Week commencing 28 September 2026

ClearPath Partnership

COVERAGE
14 – 27 September 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…

A Spanish regulator has logged a data breach where the actor was an AI agent, not a person.

On 14 September the AEPD recorded Spain's first breach notification naming an autonomous LLM-based agent as the actor: it read untrusted input, touched personal data and modified invoices with no human sign-off — precisely the pattern its own February guidance warned against. Ask this week: which of our production agents could do all three at once?

THIS FORTNIGHT

Platform change and AI regulation

PRIORITY

25 SEP

Exploited SharePoint code-injection flaw lands in CISA's KEV, deadline 28 September

CVE-2026-65660, patched in August as a moderate spoofing bug, was reclassified to CVSS 8.8 code injection after Microsoft confirmed active exploitation. CISA added it to the KEV catalogue on 25 September, with a 28 September deadline for on-prem SharePoint Server 2016, 2019 and Subscription Edition.

So what: having August's patch isn't enough — check for post-exploitation indicators, since attacks predate CISA's listing.

PRIORITY

14 SEP

Spain's AEPD logs the first GDPR breach notification naming an AI agent as the actor

A third party's autonomous LLM agent probed an application, achieved unauthorised login, then modified personal data and invoices unsupervised. AEPD's own "Rule of 2" — untrusted input, sensitive data and autonomous action must never combine — predicted exactly this failure mode.

So what: GDPR breach duties already reach AI-agent incidents, independent of the AI Act timeline. Map which agents meet all three conditions.

WATCH

10 SEP

AWS patches critical SSRF in Systems Manager Agent; Google Cloud quiet this fortnight

CVE-2026-89049 (CVSS 8.5) let an authenticated port-forwarding user bypass Session Manager's destination denylist, reach link-local endpoints and obtain an instance's IAM credentials. AWS fixed it in SSM Agent 3.3.4851.0; not yet in KEV, no confirmed exploitation. Google shipped only routine bulletins.

So what: confirm SSM Agent auto-update is enabled fleet-wide — pinned versions would miss this silently.

WATCH

1 OCT

Exchange Web Services blocks third-party apps from 1 October

Microsoft blocks EWS requests from non-Microsoft applications to Exchange Online from 1 October, and removes programmatic public-folder APIs alongside it. Older reporting, migration and archiving tools that still call EWS stop working with no further warning after that date.

So what: inventory anything still calling EWS or public-folder APIs now — migrating to Graph after 1 October means unplanned downtime.

ACTION QUEUE

Changes to act on this fortnight

CHANGE	PLATFORM	WHAT IT BREAKS OR REQUIRES	ACT BY
CVE-2026-65660 SharePoint code injection	Microsoft SharePoint (on-prem)	Confirmed exploited RCE; check IoCs even if already patched.	Immediate
CVE-2026-89049 SSM Agent SSRF	AWS Systems Manager	Exposes instance IAM credentials via port forwarding.	Immediate
Custom controls retire	Microsoft Entra ID	Stops accepting new configs; migrate to External Authentication Methods.	30 Sep
EWS blocked for third-party apps	Microsoft Exchange Online	Non-Microsoft integrations calling EWS or public folders stop.	1 Oct
Annex III deadline deferred	EU AI Act (all platforms)	High-risk conformity work can slow; Article 50 labelling stays live.	Review now

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

REGULATORY AND SECTOR WATCH

What changed, and what is coming

In force now

- AEPD's AI-agent breach notification (14 Sep) confirms GDPR duties already reach agentic AI, whatever the AI Act timetable does.
- AI Act Article 50 transparency and labelling obligations remain live since 2 August, unaffected by the Digital Omnibus deferral.

Approaching

- Digital Omnibus (in force 27 Jul) pushed Annex III high-risk obligations to 2 December 2027, and Annex I product systems to 2 August 2028.
- NCSC's interim agentic-AI guidance (20 Aug) — sandbox, credentials, logs, kill switch — previews formal guidance still to come.

Standing watch — sovereign cloud and data residency. OpenAI's new UK data-residency option and expanding government-specific deployments show model vendors racing to match hyperscaler sovereign offerings; track suppliers' data-boundary commitments as a procurement criterion.

RECOMMENDED

Three things to do before the next edition

- Check SharePoint estates for CVE-2026-65660 indicators of compromise, even where already patched.
- Update AWS SSM Agent to 3.3.4851.0 fleet-wide; don't wait for a KEV listing to act.
- Audit production AI agents against the Rule of 2 before your next agentic deployment review.

OUTLOOK — NEXT FORTNIGHT

We assess it is highly likely further AI-agent-linked breach notifications follow AEPD's, as other regulators catch up. It is a realistic possibility CISA lists CVE-2026-89049 if exploitation is confirmed. Likely: EU regulators keep treating GDPR, not the deferred AI Act timeline, as the near-term enforcement lever.

NEXT EDITION

Monday 12 October 2026. Send additions, corrections or platform intelligence to your ClearPath engagement lead.

ClearPath Partnership