INFORMACIJSKI POOBLAŠČENEC

VARNA IN ODGOVORNA UPORABA UMETNE INTELIGENCE PRI DELU

Priporočila za javne uslužbence

1. **Preverite interne akta organa, če je uporaba orodij umetne inteligence (UI) sploh dopustna – katera orodja in pod kakšnimi pogoji.**

   Če menite, da bi vam uporaba UI koristila pri vašem delu, pa uporaba orodij UI ni opredeljena v nobenem izmed aktov, o tem obvestite vaše nadrejene.

2. **V orodja UI ne vnašajte nobenih osebnih, zaupnih in drugih varovanih podatkov – če ni to izrecno dopustno in predvideno za konkretni primer uporabe določenega orodja.**

   a. **Preventiva je boljša kot kurativa**. Najmanj problematična je uporaba orodij UI, pri kateri ne vnašate osebnih, zaupnih in drugih varovanih podatkov. S tem so mišljeni predvsem podatki, ki se nanašajo na določljive posameznike, na vas ali vaše stranke oziroma zaposlene, ter razne poslovne skrivnosti in interne dokumente.

   b. Pri vnosu kakršnih koli podatkov **bodite kritični in ravnajte premišljeno**. V orodja UI ne vnašajte polnih besedil iz dokumentov, ne nalagajte celotnih datotek ali fotografij oseb.

3. **Ali je vnašanje osebnih podatkov v orodja UI kdaj vseeno dopustno?**

   a. Vsaka obdelava osebnih podatkov – na primer vnos v orodje UI, hramba, posredovanje – mora izpolnjevati vsa **pravila varstva osebnih podatkov**. Temeljiti mora na zakoniti pravni podlagi, zagotovljene morajo biti pravice posameznikov, spoštovana temeljna načela in zagotovljena ustrezna varnost podatkov. Če upoštevate vsa pravila, potem je vnos dopusten. Vendar opozarjamo, da je **večina komercialnih orodij UI trenutno problematična vsaj z vidika zagotavljanja pravic posameznikom**.

   b. Če niste prepričani, da je vnos osebnih podatkov ustrezno (zakonsko) urejen in predviden za konkretno orodje UI in način uporabe, potem osebnih podatkov v orodje UI ne vnašajte.

4. **Manj je več – če že uporabljate orodja UI pri svojem delu, poskrbite, da v njih vnašate najmanjši možen obseg podatkov, s katerim še lahko dovolj učinkovito opravite svoje delo.**

   Zavedajte se, da se **sistemi UI na podlagi vnesenih podatkov učijo** in lahko vse vnesene podatke **uporabijo za svoje nadaljnje delovanje**.

5. Ni vsako brisanje osebnih podatkov anonimizacija.

a. Zgolj **brisanje "najbolj očitnih" osebnih podatkov**, kot so ime, naslov prebivališča in EMŠO številke **še ne pomeni, da posameznika ni več mogoče prepoznati oziroma da postane anonimen**. To pomeni, da gre še vedno za obdelavo osebnih podatkov.
b. Anonimizacija pomeni, da posameznik sploh ni več določljiv. Zgolj anonimni podatki niso več osebni podatki (kot npr. statistični podatki).
c. Na to je treba še zlasti paziti pri uporabi orodij UI, saj so ta posebej dobra v povezovanju najrazličnejših podatkov, na podlagi katerih **lahko pridejo do marsikaterih novih sklepov oz. informacij**. Na hitro in "po domače" opravljeni poskusi anonimizacije v večini primerov ne bodo primerni za učinkovito varovanje posameznikovih osebnih podatkov.

6. Vedno preverite pravilnost prejetih odgovorov.

a. Namen **človeškega nadzora** je preprečiti ali čim bolj zmanjšati tveganja, ki se lahko pojavijo pri uporabi UI. Orodja UI so namreč boljša v statističnem napovedovanju kot v dejanskem razumevanju sveta.
    i. **Umetna inteligenca si lahko izmisli odgovore (t. i. "haluciniranje")**, zato vedno dvakrat **preverite pravilnost** prejetega odgovora. Zavedajte se možnosti, da podatki, ki jih uporablja izbrano orodje, niso vedno ažurni, pravilni ali dovolj široki za podajo pravilnega in zanesljivega odgovora na vaše vprašanje, predvsem pa da niso zanesljiv vir podajanja strokovnih nasvetov v zvezi z vašim delom.
    ii. **Vedno preverite, ali so odgovori nepristranski.** Predvsem poskrbite, da uporaba UI pri vašem delu ne bo imela negativnega vpliva na ranljive posameznike ali skupine ljudi. Odgovori, ki jih podajajo orodja UI, pogosto odsevajo že ustaljene predsodke, ki so se jih priučila na podlagi podatkov, na katerih so bili učena. Vaša naloga je, da takšno pristranskost zaznate in preprečite diskriminacijo.

7. Ne prenašajte odgovornosti na orodje UI.

a. Ljudje smo že po naravi nagnjeni k temu, da zelo **hitro in brez večjega razmisleka zaupamo rezultatom, ki nam jih dajo računalniški programi in da na tej podlagi sprejmemo odločitev**, ki je malodane enaka tisti, ki nam jo je ponudil program. Pri orodjih UI, ki so sposobna svoje odgovore oblikovati tako, da ti že na prvi pogled delujejo kot izčrpni in strukturirani, čeprav njihova vsebina morda sploh ni pravilna, je to še toliko bolj nevarno.
b. Dodatna **previdnost je potrebna zlasti na tistih področjih, na katerih nimamo ustreznega znanja** in se zanašamo zgolj na občutek, kaj se nam zdi pravilno, skladno z našimi življenjskimi izkušnjami.
c. Uporaba orodij UI ne sme postati izgovor, zakaj je bilo v neki zadevi odločeno na določen način. **Končna in predvsem vsebinska presoja mora še vedno ostati v človeških rokah**, odločevalec pa mora znati svoje razloge za odločitev tudi **obrazložiti**.