AI Regulation Summit

A szabályokat el lehet halasztani. A felelősséget nem. Az AI Act az Omnibus után: a működő AI-tól a jogilag védhető vállalati AI-ig

2026. 09. 07. 09:20 | Future Lab | HUN · 20 perc

Dr. Kopasz János
ügyvéd, IT – Data & Cyber praxisvezető · Taylor Wessing Hungary

Dr. Kopasz János, ügyvéd, IT – Data & Cyber praxisvezető a Taylor Wessing Hungary-nál, úgy véli, hogy a vállalatoknak túl kell lépniük az AI-ról szóló felhajtáson, hogy foglalkozzanak a digitális megfelelés összetett, többrétegű jogi rendszerével.

MIRŐL VOLT SZÓ

Dr. Kopasz János kiemeli az automatizált döntéshozatal kockázatait, egy friss, 825 millió eurós bírságra hivatkozva, amelyet az Ubernek a holland adatvédelmi hatóság szabott ki. A bírság egy olyan algoritmus használatából eredt, amelyet a sofőrök csalás elleni ellenőrzésére használtak, és amely nem rendelkezett megfelelő emberi felügyelettel, ami azt mutatja, hogy még a nagyvállalatok is súlyos következményekkel szembesülhetnek a digitális megfelelés hiányában. Például a holland hatóság úgy döntött, hogy egy algoritmus javaslatának egyszerű jóváhagyása nem tekinthető megfelelő emberi beavatkozásnak.

A prezentáció világossá teszi, hogy az Omnibus csomag csak kisebb késéseket okoz a magas kockázatú mesterséges intelligencia rendszerek esetében, míg más követelmények, mint például az átláthatóság és a címkézés, ma is érvényben maradnak. Dr. Kopasz János hangsúlyozza, hogy a mesterséges intelligencia megfeleléséhez átfogóan kell tekinteni a szerzői jogokra, az e-kereskedelemre és a fogyasztóvédelmi

törvényekre, különösen mivel a szoftvereket egyre inkább termékként osztályozzák. Ezek az elemek azt jelentik, hogy a vállalatoknak egy összetett függőségi hálózatot kell kezelniük, beleértve az alapmodelleket, a felhőinfrastruktúrát és több száz alfolyamatot, nem csupán egy szabványos szoftverlicenc aláírásával.

KIEMELT MEGÁLLAPÍTÁSOK

- Uber 825 millió eurós bírságot kapott, mert az AI-ügynöke nem gyakorolt érdemi emberi felügyeletet a sofőrök kizárására vonatkozó döntésekben.
- Az omnibusz csomag csak bizonyos magas kockázatú AI szabályokat halaszt 2027-ig vagy 2028-ig, míg az átláthatósági és címkézési követelmények jelenleg érvényben vannak.
- A megfelelés a hivatalos „papíralapú” szabályzatoktól a felhasználói felületen és a háttérrendszerekben megvalósuló gyakorlati, technikai megoldások felé tolódik.

ÜZLETI HATÁS

A vállalkozások jelentős kockázatnak vannak kitéve, ha „árnyék-AI”-ra támaszkodnak, vagy harmadik féltől származó eszközöket integrálnak anélkül, hogy ellenőriznék az adatvédelmi garanciákat. Dr. Kopasz János azt javasolja, hogy a vállalatok az AI-ügynököket alkalmazottakhoz hasonlóan kezeljék, és vezessenek nyilvántartást pozícióikról, használatukról és képességeikről. A kockázatok hatékony csökkentése érdekében a szervezeteknek ki kell jelölniük egy „karmestert”, aki átlátja a digitális jog teljes spektrumát, és üzleti szemléletű megoldásokat tud kínálni, amelyek lépést tartanak a gyors IT-fejlesztési ciklusokkal.

KÖVETKEZTETÉS

Dr. Kopasz János azzal zárja, hogy a vállalatoknak a jogi megfelelést ne hatalmas egyszeri kiadásként, hanem a magas kockázatú hiányosságok azonosítására összpontosítva kellene kezelniük. Arra ösztönzi a szervezeteket, hogy használjanak olyan speciális programokat, amelyek segítenek a fejlesztőknek a minimális kockázatú megfelelés elérésében, és segítik a vállalatokat az AI szoftverek biztonságos integrálásában meglévő szervezeti struktúráikba.

AI Regulation Summit

Rules May Be Delayed. Responsibility Cannot. The AI Act After the Omnibus: From Working AI to Legally Defensible Enterprise AI

2026. 09. 07. 09:20 | Future Lab | HUN · 20 perc

Dr. János Kopasz
Attorney-at-Law, Head of the IT, Data & Cyber Practice · Taylor Wessing Hungary

Dr. János Kopasz, Attorney-at-Law and Head of the IT, Data & Cyber Practice at Taylor Wessing Hungary, argues that companies must move beyond the hype of AI to address the complex, multi-layered legal ecosystem of digital compliance.

WHAT WAS DISCUSSED

Dr. János Kopasz highlights the risks of automated decision-making by citing a recent 825 million euro fine imposed on Uber by the Dutch Data Protection Authority. The penalty resulted from an AI agent that monitored drivers for fraud without sufficient human oversight, demonstrating that even large companies with dedicated legal teams can fail to manage algorithmic accountability. For example, the authority determined that simply approving an algorithm's suggestion did not constitute adequate human intervention.

The presentation clarifies that the Omnibus package provides only a limited delay for high-risk AI systems until 2027 or 2028, while other requirements like transparency and labeling remain active today. Dr. János Kopasz emphasizes that AI compliance is not a standalone task but involves a web of copyright, e-commerce, and consumer protection laws. These elements mean that companies must view AI as a product subject to traditional legal frameworks while simultaneously managing new technological risks.

KEY TAKEAWAYS

- Uber received an 825 million euro fine because its AI-driven driver monitoring lacked meaningful human oversight.
- The Omnibus package only delays specific high-risk AI rules, meaning transparency and labeling requirements are currently enforceable.
- AI software is increasingly classified as a product, bringing it under the scope of new product liability regulations.

BUSINESS IMPACT

The practical dimension of AI adoption requires a holistic approach where legal teams act as "conductors" who understand both technical sprints and business goals. Organizations must manage "shadow AI" and unauthorized API connections to personal models like Google Gemini to prevent data leaks. Furthermore, purchasing an AI tool involves acquiring an entire ecosystem of base models, cloud infrastructure, and subprocessors, necessitating much more rigorous due diligence than standard software licenses.

CONCLUSION

Dr. János Kopasz concludes by recommending that companies move away from "check-the-box" compliance toward a risk-based approach that identifies critical vulnerabilities. He encourages businesses to focus on high-impact gaps that could lead to serious incidents rather than attempting to solve every minor issue at once. He invites the audience to explore his specific programs designed to help developers and companies achieve minimal risk-based legal compliance efficiently.