

„AI” a vállalkozásban – lehetőség vagy adatvédelmi kockázat?

A mesterséges intelligencia az elmúlt két évben robbanásszerűen és viharos gyorsasággal jelent meg és hódított teret magának a vállalkozások mindennapjaiban. Egyre többen



használnak olyan eszközöket, mint a ChatGPT, a Microsoft Copilot vagy a Google Gemini, legyen szó ajánlatok készítéséről, marketinganyagok megírásáról, e-mailek megfogalmazásáról vagy akár ügyfélmegkeresések megválaszolásáról.

A technológia vitathatlanul jelentős és szinte emberi léptékkal felfoghatatlan előnyöket kínál. Egy jól megfogalmazott kérdésre másodpercek alatt kapunk olyan választ, amelynek elkészítése

korábban akár órákat vagy több munkavállaló együttes munkáját vette volna igénybe. Nem véletlen, hogy egyre több kis- és középvállalkozás munkatársai is napi szinten használják ezeket az eszközöket.

A valódi kérdés már régóta nem az, hogy használjuk-e a mesterséges intelligenciát, hanem az, hogy hogyan használjuk biztonságosan.

Képzeljünk el egy könyvelőirodát, egy építőipari vállalkozást vagy egy webáruházat. Egy munkatárs szeretné gyorsabban elkészíteni egy ügyfélnek szóló ajánlat szövegét, ezért bemásolja a ChatGPT-be egy korábbi ajánlat teljes tartalmát. Az anyag tartalmazza az ügyfél nevét, elérhetőségét, a szerződéses feltételeket és az árazást is. A válasz néhány másodperc alatt elkészül, a feladat sikeresnek tűnik – közben azonban a vállalkozás olyan adatokat adott át egy külső szolgáltatásnak, amelyek kezeléséről a cég vezetése valószínűleg nem is tudott.

Hasonló helyzetek nemcsak kisvállalkozásoknál fordulhatnak elő. Nemzetközi visszhangot váltott ki, amikor a Samsung több munkavállalója bizalmas vállalati információkat, forráskódokat és belső dokumentumokat töltött fel a ChatGPT-be munkavégzés közben. Az esetet követően a vállalat korlátozta a mesterséges intelligencia eszközök használatát, mivel fennállt a veszélye annak, hogy érzékeny vállalati információk kerülnek ki a szervezet ellenőrzése alól.

További információ:

- Forbes:
<https://www.forbes.com/sites/siladityaray/2023/05/02/samsung-bans-chatgpt-and-other-chatbots-for-employees-after-sensitive-code-leak/>
- Cybersecurity Dive:
<https://www.cybersecuritydive.com/news/Samsung-Electronics-ChatGPT-leak-data-privacy/647219/>

A téma adatvédelmi jelentőségét jól mutatja, hogy az európai adatvédelmi hatóságok is kiemelt figyelemmel foglalkoznak a mesterséges intelligencia rendszerekkel. Az olasz adatvédelmi hatóság (Garante) 2024. decemberében 15 millió euró bírságot szabott ki az OpenAI részére, mert álláspontja szerint az adatkezeléssel és a felhasználók tájékoztatásával kapcsolatban adatvédelmi hiányosságok merültek fel.

További információ:

- Reuters: <https://www.reuters.com/technology/italy-fines-openai-15-million-euros-over-privacy-rules-breach-2024-12-20/>
- AP News: <https://apnews.com/article/6760575ae7a29a1dd22cc666f49e605f>

Fontos hangsúlyozni, hogy a mesterséges intelligencia használata önmagában nem jelent adatvédelmi jogsértést. A kockázatot jellemzően nem maga az eszköz, hanem annak ellenőrizetlen használata okozza. A problémák többsége abból fakad, hogy a felhasználók személyes adatokat, ügyfél adatokat, szerződéseket vagy egyéb bizalmas információkat töltenek fel a rendszerbe anélkül, hogy mérlegelnék az adatkezelés következményeit.

A vállalkozások számára ezért célszerű néhány alapvető szabályt kialakítani:

- személyes adatokat és ügyfél adatokat ne töltsünk fel mesterséges intelligencia rendszerbe;
- szerződések, ajánlatok és üzleti titkok esetén alkalmazzunk anonimizálást vagy általánosítást;
- a munkavállalók számára határozzuk meg, milyen célra és milyen feltételekkel használhatók AI-eszközök;
- gondoskodjunk arról, hogy a munkatársak tisztában legyenek az adatvédelmi és információbiztonsági kockázatokkal.

A mesterséges intelligencia a következő években az eddigiekhez képest sokkal jobban a mindennapi munkavégzés részévé válik, ahogy tette ezt az internet vagy a felhőalapú szolgáltatások sora. Azok a vállalkozások azonban, amelyek időben kialakítják a biztonságos használat szabályait, nemcsak az adatvédelmi kockázatokat csökkenthetik, hanem a technológia előnyeit is hatékonyabban használhatják ki.

Szabó Péter