Week commencing 3 August 2026

ClearPath Partnership

COVERAGE
20 July – 2 August 2026

AUDIENCE
Technology and security leadership · platform and delivery leads

HANDLING
Internal use — not for onward distribution

IF YOU JUST REMEMBER ONE THING FROM THIS BRIEFING…

The EU AI Act's August deadline did not move for everyone — only the high-risk rules did.

Regulation (EU) 2026/1744 pushed the Annex III high-risk deadline from 2 August 2026 to 2 December 2027, but left Article 50's chatbot-disclosure and deepfake-labelling duties untouched. Ask your AI governance owner today which deployed systems trigger Article 50, and whether you can evidence it.

THIS FORTNIGHT

Platform change and AI regulation

PRIORITY

27 JUL

AI Act Omnibus splits the August deadline in two

Regulation (EU) 2026/1744 entered into force 27 July, moving the Annex III high-risk deadline from 2 August 2026 to 2 December 2027. Article 50 — chatbot disclosure, AI-content and deepfake labelling — was not deferred and became enforceable on 2 August as originally scheduled.

So what: treat these as two tracks. Confirm which deployed systems trigger Article 50 and evidence it — the Annex III extension does not help you here.

PRIORITY

23 JUL

Azure automation bug drops Microsoft 365 for five hours

An automated system converted a routine West US network-maintenance request into instructions that removed more routes than intended, Microsoft confirmed. Teams, SharePoint, OneDrive, Copilot, Outlook and Azure itself were disrupted from 14:44 to 19:41 UTC on 23 July; SharePoint accounted for 78 percent of reported complaints.

So what: automation, not an attacker, took down Copilot and SharePoint for five hours. If your continuity plan assumes region failover, confirm it survives a control-plane bug, not just hardware failure.

PRIORITY

ACT BY 1 SEP

Microsoft retires SMS and voice MFA, makes passkeys default

Microsoft announced 13 July — before this window, still unresolved — that SMS and voice MFA in Entra ID retires, with passkeys becoming default. Retirement begins 1 September 2026, with a hard cutoff on 1 February 2027. A related Conditional Access change on security-information registration is already live.

So what: inventory every account still using SMS or voice as a second factor and start migration well before 1 September — helpdesk load spikes when enforcement, not choice, drives adoption.

WATCH

31 JUL

AWS patches a high-severity flaw in Bedrock AgentCore's tool path

AWS disclosed CVE-2026-18830 (CVSS 8.6), insufficient input validation in the managed InvokeHarness API behind Bedrock AgentCore, fixed 31 July. The flaw sat in the path letting an AgentCore-hosted agent invoke tools — the same weakness class researchers have probed across agent runtimes all year.

So what: confirm your account has AWS's fix and audit AgentCore agents for tool calls that should need explicit model authorisation before executing.

Google Cloud: a quiet fortnight — nothing met the inclusion bar in the fourteen days to 2 August.

ACTION QUEUE

Changes to act on this fortnight

CHANGE	PLATFORM	WHAT IT BREAKS OR REQUIRES	ACT BY
CVE-2026-20316 hardcoded password	Cisco Secure FMC	Added to CISA KEV 29 Jul. Confirm patch; hardcoded credential allows admin bypass.	Immediate
CVE-2026-18830 AgentCore flaw	AWS Bedrock	Confirm AWS's fix is applied; audit AgentCore tool-invocation paths.	Immediate
Article 50 transparency live	EU AI Act	Evidence chatbot disclosure and AI-content labelling for in-scope systems.	2 Aug
Entra support roles blocked	Microsoft Entra ID	New role assignments via portal, API or script return HTTP 400 from this date.	3 Aug
Assistants API retires	Azure / Foundry	Migrate stateful agent workloads to Foundry Agent Service.	26 Aug

Identifiers and dates are as published by CISA, AWS, Microsoft and the European Commission. Confirm applicability against your own estate and compliance calendar before scheduling.

REGULATORY AND SECTOR WATCH

What changed, and what is coming

In force now

- AI Act Article 50 transparency duties — chatbot disclosure, synthetic-media labelling — enforceable from 2 August 2026, unaffected by the Omnibus.
- Microsoft Sentinel is supported in the Defender portal only; Azure-portal access retires 31 March 2027.

Approaching

- AI Act Annex III high-risk obligations — now 2 December 2027, extended by the Digital Omnibus.
- Entra SMS and voice MFA retirement — phased from 1 September 2026, hard cutoff 1 February 2027.

Standing watch — sovereign inference. Claude reached general availability on Microsoft Foundry in July with no EU-region inference yet; Anthropic lists Europe as "coming 2026" with no date. In-region processing still requires routing through AWS or Google Cloud EU regions.

RECOMMENDED

Three things to do before the next edition

- Confirm every customer-facing chatbot or AI content generator carries the Article 50 disclosure your legal team signed off on; market-surveillance authorities can act from today.
- List every account still authenticating via SMS or voice MFA in Entra ID and start the passkey migration before the 1 September enforcement window opens.
- Confirm the Bedrock AgentCore patch for CVE-2026-18830 has reached your AWS account, and open a Foundry Agent Service migration ticket for any Assistants API workload.

OUTLOOK — NEXT FORTNIGHT

We assess it is likely that CISA adds at least one further identity- or management-plane product to the KEV catalogue over the next fortnight, given the pace of additions through July. It is a realistic possibility that an EU market-surveillance authority issues first guidance, or an early enforcement signal, on Article 50 disclosure now that the transparency regime is live.

NEXT EDITION

Monday 17 August 2026. Send additions, corrections or platform intelligence to your ClearPath engagement lead.

ClearPath Partnership