EOVP-ENVP

Skupno mnenje 5/2021

o predlogu Uredbe Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci (Akt o umetni inteligenci)

18. junij 2021

Povzetek

Evropska komisija je 21. aprila 2021 predstavila predlog Uredbe Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci (v nadaljevanju: predlog). EOVP in ENVP pozdravljata skrb zakonodajalca pri obravnavanju uporabe umetne inteligence (UI) v Evropski uniji (EU) in poudarjata, da ima predlog zelo pomembne **posledice za varstvo podatkov**.

EOVP in ENVP ugotavljata, da je **pravna podlaga** predloga predvsem člen 114 Pogodbe o delovanju Evropske unije (PDEU). Predlog poleg tega temelji tudi na členu 16 PDEU, ker vsebuje posebna pravila o varstvu posameznikov pri obdelavi osebnih podatkov, zlasti omejitvi uporabe umetnointeligenčnih sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene kazenskega pregona. EOVP in ENVP opozarjata, da v skladu s sodno prakso Sodišča Evropske unije (SEU), člen 16 PDEU zagotavlja ustrezno pravno podlago v primerih, v katerih je varstvo osebnih podatkov eden od bistvenih ciljev ali elementov pravil, ki jih je sprejel zakonodajalec EU. Uporaba člena 16 PDEU vključuje tudi potrebo po **zagotavljanju neodvisnega nadzora skladnosti** z zahtevami glede obdelave osebnih podatkov, kot je zahtevano tudi v členu 8 Listine EU o temeljnih pravicah.

EOVP in ENVP v zvezi s **področjem uporabe predloga** odločno pozdravljata dejstvo, da je razširjeno na zagotavljanje in uporabo umetnointeligenčnih sistemov s strani institucij, organov ali agencij EU. Vendar **izključitev mednarodnega sodelovanja na področju kazenskega pregona iz področja uporabe predloga** vzbuja resno skrb pri EOVP in ENVP, saj taka izključitev povzroča resno tveganje izogibanja (na primer tretje države ali mednarodne organizacije uporabljajo aplikacije velikega tveganja, na katere se opirajo javni organi v EU).

EOVP in ENVP **pozdravljata pristop, ki temelji na tveganju** in je podlaga predloga. Vendar bi bilo treba ta pristop podrobneje pojasniti in koncept „tveganja za temeljne pravice" uskladiti s Splošno uredbo o varstvu podatkov in Uredbo (EU) 2018/1725 (v nadaljevanju: EUDPR), ker so vključeni vidiki v zvezi z varstvom osebnih podatkov.

EOVP in ENVP se strinjata s predlogom, ko navaja, da klasifikacija **umetnointeligenčnega sistema kot sistema velikega tveganja ne pomeni nujno, da je zakonit** sam po sebi in ga lahko uporabnik uporablja kot takega. Upravljavec **bo morda moral upoštevati dodatne zahteve, ki izhajajo iz prava EU o varstvu podatkov**. Poleg tega bi morala biti skladnost s pravnimi obveznostmi, ki izhajajo iz zakonodaje Unije (vključno glede varstva osebnih podatkov), prvi pogoj za vstop na evropski trg kot proizvod z oznako CE. Temu ustrezno EOVP in ENVP menita, da **bi bilo treba zahtevo glede zagotavljanja skladnosti s Splošno uredbo o varstvu podatkov in EUDPR vključiti v poglavje 2 naslova III**. Poleg tega EOVP in ENVP menita, da je treba prilagoditi postopek ugotavljanja skladnosti predloga, tako da tretje osebe vedno opravijo predhodna ugotavljanja skladnosti umetnointeligenčnih sistemov velikega tveganja.

Glede na veliko tveganje diskriminacije predlog prepoveduje „družbeno točkovanje", kadar se izvaja 'v določenem časovnem obdobju' ali 's strani javnih organov ali v njihovem imenu'. Vendar lahko zasebna podjetja, kot so družbeni mediji in ponudniki storitev v oblaku, tudi obdelujejo velike količine osebnih podatkov in izvajajo družbeno točkovanje. Zato **bi morala prihodnja uredba o umetni inteligenci prepovedati vse vrste družbenega točkovanja**.

Biometrična identifikacija posameznikov na daljavo v javno dostopnih prostorih je veliko tveganje za vdor v zasebno življenje posameznikov in z resnimi učinki na pričakovanje prebivalstva, da je v javnih prostorih anonimno. EOVP in ENVP zato **pozivata k splošni prepovedi kakršne koli uporabe umetne inteligence za avtomatizirano prepoznavanje človeških lastnosti v javno dostopnih prostorih**, kot je

prepoznavanje obrazov in tudi hoje, prstnih odtisov, DNK, glasu, udarcev po tipkovnici in drugih biometričnih ali vedenjskih znakov v kakršnem koli kontekstu. Enako se priporoča **prepoved umetnointeligenčnih sistemov za razvrščanje posameznikov na podlagi biometričnih podatkov v skupine** glede na etnično poreklo, spol, kakor tudi politično ali spolno usmerjenost ali druge razloge za diskriminacijo na podlagi člena 21 Listine EU o temeljnih pravicah. Nadalje EOVP in ENVP menita, da je uporaba umetne inteligence **za ugotavljanje čustev fizičnih oseb zelo nezaželena in bi jo bilo treba prepovedati.**

EOVP in ENVP pozdravljata **imenovanje ENVP za pristojni organ in organ za nadzor trga za nadzor institucij, agencij in organov Unije**. Vendar bi bilo treba vlogo in naloge ENVP dodatno pojasniti, zlasti kadar ima vlogo organa za nadzor trga. Nadalje bi prihodnja uredba o umetni inteligenci morala jasno vzpostaviti **neodvisnost nadzornih organov** pri izvajanju nalog nadzora in izvrševanja.

Imenovanje organov za varstvo podatkov za nacionalne nadzorne organe bi zagotovilo bolj usklajen regulativni pristop in pripomoglo k dosledni razlagi določb o obdelavi podatkov ter preprečevanju protislovij pri izvrševanju le teh med državami članicami. Zato EOVP in ENVP menita, da **bi bilo treba organe za varstvo podatkov imenovati za nacionalne nadzorne organe v skladu s členom 59 predloga.**

Predlog Komisiji dodeljuje prevladujočo vlogo v „Evropskem odboru za umetno inteligenco" (EOUI). Takšna vloga je v nasprotju s potrebo po neodvisnosti evropskega organa za umetno inteligenco od kakršnega koli političnega vpliva. Da se zagotovi njegova neodvisnost, bi morala prihodnja uredba o umetni inteligenci dati **večjo avtonomijo Evropskemu odboru za umetno inteligenco**, in zagotoviti, da lahko deluje na lastno pobudo.

Upoštevajoč razširjenost umetnointeligenčnih sistemov na enotnem trgu in verjetnost čezmejnih primerov, sta nujno potrebna usklajeno izvrševanje in ustrezna dodelitev pristojnosti med nacionalnimi nadzornimi organi. EOVP in ENVP predlagata načrtovanje **mehanizma, ki bo za vsak umetnointeligenčni sistem zagotovil enotno kontaktno točko tako za posameznike kakor tudi za podjetja, ki jih zadeva predmetna zakonodaja.**

Glede **peskovnikov** EOVP in ENVP **priporočata, da se pojasni njihovo področje uporabe in cilji**. Predlog bi moral tudi jasno navesti, da bi morala biti pravna podlaga za te peskovnike skladna z zahtevami, vzpostavljenimi v obstoječem okviru za varstvo podatkov.

Sistemu izdajanja potrdil, opisanem v predlogu, manjka jasna povezava z zakonodajo EU o varstvu podatkov, kakor tudi z drugo zakonodajo EU in držav članic, ki se uporablja za posamezno področje visoko rizičnega umetnointeligenčnega sistema, in ne upošteva **načel čim manjšega zbiranja podatkov in vgrajenega varstva podatkov** kot enega od vidikov, ki jih je treba upoštevati **pred pridobitvijo oznake CE**. EOVP in ENVP zato priporočata spremembo predloga, tako da se pojasni razmerje med potrdili, izdanimi na podlagi navedene uredbe, ter izdajanjem potrdil, pečati in označbami za varstvo podatkov. Nazadnje bi morali biti organi za varstvo podatkov vključeni v pripravo in vzpostavitev usklajenih standardov in skupnih specifikacij.

Glede **kodeksov ravnanja** EOVP in ENVP menita, da je **treba pojasniti**, ali naj se varstvo osebnih podatkov šteje med „dodatne zahteve", ki jih lahko obravnavajo ti kodeksi ravnanja, in zagotoviti, da „tehnične specifikacije in rešitve" niso v nasprotju s pravili in načeli veljavnega okvira EU za varstvo podatkov.

KAZALO

1 UVOD 5
2 ANALIZA KLJUČNIH NAČEL PREDLOGA 7
2.1 Področje uporabe predloga in povezava z veljavnim pravnim okvirom 7
2.2 Pristop, ki temelji na tveganju 9
2.3 Prepovedane uporabe umetne inteligence 11
2.4 Umetnointeligenčni sistemi velikega tveganja 13
2.4.1 Potreba po predhodnem ugotavljanju skladnosti, ki ga opravijo zunanje tretje osebe 13
2.4.2 Področje uporabe uredbe mora zajemati tudi umetnointeligenčne sisteme, ki se že uporabljajo 14
2.5 Upravljanje in Evropski odbor za umetno inteligenco 14
2.5.1 Upravljanje 14
2.5.2 Evropski odbor za umetno inteligenco 16
3 MEDSEBOJNI VPLIVI S PRAVNIM OKVIROM ZA VARSTVO PODATKOV 17
3.1 Povezava predloga z veljavno zakonodajo EU o varstvu podatkov 17
3.2 Peskovnik in nadaljnja obdelava (člena 53 in 54 predloga) 18
3.3 Preglednost 20
3.4 Obdelava posebnih kategorij podatkov in podatkov, povezanih s kaznivimi dejanji 20
3.5 Mehanizmi skladnosti 21
3.5.1 Izdajanje potrdil 21
3.5.2 Kodeksi ravnanja 22
4 ZAKLJUČEK 23

Evropski odbor za varstvo podatkov in Evropski nadzornik za varstvo podatkov sta,

ob upoštevanju člena 42(2) Uredbe (EU) 2018/1725 z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES[1],

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu EGP, kakor je bil spremenjen s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[2],

ob upoštevanju zahteve za skupno mnenje Evropskega nadzornika za varstvo podatkov in Evropskega odbora za varstvo podatkov z dne 22. aprila 2021 o predlogu Uredbe o določitvi harmoniziranih pravil o umetni inteligenci (Akt o umetni inteligenci),

SPREJELA NASLEDNJE SKUPNO MNENJE

1 UVOD

1. Razvoj sistemov umetne inteligence je zelo pomemben korak v razvoju tehnologij in načinu človeške interakcije z njimi. Umetna inteligenca je nabor ključnih tehnologij, ki bodo tako iz družbenega ali gospodarskega vidika temeljito spremenile naš vsakdan. V naslednjih nekaj letih je pričakovati bistvene odločitve v zvezi z umetno inteligenco, ki nam pomaga premagovati nekatere izmed največjih izzivov, s katerimi se danes soočamo na številnih področjih, in segajo od zdravja do mobilnosti ali od javne uprave do izobraževanja.

2. Ta obljubljeni napredek pa ne prihaja brez tveganj. Tveganja so dejansko zelo pomembna, saj so posamezni in družbeni učinki umetnointeligenčnih sistemov pretežno še neznani. Ustvarjanje vsebin, napovedovanje ali sprejemanje odločitev na avtomatiziran način, kot to počnejo umetnointeligenčni sistemi s tehnikami strojnega učenja ali logike in pravili verjetnostnega sklepanja, ni enako izvajanju teh aktivnosti s strani ljudi s pomočjo ustvarjalnega ali teoretičnega sklepanja, pri čemer se popolnoma zavedajo odgovornosti za posledice.

3. Umetna inteligenca bo povečala količino predvidevanj, ki so mogoča na številnih področjih, začenši z merljivimi korelacijami med podatki, ki niso vidne s človeškim očesom, vendar so vidne stroju, in tako olajšala naša življenja ter rešila veliko problemov, hkrati pa bo spodkopala našo sposobnost vzročne razlage izidov tako, da bodo pojmi, kot so preglednost, človeški nadzor in odgovornost za rezultate, postali zelo vprašljivi.

4. Podatki (osebni in neosebni) v umetni inteligenci so v številnih primerih ključni pogoj za avtonomne odločitve, ki bodo neizogibno vplivale na življenje posameznikov na različnih ravneh. Zato EOVP in ENVP že na tej stopnji odločno zatrjujeta, da ima predlog Uredbe o

[1] UL L 295, 21. 11. 2018, str. 39–98.
[2] Sklicevanje na „države članice“ v tem dokumentu je potrebno razumeti kot sklicevanje na „države članice EGP“.

določitvi harmoniziranih pravil o umetni inteligenci (Akt o umetni inteligenci) (v nadaljevanju: predlog)[3] **pomembne posledice za varstvo podatkov**.

5. Dodeljevanje naloge odločanja strojem na podlagi podatkov bo ustvarilo tveganja za pravice in svoboščine posameznikov, vplivalo na njihovo zasebno življenje in bi lahko škodilo skupinam ali celo celotnim družbam. EOVP in ENVP poudarjata, da sta pravica do zasebnega življenja in pravica do varstva osebnih podatkov, ki sta v nasprotju z domnevo avtonomije odločanja strojev kot temeljem koncepta umetne inteligence, steber vrednot EU, ki so priznane v Splošni deklaraciji človekovih pravic (člen 12), Evropski konvenciji o človekovih pravicah (člen 8) in Listini EU o temeljnih pravicah (člena 7 in 8). Uskladitev vidika rasti, ki ga zagotavlja uporaba umetne inteligence, ter centralnosti in primarnosti ljudi v primerjavi s stroji je zelo ambiciozen, toda potreben cilj.

6. EOVP in ENVP pozdravljata sodelovanje pri urejanju vseh deležnikov v umetnointeligenčni vrednostni verigi in uvedbo posebnih zahtev za ponudnike rešitev, ki imajo pomembno vlogo pri proizvodih, ki uporabljajo njihove sisteme. Odgovornosti različnih strani, uporabnika, ponudnika, uvoznika ali distributerja umetnointeligenčnega sistema je treba jasno opredeliti in dodeliti. Zlasti pri obdelavi osebnih podatkov bi bilo treba posebno pozornost nameniti doslednosti teh vlog in odgovornosti s pojmoma upravljavec podatkov in obdelovalec podatkov, ki se uporabljata v okviru varstva podatkov, saj obe normi nista skladni.

7. Predlog daje pomembno mesto pojmu človekovega nadzora (člen 14), ki ga EOVP in ENVP pozdravljata. Vendar, kot je bilo že predhodno navedeno, bi se zaradi močnega možnega vpliva nekaterih umetnointeligenčnih sistemov na posameznike ali skupine posameznikov resnična osredinjenost na človeka morala opreti na visokokvalificiran človeški nadzor in zakonito obdelavo, če taki sistemi temeljijo na obdelavi osebnih podatkov ali obdelujejo osebne podatke za izpolnjevanje svoje naloge, tako da se zagotovi spoštovanje pravice, da nismo predmet odločitve, ki temelji izključno na avtomatizirani obdelavi.

8. Poleg tega bi moral predlog zaradi podatkovno intenzivne narave številnih aplikacij umetne inteligence spodbujati sprejetje vgrajenega in privzetega pristopa varstva podatkov na vseh ravneh ter spodbujati učinkovito izvajanje načel varstva podatkov (kot je predvideno v členu 25 Splošne uredbe o varstvu podatkov in členu 27 Uredbe o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Evropske unije) z uporabo najsodobnejših tehnologij.

9. Nazadnje EOVP in ENVP poudarjata, da je to skupno mnenje predloženo le kot predhodna analiza predloga brez poseganja v kakršno koli nadaljnjo oceno in mnenje o učinkih predloga in njegovo združljivostjo z zakonodajo EU o varstvu podatkov.

[3] COM(2021) 206 final.

2 ANALIZA KLJUČNIH NAČEL PREDLOGA

2.1 Področje uporabe predloga in povezava z veljavnim pravnim okvirom

10. V skladu z obrazložitvenim memorandumom je **pravna podlaga** predloga predvsem člen 114 PDEU, ki določa sprejetje ukrepov za zagotovitev vzpostavitve in delovanja notranjega trga[4]. Predlog poleg tega temelji tudi na členu 16 PDEU, *ker vsebuje posebna pravila o varstvu posameznikov pri obdelavi osebnih podatkov*, zlasti omejitve uporabe umetnointeligenčnih sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj[5].

11. EOVP in ENVP želita spomniti, da v skladu s sodno prakso Sodišča Evropske unije člen 16 PDEU zagotavlja ustrezno pravno podlago v primerih, v katerih je varstvo osebnih podatkov eden od bistvenih ciljev ali elementov pravil, ki jih je sprejel zakonodajalec EU[6]. Uporaba člena 16 PDEU vključuje tudi potrebo zagotavljanja neodvisnega nadzora skladnosti z zahtevami glede obdelave osebnih podatkov, kot je zahtevano tudi v členu 8 Listine EU o temeljnih pravicah.

12. EOVP in ENVP poudarjata, da že obstaja celovit okvir za varstvo podatkov, sprejet na podlagi člena 16 PDEU, ki ga sestavljajo Splošna uredba o varstvu podatkov[7], Uredba o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Evropske unije (EUDPR)[8] ter Direktiva (EU) 2016/680 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj (v nadaljevanju: Direktiva o kazenskem pregonu)[9]. V skladu s predlogom se lahko le dodatne omejitve v zvezi z obdelavo biometričnih podatkov iz predloga štejejo za tiste, ki temeljijo na členu 16 PDEU in imajo zato enako pravno podlago kot Splošna uredba o varstvu podatkov, EUDPR in Direktiva o kazenskem pregonu. To ima pomembne posledice za odnos med predlogom in Splošno uredbo o varstvu podatkov, EUDPR in Direktivo o kazenskem pregonu, na splošno, kot je navedeno v nadaljevanju.

13. Glede **področja uporabe predloga** EOVP in ENVP močno pozdravljata dejstvo, da je predlog razširjen na uporabo umetnointeligenčnih sistemov s strani institucij, organov ali agencij EU. Glede na to, da lahko uporaba sistemov umetne inteligence s strani teh subjektov, podobno kot pri uporabi v državah članicah EU, pomembno vpliva tudi na temeljne pravice posameznikov,

---

[4] Obrazložitveni memorandum, str. 5.
[5] Obrazložitveni memorandum, str. 6. Glej tudi uvodno izjavo (2) predloga.
[6] Mnenje z dne 26. julija 2017, *PNR Kanada*, postopek za izdajo mnenja 1/15, ECLI:EU:C:2017:592, točka 96.
[7] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov), UL L 119, 4. 5. 2016, str. 1–88.
[8] Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES, UL L 295, 21. 11. 2018, str. 39–98.
[9] Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ, UL L 119, 4. 5. 2016, str. 89–131.

je nujno, da novi zakonodajni okvir za umetno inteligenco velja tako za države članice EU kot za institucije, urade, organe in agencije EU, da se zagotovi usklajen pristop po vsej Uniji. Ker lahko institucije, uradi, organi in agencije EU delujejo kot ponudniki in tudi uporabniki umetnointeligenčnih sistemov, ENVP in EOVP menita, da je povsem primerno vključiti te subjekte v področje uporabe predloga na podlagi člena 114 PDEU.

14. Vendar imata EOVP in ENVP resne pomisleke glede izključitve mednarodnega sodelovanja na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj iz področja uporabe, kot je to določeno v členu 2(4) predloga. Ta izključitev povzroča resno tveganje izogibanja (na primer tretje države ali mednarodne organizacije upravljajo aplikacije velikega tveganja, na katere se zanašajo javni organi v EU).

15. Razvoj in uporaba umetnointeligenčnih sistemov bosta v številnih primerih vključevala obdelavo osebnih podatkov. Zagotavljanje jasnosti odnosa med tem predlogom in veljavno zakonodajo EU o varstvu podatkov je zelo pomembno. Predlog ne posega v ter dopolnjuje Splošno uredbo o varstvu podatkov, EUDPR in Direktivo o kazenskem pregonu. V uvodnih izjavah predloga je pojasnjeno, da bi morala biti uporaba umetnointeligenčnih sistemov še vedno v skladu z zakonodajo o varstvu podatkov, **EOVP in ENVP pa močno priporočata, da se v členu 1 predloga pojasni, da se zakonodaja Unije o varstvu osebnih podatkov**, zlasti Splošna uredba o varstvu podatkov, EUDPR, Direktiva o zasebnosti in elektronskih komunikacijah[10] ter Direktiva o kazenskem pregonu, uporablja za vsako obdelavo osebnih podatkov, ki spada na področje uporabe predloga. Ustrezna uvodna izjava bi morala prav tako pojasniti, da namen predloga ni vplivati na uporabo veljavnih zakonov EU, ki urejajo obdelavo osebnih podatkov, vključno z nalogami in pooblastili neodvisnih nadzornih organov, pristojnih za spremljanje skladnosti s temi instrumenti.

[10] Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), kakor je bila spremenjena z Direktivo 2009/136/ES in Direktivo 2009/136/ES.

2.2 Pristop, ki temelji na tveganju

16. EOVP in ENVP **pozdravljata pristop, ki temelji na tveganju** in je podlaga predloga. Predlog bi se uporabljal za vse umetnointeligenčne sisteme, vključno s tistimi, ki ne vključujejo obdelave osebnih podatkov, vendar lahko še vedno vplivajo na interese ali temeljne pravice in svoboščine.

17. EOVP in ENVP ugotavljata, da nekatere določbe predloga ne upoštevajo tveganj za skupine posameznikov ali celotno družbo (na primer kolektivni učinki s posebnim pomenom, kot je skupinska diskriminacija ali izražanje političnih mnenj v javnih prostorih). EOVP in ENVP priporočata, da se družbena oziroma skupinska tveganja, ki jih predstavljajo umetnointeligenčni sistemi, prav tako enako ocenijo in ublažijo.

18. EOVP in ENVP menita, da bi bilo treba pojasniti pristop, ki temelji na tveganju, ki je podlaga predloga, koncept „tveganja za temeljne pravice“ pa **uskladiti s Splošno uredbo o varstvu podatkov**, če pridejo v poštev vidiki varstva osebnih podatkov. Ne glede na to, ali so to končni uporabniki, preprosto posamezniki, na katere se nanašajo podatki, ali druge osebe, ki jih zadeva umetnointeligenčni sistem, se zdi, da je odsotnost kakršnega koli sklicevanja v besedilu na posameznika, na katerega vpliva umetnointeligenčni sistem, vrzel v predlogu. Vsekakor bi morale obveznosti, naložene akterjem v razmerju do prizadetih oseb, konkretneje izhajati iz varstva posameznika in njegovih pravic. Zato EOVP in ENVP pozivata zakonodajalce, naj v predlogu izrecno obravnavajo **pravice in pravna sredstva, ki so na voljo posameznikom**, za katere se uporabljajo umetnointeligenčni sistemi.

19. EOVP in ENVP sta seznanjena z odločitvijo, da se zagotovi izčrpen seznam **umetnointeligenčnih sistemov velikega tveganja**. Ta odločitev bi lahko ustvarila črno-beli učinek s šibkimi zmožnostmi privabljanja zelo tveganih situacij, kar bi ogrozilo splošni pristop, ki temelji na tveganju, ki je podlaga predloga. Poleg tega ta seznam umetnointeligenčnih sistemov velikega tveganja, ki je podrobno opisan v prilogah II in III predloga, ne vsebuje nekaterih vrst primerov uporabe, ki vključujejo znatna tveganja, kot je uporaba umetne inteligence za določanje zavarovalne premije ali ocenjevanje medicinskega zdravljenja ali za namene zdravstvenih raziskav. EOVP in ENVP poudarjata tudi, da bo treba ti prilogi redno posodabljati, da se zagotovi ustreznost njunega področja uporabe.

20. Predlog od **ponudnikov** umetnointeligenčnega sistema zahteva, da opravijo oceno tveganja, vendar bodo v večini primerov upravljavci (podatkov) **uporabniki** in ne ponudniki umetnointeligenčnih sistemov (na primer uporabnik sistema za prepoznavanje obraza je „upravljavec“ in ga zato ne zavezujejo zahteve za ponudnike umetne inteligence velikega tveganja iz predloga).

21. Poleg tega ponudnik **ne bo vedno mogel oceniti vseh uporab** umetnointeligenčnega sistema. Zato bo začetna ocena tveganja splošnejša od tiste, ki jo opravi uporabnik umetnointeligenčnega sistema. Tudi če začetna ocena tveganja, ki jo opravi ponudnik, ne kaže, da umetnointeligenčni sistem v skladu s predlogom spada med sisteme „velikega tveganja“, to ne bi smelo izključevati **naknadne (bolj razčlenjene) ocene** (ocena učinka glede varstva podatkov v skladu s členom 35 Splošne uredbe o varstvu podatkov, členom 39 EUDPR ali

členom 27 Direktive o kazenskem pregonu), **ki bi jo moral opraviti uporabnik sistema** ob upoštevanju okvira uporabe in posebnih primerov uporabe. Razlaga, ali bo v skladu s Splošno uredbo o varstvu podatkov, EUDPR in Direktivo o kazenskem pregonu, določena vrsta obdelave verjetno povzročila veliko tveganje, se opravi neodvisno od predloga. Vendar klasifikacija umetnointeligenčnega sistema kot sistema velikega tveganja zaradi njegovega učinka na temeljne pravice[11] **sproži domnevo „velikega tveganja“ v skladu s Splošno uredbo o varstvu podatkov, EUDPR in Direktivo o kazenskem pregonu, če se obdelujejo osebni podatki.**

22. **EOVP in ENVP se strinjata s predlogom, ko opredeljuje, da razvrstitev umetnointeligenčnega sistema med sisteme velikega tveganja ne pomeni nujno, da je zakonit *sam po sebi* in ga lahko uporabnik uporablja kot takega. Upravljavec bo morda moral izpolnjevati dodatne zahteve iz prava EU o varstvu podatkov.** Poleg tega je treba v predlogu obravnavati in odpraviti razloge v členu 5 predloga, ki drugače kot prepovedani sistemi načeloma dopuščajo sisteme velikega tveganja, zlasti ker predlagana oznaka CE še ne pomeni, da je povezana obdelava osebnih podatkov zakonita.

23. Vendar bi morala biti skladnost s pravnimi obveznostmi iz zakonodaje Unije (vključno s tistimi o varstvu osebnih podatkov) prvi pogoj za vstop na evropski trg kot proizvod z oznako CE. V ta namen EOVP in ENVP **priporočata, da se v poglavje 2 naslova III predloga vključi zahteva za zagotovitev skladnosti s Splošno uredbo o varstvu podatkov in EUDPR**. Te zahteve se revidirajo (z revizijo s strani tretje osebe) pred dodelitvijo oznake CE v skladu z načelom odgovornosti. V okviru te ocene s strani tretje osebe bo zlasti pomembna začetna ocena učinka, ki jo bo izvedel ponudnik.

24. Ob upoštevanju zapletenosti, ki jo prinaša razvoj umetnointeligenčnih sistemov, je treba poudariti, da lahko tehnične značilnosti umetnointeligenčnih sistemov (na primer vrsta umetnointeligenčnega pristopa) povzročijo večja tveganja. Zato bi bilo treba pri vsaki oceni tveganja umetnointeligenčnega sistema upoštevati **tehnične značilnosti** skupaj z njegovimi **posebnimi primeri uporabe in okoliščinami**, v katerih sistem deluje.

25. Glede na zgoraj navedeno EOVP in ENVP priporočata, da se v predlogu določi, da **ponudnik** izvede začetno oceno tveganja za zadevni umetnointeligenčni sistem **ob upoštevanju primerov uporabe** (ki se določijo v predlogu, na primer z dopolnitvijo točke 1(a) Priloge III, kjer primeri uporabe biometričnih umetnointeligenčnih sistemov niso omenjeni) in da **uporabnik** umetnointeligenčnega sistema kot upravljavec kakovosti podatkov v skladu z zakonodajo EU o varstvu podatkov (kadar je to potrebno) izvede oceno učinka v zvezi z varstvom podatkov, kot je podrobno določeno v členu 35 Splošne uredbe o varstvu podatkov, členu 39 EUDPR in členu 27 Direktiva o kazenskem pregonu, pri čemer ne upošteva samo

[11] Agencija Evropske unije za temeljne pravice je že obravnavala potrebo po izvajanju ocene učinka na temeljne pravice pri uporabi umetne inteligence ali povezanih tehnologij. V svojem poročilu iz leta 2020 z naslovom “Getting the future right – Artificial intelligence and fundamental rights” [Pravilno oblikovanje prihodnosti – umetna inteligenca in temeljne pravice] je opredelila “pasti pri uporabi umetne inteligence, na primer pri policijskem predvidevanju, medicinskih diagnozah, socialnih storitvah in ciljno usmerjenem oglaševanju” ter poudarila, “da bi morale zasebne in javne organizacije izvesti ocene, kako bi lahko umetna inteligenca škodovala temeljnim pravicam”, da bi se zmanjšale negativne posledice za posameznike.

tehničnih značilnosti in **primera uporabe**, ampak **tudi posebne okoliščine**, v katerem bo umetna inteligenca delovala.

26. Poleg tega bi bilo treba pojasniti nekatere izraze iz Priloge III k predlogu, na primer izraz „bistvene zasebne storitve“ ali mali ponudnik, ki za lastno uporabo uporablja umetno inteligenco za oceno kreditne sposobnosti.

2.3 Prepovedane uporabe umetne inteligence

27. EOVP in ENVP menita, da je treba **intruzivne oblike umetne inteligence**, zlasti tiste, ki lahko vplivajo na človekovo dostojanstvo, obravnavati kot prepovedane umetnointeligenčne sisteme v skladu s členom 5 predloga, namesto da so zgolj razvrščene kot „veliko tveganje“ v Prilogi III k predlogu, kot so tiste iz točke 6. To velja zlasti za primerjave podatkov, ki v velikem obsegu vplivajo tudi na osebe, ki niso dale povoda za policijsko opazovanje ali so dale le majhen povod, ali za obdelavo, ki krši načelo omejitve namena v skladu z zakonodajo o varstvu podatkov. Za uporabo umetne inteligence na področju policijskega pregona in preprečevanja, odkrivanja in preiskovanja kaznivih dejanj so potrebna posebna, natančna, predvidljiva in sorazmerna pravila, ki morajo upoštevati interese zadevnih oseb in učinke na delovanje demokratične družbe.

28. Člen 5 predloga tvega, da zgolj navidezno podpira „vrednote“ in prepovedi umetnointeligenčnih sistemov v nasprotju s takšnimi vrednotami. Dejansko merila iz člena 5 za „klasifikacijo“ umetnointeligenčnih sistemov kot prepovedanih **omejujejo področje uporabe prepovedi** v takem obsegu, da bi se lahko v praksi izkazala kot brezpredmetna (na primer „ki povzroča ali bi verjetno lahko povzročil [...] fizično ali psihično škodo“ v točkah (a) in (b) člena 5(1); omejitev na javne organe v točki (c) člena 5(1); nejasno besedilo v podtočkah (i) in (ii) točke (c); omejitev zgolj na biometrično identifikacijo na daljavo „v realnem času“ brez kakršne koli jasne opredelitve itd.).

29. Zlasti uporaba umetne inteligence za „družbeno točkovanje“, kot je predvidena v točki (c) člena 5(1) predloga, lahko povzroči diskriminacijo in je v nasprotju s temeljnimi vrednotami EU. Predlog prepoveduje te prakse zgolj, kadar se izvajajo „v določenem časovnem obdobju“ ali „s strani javnih organov ali v njihovem imenu“. Zasebna podjetja, kot so družbeni mediji in ponudniki storitev v oblaku, lahko obdelujejo velike količine osebnih podatkov in izvajajo družbeno točkovanje. Zato **bi moral predlog prepovedati vse vrste družbenega točkovanja**. Opozoriti je treba, da v kontekstu preprečevanja, odkrivanja in preiskovanja kaznivih dejanj člen 4 Direktive o kazenskem pregonu take dejavnosti že znatno omejuje, če jih v praksi celo ne prepoveduje.

30. **Biometrična identifikacija posameznikov na daljavo** v javno dostopnih prostorih pomeni veliko tveganje vdora v zasebno življenje posameznikov. EOVP in ENVP zato **menita, da je potreben strožji pristop**. Uporaba umetnointeligenčnih sistemov bi lahko povzročila resne težave glede sorazmernosti, saj lahko vključuje obdelavo podatkov neselektivnega in nesorazmernega števila posameznikov za identifikacijo le nekaj posameznikov (na primer potniki na letališčih in železniških postajah). Breztrenjska narava sistemov biometrične identifikacije na daljavo pomeni tudi težave s transparentnostjo in postavlja vprašanja,

povezana s pravno podlago za obdelavo v skladu z zakonodajo EU (LED, Splošna uredba o varstvu podatkov, EUDPR in druga veljavna zakonodaja). Problem glede načina ustreznega obveščanja posameznikov o tej obdelavi je še vedno nerešen, prav tako pa je še nerešeno učinkovito in pravočasno uveljavljanje pravic posameznikov. Enako velja za **nepopravljiv, resen vpliv na** (razumno) **pričakovanje prebivalstva o anonimnosti v javnih prostorih**, posledica tega pa je neposreden negativen učinek na uveljavljanje svobode izražanja, zbiranja, združevanja kakor tudi svobode gibanja.

31. Točka (d) člena 5(1) predloga določa obsežen **seznam izjemnih primerov**, v katerih je dovoljena biometrična identifikacija na daljavo v javno dostopnih prostorih v realnem času za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. EOVP in ENVP menita, da je **ta pristop pomanjkljiv** glede več vidikov: prvič, ni jasno, kaj bi bilo treba razumeti kot „znatno zamudo“ in kako bi jo bilo treba upoštevati kot olajševalni dejavnik, pri čemer je treba upoštevati, da lahko sistem za množično identifikacijo v samo nekaj urah identificira več tisoč posameznikov. Poleg tega intruzivnost obdelave ni vedno odvisna od tega, ali se identifikacija opravi v realnem času ali ne. Naknadna biometrična identifikacija na daljavo bo v kontekstu političnega protesta verjetno močno negativno vplivala na uveljavljanje temeljnih pravic in svoboščin, kot sta svoboda zbiranja in združevanja, ter bolj na splošno temeljnih načel demokracije. Drugič, intruzivnost obdelave ni nujno odvisna od njenega namena. Uporaba tega sistema za druge namene, kot je zasebno varovanje, pomeni enako grožnjo za temeljne pravice do spoštovanja zasebnega in družinskega življenja ter varstva osebnih podatkov. Nazadnje bo tudi ob predvidenih omejitvah potencialno število osumljencev ali storilcev kaznivih dejanj skoraj vedno „dovolj veliko“, da bo upravičevalo nenehno uporabo umetnointeligenčnih sistemov za odkrivanje osumljencev, kljub dodatnim pogojem iz člena 5(2) do člena 5(4) predloga. Zdi se, da sklepanje, na katerem temelji predlog, zanemarja, da pri spremljanju odprtih območij obveznosti iz zakonodaje EU o varstvu podatkov ni treba izpolnjevati le za spremljanje osumljencev, temveč tudi za vse tiste, ki se dejansko spremljajo.

32. EOVP in ENVP na podlagi vseh teh razlogov **pozivata k splošni prepovedi kakršne koli uporabe umetne inteligence za avtomatizirano prepoznavanje človeških lastnosti v javno dostopnih prostorih, kot so prepoznavanje obrazov in tudi hoje, prstnih odtisov, DNK, glasu, udarcev po tipkovnici in drugih biometričnih ali vedenjskih znakov, v kakršnem koli okviru**. Trenutni pristop predloga je opredeliti in našteti vse umetnointeligenčne sisteme, ki bi jih bilo treba prepovedati. Zato bi bilo treba zaradi doslednosti v členu 5 predloga prepovedati **umetnointeligenčne sisteme za obsežno identifikacijo na daljavo v spletnih prostorih**. EOVP in ENVP ob upoštevanju Direktive o kazenskem pregonu, EUDPR in Splošne uredbe o varstvu podatkov ne moreta razbrati, kako bi lahko taka vrsta prakse izpolnila zahteve glede nujnosti in sorazmernosti, kar naposled izhaja iz tega, kar Sodišče Evropske unije in Evropsko sodišče za človekove pravice štejeta kot sprejemljive posege v temeljne pravice.

33. Poleg tega EOVP in ENVP tako za javne organe in zasebne subjekte **priporočata prepoved umetnointeligenčnih sistemov, ki posameznike na podlagi biometričnih podatkov (na primer prepoznavanja obraza) razvrščajo v skupine glede na etnično pripadnost, spol, kakor tudi politično ali spolno usmerjenost ali druge razloge za diskriminacijo, ki so prepovedani v skladu s členom 21 Listine EU o temeljnih pravicah, ali** sisteme umetne

inteligence, katerih znanstvena veljavnost ni dokazana ali ki so v neposrednem nasprotju z bistvenimi vrednotami EU (na primer poligraf, točki 6 (b) in 7 (a) Priloge III). Skladno s tem bi bilo treba **v členu 5 prepovedati** „**biometrično kategorizacijo**“.

34. **Na človekovo dostojanstvo vpliva tudi določitev ali razvrstitev s strani računalnika glede prihodnjega obnašanja, ki je neodvisno od njegove lastne svobodne volje**. Umetnointeligenčni sistemi, namenjeni uporabi s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj za individualne ocene tveganja fizičnih oseb, za oceno tveganja, ali bo fizična oseba storila ali ponovila kaznivo dejanje, prim. točka 6(a) Priloge III, ali za napovedovanje storitve ali ponovitve dejanskega ali potencialnega kaznivega dejanja na podlagi profiliranja fizičnih oseb ali ocenjevanja osebnostnih lastnosti in značilnosti ali preteklih kaznivih ravnanj, prim. točka 6(e) Priloge III, ki se uporabljajo v skladu s predvidenim namenom, bodo privedli do ključne odvisnosti policije in sodstva pri sprejemanju odločitev in s tem objektiviziranja prizadetih ljudi. Taki umetnointeligenčni sistemi, ki zadevajo bistvo pravice do človekovega dostojanstva, bi morali biti prepovedani v členu 5.

35. EOVP in ENVP nadalje menita, da je uporaba umetne inteligence za **sklepanje o čustvih fizičnih oseb zelo nezaželena in bi jo bilo treba prepovedati**, razen v nekaterih natančno opredeljenih primerih uporabe, in sicer za zdravstvene ali raziskovalne namene (na primer pacienti, pri katerih je pomembno prepoznavanje čustev), vedno z ustreznimi zaščitnimi ukrepi in seveda ob upoštevanju vseh drugih pogojev varstva podatkov in omejitev, vključno z omejitvijo namena.

2.4 Umetnointeligenčni sistemi velikega tveganja

2.4.1 Potreba po predhodnem ugotavljanju skladnosti, ki ga opravijo zunanje tretje osebe

36. EOVP in ENVP pozdravljata, da je treba za umetnointeligenčne sisteme, ki pomenijo veliko tveganje, opraviti predhodno oceno skladnosti, preden se lahko dajo na trg ali kako drugače začnejo delovati v EU. Načeloma je ta regulativni model dobrodošel, saj zagotavlja dobro ravnotežje med prijaznostjo do inovacij in visoko stopnjo proaktivnega varstva temeljnih pravic. Za uporabo v posebnih okoljih, kot so postopki odločanja javnih služb ali kritična infrastruktura, je treba določiti načine za preiskavo celotne izvorne kode.

37. Vendar EOVP in ENVP zagovarjata prilagoditev postopka ugotavljanja skladnosti v skladu s členom 43 predloga, tako da je **treba za umetno inteligenco velikega tveganja praviloma izvesti predhodno ugotavljanje skladnosti s strani tretjih oseb**. Čeprav ocena skladnosti s strani tretjih oseb za obdelavo osebnih podatkov velikega tveganja ni zahtevana v Splošni uredbi o varstvu podatkov ali EUDPR, tveganja umetnointeligenčnih sistemov niso še v celoti razumljena. Splošna vključitev obveznosti za ugotavljanje skladnosti s strani tretjih oseb bi zato dodatno okrepila pravno varnost in zaupanje v vse umetnointeligenčne sisteme velikega tveganja.

2.4.2 Področje uporabe uredbe mora zajemati tudi umetnointeligenčne sisteme, ki se že uporabljajo

38. V skladu s členom 43(4) predloga, bi morali biti umetnointeligenčni sistemi velikega tveganja ob vsaki bistveni spremembi predmet novega postopka ugotavljanja skladnosti. Prav je, da se zagotovi, da umetnointeligenčni sistemi izpolnjujejo zahteve iz Uredbe o umetni inteligenci v svoji celotni dobi trajanja. Umetnointeligenčni sistemi, ki so bili dani na trg ali v uporabo pred začetkom uporabe predlagane uredbe (ali 12 mesecev po tem v primeru obsežnih informacijskih sistemov iz Priloge IX), so izključeni iz njihovega področja uporabe, razen če se pri teh sistemih „bistveno spremeni“ zasnova ali predvideni namen (člen 83).

39. Vendar prag za „bistvene spremembe“ ni jasen. Točka 66 uvodne izjave predloga določa nižji prag za vnovično ugotavljanje skladnosti „ob vsaki spremembi, ki bi lahko vplivala na skladnost“. Podoben prag bi bil primeren za člen 83, vsaj za umetnointeligenčne sisteme velikega tveganja. Da bi se zapolnile morebitne vrzeli v zaščiti, morajo poleg tega umetnointeligenčni sistemi, ki so že vzpostavljeni in delujejo, po določeni izvedbeni fazi izpolnjevati tudi vse zahteve iz Uredbe o umetni inteligenci.

40. Številne možnosti obdelave osebnih podatkov in zunanja tveganja tudi vplivajo na varnost umetnointeligenčnih sistemov. Osredinjenost člena 83 na „bistvene spremembe zasnove ali predvidenega namena“ ne vključuje sklicevanja na spremembe zunanjih tveganj. Zato bi bilo treba v člen 83 predloga vključiti sklicevanje na spremembe scenarija v primeru groženj, ki izhajajo iz zunanjih tveganj, na primer kibernetskih napadov, nasprotovalnih napadov in utemeljenih pritožb potrošnikov.

41. Ker je začetek uporabe predviden 24 mesecev po začetku veljavnosti prihodnje Uredbe, EOVP in ENVP menita, da ni primerno izvzeti umetnointeligenčnih sistemov, ki so že bili dani na trg, za še daljše obdobje. Čeprav predlog določa tudi, da se zahteve iz Uredbe upoštevajo pri oceni vsakega obsežnega informacijskega sistema, kot je določeno v pravnih aktih iz Priloge IX, EOVP in ENVP menita, da bi se morale zahteve glede začetka uporabe umetnointeligenčnih sistemov uporabljati od datuma začetka uporabe prihodnje Uredbe.

2.5 Upravljanje in Evropski odbor za umetno inteligenco

2.5.1 Upravljanje

42. EOVP in ENVP pozdravljata imenovanje ENVP za pristojni organ in organ za nadzor trga za nadzor institucij, agencij in organov Unije, kadar spadajo na področje uporabe tega predloga. ENVP je pripravljen izpolniti svojo novo vlogo regulatorja umetne inteligence za javno upravo EU. Poleg tega vloga in naloge ENVP niso dovolj opredeljene in bi jih bilo treba v predlogu dodatno pojasniti, zlasti ko gre za njegovo vlogo kot organ za nadzor trga.

43. EOVP in ENVP potrjujeta dodelitev finančnih sredstev, ki so v predlogu predvidena za Evropski odbor za umetno inteligenco in ENVP kot priglasitveni organ. Vendar pa bi izpolnjevanje novih nalog, predvidenih za ENVP, ne glede na to, ali deluje kot priglašeni organ, zahtevalo znatno večje finančne in človeške vire.

44. Prvič, ker besedilo člena 63(6) navaja, da ENVP „deluje kot organ za nadzor trga“ za institucije, agencije in organe Unije, ki spadajo na področje uporabe predloga, kar ne pojasnjuje, ali naj se ENVP šteje za popolnoma vključen „organ za nadzor trga“, kot je predvideno v Uredbi (EU) 2019/1020. To sproža vprašanja o dolžnostih in pristojnostih ENVP v praksi. Drugič, pod pogojem, da je odgovor na predhodno vprašanje pritrdilen, ni jasno, kako lahko vloga ENVP, kot je predvidena v EUDPR, izpolnjuje nalogo, predvideno v členu 11 Uredbe (EU) 2019/1020, ki vključuje „učinkovit nadzor trga znotraj svojega ozemlja proizvodov, ki so dostopni na spletu“ ali „fizične in laboratorijske preglede na podlagi reprezentativnih vzorcev“. Obstaja tveganje, da bi prevzem novega sklopa nalog brez dodatnih pojasnil v predlogu lahko ogrozil izpolnjevanje obveznosti kot nadzornika za varstvo podatkov.

45. Vendar EOVP in ENVP poudarjata, da se nekatere določbe predloga, ki opredeljujejo naloge in pristojnosti različnih pristojnih organov v skladu z zakonodajo o umetni inteligenci, njihove odnose, naravo in jamstvo njihove neodvisnosti, v tej fazi zdijo nejasne. Uredba 2019/1020 določa, da mora biti organ za nadzor trga neodvisen, osnutek uredbe pa ne zahteva, da so nadzorni organi neodvisni, in od njih celo zahteva, da Komisiji poročajo o nekaterih nalogah, ki jih izvajajo organi za nadzor trga, ki so lahko različne institucije. Ker je v predlogu navedeno tudi, da bodo organi za varstvo podatkov organi za nadzor trga za umetnointeligenčne sisteme, ki se uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (odstavek 5 člena 63), to prav tako pomeni, da bodo zanje, po možnosti prek njihovega nacionalnega nadzornega organa, veljale obveznosti poročanja Komisiji (odstavek 2 člena 63), kar se zdi nezdružljivo z njihovo neodvisnostjo.

46. Zato EOVP in ENVP menita, da je treba te določbe pojasniti, da bi bile skladne z Uredbo 2019/1020, EUDPR ter Splošno uredbo o varstvu podatkov, predlog pa bi moral jasno določiti, da morajo biti nadzorni organi v skladu z uredbo o umetni inteligenci pri opravljanju svojih nalog popolnoma neodvisni, saj bi bilo to bistveno jamstvo za ustrezen nadzor in izvrševanje prihodnje uredbe.

47. EOVP in ENVP želita tudi opozoriti, da organi za varstvo podatkov že izvršujejo Splošno uredbo o varstvu podatkov, EUDPR in Direktivo o kazenskem pregonu, za umetnointeligenčne sisteme, ki vključuje osebne podatke, da bi zagotovili varstvo temeljnih pravic in zlasti pravice do varstva podatkov. Zato organi za varstvo podatkov deloma, kot se to zahteva v Predlogu za nacionalne nadzorne organe, že razumejo umetnointeligenčne tehnologije, podatke in podatkovno računalništvo, temeljne pravice, ter imajo strokovno znanje za ocenjevanje tveganj za temeljne pravice, ki jih predstavljajo nove tehnologije. Poleg tega so določbe predloga, kadar sistemi umetne inteligence temeljijo na obdelavi osebnih podatkov ali obdelujejo osebne podatke, neposredno prepletene s pravnim okvirom za varstvo podatkov, kar bo veljalo za večino umetnointeligenčnih sistemov, ki spadajo na področje uporabe uredbe. Posledično bodo pristojnosti nadzornih organov v okviru predloga in organov za varstvo podatkov medsebojno povezane.

48. Zato bi imenovanje organov za varstvo podatkov kot nacionalnih nadzornih organov zagotovilo bolj harmoniziran regulativni pristop in pripomoglo k dosledni razlagi določb o obdelavi podatkov ter preprečilo protislovja pri izvrševanju med državami članicami. Vsem deležnikom v vrednostni verigi umetne inteligence bi prav tako koristilo, če bi imeli enotno kontaktno točko

za vse postopke obdelave osebnih podatkov, ki spadajo na področje uporabe predloga, in omejili interakcije med dvema različnima regulativnima organoma za obdelavo, ki ju zadevata predlog in Splošna uredba o varstvu podatkov. Zato EOVP in ENVP menita, da **bi bilo treba organe za varstvo podatkov imenovati za nacionalne nadzorne organe v skladu s členom 59 predloga**.

49. V vsakem primeru, če predlog vsebuje posebna pravila o varstvu posameznikov v zvezi z obdelavo osebnih podatkov, sprejeta na podlagi člena 16 PDEU, morajo skladnost s temi pravili, zlasti omejitvami uporabe umetnointeligenčnih sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, **nadzorovati neodvisni organi**.

50. Vendar v predlogu ni izrecne določbe, ki bi pristojnost za zagotavljanje skladnosti s temi pravili dodelila nadzoru neodvisnih organov. Edino sklicevanje na pristojne nadzorne organe za varstvo podatkov v skladu s Splošno uredbo o varstvu podatkov ali Direktivo o kazenskem pregonu, je v členu 63(5) predloga, vendar le kot organi za „nadzor trga“ in alternativno z nekaterimi drugimi organi. EOVP in ENVP menita, da takšna ureditev ne zagotavlja skladnosti z zahtevo po neodvisnem nadzoru iz člena 16(2) PDEU in člena 8 Listine EU o temeljnih pravicah.

2.5.2 Evropski odbor za umetno inteligenco

51. S predlogom se ustanavlja Evropski odbor za umetno inteligenco. EOVP in ENVP priznavata potrebo po dosledni in usklajeni uporabi predlaganega okvira ter vključevanju neodvisnih strokovnjakov v razvoj politike EU o umetni inteligenci. Predlog hkrati predvideva, da bo prevladujoča vloga podeljena Komisiji. Ne samo, da bi bila slednja del Evropskega odbora za umetno inteligenco, temveč bi mu tudi predsedovala in imela pravico veta na sprejetje poslovnika Evropskega odbora za umetno inteligenco. To je v nasprotju s potrebo po evropskem organu za umetno inteligenco, ki je neodvisen od političnega vpliva. Zato EOVP in ENVP menita, da bi morala prihodnja uredba o umetni inteligenci dati **večjo avtonomijo Evropskemu odboru za umetno inteligenco**, da bi mu dejansko zagotovila dosledno uporabo uredbe na enotnem trgu.

52. EOVP in ENVP prav tako ugotavljata, da Evropskemu odboru za umetno inteligenco niso podeljene nikakršne pristojnosti za izvrševanje predlagane uredbe. Upoštevajoč razširjenost umetnointeligenčnih sistemov na enotnem trgu in verjetnost čezmejnih primerov je ključna potreba po harmoniziranem izvrševanju in ustrezno razporeditvijo pristojnosti med nacionalnimi nadzornimi organi. EOVP in ENVP zato priporočata, da se v prihodnji uredbi o umetni inteligenci določijo mehanizmi sodelovanja med nacionalnimi nadzornimi organi. EOVP in ENVP predlagata uvedbo mehanizma, ki bi zagotavljal enotno kontaktno točko za posameznike, ki jih zadeva zakonodaja, kakor tudi za podjetja, za vsak umetnointeligenčni sistem, Evropski odbor za umetno inteligenco pa lahko za organizacije, katerih dejavnost pokriva več kot polovico držav članic EU, imenuje nacionalni organ, ki bo odgovoren za izvrševanje uredbe o umetni inteligenci za ta umetnointeligenčni sistem.

53. Poleg tega, upoštevajoč neodvisno naravo organov, ki sestavljajo Evropski odbor za umetno inteligenco, bi morali slednji imeti pravico, da ukrepajo na lastno pobudo in ne le zagotavljajo svetovanje in pomoč Komisiji. EOVP in ENVP zato poudarjata potrebo po razširitvi poslanstva, dodeljenega Evropskemu odboru za umetno inteligenco, ki poleg tega ne ustreza nalogam, navedenim v predlogu.

54. Za izpolnitev teh namenov **mora imeti Evropski odbor za umetno inteligenco zadostna in ustrezna pooblastila**, pojasniti pa je treba tudi njegov pravni položaj. Zlasti da bi materialna uporaba prihodnje uredbe ostala ustrezna, se zdi nujno, da se v njen razvoj vključijo organi, pristojni za njeno izvrševanje. Zato EOVP in ENVP priporočata, da se Evropski odbor za umetno inteligenco pooblasti, da lahko predlaga Komisiji spremembe Priloge I, v kateri so opredeljene tehnike in pristopi umetne inteligence, ter Priloge III, v kateri so navedeni umetnointeligenčni sistemi velikega tveganja iz člena 6(2). Komisija bi se morala pred vsako spremembo teh prilog tudi posvetovati z Evropskim odborom za umetno inteligenco.

55. Odstavek 4 člena 57 predloga predvideva izmenjave med Evropskim odborom za umetno inteligenco in drugimi organi, uradi, agencijami in svetovalnimi skupinami Unije. Ob upoštevanju svojega prejšnjega dela na področju umetne inteligence in strokovnega znanja na področju človekovih pravic, EOVP in ENVP priporočata, da se preuči možnost, da bi bila Agencija za temeljne pravice ena od opazovalk v Evropskem odboru za umetno inteligenco.

3 MEDSEBOJNI VPLIVI S PRAVNIM OKVIROM ZA VARSTVO PODATKOV

3.1 Povezava predloga z veljavno zakonodajo EU o varstvu podatkov

56. Jasno opredeljena povezava predloga z veljavno zakonodajo o varstvu podatkov je bistven prvi pogoj za zagotovitev in ohranjanje spoštovanja in uporabe pravnega reda EU na področju varstva osebnih podatkov. Takšno pravo EU, zlasti Splošno uredbo o varstvu podatkov, EUDPR in Direktivo o kazenskem pregonu, je treba upoštevati kot prvi pogoj, na katerem lahko temeljijo prihodnji zakonodajni predlogi, ne da bi vplivali na veljavne določbe ali posegali vanje, vključno s pristojnostmi nadzornih organov in upravljanjem.

57. Po mnenju EOVP in ENVP se je zato v predlogu pomembno jasno ogniti vsakršni neskladnosti in morebitnemu navzkrižju s Splošno uredbo o varstvu podatkov, EUDPR in Direktivo o kazenskem pregonu . To ni samo zaradi pravne varnosti, temveč tudi za to, da se prepreči, da bi predlog neposredno ali posredno ogrozil temeljno pravico do varstva osebnih podatkov, kot je določena v členu 16 PDEU in členu 8 Listine EU o temeljnih pravicah.

58. Predvsem samoučljivi stroji bi lahko zaščitili osebne podatke posameznikov le, če je to vključeno že v zasnovi. Bistvena je tudi takojšnja možnost uveljavljanja pravic posameznikov iz člena 22 (Avtomatizirano sprejemanje posameznih odločitev, vključno s profiliranjem) Splošne uredbe o varstvu podatkov ali člena 23 EUDPR, ne glede na namene obdelave. Glede tega je treba v umetnointeligenčnih sistemih že od vsega začetka zagotoviti druge pravice posameznikov, na katere se nanašajo osebni podatki, v zvezi s pravico do izbrisa ter pravico

do popravka v skladu z zakonodajo o varstvu podatkov, ne glede na izbrani pristop umetne inteligence ali tehnično zgradbo.

59. Uporaba osebnih podatkov za učenje sistemov umetne inteligence lahko privede do oblikovanja pristranskih vzorcev odločanja v jedru umetnointeligenčnega sistema. Zato so potrebni različni zaščitni ukrepi in zlasti usposobljen človeški nadzor v takih postopkih, da se zagotovita spoštovanje in zagotavljanje pravic posameznikov, na katere se nanašajo osebni podatki, ter da se preprečijo kakršni koli negativni učinki za posameznike. Pristojni organi bi morali imeti tudi možnost, da predlagajo smernice za oceno pristranskosti v umetnointeligenčnih sistemih in pomagajo pri izvajanju človeškega nadzora.

60. Posamezniki, na katere se nanašajo osebni podatki, bi morali biti vedno obveščeni o pravni podlagi za takšno obdelavo, splošni razlagi logike (postopka) in področju uporabe umetnointeligenčnega sistema, kadar se njihovi podatki uporabljajo za umetnointeligenčno usposabljanje in/ali napovedovanje. Glede tega bi bilo treba v teh primerih vedno zagotoviti pravico posameznikov do omejitve obdelave (člen 18 Splošne uredbe o varstvu podatkov in člen 20 EUDPR) ter do izbrisa podatkov (člen 16 Splošne uredbe o varstvu podatkov in člen 19 EUDPR). Poleg tega bi moral imeti upravljavec izrecno obveznost, da posameznika, na katerega se nanašajo osebni podatki, obvesti o veljavnih rokih za ugovor, omejitev, izbris podatkov itd. Sistem umetne inteligence mora biti sposoben izpolniti vse zahteve glede varstva podatkov z ustreznimi tehničnimi in organizacijskimi ukrepi. Pravica do pojasnila bi morala zagotoviti dodatno preglednost.

3.2 Peskovnik in nadaljnja obdelava (člena 53 in 54 predloga)

61. V okviru veljavnih pravnih in moralnih omejitev je pomembno spodbujati evropske inovacije z orodji, kot je peskovnik. Peskovnik ponuja možnost zagotavljanja zaščitnih ukrepov, potrebnih za vzpostavitev zaupanja in zanašanja na umetnointeligenčne sisteme. V zapletenih okoljih bodo strokovnjaki za umetno inteligenco težko ustrezno pretehtali vse interese. Zlasti mala in srednja podjetja z omejenimi viri, ki delujejo v regulativnem peskovniku, lahko dobijo hitrejši vpogled in s tem pospešijo inovacije.

62. V oddelku 3 člena 53 predloga je navedeno, da peskovnik ne vpliva na pooblastila za nadzor in popravne ukrepe. Če je to pojasnilo koristno, je treba pripraviti tudi vodila ali smernice o tem, kako vzpostaviti dobro ravnotežje med vlogo nadzornega organa na eni strani in zagotavljanjem podrobnih smernic prek peskovnika na drugi strani.

63. V oddelku 6 člena 53 je navedeno, da se načini in pogoji delovanja peskovnikov določijo v izvedbenih aktih. Pomembno je, da se pripravijo posebne smernice za zagotovitev doslednosti in podpore pri vzpostavljanju in delovanju peskovnikov. Vendar bi lahko zavezujoči izvedbeni akti omejili možnost vsake države članice, da peskovnik prilagodi svojim potrebam in lokalnim praksam. Zato EOVP in ENVP priporočata, naj namesto tega Evropski odbor za umetno inteligenco določi smernice za peskovnike.

64. Člen 54 predloga želi zagotoviti pravno podlago za nadaljnjo obdelavo osebnih podatkov za razvoj določenih umetnointeligenčnih sistemov v javnem interesu v regulativnem peskovniku

za umetno inteligenco. Povezava med členoma 54(1) in 54(2) ter uvodno izjavo 41 predloga ter s tem tudi z veljavno zakonodajo EU o varstvu podatkov ostaja nejasna. Vendar je s Splošno uredbo o varstvu podatkov in EUDPR že vzpostavljena podlaga za „nadaljnjo obdelavo“. Zlasti v primerih, ko je omogočanje nadaljnje obdelave v javnem interesu, uravnoteženje interesov upravljavca in interesov posameznika, na katerega se nanašajo osebni podatki, ne sme ovirati inovacij. Člen 54 predloga trenutno ne obravnava dveh pomembnih vprašanj, in sicer, (1.) v katerih okoliščinah in na podlagi katerih (dodatnih) meril se tehtajo interesi posameznikov, na katere se nanašajo osebni podatki, in (2.) ali se bodo ti umetnointeligenčni sistemi uporabljali samo v peskovniku. EOVP in ENVP pozdravljata zahtevo po zakonodaji Unije ali države članice pri obdelavi osebnih podatkov, zbranih v okviru Direktive o kazenskem pregonu, v peskovniku, vendar priporočata, da se podrobneje opredeli, kaj je predvideno v tem dokumentu, in sicer tako, da se uskladi s Splošno uredbo o varstvu podatkov in EUDPR, zlasti s pojasnitvijo, da mora biti pravna podlaga za te peskovnike skladna z zahtevami iz člena 23(2) Splošne uredbe o varstvu podatkov in členom 25 EUDPR, ter natančno določi, da je treba vsako uporabo peskovnika temeljito oceniti. To velja tudi za celoten seznam pogojev iz točk (b) do (j) člena 54(1).

65. Nekateri dodatni premisleki glede ponovne uporabe podatkov iz člena 54 predloga kažejo, da uporaba peskovnika zahteva veliko virov in da je zato realno pričakovati, da bi le majhno število podjetij dobilo priložnost za sodelovanje. Sodelovanje v peskovniku bi lahko bila konkurenčna prednost. Za omogočanje ponovne uporabe podatkov bi bilo treba skrbno preučiti, kako izbrati udeležence, da se zagotovi, da spadajo v področje uporabe, in prepreči nepoštena obravnava. EOVP in ENVP sta zaskrbljena, da se omogočanje ponovne uporabe podatkov v okviru peskovnika razlikuje od pristopa k odgovornosti iz Splošne uredbe o varstvu podatkov, po kateri odgovornost nosi upravljavec podatkov in ne pristojni organ.

66. Poleg tega EOVP in ENVP menita, da glede na cilje peskovnika, ki so razvoj, preizkušanje in potrjevanje umetnointeligenčnih sistemov, peskovniki ne morejo spadati na področje uporabe Direktive o kazenskem pregonu. Direktiva o kazenskem pregonu določa ponovno uporabo podatkov za znanstvene raziskave, za podatke, obdelane za ta sekundarni namen, pa se bo uporabljala Splošna uredba o varstvu podatkov ali EUDPR in ne več Direktiva o kazenskem pregonu.

67. Ni jasno, kaj bo regulativni peskovnik obsegal. Postavlja se vprašanje, ali predlagani regulativni peskovnik vključuje infrastrukturo informacijske tehnologije v vsaki državi članici z nekaterimi dodatnimi pravnimi podlagami za nadaljnjo obdelavo, ali pa zgolj ureja dostop do regulativnega strokovnega znanja in smernic. EOVP in ENVP pozivata zakonodajalca, naj ta koncept pojasni v predlogu in v njem jasno navede, da regulativni peskovnik ne pomeni obveznosti pristojnih organov, da zanj zagotovijo tehnično infrastrukturo. V vsakem primeru je treba pristojnim organom zagotoviti finančne in človeške vire v skladu s tem pojasnilom.

68. Nazadnje želita EOVP in ENVP poudariti razvoj čezmejnih umetnointeligenčnih sistemov, ki bodo na voljo celotnemu evropskemu enotnemu digitalnemu trgu. V primeru takih umetnointeligenčnih sistemov regulativni peskovnik kot orodje za inovacije ne sme postati ovira za čezmejni razvoj. Zato EOVP in ENVP priporočata usklajen čezmejni pristop, ki je na

nacionalni ravni še vedno dovolj na voljo za vsa mala in srednja podjetja ter zagotavlja skupni okvir po Evropi, ne da bi bil preveč omejevalen. Najti je treba ravnotežje med evropskim usklajevanjem in nacionalnimi postopki, da se prepreči nasprotujoče izvajanje prihodnje uredbe o umetni inteligenci, kar bi lahko zavrlo inovacije po vsej EU.

3.3 Preglednost

69. EOVP in ENVP pozdravljata, da se sistemi umetne inteligence z visokim tveganjem morajo registrirati v javni podatkovni zbirki (členi 51 in 60 predloga). To podatkovno zbirko bi bilo treba izrabiti kot priložnost, da se širši javnosti zagotovijo informacije o področju uporabe umetnointeligenčnega sistema ter o znanih pomanjkljivostih in incidentih, ki bi lahko ogrozili njegovo delovanje, ter o ukrepih, ki so jih ponudniki sprejeli za njihovo obravnavo in odpravo.

70. Ključno demokratično načelo je uporaba sistema zavor in ravnovesij. Zato je dejstvo, da se obveznost preglednosti ne uporablja za umetnointeligenčne sisteme, ki se uporabljajo za odkrivanje, preprečevanje, preiskovanje ali pregon kaznivih dejanj, preširoka izjema. Razlikovati je treba med umetnointeligenčnimi sistemi, ki se uporabljajo za odkrivanje ali preprečevanje, in umetnointeligenčnimi sistemi, katerih namen je preiskovanje ali pomoč pri pregonu kaznivih dejanj. Zaščitni ukrepi za preprečevanje in odkrivanje morajo biti močnejši zaradi domneve nedolžnosti. EOVP in ENVP poleg tega obžalujeta, da v predlogu ni previdnostnih opozoril, kar bi lahko razumeli kot zeleno luč za uporabo celo nepreverjenih umetnointeligenčnih sistemov ali aplikacij velikega tveganja.

71. V primerih, ko je javnosti mogoče zagotoviti malo preglednosti ali ji je ni mogoče zagotoviti zaradi tajnosti, bi morali biti vzpostavljeni zaščitni ukrepi tudi v dobro delujoči demokraciji, ti umetnointeligenčni sistemi pa bi morali biti registrirani pri pristojnem nadzornem organu in slednjemu zagotavljati preglednost.

72. Zagotavljanje preglednosti umetnointeligenčnih sistemov je zelo zahteven cilj. Popolnoma kvantitativni pristop odločanja številnih umetnointeligenčnih sistemov, ki se po naravi razlikuje od človeškega pristopa, ki se večinoma zanaša na vzročno in teoretično sklepanje, je lahko v nasprotju s potrebo po pridobitvi predhodne razumljive razlage strojnih rezultatov. Uredba bi morala spodbujati nove, bolj proaktivne in pravočasne načine za obveščanje uporabnikov umetnointeligenčnih sistemov o statusu (odločanja), kje se sistem kadar koli nahaja, ter zagotoviti zgodnje opozarjanje o morebitnih škodljivih posledicah, tako da se posamezniki, katerih pravice in svoboščine bi lahko bile kršene s strani avtonomnih odločitev stroja, lahko odzovejo ali popravijo odločitev.

3.4 Obdelava posebnih kategorij podatkov in podatkov, povezanih s kaznivimi dejanji

73. Obdelavo posebnih kategorij podatkov na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj urejajo določbe okvira EU za varstvo podatkov, vključno z Direktivo o kazenskem pregonu, in njeno implementacijo na nacionalni ravni. Predlog zatrjuje, da ne zagotavlja splošne pravne podlage za obdelavo osebnih podatkov, vključno s posebnimi kategorijami osebnih podatkov, prim. uvodna izjava 41. Hkrati je v členu 10(5) predloga navedeno, da „lahko ponudniki takih sistemov obdelujejo posebne kategorije osebnih podatkov“.

Poleg tega ista določba zahteva dodatne zaščitne ukrepe in navaja tudi primere. Zato se zdi, da je predlog v tem delu v navzkrižju s Splošno uredbo o varstvu podatkov, Direktivo o kazenskem pregonu in EUDPR. Čeprav EOVP in ENVP pozdravljata poskus vzpostavitve ustreznih zaščitnih ukrepov, je potreben skladnejši regulativni pristop, saj se sedanje določbe ne zdijo dovolj jasne, da bi ustvarile pravno podlago za obdelavo posebnih kategorij podatkov, in jih je treba dopolniti z dodatnimi zaščitnimi ukrepi, ki jih je treba še oceniti. Poleg tega bo treba pri zbiranju osebnih podatkov z obdelavo v okviru Direktive o kazenskem pregonu, upoštevati morebitne dodatne zaščitne ukrepe in omejitve, ki izhajajo iz prenosov Direktive o kazenskem pregonu v nacionalno pravo.

3.5 Mehanizmi skladnosti

3.5.1 Izdajanje potrdil

74. Eden glavnih stebrov predloga je izdajanje potrdil. Sistem izdajanja potrdil, opisan v predlogu, temelji na strukturi subjektov (priglasitveni organi/priglašeni organi/Komisija) in mehanizmu za ugotavljanje skladnosti/izdajanje potrdil, ki zajema obvezne zahteve, ki se uporabljajo za umetnointeligenčne sisteme velikega tveganja, ter temelji na evropskih harmoniziranih standardih v skladu z Uredbo (EU) št. 1025/2012 in skupnih specifikacijah, ki jih določi Komisija. Ta mehanizem se razlikuje od sistema izdajanja potrdil, katerega namen je zagotoviti skladnost s pravili in načeli o varstvu podatkov iz členov 42 in 43 Splošne uredbe o varstvu podatkov. Vendar ni jasno, kako se lahko potrdila, ki jih izdajo priglašeni organi v skladu s predlogom, povežejo z izdajanjem potrdil, pečati in označbami za varstvo podatkov, ki jih določa Splošna uredba o varstvu podatkov, v nasprotju s tem, kar je določeno za druge vrste potrdil (glej člen 42(2) v zvezi s potrdili izdanimi v skladu z Uredbo (EU) 2019/881).

75. Če umetnointeligenčni sistemi velikega tveganja temeljijo na obdelavi osebnih podatkov ali obdelujejo osebne podatke za izpolnitev svoje naloge, lahko te neskladnosti povzročijo pravno negotovost za vse zadevne organe, saj lahko privedejo do situacij, v katerih bi se umetnointeligenčni sistemi, potrjeni v skladu s predlogom in označeni z oznako skladnosti CE, ko bodo dani na trg ali v uporabo, lahko uporabljali na način, ki ni skladen s pravili in načeli varstva podatkov.

76. Predlog ne vsebuje jasne povezave z zakonodajo o varstvu podatkov ter drugo zakonodajo EU in držav članic, ki se uporablja za vsako „področje“ umetnointeligenčnega sistema velikega tveganja iz Priloge III. Predlog bi moral zlasti vključevati načeli najmanjšega obsega podatkov in vgrajenega varstva podatkov kot enega od vidikov, ki jih je treba upoštevati pred pridobitvijo oznake CE, glede na možno visoko stopnjo poseganja umetnointeligenčnih sistemov velikega tveganja v temeljni pravici do zasebnosti in varstva osebnih podatkov ter potrebo po zagotovitvi visoke ravni zaupanja v umetnointeligenčni sistem. EOVP in ENVP zato priporočata spremembo predloga, tako da se pojasni razmerje med potrdili, izdanimi na podlagi navedene uredbe, ter izdajanjem potrdil, pečati in označbami za varstvo podatkov. Nazadnje, organi za varstvo podatkov bi morali biti vključeni v pripravo in vzpostavitev harmoniziranih standardov in skupnih specifikacij.

77. Glede člena 43 predloga, ki se nanaša na ugotavljanje skladnosti, se zdi odstopanje od postopka ugotavljanja skladnosti iz člena 47 zelo široko, saj vključuje preveč izjem, kot so izjemni razlogi javne varnosti ali varstva življenja in zdravja ljudi, varstva okolja ter varstva ključnih industrijskih in infrastrukturnih sredstev. Zakonodajalcem predlagamo, da jih zožijo.

3.5.2 Kodeksi ravnanja

78. Komisija in države članice v skladu s členom 69 predloga spodbujajo in olajšujejo pripravo kodeksov ravnanja, namenjenih spodbujanju ponudnikov umetnointeligenčnih sistemov, ki niso velikega tveganja, k prostovoljni uporabi zahtev, ki se uporabljajo za umetnointeligenčne sisteme velikega tveganja, ter dodatnih zahtev. EOVP in ENVP v skladu z uvodno izjavo 78 Splošne uredbe o varstvu podatkov priporočata opredelitev in določitev sinergij med temi instrumenti in kodeksi ravnanja, določenimi v Splošni uredbi o varstvu podatkov, ki podpirajo skladnost z varstvom podatkov. Glede tega je treba pojasniti, ali je treba varstvo osebnih podatkov šteti med „dodatne zahteve“, ki jih lahko obravnavajo kodeksi ravnanja iz člena 69(2). Prav tako je pomembno zagotoviti, da „tehnične specifikacije in rešitve“, ki jih obravnavajo kodeksi ravnanja iz člena 69(1) in so namenjene spodbujanju skladnosti z zahtevami osnutka uredbe o umetni inteligenci, niso v nasprotju s pravili in načeli Splošne uredbe o varstvu podatkov in EUDPR. S tem bi upoštevanje teh orodij s strani ponudnikov umetnointeligenčnih sistemov, ki niso velikega tveganja, če taki sistemi temeljijo na obdelavi osebnih podatkov ali obdelujejo osebne podatke za izpolnitev svoje naloge, pomenilo dodano vrednost, saj bo to zagotovilo, da bodo lahko upravljavci in obdelovalci izpolnili svoje obveznosti glede varstva podatkov pri uporabi teh sistemov.

79. Hkrati bi bil pravni okvir za zaupanja vredno umetno inteligenco dopolnjen z vključevanjem kodeksov ravnanja, tako da bi se okrepilo zaupanje v uporabo te tehnologije, ker je varna in skladna z zakonodajo ter vključuje spoštovanje temeljnih pravic. Vendar bi bilo treba zasnovo teh instrumentov okrepiti z načrtovanjem mehanizmov, namenjenih preverjanju, ali ti kodeksi ravnanja zagotavljajo učinkovite „tehnične specifikacije in rešitve“ ter določajo „jasne cilje in ključne kazalnike uspešnosti za merjenje doseganja teh ciljev“ kot sestavni deli zadevnih kodeksov ravnanja. Poleg tega lahko odsotnost sklicevanja na (obvezne) mehanizme za spremljanje kodeksov ravnanja, zasnovanih za preverjanje, ali ponudniki umetnointeligenčnih sistemov, ki niso velikega tveganja, izpolnjujejo njihove določbe, ter možnost, da posamezni ponudniki pripravijo (in sami izvajajo) navedene kodekse (glej oddelek 5.2.7 obrazložitvenega memoranduma), dodatno oslabita učinkovitost in izvršljivost teh instrumentov.

80. Nazadnje EOVP in ENVP zahtevata pojasnila v zvezi z vrstami pobud, ki jih lahko razvije Komisija v skladu z uvodno izjavo 81 predloga, „da se olajša zmanjšanje tehničnih ovir za čezmejno izmenjavo podatkov za razvoj umetne inteligence“.

4 ZAKLJUČEK

81. Čeprav EOVP in ENVP pozdravljata predlog Komisije in menita, da je takšna uredba potrebna za zagotavljanje temeljnih pravic državljanov in prebivalcev EU, menita, da je treba predlog prilagoditi glede več vprašanj, da se zagotovita njegova uporabnost in učinkovitost.

82. Glede na zapletenost predloga in vprašanj, ki si jih prizadeva reševati, je treba opraviti še veliko dela, da bo predlog ustvaril dobro delujoč pravni okvir, ki bo učinkovito dopolnjeval Splošno uredbo o varstvu podatkov pri varovanju temeljnih človekovih pravic in hkrati spodbujal inovacije. EOVP in ENVP bosta še naprej na voljo za zagotavljanje svoje podpore na tem potovanju.

Bruselj, 18. junij 2021

Za Evropski odbor za varstvo podatkov	Za Evropskega nadzornika za varstvo podatkov
Predsednik	Nadzornik
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI