AI NA VRIJEME / KONTROLNI POPIS

Smijem li ovo poslati AI-ju?

Prođite provjeru prije slanja poruke, slike ili dokumenta javnom AI alatu. Nejasan odgovor razlog je da stanete.

- ☐ Sadržaj ne sadrži lozinku, jednokratni kod, privatni ključ ni drugu aktivnu pristupnu tajnu.
- ☐ Provjerio/la sam ima li osobnih podataka i podataka drugih ljudi, uključujući djecu.
- ☐ Nisam previdio/la zdravlje, plaće, dugovanja, životopise, identifikacijske dokumente ili druge osjetljive informacije.
- ☐ Znam smijem li podijeliti povjerljivi poslovni sadržaj, neobjavljenu ponudu ili interni dokument.
- ☐ Najprije sam pokušao/la pitanje postaviti bez cijele datoteke, koristeći opći ili izmišljeni primjer.
- ☐ Uklonio/la sam nepotrebne detalje, komentare, metapodatke i sadržaj skriven u drugim listovima dokumenta.
- ☐ Brisanje imena nisam zamijenio/la s pravom anonimizacijom. Osoba se može prepoznati i iz konteksta.
- ☐ Za poslovne podatke koristim procijenjen i odobren sustav, uz potrebnu pravnu osnovu i zaštitne mjere.
- ☐ Provjerio/la sam pravila konkretnog računa. Plaćanje i isključeno treniranje sami ne daju ovlast za slanje.
- ☐ Znam kako ću provjeriti dobiveni odgovor prije nego što ga upotrijebim.

Ako ste već poslali aktivnu tajnu, promijenite je ili opozovite. Za poslovni incident odmah obavijestite odgovornu osobu. Brisanje razgovora samo po sebi ne rješava incident.

Izvori: AZOP: Preporuka za sigurno korištenje LLM alata; EU: Uredba 2016/679, Opća uredba o zaštiti podataka; OpenAI: Data Controls FAQ; OpenAI: Temporary Chat FAQ.

Pripada vodiču: Što nikad ne biste trebali upisati u ChatGPT, Gemini, Claude ili drugi AI.