

Az „MI-ügynökök” működésének szabályozási jövőképe

Domokos Márton | CMS Budapest

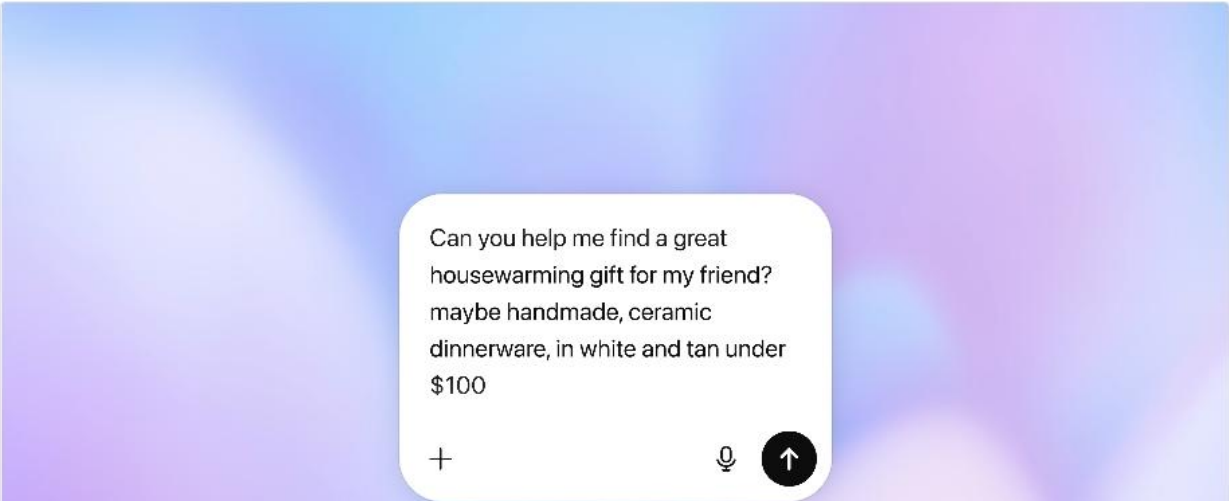
2026. május 27.

Bevezető gondolatok - a szabályozási jövőkép tárgya (1)

September 29, 2025 Product

Buy it in ChatGPT: Instant Checkout and the Agentic Commerce Protocol

We're taking first steps toward agentic commerce in ChatGPT with new ways for people, AI agents, and businesses to shop together.



Can you help me find a great housewarming gift for my friend? maybe handmade, ceramic dinnerware, in white and tan under \$100

+

🎤

↑

Bevezető gondolatok - a szabályozási jövőkép tárgya (2)

A mesterséges intelligencia simán megtervezi a nyaralásodat. De mi lesz, ha fizetni is akar helyetted?

HÁGYABORSZÁG
Forbes

The Transformative Impact Of AI Agents On Retail:
Navigating Power Dynamics And The Rise Of AI
Agent Optimization

Dell Technologies By [Cindy Carlson](#), Brand Contributor.
for [Dell Technologies](#), [BRANDVOICE](#) | Paid Program

Published Apr 23, 2026, 12:32pm EDT

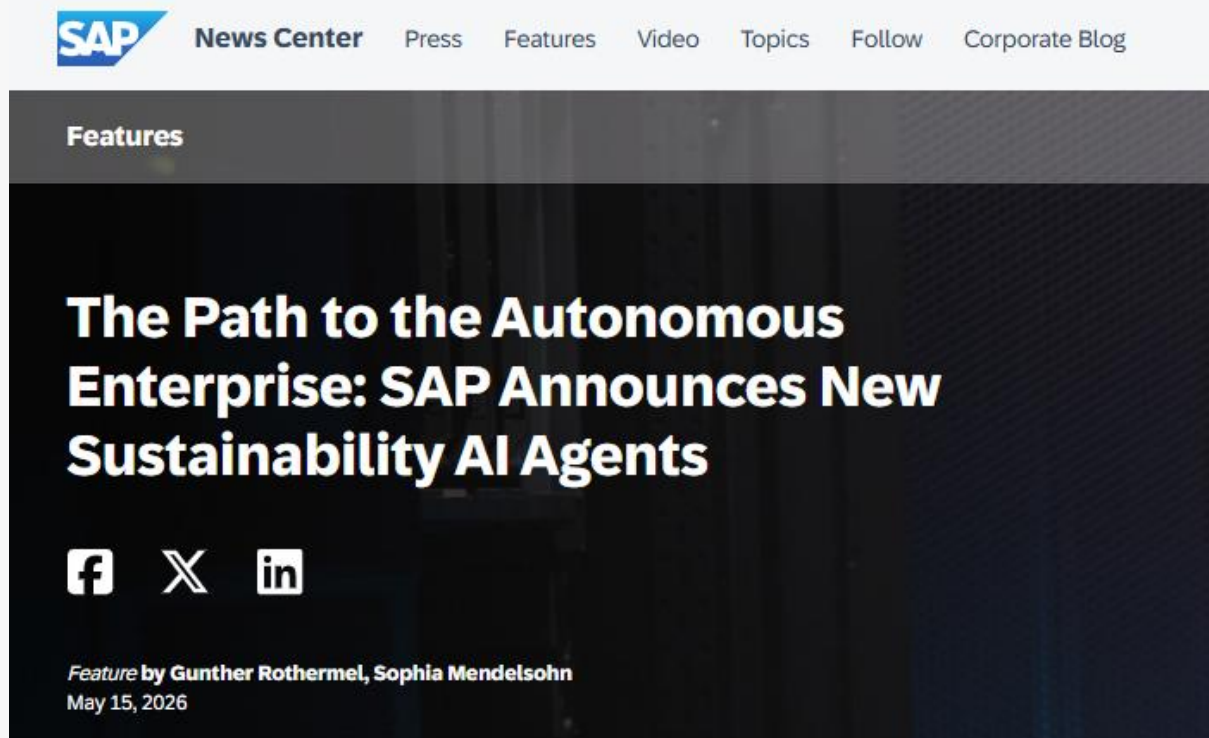
Forbes

„A kereskedelem új valósága.”

„A fogyasztók soha nem látott mértékű megerősítése.”

„A kereskedelem szabályainak újraírása.”

Bevezető gondolatok - a szabályozási jövőkép tárgya (3)



Fenntarthatósági Szabályozási MI-ügynök

Lábnyom-optimalizáló MI-ügynök

Csomagolási megfelelési MI-ügynök

Munkavédelmi MI-ügynök

Az MI-ügynökök általános jellemzői (1)



Stegosaurus Scene | THE LOST WORLD: JURASSIC PARK (1997)

Az MI-ügynökök általános jellemzői (2)

Nyílt végű feladatok / külső műveletek: szöveg-, kód-, multimédiás tartalomgenerálás + információk elküldése, felhasználókkal való interakció, kód futtatása, szerződések végrehajtása, eszközök vezérlése – adaptív döntéshozatal, korlátozott emberi iránymutatás.

Memória és alkalmazkodóképesség: lehetővé teszi a kontextus meghatározását, tapasztalatok felhalmozását, a viselkedés felhasználói reakciókhoz való igazítását, visszajelzések és önértékelés alapján fejlődik, nyelvi képességek és rövid és hosszú távú memória alkalmazásával.

Proaktivitás: a háttérben végrehajtott műveleteik segítségével naprakész információkat szerezhet, előre jelezhet igényeket vagy problémákat, műveleteket kezdeményezhet, munkafolyamatokat optimalizálhat.

Tervezés és következtetés: meghatározott célok elérése érdekében lehetővé teszi műveletsorozatok megtervezését, alternatívák értékelésével, autonóm módon részfeladatok meghatározásával, és az optimális eredmények prioritizálásával.

Az MI-ügynökök általános jellemzői (3)

Nézd át az adatfeldolgozási szerződést az adatfeldolgozó szempontjából.

Copy Save prompt Edit query

Reasoning ▾

- Assessing query
- The user is asking me to review the data processing agreement from the perspective of the data processor. Let me first read the document to understand its contents.
- Áttekintem az adatfeldolgozási szerződést az adatfeldolgozó szemszögéből. Először beolvasom a dokumentumot.

⊞ Selecting document for editing

 New Data Processing Agreement Template EN.docx Word

- Reading full document
- Now I have a comprehensive view of the Data Processing Agreement. Let me analyze it from the Data Processor's perspective and identify key risks, concerns, and problematic provisions. Let me also look at the tracked changes (redlines) that have been inserted.

Key issues from the Data Processor's perspective:

1. Clause 7.1(c) - P:66: New insertion (by CMS) in Hungarian requiring the Processor to document all instructions and retain them for 3 years. This is a burden on the Processor but somewhat standard.

Az MI-ügynökök általános jellemzői (4)



Az MI-ügynökök általános jellemzői (5)



Amire az adatvédelmi jogász már felkapja a fejét...

➤ **Interakció a környezettel:** érzékelők, alkalmazásprogramozási interfészek (APIk), kamerák stb. segítségével valós időben értelmezik a környezetet és dolgozzák fel a bemeneteket.

➤ **„Szolgáltatáshívások” (service calls) végrehajtása:** APIkhoz, adatbázisokhoz, weboldalakhoz vagy más eszközökhöz való kapcsolódás és azok használata útján - online szolgáltatások vagy helyi szolgáltatások (például alkalmazások, kód futtatási képességek vagy a felhasználó rendszerén tárolt adatok).

➤ **„Többügynökös” (multi-agent) architektúrák:** az egyes MI-ügynökök viselkedése és felelősségi köre szigorúan meghatározott, az információkat és döntéseket megosztják egymással, valamint összetettebb célok elérése érdekében képesek együttműködni, versenyezni vagy tárgyalni egymással.

Az MI-ügynök szabályozási „jelenképe” (1)



Brüsszel, 2025.7.29.
C(2025) 5053 final

A BIZOTTSÁG KÖZLEMÉNYE

A Bizottság iránymutatása az (EU) 2024/1689 rendelet (a mesterséges intelligenciáról szóló rendelet) által meghatározott mesterségesintelligencia-rendszerek fogalommeghatározásáról

„AI-rendszer”: olyan gépi alapú rendszer, amelyet úgy terveztek, hogy különböző szintű autonómiával működjön, amely bevezetését követően alkalmazkodóképességet tanúsíthat, és amely a kapott bemenet alapján – explicit vagy implicit célok érdekében – kikövetkezteti, miként generáljon olyan kimeneteket, például előrejelzéseket, tartalmakat, ajánlásokat vagy döntéseket, amelyek befolyásolhatják a fizikai vagy a virtuális környezetet.

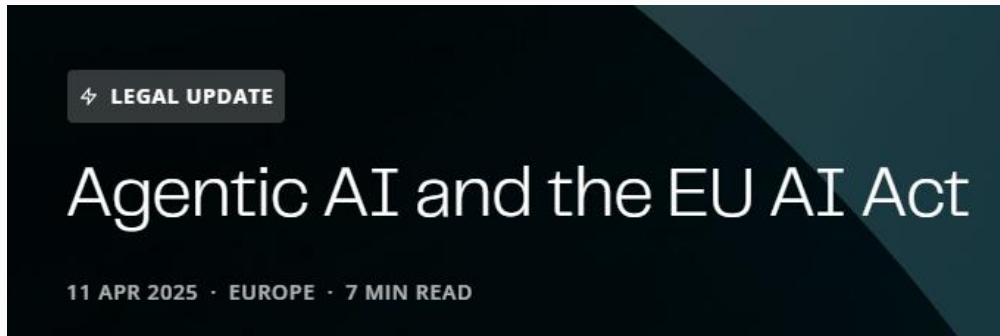


Az MI-ügynök szabályozási „jelenképe” (2)



„Az MI-ügynök besorolása az EU AI Act alapján valamely konkrét kockázati kategóriába az MI-ügynök konkrét alkalmazási környezetétől, valamint az alapvető jogokra vagy a biztonságra gyakorolt lehetséges hatásától függ.”

„The classification of agentic AI into a specific risk category under the EU AI Act is contingent upon its contextual application and potential impact on fundamental rights or safety.”



Az MI-ügynök szabályozási „jelenképe” (3)

„A” rész: Mesterséges Intelligencia (MI)-rendszer használatára vonatkozó általános kérdések		
KÉRDÉS		VÁLASZ
1. Működése alapján MI-rendszernek ¹ minősül-e a rendszer? (igen /nem)	igen	
3. Ismertesse, hogy az MI rendszer melyik kockázati kategóriába sorolják az EU AI Act szerint.		
4. Kérjük mutassa be részletesebben az MI-rendszert, így különösen, hogy milyen üzleti folyamatokban (például: logisztika, ügyfélszolgálat) alkalmazzák ²		
5. Az MI-rendszer az informatikai rendszer fő funkcionalitását vagy kiegészítő funkcionalitását adja ? ³		
6. Az MI-rendszer (i) külső szolgáltató „dobozos” MI-rendszere, (ii) külső szolgáltató által egyedi igények szerint továbbfejlesztett MI-rendszer, vagy (iii) saját hatáskörben vagy egyedi igény alapján fejlesztett MI-rendszer ? ⁴		
7. Rendelkezésre áll-e dokumentáció az MI-rendszer működésére és használatára vonatkozóan ? ⁵ Ha van, kérjük, szíveskedjenek rendelkezésre bocsátani magyar vagy angol nyelven.		

Az MI-ügynök szabályozási „jelenképe” (4)

Table 3.3. Illustrative definitions of agentic AI

Source	Definition
IBM (2025 ^[20])	Agentic AI systems are software systems that leverage AI agents (together with other components like tools, planners, memory, and datasets), pursue goals, and can operate autonomously.
Chan et al. (2023 ^[43])	We identify 4 key characteristics associated with increasing agency in algorithmic systems, especially in combination: underspecification, directness of impact, goal-directedness, and long-term planning. (1) Underspecification: the degree to which the algorithmic system can accomplish a goal provided by operators or designers, without a concrete specification of how the goal is to be accomplished. (2) Directness of impact: the degree to which the algorithmic system's actions affect the world without mediation or intervention by a human, i.e. without a human in the loop. (3) Goal-directedness: the degree to which the system acts as if it is designed/trained to achieve a particular quantifiable objective. (4) Long-term planning: the degree to which the algorithmic system is designed/trained to make decisions that are temporally dependent upon one another to achieve a goal and/or make predictions over a long time horizon.
Shavit et al. (2023 ^[44])	Agentic AI systems are characterised by the ability to take actions which consistently contribute towards achieving goals over an extended period of time, without their behaviour having been specified in advance.... We define the degree of agenticness in a system as “the degree to which a system can adaptably achieve complex goals in complex environments with limited direct supervision.” [...] we will generally refer to systems exhibiting high degrees of agenticness as “agentic AI systems,” to emphasise that agenticness [...] we will generally conceptualize agentic AI systems as operating in pursuit of goals defined by humans and in environments determined by humans (and often in co-operation with human “teammates”), rather than fully-autonomous systems that set their own goals.
Miehling et al. (2025 ^[40])	An agentic AI system, or simply agentic system, is a collection of agents interacting with humans and the environment with the objective of fulfilling specified goals. Practically, an agent is an LLM or large multimodal model (LMM) with access to tools — specialised components/functionalities like APIs, external services, computational resources, or domain-specific software — that allow it to perform specific operations in the environment. In this sense, tools define both the capabilities (actions) of the agent and the information (via observations/signals) that can be obtained from the environment. The human is responsible for seeding the initial task specification, providing clarification, and authorizing any (agent) actions that need human approval (Shavit et al., 2023). Given the task specification, an agent is able to interact with other agents (agent-agent interaction) to facilitate task decomposition/planning and delegation. This interaction can be co-operative or competitive, e.g., in the case of limited compute. The environment consists of everything external to the agentic system. This includes infrastructure (computers), other humans, other agents, and even other agentic systems.
Sapkota, Roumeliotis and Karkee (2025 ^[25])	Agentic AI systems represent an emergent class of intelligent architectures in which multiple specialised agents collaborate to achieve complex, high-level objectives. As defined in recent frameworks, these systems are composed of modular agents each tasked with a distinct subcomponent of a broader goal and co-ordinated through either a centralised orchestrator or a decentralised protocol. This structure signifies a conceptual departure from the atomic, reactive behaviours typically observed in single-agent architectures, toward a form of system-level intelligence characterised by dynamic inter-agent collaboration. A key enabler of this paradigm is goal decomposition, wherein a user-specified objective is automatically parsed and divided into smaller, manageable tasks by planning agents. These subtasks are then distributed across the agent network. Multi-step reasoning and planning mechanisms facilitate the dynamic sequencing of these subtasks, allowing the system to adapt in real time to environmental shifts or partial task failures. This ensures robust task execution even under uncertainty. Inter-agent communication is mediated through distributed communication channels, such as asynchronous messaging queues, shared memory buffers, or intermediate output exchanges, enabling co-ordination without necessitating continuous central oversight. Furthermore, reflective reasoning and memory systems allow agents to store context across multiple interactions, evaluate past decisions, and iteratively refine their strategies. Collectively, these capabilities enable Agentic AI systems to exhibit flexible, adaptive, and collaborative intelligence that exceeds the operational limits of individual agents.
CSET (2024 ^[42])	Goal complexity: More agentic systems pursue complex, longer-term goals—or even a variety of different goals. Less agentic systems carry out individual, more explicitly defined tasks. Environment complexity: More agentic systems can operate effectively in more open-ended and complicated settings, where the number of possible states and actions available to the agent is larger and the dynamics governing what will happen next in the environment are more difficult to model. Less agentic systems can operate effectively only in simpler and more predictable settings.

A szabályozási jövőkép – fejlesztői / felhasználói oldalról



01 ↘

Lehetséges sérülékenységek és fenyegetések?

02 ↘

Lehetséges megfelelési szempontok és intézkedések?

**AGENTIC ARTIFICIAL
INTELLIGENCE
FROM THE PERSPECTIVE OF
DATA PROTECTION**



„Technikai ködösítés” vs. pontos fogalomhasználat



„Checkbox security” vs. „safe failure”

Hogyan kerülhetjük el a „technikai kódösítést”? (1)

1.

Az értéklánc szereplőinek felelőssége: adatkezelő, közös adatkezelő, adatfeldolgozó.

2.

A feladatok jellege és az automatizáció mértéke: a GDPR 22. cikk (*Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást*) alkalmazhatósága. (Az MI-ügynök céljainak eléréséhez szükséges megnövekedett számú lépés és döntés ugyanakkor csökkentheti az érdemi emberi beavatkozás lehetőségét.)

3.

Célok és eszközök kijelölése, valamint rugalmas feladatmeghatározás: megfelelés a „célhoz kötöttség” elvének.

Hogyan kerülhetjük el a „technikai ködösítést”? (2)

4. Az adatkör meghatározása: megfelelés az „adattakarékosság” elvének.

→ Meg kell határozni cél eléréséhez szükséges adatbázisokat, valamint a személyes adatok típusát és mennyiségét.

→ Hozzáférési és adatmegosztási jogosultságok + adatgyűjtési szabályok.

5. Személyes adatok különleges kategóriáinak tervezett vagy nem tervezett kezelése / kikövetkeztetése.

6. Átláthatóság és érintetti jogok: hozzáférés biztosítása, az adatkezelés nyomkövetése (adott esetben megszüntetése), és az adatok további megosztásának szabályozása.

→ Az érintettek helyesbítési jogának érdekében fontos az adatok forrásának azonosíthatósága.

→ Elszámoltathatóság: milyen adatokat használ az MI-ügynök, milyen pontokon, illetve hogyan kerül sor döntéshozatalra.

Hogyan kerülhetjük el a „technikai ködösítést”? (3)

7. „Shadow AI agent” / „short-term AI agent” – a belső szabályzatok fontossága („BYOAgentic” - Build Your Own Agentic)

8. Új kiberbiztonsági fenyegetések és egyéb veszélyek: az MI-ügynök működési céljaiban megjelenő torzítások, az MI-ügynök érvelésének támadása vagy manipulációja, valamint az MI-ügynök memóriájában kezelt adatok mérgezése.

9. Szolgáltatások integrációja – harmadik fél szolgáltatások használati és adatvédelmi feltételeinek betartása.

10. Csökkenteni a „láncreakciós hallucináció” kockázatát (*cascading hallucination*) - a „pontosság” elvének betartása érdekében.

→ Az MI-ügynök pontatlan, de hihető információt hoz létre (ami akár személyes adatot is tartalmazhat), és ezt az általa használt eszközökön, illetve adatbázisokon keresztül, vagy más MI ügynökkel való interakcióján továbbítja –segíti a pontatlan információ gyors terjedését, más rendszerekben vagy döntési folyamatok során.

→ A „pontosság” elvének betartása érdekében fontos az MI ügynök működésének nyomonkövetése. A memóriában tárolt pontatlan adatok (akár tanult, akár hallucinált formában) hatással lehetnek az MI ügynök segítségével hozott döntésekre.

Gyakorlati példák a kockázatokra

'Moltbook' social media site for AI agents had big security hole, cyber firm Wiz says



Correcting the Financial Times report about AWS, Kiro, and AI

Share



Written by Amazon Staff

February 20, 2026

1 min read

We want to address the inaccuracies in the [Financial Times' reporting](#) yesterday. The brief service interruption they reported on was the result of user error—specifically misconfigured access controls—not AI as the story claims.

Amazon News

BUSINESS INSIDER

Replit's CEO apologizes after its AI agent wiped a company's code base in a test run and lied about it

Néhány szó az MI-ügynök autonómiájáról (1)



Autonómia:

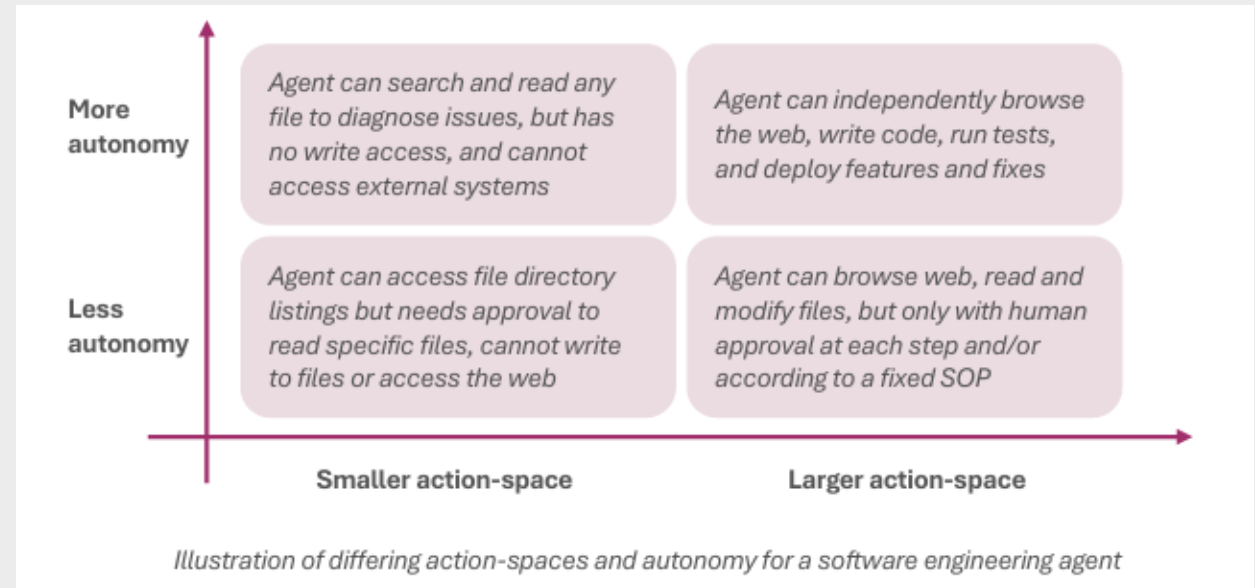
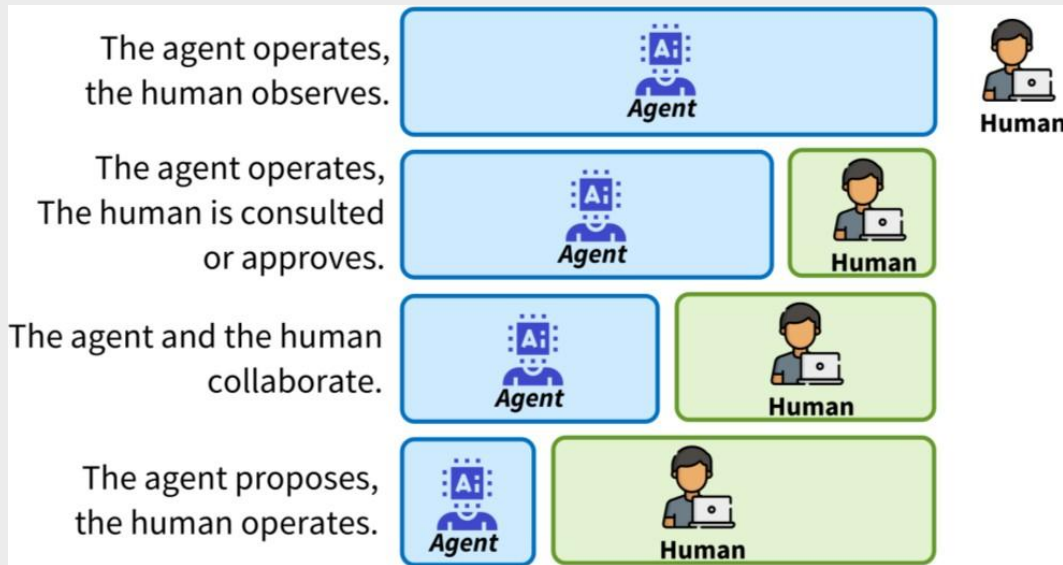
képes folyamatos emberi beavatkozás nélkül működni.



DE:

a rendszert tervező és finomhangoló fejlesztő, a telepítésért és konfigurációért felelős személyek, valamint a célokat, eszközöket, hozzáférési jogosultságokat meghatározó személyek által előzetesen meghatározott céloktól és szabályoktól függ.

Néhány szó az MI-ügynök autonómiájáról (2)



Néhány szó az MI-ügynök autonómiájáról (3)



EUROPEAN DATA PROTECTION SUPERVISOR

[Home](#)

[About](#)

[Data Protection](#)

[Artificial Intelligence](#)

[Press & Publications](#)

[Home](#) > [Data Protection](#) > [Our work](#) > [TechDispatch #2/2025 - Human Oversight of Automated Decision-Making](#)

TechDispatch #2/2025 - Human Oversight of Automated Decision-Making



[Translate this page](#)



Néhány szó az MI-ügynök autonómiájáról (4)

Meta AI agent's instruction causes large sensitive data leak to employees

The logo for The Guardian news outlet, featuring the words "The Guardian" in a white serif font on a dark blue rectangular background.

Assumption: That human operators possess the authority to decide

Another common misconception is that human operators will always retain meaningful authority to override the suggestions provided by automated systems - some authors refer to this as *agency*.^[24]

This assumption fails to account for the practical limitations on independence and expertise that might constrain an operator's ability to deviate from system recommendations.

Operators may choose not to override a system's output due to fear of potential consequences, particularly if the system's recommendation is later found to be correct. **This hesitation reflects a lack of perceived agency.**

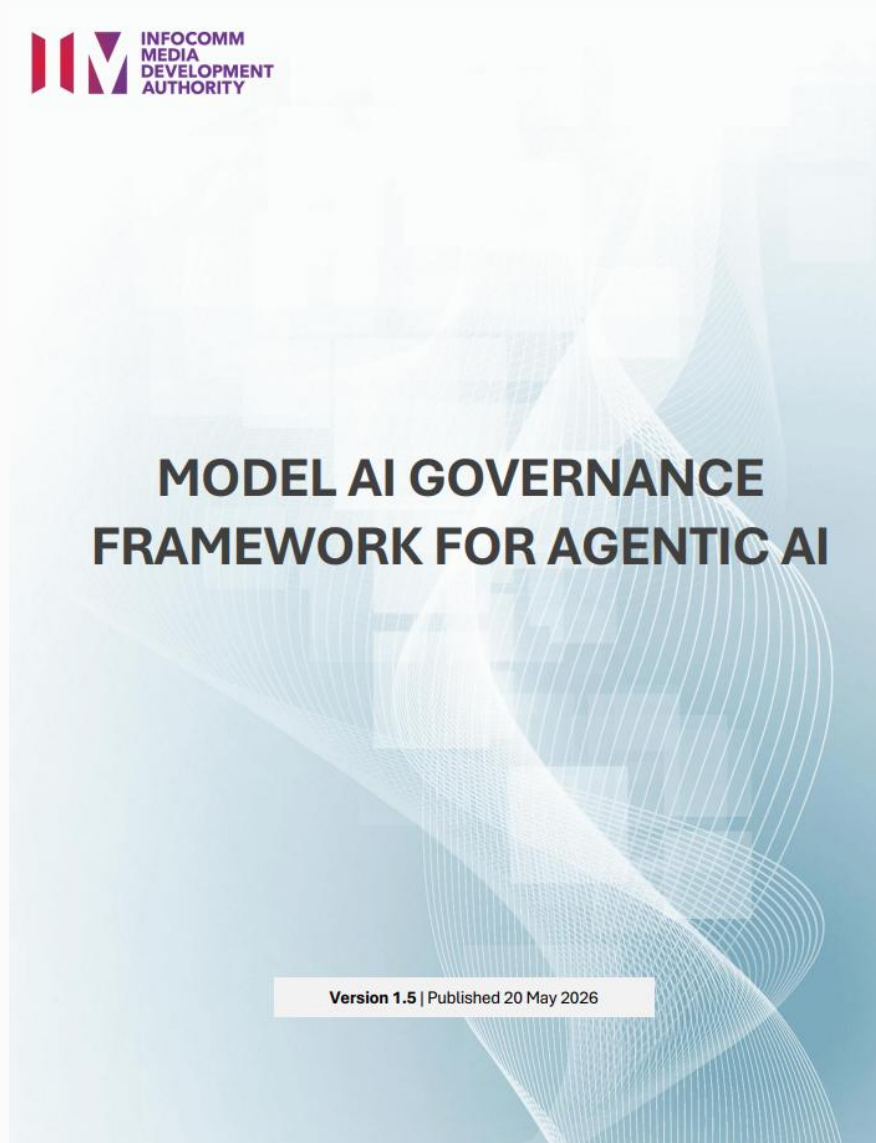
Moreover, when systems operate on complex or highly specialized data, operators may delegate to the system's apparent expertise, feeling insufficiently qualified to challenge its outputs.^[25] This perceived imbalance in knowledge can discourage intervention and reinforce reliance on the system, even in situations where human judgment is necessary.

Example: *In 2020, the UK exams regulator, Ofqual, deployed an algorithm to standardize GCSE^[26] and A-level grades based on historical school performance. This approach led to approximately 40% of students receiving lower grades than their teachers had predicted, disproportionately affecting students from disadvantaged backgrounds.*^[27]

Despite the algorithm's significant impact, human oversight was insufficient and lacked clear authority. The Royal Statistical Society offered to assist in reviewing the algorithm but was met with non-disclosure agreements and limited engagement. Furthermore, the External Advisory Group set up by Ofqual had no power to alter the algorithm's application.

This lack of human agency rendered the oversight ineffective, highlighting the risks of symbolic rather than substantive human involvement in ADM systems.

A szabályozási jövőkép – “governance” oldalról (1)



A szabályozási jövőkép – “governance” oldalról (2)

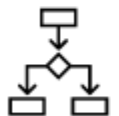


Key decision makers

Who: Leaders who define strategic decisions and high-level policies for the organisation e.g. board members, C-suite executives, managing directors, or department leaders.

Key responsibilities can include:

- Setting high-level goals for use of agents
- Defining permitted operational use cases for agents, including limits on agent’s data access
- Setting the overall governance approach, including risk management frameworks and escalation processes



Product teams

Who: These roles oversee the translation of stakeholder needs or business goals into a technical agentic solution e.g. Product Managers, UI / UX Designers, AI Engineers, Software Engineers

Key responsibilities can include:

- Defining the design and requirements for agents, as well as any feature controls or phased rollouts
- Reliable implementation of agents i.e. development, pre-deployment testing and post-deployment monitoring across the agent lifecycle
- Educating users on responsible use of agentic product



Cybersecurity teams

Who: These roles oversee the protection of agentic systems from cyber threats, by implementing and managing security measures, identifying vulnerabilities, and responding to incidents e.g. Chief Security Officer, Cyber Security Specialist, Penetration Tester

Key responsibilities can include:

- Defining baseline security guardrails and secure-by-design templates that technical teams should implement or adapt to the agentic system being deployed
- Conducting regular red teaming and threat modelling



Users

Who: Any individual who utilises the output of the agents to contribute to an organisational goal e.g. company employees making decisions or automating workflows and practices.

Key responsibilities can include:

- Ethical and responsible usage of agents
- Attending required training, complying with usage policies, timely reporting of bugs or issues with agents

A szabályozási jövőkép – hatósági oldalról

➤ Egy lehetséges hatósági megközelítés



The screenshot shows the top navigation bar of the Information Commissioner's Office (ICO) website. The logo 'ico.' is on the left, followed by the tagline 'The ICO exists to empower you through information.' and a search bar. The navigation menu includes 'Home', 'For the public', 'For organisations', 'Make a complaint', 'Action we've taken', and 'About the ICO'. Below the navigation bar, the breadcrumb trail reads 'About the Information Commissioner's Office / Media centre / News, blogs and speeches / AI'll get that! Agentic commerce could signal the dawn of personal shopping 'AI-gents''. The main heading of the article is 'AI'll get that! Agentic commerce could signal the dawn of personal shopping 'AI-gents''. Below the heading, the date 'Date 8 January 2026' and the type 'Type News' are displayed.

- ICO Tech Futures: Agentic AI
- ICO Innovation Advice Service - ingyenes tanácsadás új termékek fejlesztését kísérletelő adatvédelmi problémák megoldásához.
- ICO Regulatory Sandbox.

Záró gondolat



„Jelentős kihívást az episztemikus túlterheltség: rendkívül sok a biztonsági ajánlás, és nehéz meghatározni, hogy konkrét felhasználási esetekben melyeket kell alkalmazni.”



Security Threats to Agentic AI

How does agentic AI security differ from AI security?

In addition to traditional cybersecurity risks and risks inherent to all LLMs, agentic AI systems present novel risks through their additional capabilities in planning, action-taking, and tool use.

First, there are additional attack surfaces to secure.



Agents have memory and planning systems that could be targeted to cause undesired behavior, such as through poisoning attacks (Chen et al., 2024). They also require interfaces with other systems which could contain vulnerabilities, such as APIs and privileges for accessing databases and tools. Furthermore, they often leverage bespoke tools that could be vulnerable themselves. The additional quantity and complexity of potential vulnerabilities means additional attention and procedures are required for security.

Second, agents can potentially take rogue actions.



Given their autonomy and access to sensitive systems, agents can potentially take harmful actions. One mechanism potentially leading to this is prompt injections, where inputs (from a user or from untrusted data an agent reads) manipulate the agent and override its intended instructions. Mitigations for these attacks are still being researched; there are currently no measures to guarantee robustness of the AI itself, so effective security requires classical cybersecurity measures in other parts of the overall system such as (but not limited to) data the agent consumes and/or human review of decisions. Ultimately, there is unavoidable uncertainty in the actions of agents consuming untrusted data or using unverified components. It is necessary for security policy to accept that such agents have potential to be hijacked, and mitigate the risk of actions the agent may consequently take.

Harmful actions can also arise through misalignment, either from the agent misunderstanding the user's intent and pursuing undesired tasks, or through agents having undesired goals as a result of imperfect training or other construction processes. For example, coding agents may try to cheat their way to passing tests instead of completing the task the user intended (OpenAI, 2025a). Mitigating these risks requires attention throughout the lifecycle of the agent, such as careful alignment procedures in the design and training, testing before deployment, and oversight during deployment to address potential evolving conditions and failures.

Köszönöm a figyelmet!



Dr. Domokos Márton
Senior Tanácsadó

T +36 1 483 4824

E marton.domokos@cms-cmno.com



Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.

cms-lawnow.com

The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice. It was prepared in co-operation with local attorneys.

CMS EEIG (CMS EEIG) is a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices; details can be found under "legal information" in the footer of cms.law.

CMS locations:

Aberdeen, Abu Dhabi, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Bergen, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Cúcuta, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Liverpool, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Mexico City, Milan, Mombasa, Monaco, Munich, Muscat, Nairobi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Rome, Santiago de Chile, Sarajevo, Shanghai, Sheffield, Singapore, Skopje, Sofia, Stavanger, Strasbourg, Stuttgart, Tel Aviv, Tirana, Vienna, Warsaw, Zagreb and Zurich.

cms.law