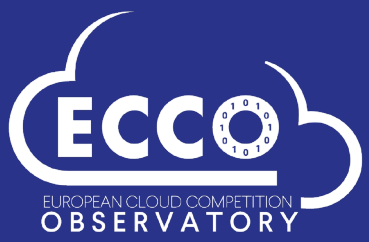

European Cloud Competition Observatory

Fourth Report

September 2026

The European Cloud Competition Observatory (ECCO) was created to build awareness of unfair software licensing conditions that hamper growth and development of Europe's cloud sector, as well as to provide updates on ongoing actions against those players who use these unfair licensing practices. ECCO is an independent monitoring body comprising CISPE (Cloud Infrastructure Services Providers of Europe) members plus the support, as observers, of European customer organizations, such as Cigref in France and Beltug in Belgium. It operates as an independent body under the auspices of CISPE. Guided by CISPE and European customer organizations, ECCO will monitor software, cloud, and AI giants whose practices restrict cloud choices for European customers.

For simplicity, ECCO has adopted a Red/Amber/Green (RAG) rating for each of the issues it considers. Green = On-Track, significant and sufficient progress towards ending unfair software licensing practices is being made. Amber = Off-Track, there are concerns either that progress has stalled, or that barriers to resolution are proving hard to overcome. Red = Critical, insufficient progress has been made at the time of the report.

This fourth report covers two vendors.

Part one focuses on Broadcom (VMware), documenting ECCO's assessment of continued and escalating unfair licensing practices, Broadcom's active deployment of delay tactics within the European Commission's antitrust investigation, and its wholly misleading sovereignty claims in the European market.

Part two escalates ECCO's assessment of SAP, where newly introduced API restrictions and agentic AI licensing changes raise serious concerns about foreclosure of third-party competition in the emerging enterprise AI market.

ECCO continues to monitor Microsoft's conduct and, at this time, maintains Microsoft's Green status. Microsoft is working closely with European cloud infrastructure service providers to implement the commitments made under its agreement with CISPE, finalised in July 2025. Beyond those commitments, Microsoft's recent decision to harmonise the cost of Extended Security Updates (ESU) for all customers, regardless of their choice of cloud, addresses a key element of CISPE's original complaint and demonstrates a continued willingness to recognise and respond to concerns raised by CISPE and others. New collaborations, under the European Cloud Accelerator, such as the co-development of a cloud-based onboarding tool for SMEs joining Catena-X, the automotive data space, show promise in extending the partnership into areas of mutual benefit, creating new growth opportunities for cloud providers.

Broadcom

Overall Status

RED

Overall Status – CRITICAL: Broadcom's conduct has deteriorated markedly since the Third Report (October 2025). Unfair licensing practices continue unchecked, end-customer BYOL rights have deteriorated significantly, procedural obstruction of the European Commission's antitrust investigation has intensified, and Broadcom is actively misleading the market with false sovereignty claims. No meaningful engagement with CISPE's remediation proposals has occurred.

Executive Summary

Since ECCO's Third Report in October 2025, the situation facing European cloud infrastructure service providers (CSPs) dependent on Broadcom's VMware technologies has continued to deteriorate on multiple fronts. Five principal areas of concern define this Fourth Report:

- Exclusion of the vast majority of European CSPs from offering VMware services under any terms
- Removal of end customers' BYOL rights, restricting them to a "choice" among a few handfuls of European companies to host their BYOL workloads.
- Ongoing and escalating unfair software licensing practices, including further unilateral contractual changes and cost increases that are driving European CSPs out of the market.
- Active delay tactics and procedural obstruction by Broadcom within the European Commission's antitrust investigation, including the invocation of US legal privilege to shield its own documents while simultaneously seeking to compel disclosure of confidential submissions from CISPE members.
- Broadcom's misleading sovereignty claims in respect of VMware Cloud Foundation (VCF).

Taken together, these developments represent a serious and continuing attempt by Broadcom to restructure the market in its favour. This is a threat not only to the viability of European cloud infrastructure providers but to the integrity of EU competition enforcement. Since the last report, CISPE has filed a competition case against Broadcom with the European Commission and is calling for urgent interim measures. In this context, ECCO has no alternative but to maintain Broadcom's status at Red – Critical.

Ongoing Unfair Software Licensing Practices

RED	**Licensing Practices**: Unfair and anticompetitive licensing terms continue to be imposed across European CSPs. No remediation has been offered or agreed. Cost increases of ten times or more at renewal remain widespread.

ECCO's assessment of Broadcom's licensing conduct has not changed since the Third Report. If anything, the evidence gathered over the intervening period reinforces the conclusion that Broadcom is systematically exploiting its dominant position in the server virtualisation market to impose terms that are harmful to European cloud providers and their customers.

Since that last report, these harms have been amplified by two further market-harming actions taken by Broadcom:

1. The abrupt closure of the partner programme which removes the right to sell VMware from thousands of resellers at a stroke; and
2. The severe restriction on Bring Your Own Licence (BYOL) terms for end customers.

Cancellation of Partner Programme

VMware virtualisation software remains, in the Commission's own words, technically complex to replace, with switching "disruptive to the business, and time-consuming." Broadcom continues to exploit this dependency.

In January, the negative situation was exacerbated by Broadcom's unilateral closure of its main reseller programme, utilised by cloud service providers across Europe to provide virtualisation services essential to wider cloud deployments. In an email to its partner community on 26th January 2026, Broadcom bluntly announced:

> **"As part of Broadcom's ongoing efforts to align [its] VMware partner ecosystem with our strategic priorities and the needs of [its] customers, [Broadcom/VMware] are providing this formal notice that [it has] closed the current Broadcom Advantage Partner Program for VMware Cloud Service Provider (VCSP) partners, and will not be renewing any [...] VCSP partner contracts with Broadcom after 26 January 2026."**

The email goes on to inform partners that after 31st March 2026 they are forbidden to:

> **"...execute any new Aggregate commitment contracts nor any renewals for existing commitment contracts."**

All existing contracts with customers for VMware will end on their termination date and cannot be renewed. For many, this will occur within 12 months. Essentially, vast

swathes of Europe's cloud ecosystem were, at a stroke, denied access to a crucial product for which there are no immediate alternatives. VMware is the de-facto virtualisation software not only provided by CSPs but integrated into their own cloud service products. Re-engineering, even where it is possible, is a multi-year and multi-million Euro project. Thus, this arbitrary refusal to deal threatens the commercial viability of many CSPs across Europe. It is this fact that led CISPE to make its filing to DG Competition and to call for Interim Measures to prevent immediate and far-reaching harm to individual companies and the market as a whole.

Changes to BYOL Hurt Customers and Vendors

Broadcom has made changes, identified in May 2026, to its Bring Your Own Licence (BYOL) scheme that further restricted choice for customers. Before these changes, VMware end customers had the option to use existing on-prem VMware licences to move to a cloud of their choice provided that the software ran on dedicated infrastructure owned and operated by the CSP. The system was essentially permissive and gave customers a wide choice of local and international cloud service providers.

For Vendors already locked out of the Broadcom reseller programme it offered one final contingency plan, albeit not actually a cloud service and requiring significant hardware investment, through which they could continue to serve select customers' VMware workloads. Customers buy the VMware licenses and then provide them to the CSP to deliver the service.

The latest programme changes slammed shut that final route to market. The new restrictive BYOL scheme only allows customers to select a Broadcom Certified Cloud Service – of which, thanks to previous restrictions, there are few remaining. Not only does this destroy choice, but by creating mini-monopolies in regions and sectors, it creates lock-in and potential price inflation.

For high-risk and sovereign workloads, the relevant measure is not whether a workload can move between Certified Cloud Service, but whether the customer has a choice of a trusted national provider at all.

CISPE members from across the EU have provided evidence as to how this change is exclusionary and anti-competitive, favouring a select few suppliers and concentrating the market into a channel entirely dependent on Broadcom.

One CISPE member had been counting on BYOL to keep serving regulated public-sector and critical-infrastructure accounts on dedicated hardware it owns and operates. These changes make that impossible. The sensitivity of data means that it cannot simply be transferred to another provider giving both vendor and customer no clear alternative.

Another CSP whose entire cloud offering runs on VMware, hosts the student information system used by the majority universities in the country as well as

healthcare applications (medical imaging, laboratory systems) and the systems of various government bodies. Its principal recourse was precisely BYOL on dedicated hardware it owns and manages, with licences procured through public procurement frameworks. The latest change forces these public and healthcare services into migration at renewal at latest, creating a severe time pressure (even migrating to another VMware environment might take over a year), with real risk of disruption and substantial additional cost - costs that, because the services are publicly funded, are ultimately borne by citizens and taxpayers.

Continued Unilateral Programme Changes

CISPE members continue to report licence cost increases of ten times or more compared to pre-acquisition VMware pricing. These increases are not the result of market competition or value-based pricing: they reflect Broadcom's ability to levy charges unconstrained by competitive alternatives.

Since October 2025, Broadcom has continued to make unilateral changes to partner programmes and licensing structures. The revamped VMware Cloud Service Provider (VCSP) programme, which was rolled out globally in the latter part of 2025, has further fragmented the market. By requiring partners to choose between reseller and service provider roles, Broadcom has structurally undermined the flexible business models upon which many European SME providers depend.

The elimination of overage-based licensing – under which CSPs could flexibly provision virtualisation capacity and reconcile usage in arrears – continues to impose severe commercial and operational constraints. CSPs are now forced to pre-commit to core counts, removing the elasticity that is fundamental to cloud service delivery. The commercial consequences for providers with fluctuating customer demands are severe.

Broadcom's enforcement of fixed licence commencement and termination dates, which prevent alignment with customer contract terms, continues to extract commercially unjustified fees from CSPs. When multiplied across large core-count deployments, such misalignments represent material financial extraction with no corresponding commercial value.

Finally, evidence from the market reveals that following the cancelling of the partner programme, those invited to new the programme have seen an additional 15% increase in licence fees. Broadcom's draconian approach to partner management leaves even those remaining within the programme with no ability to negotiate or to resist unilateral changes or increases to prices. They are locked-in just as firmly as customers.

The Kill-Switch: Now Confirmed

As flagged in the Third Report, CISPE had received warnings about a potential 'kill-switch' or degradation mechanism within VMware's licensing infrastructure. That concern has since been confirmed. Broadcom's Compliance Reporting mechanism, embedded in VCF Specific Program Documentation (v9.0 and later), mandates a Compliance Report every 180 days. Failure to comply triggers management-plane degradation and blocking. This is, in effect, an automated enforcement mechanism that can render a customer's virtualisation environment non-functional.

The existence of a mechanism capable of remotely degrading or disabling VMware functionality – on which thousands of European businesses and public sector organisations depend – represents an extraordinary and disproportionate exercise of market power. It also raises profound questions about the resilience and security of European digital infrastructure. - CISPE.

This mechanism operates irrespective of whether the software is deployed in a sovereign data centre or on-prem. There are no alternative management tools to which customers can turn. The lock-in is structural, deliberate, and complete.

Delay Tactics and Procedural Obstruction

RED

Procedural Conduct: Broadcom is actively obstructing the European Commission's antitrust investigation through a combination of legal challenges, invocation of US legal privilege, and requests to suspend regulatory proceedings. These are not legitimate procedural steps: they are a calculated strategy to delay and dilute effective enforcement.

CISPE formally presented its complaint to DG Comp on 19th March 2026 and emphasised the urgency of the situation with is submission for interim measures. However, despite several meetings with the Commission's case team and detailed response to requests for information, no formal investigation has been announced. Without robust and immediate action from the Commission to open an investigation and apply interim measures, there is no pressure for Broadcom to change its behaviour. Broadcom has made no overtures to CISPE and has not engaged with its proposals. Instead, as detailed below, it has used legal ploys to try to obstruct any investigation into its anti-competitive actions. This is not a neutral act. It reflects a deliberate strategy to maintain maximum commercial leverage over European providers who have no viable near-term alternatives.

The complaint called for action in five areas of concern.

- Return to predictable and fair business relationships, including minimum six-month advance notice of changes;
- Better support for smaller CSPs, including time extensions for onboarding as white-label customers;
- Flexibility for larger CSPs, including fair pricing for peak usage and relief from penalties for underusage;
- Partner programme access reform to allow smaller CSPs to attain higher-tier status; and
- End-customer privacy protections allowing services to be delivered without disclosing customer identities or workload data through the usage meter.

Asymmetric Disclosure: The Double Standards

Broadcom has adopted a transparently self-serving approach to disclosure in the antitrust proceedings. On one hand, it has sought to withhold correspondence with its internal US legal advisers from scrutiny by European authorities, invoking legal professional privilege under US law. On the other, it has simultaneously sought the disclosure of confidential information submitted by CISPE as part of the challenge to the VMware acquisition.

This combination – opacity for Broadcom's own documents, disclosure for its opponents' confidential submissions – represents an unacceptable double standard.

Suspension of the Commission's Investigation

Beyond the disclosure asymmetry, Broadcom has sought to suspend the European Commission's Request for Information (RFI) relating to the antitrust investigation, pending resolution of its appeal before the European Court. This is not a routine procedural step. It is a deliberate attempt to delay the very investigative process that could result in interim protective measures – measures urgently needed to protect European CSPs from the commercial harm they are already suffering.

In fast-moving technology markets, delays in enforcement are not procedurally neutral. Each month that passes without interim protection allows Broadcom's commercial conduct to continue, licensing terms to be locked in, and the market position of European CSPs to deteriorate further. Time is a strategic asset, and Broadcom is using litigation to consume it.

Implications for the Integrity of EU Enforcement

ECCO is deeply concerned that Broadcom's procedural strategy, if permitted to succeed, could set a damaging precedent for competition enforcement in the EU. If dominant technology companies can routinely invoke foreign legal privilege to shield documents from European investigators, the credibility and effectiveness of EU competition law will be significantly undermined.

ECCO calls on the European Commission and the EU Courts to preserve the integrity of the investigation, to resist Broadcom's attempts to delay or suspend proceedings, and to apply disclosure requirements even-handedly to all parties.

CISPE's Challenge to the Original Merger Decision

As noted in the Third Report, CISPE filed an action for annulment before the General Court of the European Union in July 2025, challenging the Commission's 2023 decision to approve Broadcom's acquisition of VMware. ECCO continues to monitor this action closely. The grounds for challenge – errors in law and manifest errors of assessment in the competitive analysis, including failures to properly assess foreclosure risk, bundling, and innovation effects – remain well-founded and are supported by the evidence that has emerged since the acquisition completed.

The Commission's two-year delay in publishing the merger decision – which itself has been characterised as a breach of the principles of good administration in a separate complaint to the European Ombudsman – deprived market participants of the opportunity to scrutinise its reasoning at the time most relevant to their commercial decisions.

Broadcom's Sovereignty Claims are Misrepresentative

RED

Sovereignty Compliance: Broadcom's VMware Cloud Foundation (VCF) fails to meet sovereignty or resilience requirements for software used by cloud services under the CISPE Sovereign and Resilient Cloud Framework. Only 3 of 52 assessed elements comply. Broadcom's public claims to be building 'Europe's sovereign cloud' are misleading and must be challenged.

Broadcom has mounted an active marketing campaign in Europe promoting VMware Cloud Foundation as an enabler of cloud sovereignty for European providers and their customers. It has made this claim at conferences, through advertising, and across communications channels. CISPE's independent assessment, conducted using its Sovereign and Resilient Cloud Service Framework, demonstrates conclusively that these claims are false.

The CISPE Sovereign and Resilient Cloud Framework Assessment

CISPE's assessment of VCF against the CISPE Sovereign and Resilient Cloud Framework found that the product fails to meet the requirements for Sovereign status and, critically, also fails to meet the requirements for the alternative Resilient status, which is specifically designed to provide assurance to customers using non-sovereign cloud services.

The failures fall into two principal categories: Sofware Dependency and Operational Autonomy.

Software Dependency

Section 3.B of the CISPE Framework requires customers to have meaningful control over critical software, including the ability to inspect, maintain, move, and replicate it. VCF is a proprietary, closed-source stack published by a US-controlled entity subject to Export Administration Regulations (EAR), OFAC tariffs, and CLOUD Act jurisdiction. Broadcom's terms and conditions provide no source-code escrow, no substitution plan, no Data Act certification, and only limited maintenance commitments.

The fact that VCF can be deployed in a European data centre or on-prem does not alter this dependency. Broadcom retains unilateral control as the sole source of patches, updates, and maintenance. If Broadcom chooses to withdraw support – or is compelled by US legal or executive action to do so – customers are left with a rapidly degrading, unlicensed virtualisation layer. This is not a theoretical risk. Broadcom has already demonstrated its willingness to act unilaterally against customers.

Operational Autonomy

Section 3.C of the CISPE Framework requires adequate protections against operational risks including service removal, interference, and degradation. As set out in Section 1 of this Report, the Compliance Reporting mechanism introduced in VCF v9.0 mandates a Compliance Report every 180 days, with management-plane degradation and blocking as the documented consequence of non-compliance. This mechanism – which CISPE regards as a kill-switch – directly contradicts the requirement for operational resilience of any cloud service relying upon it.

Neither sovereign data centre deployment nor on-prem installations remove the obligation to comply with this reporting mechanism. Without alternative management tools, customers risk lock-into a non-sovereign, non-resilient software platform regardless of where it is physically hosted.

Implications for CADA Certification

CISPE believes that the same structural failures in the way VCF is licensed and operated mean that it would also fail to achieve anything above Level 1 certification under the recently announced sovereignty framework within the Cloud and AI Development Act (CADA). Customers and procurement authorities should be aware that selecting VCF as the virtualisation foundation for a sovereign or resilient cloud architecture is unlikely to meet the sovereignty requirements of the CADA framework.

Consumer Protection and Market Transparency

Hundreds of European cloud infrastructure service providers, and thousands of their customers, depend on VCF as the virtualisation layer of their cloud environments. Many of these organisations are making procurement and infrastructure decisions on the basis of Broadcom's public claims. Those claims are not supported by the evidence.

CISPE calls on the European Commission, national competition authorities, and consumer protection bodies to investigate the accuracy of Broadcom's sovereignty marketing and to take steps to ensure that customers – particularly public sector bodies and critical infrastructure operators – are not misled into procuring solutions that cannot meet their regulatory and operational requirements.

Summary and Next Steps

Across all five dimensions assessed in Part One of this Report – licensing conduct, procedural behaviour, and sovereignty claims – Broadcom's conduct falls materially short of what is acceptable in a well-functioning, rule-of-law-based market.

ECCO's key observations and calls to action are as follows:

1. **The European Commission should resist Broadcom's attempts to suspend the antitrust investigation and should proceed swiftly to consider and impose interim protective measures.** European cloud providers cannot wait years for enforcement to produce results. Interim measures are urgently needed now.
2. **The EU Courts should enforce disclosure obligations even-handedly.** Broadcom should not be permitted to invoke US legal privilege to shield documents from European investigators.
3. **Regulators and procurement authorities should scrutinise Broadcom's sovereignty marketing claims.** VCF does not meet CISPE's sovereignty or resilience requirements and is unlikely to meet CADA Level 2 or above. Public sector and critical infrastructure procurement decisions should reflect this reality.
4. **ECCO will continue to monitor all aspects of this situation** and will report further developments as they arise, including the progress of CISPE's annulment action, any Commission enforcement decisions, and any further unilateral changes to Broadcom's licensing terms or partner programmes.

In the current circumstances, ECCO has no alternative but to maintain Broadcom's status at Red – Critical. The evidence gathered since the Third Report confirms that the situation is not improving. On the contrary, it is becoming more acute. ECCO urges all relevant authorities to act with the urgency that the protection of European cloud infrastructure – and European digital sovereignty – demands.

SAP: Licensing Strategy Raises Serious Competition Concerns

ECCO's Third Report flagged SAP as a vendor of concern, noting changes to licensing terms that risked extending lock-in and reducing opportunities for customers to run SAP's leading ERP software on third-party cloud infrastructure. Those concerns included intensifying pressure on customers to host exclusively through SAP RISE – SAP's proprietary cloud programme – and the removal of certification for European cloud providers as approved hosting partners.

The European Commission has also opened an inquiry into SAP's support contracts, which may, in the Commission's own words, "prevent customers from 'mixing and matching' maintenance and support services from different suppliers at different price and support levels despite it being more convenient for them."

In April 2026 CISPE raised concerns regarding the way SAP was throttling access to data in a bid to control an Agentic AI layer rapidly becoming the de-facto route for enterprises to access and use their data. ECCO has looked at this issue as well as longer-running anti-competitive concerns. It suggests there are concerns to be answered in two main areas:

1. Traditional Antitrust Measures that direct customers to SAP's own cloud offers.
2. Emerging concerns over restrictions to agentic AI data access.

Since the Third Report, SAP has moved further and faster in a direction that warrants escalated attention. The focus of this new chapter is SAP's emerging strategy in the agentic AI domain – a market that is rapidly becoming the primary interface layer for enterprise data. The concerns are specific, substantial, and in ECCO's assessment potentially anticompetitive.

Traditional Anti-trust Concerns

AMBER

SAP Competes with its own partners: Since 2023 SAP has progressively used access to innovation and new product capabilities as a lever to drive customers to its cloud offers. Moreover, it increases prices and excludes non-SAP cloud-based deployments from the latest innovations. Amber – Concerns.

On 20th July 2023, at its annual press conference SAP announced that all future innovations would be delivered cloud-first. This was presented as an important step from a company that previously had relied on complex on-prem deployments to deliver the high-stakes enterprise resource planning (ERP) software upon which so many organisations depend.

It outlined two routes to continue to benefit from new innovations, with AI specifically called out. These were the SAP RISE programme – essentially SAP's private cloud offer, and SAP GROW which allowed SAP to be hosted in certain partners' public clouds.

There was immediate pushback, not least from customers who had invested millions in licensing and integrating SAP S/4 HANA on their on-prem infrastructure. SAP's response was that these innovations, including the newly announced AI assistant Joule, would only work on cloud infrastructure.

However, by early 2026, SAP was able to announce that Joule and other 'cloud-first' innovations, would now be available to on-prem customers. There was a big caveat. These new products and developments will only be available to those that commit to a transition to SAP RISE.

This speaks to a 'traditional' antitrust concern – that customers are being offered differentiated (and lower grade) products unless they migrate to SAP's own cloud infrastructure.

Similarly, because the latest AI developments are only available on SAP RISE, partners using the SAP GROW programme to host SAP on their own infrastructure, are also excluded. These partners include the major public cloud vendors AWS, Microsoft Azure and Google Cloud. Customers are therefore effectively deprived of choice and locked-in to the SAP ecosystem.

Forthcoming Changes to Licensing Will Favour the Biggest Players

SAP also announced at SAPPIRE 2026 changes to how it bills for its software. Historically, since the shift away from permanent licensing, SAP has charged on a consumption rate. The more you used the software, the more it cost. At SAPPHIRE it announced that partners would be charged on a per-server basis (ie capacity-based). There would be caps for certain scenarios.

Whilst this does create a higher-level of cost predictability for customers, it also creates market-distorting effects for partners.

- It will immediately make it more expensive to offer SAP services on non-SAP clouds as service providers will pay for the total server capacity they need irrespective of usage, whilst SAP can continue to charge based on direct customers' actual usage.
- It will also favour those with large SAP customer bases who can defray per-server costs over a wider number of customers. Smaller players, or those who offer some SAP services alongside other cloud services, may well be priced out of the market.
- Finally, the caps favour the very largest partners, hyperscalers, who will quickly reach the capped prices and then see increased margins for all SAP services offered beyond them.

To date, these new abused of traditional anti-trust regulations have gone unchallenged. ECCO believes that the European Commission should investigate these as part of any wider investigation of SAP's leveraging its market power in delivering ERP solutions.

Emerging AI Competition Concerns

AMBER

SAP Agentic AI Licensing Practices: SAP's newly introduced API restrictions and shift to consumption-based billing for AI agents raise serious concerns about foreclosure of third-party competition in the emerging enterprise AI market. The combination of agent discrimination, preferential access for incumbent partners, and escalating unit costs warrants active regulatory scrutiny. Amber – Concerns.

Agent Discrimination: Closing the API Door

In late April 2026, SAP updated its API policy, describing the changes as a clarification of "design-intended use" intended to "protect platform stability and security." The substance of the change, set out in Section 2.2.2 of API Policy v4/2026, was considerably more far-reaching: SAP's APIs may no longer be used for "interaction or integration with (semi-) autonomous or generative AI systems that plan, select or execute sequences of API calls." In plain terms, SAP has banned third-party AI agents from accessing its platform through standard APIs.

The significance of this change cannot be overstated. Agentic AI – systems capable of autonomously executing complex, multi-step tasks – is rapidly becoming the dominant paradigm for enterprise software interaction. For the large proportion of European enterprises whose business-critical data lives in SAP systems, whoever controls agent access to that data controls the competitive conditions for every AI service built on top of it. SAP has chosen to exercise that control unilaterally and restrictively.

Preferential Access: Friends, Family, and the Danger of Gatekeeping

SAP has carved out a limited category of endorsed agents permitted to access its platform. These currently include SAP's own AI agent Joule and NVIDIA's NemoClaw. SAP has reserved to itself the power to determine which other agents may be added to this approved list.

This gatekeeping function raises immediate concerns related to the Digital Markets Act and wider competition law. . Third-party developers building agentic AI solutions face fundamental uncertainty: they cannot know in advance whether their agents will be permitted to interact with SAP data. This uncertainty is itself a competitive harm – it chills investment and innovation in alternative agent architectures, particularly among smaller and newer market entrants who lack the negotiating leverage to secure endorsed status through partnership arrangements.

The existing arrangement is illustrative. Microsoft's Copilot – a long-standing SAP partner and dominant player in its own adjacent markets – has secured bi-directional integration with Joule and endorsed status. For hyperscalers and large US technology companies, SAP's restrictions are an inconvenience to be negotiated around. For smaller and mid-sized European cloud providers building orchestration layers, sector-specific AI applications, or integration services on top of SAP environments, the same restrictions can be existential.

Openness between dominant players is more of an oligarchy that continues to restrict access to smaller independent providers. The ability to 'pick winners' and provide access to 'friends' and aligned businesses is a market distortion in itself.

Under EU competition law, the relevant question is not whether SAP has the right to manage its APIs, but whether a dominant company is using technical restrictions to foreclose competition in adjacent markets. SAP's position in business-critical ERP across European enterprises is not merely large – it is entrenched. Finance, procurement, supply chain, and HR data for a large proportion of the continent's major organisations resides within SAP systems. Restricting third-party AI agent access while steering customers towards SAP's own tools and preferred partners must be examined as a potential abuse of that dominant position.

ECCO believes these restrictions disproportionately foreclose smaller European providers from competing in the emerging market for enterprise AI services.

Data Act Compliance: Assurances Without Evidence

SAP's API policy changes raise significant questions under the EU Data Act, which is designed to enable portability of data between functionally equivalent services and to ensure that users can switch, port data, and operate simultaneously across providers without artificial friction. The Data Act is explicit that security considerations cannot serve as a blanket justification for denying interoperability and data portability.

SAP's accompanying FAQ documentation bluntly asserts that the new API restrictions do not affect its legal obligations on data portability. It provides no detail or substantiation for this claim. Using an updated API policy to enforce a digital border that can deny access to third-party AI agents would appear to impinge on the spirit, if not the letter, of the Data Act.

ECCO calls on the Commission to seek clarity from SAP on the legal basis for its position.

Consumption Pricing and Escalating Costs

The API restrictions do not operate in isolation. They are compounded by a parallel commercial transformation: SAP's shift from per-seat to a combination of usage-based billing and value-based billing for AI functionality. Where enterprise software costs were previously predictable and tied to user numbers, they are now tied to "agent actions" – a unit of measurement that SAP itself has yet to define with precision.

Gartner's assessment is direct: "Depending on how SAP defines an 'action,' the number of events incurring fees risks quickly spiralling upwards." SAP has confirmed that AI Unit purchases are estimated based on expected "agent actions for an autonomous domain," with the company promising future "Autonomous Domain Blueprints" to guide deployment cost estimates. For customers attempting to plan and budget enterprise AI deployments, this level of commercial uncertainty is not acceptable.

Anecdotal evidence from customers further suggests that, following the exclusion of third-party AI tools, costs for SAP's own AI units have risen by approximately 15%. The logic is circular and the harm is clear: third-party agents are excluded from standard API access; the only available route is through SAP's own connector, Joule, or within the SAP ecosystem; and the cost of those endorsed interactions rises once customers are locked in. This is a new form of anti-competition playbook applied for the AI age.

The Case for Regulatory Action

ECCO was established to maintain ongoing scrutiny of conduct that damages European cloud market openness. The argument that SAP deserves softer treatment as a European technology company misunderstands both the purpose of European regulation and competition law and the nature of the harm. European enterprises and smaller cloud providers are not well served by a European champion that uses its market dominance to close adjacent markets.

Europe has invested considerable regulatory capital in building an open, multi-cloud ecosystem through the Data Act, and the proposed Cyber Security Act 2 (CSA2). These instruments were designed precisely to ensure that the shift to cloud and AI does not replicate the monopolistic patterns of the enterprise software era. If AI agents are now the critical infrastructure layer for enterprise computing – and the evidence strongly suggests they are – then restrictions on how those agents operate within dominant systems are foundational competition questions, not peripheral technical ones.

As the European Commission seeks to accelerate Industrial AI Adoption, and have appointed none other than former SAP CEO Jim Hagemann Snabe as a Special Envoy to assist, it is increasingly important that anti-competitive business practices are not allowed to take hold.

ECCO calls on the European Commission to extend its existing inquiry into SAP's support practices to encompass the API restrictions and agentic AI licensing strategy described in this chapter. The Commission should specifically examine whether SAP's conduct constitutes an abuse of dominance through foreclosure of the emerging enterprise AI agent market, and whether its API policy and contractual terms are compliant with the Data Act.

About CISPE

CISPE (Cloud Infrastructure Services Providers in Europe) represents Europe's leading cloud infrastructure service providers and promotes an open, competitive, sovereign, and EU-compliant cloud market across Europe.

About ECCO

The European Cloud Competition Observatory (ECCO) was created as part of CISPE's anti-competition settlement agreement with Microsoft. ECCO is an independent monitoring body comprising CISPE members plus the support, as observers, of European customer organizations, such as Cigref in France and Beltug in Belgium. It operates as an independent body under the auspices of CISPE.

ECCO
EUROPEAN CLOUD COMPETITION
OBSERVATORY