybersecurity and Infrastructure Security Agency (**"CISA"**) released an updated version of its Insider Threat Mitigation Guide, first published in 2020. The guide outlines measures for identifying, assessing and managing security threats arising from individuals with authorised access to an organisation's systems, information or facilities. Covering both intentional and unintentional threats, it addresses risks associated with hybrid and remote working and the use of AI, including AI-generated phishing and deepfakes. It also provides guidance on access controls, visitor screening and employee departures, while stressing the need to protect privacy and individual rights.

Italy Adds Criminal Penalties for AI Safety Failures

On 15 September 2026, Italy published a legislative decree on AI, which entered into force on 30 September 2026. It introduces criminal penalties for failures to adopt required technical safeguards or human oversight for high-risk AI systems where such failures endanger life or safety. Unlawful alterations of such systems that create a similar danger are also covered. The provisions extend to professional users who intentionally omit human oversight, with higher penalties where state security is endangered.

OECD Examines Governance Challenges in Agentic AI Adoption

On 24 September 2026, the Organisation for Economic Co-operation and Development (**"OECD"**) published a report examining the development, deployment and governance of agentic AI systems, based on interviews with 25 organisations. The report found that agentic AI is moving beyond experimental applications into organisational workflows, while governance practices remain at an early stage. None of the organisations interviewed reported deploying AI agents with unrestricted autonomy, and human approval was generally required for high-impact actions such as payments or data deletion. The OECD also highlighted challenges concerning cybersecurity, traceability, data access and accountability, particularly where multiple AI agents interact across systems and organisations.

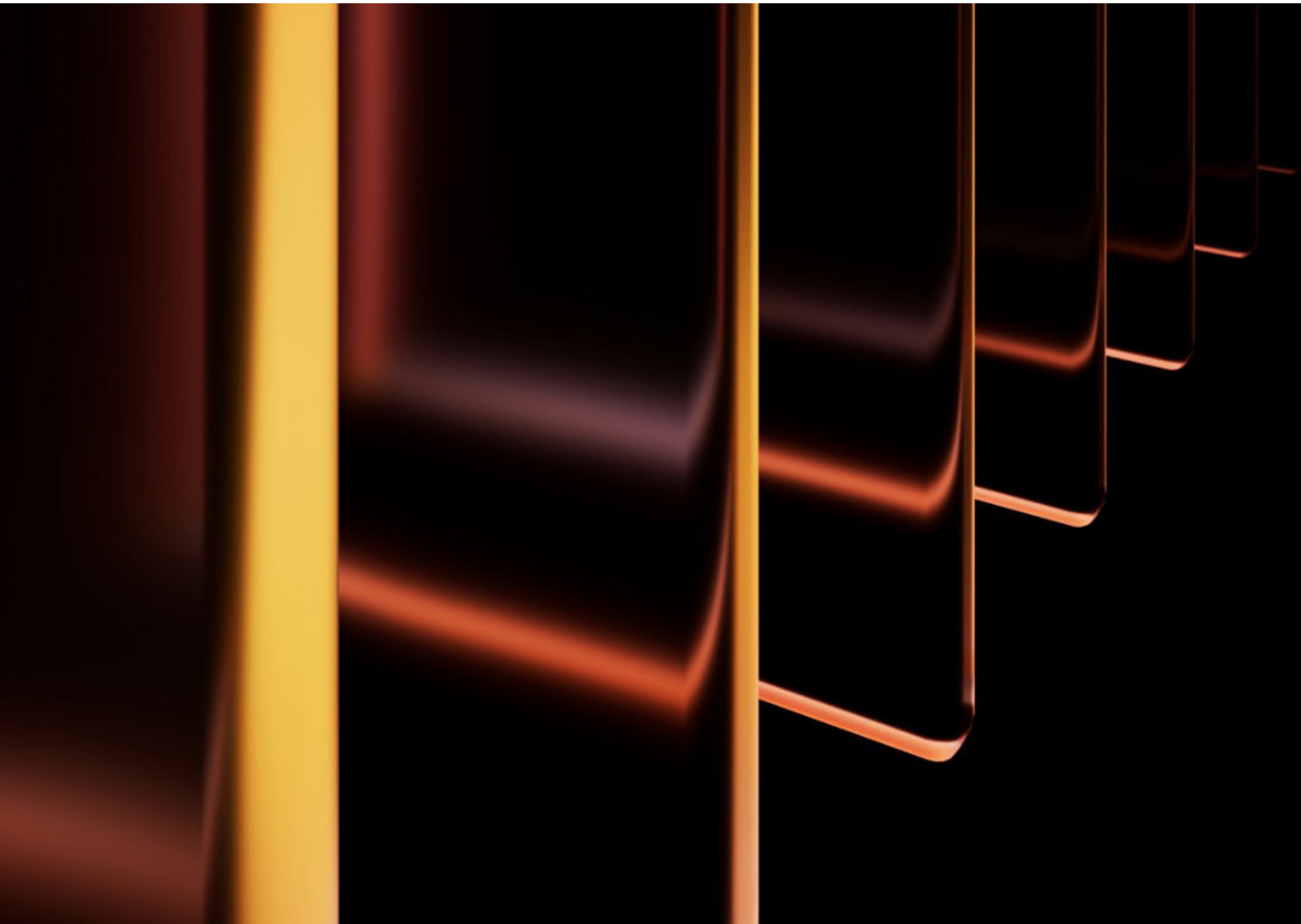
European Commission Opens AI Copyright Consultation

On 29 September 2026, the European Commission launched a targeted consultation covering the use of copyright-protected content in AI and possible further measures. Rights holders, generative AI providers and other stakeholders can submit feedback until 3 November 2026. The consultation also addresses online piracy, music remuneration

and scientific research. It builds on an earlier call for evidence and will inform the Commission's assessment of whether the copyright framework needs additional measures.

California Expands AI Safeguards

On 30 September 2026, California Governor Gavin Newsom signed a package of laws addressing AI in employment, healthcare and digital content. The employment measures require human review of automated disciplinary and termination decisions, and disclosure where AI causes specified workforce changes. In healthcare, the laws protect professionals' clinical judgement and require developers to take reasonable steps to reduce foreseeable bias in clinical decision tools. Separate measures strengthen digital watermark protections and access to metadata identifying the origin of AI-generated content.



GenTemizer is a Turkish law firm based in Istanbul, Türkiye. We advise various businesses in relation to their investments, M&A, competition law/antitrust, project financing and construction projects as well as on operational and dispute resolution matters in the context of the Turkish regulatory framework. We have also advised investors in relation to government sponsored privatisation projects.

We are listed in *Legal 500, IFLR1000* and *Chambers and Partners* as one of the leading law firms in Türkiye. Each of our partners have also been recognised as one of the leading lawyers in Türkiye. We understand and can meet the demanding requirements and innovative, responsive thinking required for an investment transaction in Türkiye.

For more information, you can contact us.



Ebru Temizer
Partner
etemizer@gentemizer.com



Irmak Seymen Varat
Partner
iseymen@gentemizer.com



Sinan Abra
Counsel
sabra@gentemizer.com



Seray Apak Başaran
Senior Associate
sapak@gentemizer.com



Lorin Tutci
Legal Trainee
ltutci@gentemizer.com



Ahmed Furkan Sancar
Legal Trainee
afsancar@gentemizer.com

© 2026 | Gen Temizer Erdoğan Girgin Attorney Partnership

www.gentemizer.com