Svet
Evropske unije

Bruselj, 23. april 2021
(OR. en)

8115/21

Medinstitucionalna zadeva:
2021/0106 (COD)

TELECOM 156
JAI 429
COPEN 191
CYBER 108
DATAPROTECT 103
EJUSTICE 41
COSI 69
IXIM 74
ENFOPOL 148
FREMP 103
RELEX 347
MI 271
COMPET 275
IA 60
CODEC 573

SPREMNI DOPIS

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	22. april 2021
Prejemnik:	generalni sekretar Sveta Evropske unije Jeppe TRANHOLM-MIKKELSEN
Št. dok. Kom.:	COM(2021) 206 final
Zadeva:	Predlog uredbe Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci (akt o umetni inteligenci) in spremembi nekaterih zakonodajnih aktov unije

Delegacije prejmejo priloženi dokument COM(2021) 206 final.

Priloga: COM(2021) 206 final

EVROPSKA
KOMISIJA

Bruselj, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

O DOLOČITVI HARMONIZIRANIH PRAVIL O UMETNI INTELIGENCI (AKT O UMETNI INTELIGENCI) IN SPREMEMBI NEKATERIH ZAKONODAJNIH AKTOV UNIJE

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

OBRAZLOŽITVENI MEMORANDUM

1. OZADJE PREDLOGA

1.1. Razlogi za predlog in njegovi cilji

Ta obrazložitveni memorandum je priložen k predlogu uredbe o določitvi harmoniziranih pravil o umetni inteligenci (akt o umetni inteligenci). Umetna inteligenca je hitro razvijajoča se skupina tehnologij, ki lahko prinese številne gospodarske in družbene koristi v celotnem spektru industrij in družbenih dejavnosti. Uporaba umetne inteligence lahko z izboljšanjem napovedi, optimizacijo delovanja in dodeljevanja virov ter po meri prilagojeno dobavo storitev podpira družbeno in okoljsko koristne rezultate ter zagotavlja ključne konkurenčne prednosti za podjetja in evropsko gospodarstvo. Tako ukrepanje je še zlasti potrebno v sektorjih z velikim učinkom, kot so podnebne spremembe, okolje in zdravje, javni sektor, finance, mobilnost, notranje zadeve in kmetijstvo. Vendar pa lahko isti elementi in tehnike, ki omogočajo družbeno-ekonomske koristi umetne inteligence, prinašajo tudi nova tveganja ali negativne posledice za posameznike ali družbo. Glede na hitrost tehnoloških sprememb in možne izzive se je EU zavezala, da si bo prizadevala za uravnotežen pristop. V interesu Unije je ohraniti vodilno vlogo EU na področju tehnologije ter zagotoviti, da bodo Evropejci imeli koristi od novih tehnologij, ki so razvite in delujejo v skladu z vrednotami, temeljnimi pravicami in načeli Unije.

S tem predlogom se uresničuje politična zaveza predsednice von der Leyenove, ki je v svojih političnih smernicah za Komisijo 2019–2024 „Bolj ambiciozna Unija“[1]napovedala, da bo Komisija predlagala zakonodajo za harmoniziran evropski pristop k človeškim in etičnim posledicam umetne inteligence. Po tej objavi je Komisija 19. februarja 2020 objavila belo knjigo o umetni inteligenci s podnaslovom Evropski pristop k odličnosti in zaupanju[2]. V beli knjigi so predstavljene možnosti politike za doseganje dvojnega cilja, tj. spodbujanja uporabe umetne inteligence in odpravljanja tveganj, povezanih z nekaterimi vrstami uporabe te tehnologije. Namen tega predloga je uresničiti drugi cilj razvoja ekosistema zaupanja s predlogom pravnega okvira za zaupanja vredno umetno inteligenco. Predlog temelji na vrednotah in temeljnih pravicah EU, njegov namen pa je ljudem in drugim uporabnikom zagotoviti zaupanje v rešitve, ki temeljijo na umetni inteligenci, ter spodbuditi podjetja, da jih razvijajo. Umetna inteligenca bi morala biti orodje za ljudi in delovati v dobro družbi s končnim ciljem povečati blaginjo ljudi. Pravila za umetno inteligenco, ki je na voljo na trgu Unije ali kako drugače vpliva na ljudi v Uniji, bi morala biti zato humanocentrična, da bi ljudje lahko zaupali, da se tehnologija uporablja na varen način in v skladu z zakonodajo, vključno s spoštovanjem temeljnih pravic. Po objavi bele knjige je Komisija začela obsežno posvetovanje z deležniki, ki je naletelo na veliko zanimanje številnih deležnikov, ki so večinoma podprli regulativno posredovanje za reševanje izzivov in pomislekov, ki jih povzroča vse širša uporaba umetne inteligence.

Predlog je tudi odgovor na izrecne zahteve Evropskega parlamenta (EP) in Evropskega sveta, ki sta večkrat pozvala k zakonodajnim ukrepom za zagotovitev dobro delujočega notranjega trga za umetnointeligenčne sisteme, na katerem so koristi in tveganja umetne inteligence ustrezno obravnavani na ravni Unije. Podpira cilj, da Unija postane vodilna v svetu pri

[1] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_sl.pdf.

[2] Evropska komisija, bela knjiga o umetni inteligenci – evropski pristop k odličnosti in zaupanju, COM(2020) 65 final, 2020.

razvoju varne, zaupanja vredne in etične umetne inteligence, kot je navedel Evropski svet[3], ter zagotavlja zaščito etičnih načel, kot je izrecno zahteval Evropski parlament[4].

Evropski svet je leta 2017 pozval k „občutku nujnosti pri obravnavi nastajajočih trendov“, vključno z „vprašanji, kot je umetna inteligenca ..., ob hkratnem zagotavljanju visoke ravni varstva podatkov, digitalnih pravic in etičnih standardov“[5]. Svet je v sklepih iz leta 2019 o usklajenem načrtu za razvoj in uporabo umetne inteligence, izdelane v Evropi[6], dodatno poudaril, da je treba zagotoviti polno spoštovanje pravic evropskih državljanov, ter pozval k pregledu obstoječe ustrezne zakonodaje, da bo ustrezala novim priložnostim in izzivom, ki jih prinaša umetna inteligenca. Evropski svet je pozval tudi k jasni določitvi vrst uporabe umetne inteligence, ki jih je treba obravnavati kot uporabe velikega tveganja[7].

V najnovejših sklepih z dne 21. oktobra 2020 je bilo nadalje pozvano k obravnavi neprepustnosti, kompleksnosti, pristranskosti, določene stopnje nepredvidljivosti in delno avtonomnega vedenja nekaterih umetnointeligenčnih sistemov, da se zagotovi njihova združljivost s temeljnimi pravicami in olajša izvrševanje pravnih predpisov[8].

Tudi Evropski parlament je opravil veliko dela na področju umetne inteligence. Oktobra 2020 je sprejel več resolucij, povezanih z umetno inteligenco, med drugim o etiki[9], odgovornosti[10] in avtorskih pravicah[11]. Leta 2021 sta sledili resoluciji o umetni inteligenci v kazenskih zadevah[12] ter v izobraževanju, kulturi in avdiovizualnem sektorju[13]. Resolucija Evropskega parlamenta o okviru za etične vidike umetne inteligence, robotike in sorodne tehnologije Komisiji izrecno priporoča, da predlaga zakonodajne ukrepe za izkoriščanje priložnosti in koristi umetne inteligence, hkrati pa zagotovi zaščito etičnih načel. Resolucija vključuje besedilo zakonodajnega predloga uredbe o etičnih načelih za razvoj, uvajanje in uporabo umetne inteligence, robotike in sorodnih tehnologij. V skladu s politično zavezo, ki jo je predsednica von der Leyenova izrazila v svojih političnih smernicah glede resolucij, ki jih je Evropski parlament sprejel v skladu s členom 225 PDEU, ta predlog upošteva navedeno resolucijo Evropskega parlamenta ob polnem upoštevanju načel sorazmernosti, subsidiarnosti in boljše priprave zakonodaje.

---

3 Evropski svet, izredno zasedanje Evropskega sveta (1. in 2. oktobra 2020) – sklepi, EUCO 13/20, 2020, str. 6.

4 Resolucija Evropskega parlamenta z dne 20. oktobra 2020 s priporočili Komisiji o okviru etičnih vidikov umetne inteligence, robotike in sorodnih tehnologij, 2020/2012(INL).

5 Evropski svet, *zasedanje Evropskega sveta (19. oktober 2017) – sklep* EUCO 14/17, 2017, str. 8.

6 Svet Evropske unije, *Umetna inteligenca (b) Sklepi o usklajenem načrtu o umetni inteligenci – sprejetje* 6177/19, 2019.

7 Evropski svet, *izredno zasedanje Evropskega sveta (1. in 2. oktobra 2020) – sklepi*, EUCO 13/ 2020.

8 Svet Evropske unije, *Sklepi predsedstva – Listina o temeljnih pravicah v kontekstu umetne inteligence in digitalnih sprememb*, 11481/20, 2020.

9 Resolucija Evropskega parlamenta z dne 20. oktobra 2020 o okviru etičnih vidikov umetne inteligence, robotike in sorodnih tehnologij, 2020/2012(INL).

10 Resolucija Evropskega parlamenta z dne 20. oktobra 2020 o ureditvi civilne odgovornosti za področje umetne inteligence, 2020/2014(INL).

11 Resolucija Evropskega parlamenta z dne 20. oktobra 2020 o pravicah intelektualne lastnine pri razvoju tehnologije umetne inteligence, 2020/2015(INI).

12 Osnutek poročila Evropskega parlamenta, Umetna inteligenca v kazenskem pravu in njena uporaba v policiji in pravosodnih organih na področju kazenskih zadev, 2020/2016(INI).

13 Osnutek poročila Evropskega parlamenta, Umetna inteligenca v izobraževanju, kulturi in avdiovizualnem sektorju, 2020/2017(INI). V zvezi s tem je Komisija sprejela akcijski načrt za digitalno izobraževanje za obdobje 2021–2027: Novi temelji za izobraževanje in usposabljanje v digitalni dobi, ki predvideva razvoj etičnih smernic za uporabo umetne inteligence in podatkov v izobraževanju – sporočilo Komisije COM(2020) 624 final.

V tem političnem kontekstu Komisija predlaga regulativni okvir za umetno inteligenco z naslednjimi **posebnimi cilji**:

- zagotoviti, da so umetnointeligenčni sistemi, ki so dani na trg Unije in se uporabljajo, varni ter spoštujejo obstoječo zakonodajo o temeljnih pravicah in vrednotah Unije;
- zagotoviti pravno varnost za olajšanje naložb in inovacij na področju umetne inteligence;
- izboljšati upravljanje in učinkovito izvrševanje obstoječe zakonodaje o temeljnih pravicah in varnostnih zahtevah, ki se uporabljajo za umetnointeligenčne sisteme;
- olajšati razvoj enotnega trga za zakonite, varne in zaupanja vredne uporabe umetne inteligence ter preprečiti razdrobljenost trga.

Za doseganje teh ciljev ta predlog predstavlja uravnotežen in sorazmeren horizontalni regulativni pristop k umetni inteligenci, ki je omejen na minimalne zahteve, potrebne za obravnavo tveganj in težav, povezanih z umetno inteligenco, brez neupravičenega omejevanja ali oviranja tehnološkega razvoja ali drugega nesorazmernega povečanja stroškov dajanja rešitev umetne inteligence na trg. Predlog določa robusten in prožen pravni okvir. Po eni strani je celovit in s svojimi temeljnimi regulativnimi odločitvami primeren za prihodnost, vključno z zahtevami, ki temeljijo na načelih, ki jih morajo izpolnjevati umetnointeligenčni sistemi. Po drugi strani pa uvaja sorazmeren regulativni sistem, ki temelji na dobro opredeljenem regulativnem pristopu na podlagi tveganja, ki ne ustvarja nepotrebnih omejitev trgovine, pri čemer je pravno posredovanje prilagojeno tistim konkretnim situacijam, v katerih obstaja utemeljen razlog za zaskrbljenost ali v katerih je tako zaskrbljenost mogoče razumno pričakovati v bližnji prihodnosti. Hkrati pravni okvir vključuje prožne mehanizme, ki mu omogočajo dinamično prilagajanje glede na razvoj tehnologije in pojavljanje novih zaskrbljujočih razmer.

Predlog določa harmonizirana pravila za razvoj, dajanje na trg in uporabo umetnointeligenčnih sistemov v Uniji na podlagi sorazmernega pristopa, ki temelji na tveganju. Predlaga enotno opredelitev umetne inteligence, ki bo primerna za prihodnost. Nekatere posebej škodljive prakse umetne inteligence so prepovedane, saj so v nasprotju z vrednotami Unije, medtem ko so predlagane posebne omejitve in zaščitni ukrepi v zvezi z nekaterimi uporabami sistemov za biometrično identifikacijo na daljavo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Predlog določa trdno metodologijo tveganja za opredelitev umetnointeligenčnih sistemov „velikega tveganja“, ki predstavljajo bistveno tveganje za zdravje in varnost ali temeljne pravice oseb. Ti umetnointeligenčni sistemi bodo morali izpolnjevati niz horizontalnih obveznih zahtev za zaupanja vredno umetno inteligenco in upoštevati postopke ugotavljanja skladnosti, preden bodo lahko dani na trg Unije. Predvidljive, sorazmerne in jasne obveznosti so naložene tudi ponudnikom in uporabnikom teh sistemov, da se zagotovita varnost in spoštovanje obstoječe zakonodaje o varstvu temeljnih pravic v celotnem življenjskem ciklu umetnointeligenčnih sistemov. Za nekatere posebne umetnointeligenčne sisteme so predlagane le minimalne obveznosti glede preglednosti, zlasti kadar se uporabljajo klepetalni boti ali „globoki ponaredki“.

Predlagana pravila se bodo izvajala s sistemom upravljanja na ravni držav članic, ki bo temeljil na že obstoječih strukturah, in mehanizmom sodelovanja na ravni Unije z ustanovitvijo Evropskega odbora za umetno inteligenco. Predlagani so tudi dodatni ukrepi za podporo inovacijam, zlasti z regulativnimi peskovniki za umetno inteligenco in drugimi ukrepi za zmanjšanje regulativnega bremena ter podporo malim in srednje velikim podjetjem (MSP) ter zagonskim podjetjem.

1.2. Skladnost z veljavnimi predpisi s področja zadevne politike

Horizontalna narava predloga zahteva popolno skladnost z obstoječo zakonodajo Unije, ki se uporablja za sektorje, v katerih se umetnointeligenčni sistemi velikega tveganja že uporabljajo ali se bodo verjetno uporabljali v bližnji prihodnosti.

Skladnost je zagotovljena tudi z Listino EU o temeljnih pravicah in obstoječo sekundarno zakonodajo Unije o varstvu podatkov, varstvu potrošnikov, nediskriminaciji in enakosti spolov. Predlog ne posega v splošno uredbo o varstvu podatkov (Uredba (EU) 2016/679) in direktivo o kazenskem pregonu (Direktiva (EU) 2016/680) ter ju dopolnjuje z nizom harmoniziranih pravil, ki se uporabljajo za oblikovanje, razvoj in uporabo nekaterih umetnointeligenčnih sistemov velikega tveganja ter omejitve nekaterih uporab sistemov za biometrično identifikacijo na daljavo. Poleg tega predlog dopolnjuje obstoječe pravo Unije o nediskriminaciji s posebnimi zahtevami, katerih cilj je čim bolj zmanjšati tveganje diskriminacije v algoritmih, zlasti v zvezi z oblikovanjem in kakovostjo nabora podatkov, ki se uporabljajo za razvoj umetnointeligenčnih sistemov, dopolnjenih z obveznostmi za testiranje, obvladovanja tveganja, dokumentacije in človekovega nadzora v celotnem življenjskem ciklu umetnointeligenčnih sistemov. Predlog ne posega v uporabo konkurenčnega prava Unije.

Kar zadeva umetnointeligenčne sisteme velikega tveganja, ki so varnostne komponente proizvodov, bo ta predlog vključen v obstoječo sektorsko varnostno zakonodajo, da se zagotovi skladnost, prepreči podvajanje in čim bolj zmanjša dodatna obremenitev. Zlasti v zvezi z umetnointeligenčnimi sistemi velikega tveganja, povezanimi s proizvodi, ki jih zajema zakonodaja novega zakonodajnega okvira (npr. stroji, medicinski pripomočki, igrače), se bodo zahteve za umetnointeligenčne sisteme iz tega predloga preverjale v okviru obstoječih postopkov ugotavljanja skladnosti v skladu z ustrezno zakonodajo novega zakonodajnega okvira. V zvezi z medsebojnim učinkom zahtev je cilj zakonodaje o novem zakonodajnem okviru zagotoviti splošno varnost končnega proizvoda in zato lahko vsebuje posebne zahteve v zvezi z varno vključitvijo umetnointeligenčnega sistema v končni proizvod, čeprav naj bi zahteve tega predloga vključevale varnostna tveganja, značilna za umetnointeligenčne sisteme. Predlog uredbe o strojih, sprejet istega dne kot ta predlog, v celoti odraža ta pristop. Za umetnointeligenčne sisteme velikega tveganja, povezane s proizvodi, za katere velja ustrezna zakonodaja starega pristopa (npr. letalstvo, avtomobili), se ta predlog ne bi neposredno uporabljal. Vendar bo treba pri sprejemanju ustrezne izvedbene ali delegirane zakonodaje na podlagi navedenih aktov upoštevati predhodne bistvene zahteve za umetnointeligenčne sisteme velikega tveganja iz tega predloga.

V zvezi z umetnointeligenčnimi sistemi, ki jih zagotavljajo ali uporabljajo regulirane kreditne institucije, bi bilo treba organe, pristojne za nadzor zakonodaje Unije o finančnih storitvah, določiti kot pristojne organe za nadzor zahtev iz tega predloga, da se zagotovi skladno izvrševanje obveznosti iz tega predloga in zakonodaje Unije o finančnih storitvah, kadar se umetnointeligenčni sistemi do določene mere implicitno regulirajo v zvezi s sistemom notranjega upravljanja kreditnih institucij. Za nadaljnjo krepitev skladnosti so postopek ugotavljanja skladnosti in nekatere postopkovne obveznosti ponudnikov iz tega predloga vključeni v postopke iz Direktive 2013/36/EU o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru[14].

[14] Direktiva 2013/36/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij in investicijskih podjetij, spremembi Direktive 2002/87/ES in razveljavitvi direktiv 2006/48/ES in 2006/49/ES. Besedilo velja za EGP (UL L 176, 27.6.2013, str. 338).

Ta predlog je skladen tudi z veljavno zakonodajo Unije o storitvah, vključno s posredniškimi storitvami, ki jih urejata Direktiva o elektronskem poslovanju 2000/31/ES[15] in nedavni predlog Komisije za akt o digitalnih storitvah[16].

V zvezi z umetnointeligenčnimi sistemi, ki so komponente obsežnih informacijskih sistemov na območju svobode, varnosti in pravice, ki jih upravlja Agencija Evropske unije za operativno upravljanje obsežnih informacijskih sistemov (eu-LISA), se predlog ne bo uporabljal za tiste umetnointeligenčne sisteme, ki so bili dani na trg ali v uporabo pred pretekom enega leta od datuma začetka uporabe te uredbe, razen če se zaradi nadomestitve ali spremembe navedenih pravnih aktov bistveno spremeni zasnova ali predvideni namen zadevnega umetnointeligenčnega sistema ali umetnointeligenčnih sistemov.

1.3. Skladnost z drugimi politikami Unije

Predlog je del širšega celovitega svežnja ukrepov za reševanje težav, ki jih povzročata razvoj in uporaba umetne inteligence, kot je obravnavano v beli knjigi o umetni inteligenci. Zato sta zagotovljena skladnost in dopolnjevanje z drugimi tekočimi ali načrtovanimi pobudami Komisije, ki so prav tako namenjene obravnavi teh težav, vključno z revizijo sektorske zakonodaje o proizvodih (npr. direktiva o strojih, direktiva o splošni varnosti proizvodov) in pobudami, ki obravnavajo vprašanja odgovornosti v zvezi z novimi tehnologijami, vključno z umetnointeligenčnimi sistemi. Te pobude bodo nadgradile in dopolnile ta predlog, da bi zagotovili pravno jasnost in spodbudili razvoj ekosistema zaupanja v umetno inteligenco v Evropi.

Predlog je v skladu tudi s splošno digitalno strategijo Komisije, saj prispeva k spodbujanju tehnologije, ki deluje za ljudi, kar je eden od treh glavnih stebrov usmeritve in ciljev politike, navedenih v sporočilu „Oblikovanje digitalne prihodnosti Evrope“[17]. Določa skladen, učinkovit in sorazmeren okvir za zagotovitev, da se bo umetna inteligenca razvijala na način, ki spoštuje pravice ljudi in si zasluži njihovo zaupanje, s čimer bo Evropa postala pripravljena na digitalno dobo in bo naslednjih deset let postalo **digitalno desetletje**[18].

Poleg tega je spodbujanje inovacij na podlagi umetne inteligence tesno povezano z **aktom o upravljanju podatkov**[19]**, direktivo o odprtih podatkih**[20] in drugimi pobudami v okviru **evropske strategije za podatke**[21], ki bodo vzpostavile zaupanja vredne mehanizme in storitve za ponovno uporabo, souporabo in združevanje podatkov, bistvenih za razvoj visokokakovostnih modelov na podatkih temelječe umetne inteligence.

Predlog tudi znatno krepi vlogo Unije pri oblikovanju svetovnih norm in standardov ter spodbujanju zaupanja vredne umetne inteligence, ki je v skladu z vrednotami in interesi Unije. Uniji zagotavlja močno podlago za nadaljnje sodelovanje z zunanjimi partnerji, vključno s tretjimi državami, in na mednarodnih forumih o vprašanjih, povezanih z umetno inteligenco.

---

15 Direktiva 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (direktiva o elektronskem poslovanju) (UL L 178, 17.7.2000, str. 1).

16 Glej predlog uredbe Evropskega parlamenta in Sveta o enotnem trgu digitalnih storitev (akt o digitalnih storitvah) in spremembi Direktive 2000/31/ES, COM/2020/825 final.

17 Sporočilo Komisije, Oblikovanje digitalne prihodnosti Evrope, COM/2020/ 67 final.

18 2030 Digital Compass: the European way for the Digital Decade (Digitalni kompas za leto 2030: evropska pot v digitalno desetletje).

19 Predlog uredbe o evropskem upravljanju podatkov (akt o upravljanju podatkov), COM/2020/767.

20 Direktiva (EU) 2019/1024 Evropskega parlamenta in Sveta z dne 20. junija 2019 o odprtih podatkih in ponovni uporabi informacij javnega sektorja, PE/28/2019/REV/1 (UL L 172, 26.6.2019, str. 56).

21 Sporočilo Komisije z naslovom Evropska strategija za podatke (COM(2020) 66 final).

2. PRAVNA PODLAGA, SUBSIDIARNOST IN SORAZMERNOST

2.1. Pravna podlaga

Pravna podlaga tega predloga je predvsem člen 114 Pogodbe o delovanju Evropske unije (v nadaljnjem besedilu: PDEU), ki določa sprejetje ukrepov za zagotovitev vzpostavitve in delovanja notranjega trga.

Ta predlog je osrednji del strategije EU za enotni digitalni trg. Glavni cilj tega predloga je zagotoviti pravilno delovanje notranjega trga z določitvijo harmoniziranih pravil, zlasti o razvoju, dajanju na trg Unije ter uporabi proizvodov in storitev, ki uporabljajo tehnologije umetne inteligence ali se zagotavljajo kot samostojni umetnointeligenčni sistemi. Nekatere države članice že razmišljajo o nacionalnih predpisih, s katerimi bi zagotovile, da bo umetna inteligenca varna ter da se bo razvijala in uporabljala v skladu z obveznostmi glede temeljnih pravic. To bo verjetno povzročilo dve glavni težavi: (i) razdrobljenost notranjega trga na bistvene elemente, zlasti glede zahtev za proizvode in storitve umetne inteligence, njihovega trženja, uporabe, odgovornosti in nadzora s strani javnih organov, ter (ii) znatno zmanjšanje pravne varnosti za ponudnike in uporabnike umetnointeligenčnih sistemov glede tega, kako se bodo obstoječa in nova pravila uporabljala za te sisteme v Uniji. Glede na širok čezmejni pretok proizvodov in storitev je ti dve težavi mogoče najbolje rešiti s harmoniziranjem zakonodaje EU.

V predlogu so namreč opredeljene skupne obvezne zahteve, ki veljajo za zasnovo in razvoj nekaterih umetnointeligenčnih sistemov, preden so dani na trg, ter ki se bodo podrobneje določile s harmoniziranimi tehničnimi standardi. Predlog obravnava tudi razmere po dajanju umetnointeligenčnih sistemov na trg s harmoniziranjem načina izvajanja naknadnih kontrol.

Poleg tega je glede na to, da ta predlog vsebuje nekatera 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, primerno, da je podlaga za to uredbo, kar zadeva navedena posebna pravila, člen 16 PDEU.

2.2. Subsidiarnost (za neizključno pristojnost)

Zaradi narave umetne inteligence, ki se pogosto opira na velike in raznolike nabore podatkov ter je lahko vgrajena v kateri koli proizvod ali storitev, ki prosto kroži na notranjem trgu, države članice same ne morejo učinkovito doseči ciljev tega predloga. Poleg tega bo nastajajoči mozaik potencialno različnih nacionalnih pravil oviral nemoten pretok proizvodov in storitev, povezanih z umetnointeligenčnimi sistemi, po vsej EU ter bo neučinkovit pri zagotavljanju varnosti in zaščite temeljnih pravic in vrednot Unije v različnih državah članicah. Nacionalni pristopi k reševanju težav bodo zgolj ustvarili dodatno pravno negotovost in ovire ter upočasnili uvajanje umetne inteligence na trg.

Cilje tega predloga je mogoče bolje doseči na ravni Unije, da se prepreči nadaljnja razdrobljenost enotnega trga na potencialno nasprotujoče si nacionalne okvire, ki bi preprečevali prost pretok blaga in storitev, ki vključujejo umetno inteligenco. Trden evropski regulativni okvir za zaupanja vredno umetno inteligenco bo zagotovil tudi enake konkurenčne pogoje in zaščitil vse ljudi, hkrati pa okrepil konkurenčnost in industrijsko podlago Evrope na področju umetne inteligence. Samo s skupnim ukrepanjem na ravni Unije je mogoče zaščititi tudi digitalno suverenost Unije ter izkoristiti njena orodja in regulativna pooblastila za oblikovanje predpisov in standardov na svetovni ravni.

2.3. Sorazmernost

Predlog temelji na obstoječih pravnih okvirih ter je sorazmeren in potreben za doseganje svojih ciljev, saj upošteva pristop, ki temelji na tveganju, in uvaja regulativna bremena le, kadar je verjetno, da bo umetnointeligenčni sistem predstavljal veliko tveganje za temeljne pravice in varnost. Za druge umetnointeligenčne sisteme, ki ne predstavljajo velikega tveganja, so predpisane le zelo omejene obveznosti glede preglednosti, na primer v smislu zagotavljanja informacij za opozarjanje na uporabo umetnointeligenčnega sistema v stikih z ljudmi. Za umetnointeligenčne sisteme velikega tveganja so zahteve po visokokakovostnih podatkih, dokumentaciji in sledljivosti, preglednosti, človekovem nadzoru, točnosti in robustnosti nujno potrebne za zmanjševanje tveganj za temeljne pravice in varnost, ki jih povzroča umetna inteligenca in ki jih ne vključujejo drugi obstoječi pravni okviri. Harmonizirani standardi ter podporna navodila in orodja za zagotavljanje skladnosti bodo ponudnikom in uporabnikom pomagali pri izpolnjevanju zahtev iz predloga ter zmanjšali njihove stroške. Stroški, ki jih imajo operaterji, so sorazmerni z doseženimi cilji ter gospodarskimi koristmi in koristmi za ugled, ki jih operaterji lahko pričakujejo od tega predloga.

2.4. Izbira instrumenta

Izbira uredbe kot pravnega instrumenta je utemeljena s potrebo po enotni uporabi novih pravil, kot so opredelitev umetne inteligence, prepoved nekaterih škodljivih praks, podprtih z omogočeno umetno inteligenco, in klasifikacija nekaterih umetnointeligenčnih sistemov. Neposredna uporaba uredbe v skladu s členom 288 PDEU bo zmanjšala pravno razdrobljenost ter olajšala razvoj enotnega trga za zakonite, varne in zaupanja vredne umetnointeligenčne sisteme. To bo dosegla zlasti z uvedbo harmoniziranega sklopa temeljnih zahtev v zvezi z umetnointeligenčnimi sistemi, razvrščenimi kot sistemi velikega tveganja, ter obveznosti za ponudnike in uporabnike teh sistemov, s čimer bo izboljšala varstvo temeljnih pravic in zagotovila pravno varnost tako za operaterje kot za potrošnike.

Hkrati določbe uredbe niso pretirano predpisujoče in dopuščajo različne ravni ukrepanja držav članic glede elementov, ki ne ogrožajo ciljev pobude, zlasti notranje organizacije sistema nadzora trga in sprejetja ukrepov za spodbujanje inovacij.

3. REZULTATI NAKNADNIH OCEN, POSVETOVANJ Z ZAINTERESIRANIMI STRANMI IN OCEN UČINKA

3.1. Posvetovanje z deležniki

Ta predlog je rezultat obsežnega posvetovanja z vsemi glavnimi deležniki, pri katerem je Komisija uporabila splošna načela in minimalne standarde za posvetovanje z zainteresiranimi stranmi.

Spletno javno posvetovanje se je začelo 19. februarja 2020 ob objavi bele knjige o umetni inteligenci in je trajalo do 14. junija 2020. Cilj tega posvetovanja je bil zbrati stališča in mnenja o beli knjigi. Usmerjeno je bilo na vse deležnike iz javnega in zasebnega sektorja, vključno z vladami, lokalnimi upravnimi organi, komercialnimi in nekomercialnimi organizacijami, socialnimi partnerji, strokovnjaki, akademiki in državljani. Po analizi vseh prejetih odzivov je Komisija na svoji spletni strani objavila njihov povzetek in posamezne odzive[22].

[22] Vse rezultate posvetovanja si oglejte tukaj.

Skupno je bilo prejetih 1 215 prispevkov, od tega 352 prispevkov podjetij ali poslovnih organizacij/združenj, 406 prispevkov posameznikov (92 % posameznikov iz EU), 152 prispevkov v imenu akademskih/raziskovalnih ustanov in 73 prispevkov javnih organov. Glasove civilne družbe je zastopalo 160 anketirancev (med njimi 9 potrošniških organizacij, 129 nevladnih organizacij in 22 sindikatov), 72 anketirancev pa je prispevalo kot „drugi“. Od 352 predstavnikov iz gospodarstva in industrije jih je bilo 222 podjetij in predstavnikov podjetij, od tega 41,5 % mikro, malih in srednje velikih podjetij. Ostalo so bila poslovna združenja. Na splošno je 84 % odgovorov iz gospodarstva in industrije prišlo iz EU-27. Odvisno od vprašanja je od 81 do 598 anketirancev za vnos pripomb uporabilo možnost prostega besedila. Preko spletnega mesta EUSurvey je bilo predloženih več kot 450 dokumentov o stališčih, ki so bili bodisi priloženi odgovorom na vprašalnik (več kot 400) bodisi poslani kot samostojni prispevki (več kot 50).

Na splošno se deležniki strinjajo, da je treba ukrepati. Velika večina deležnikov se strinja, da obstajajo zakonodajne vrzeli ali da je potrebna nova zakonodaja. Vendar pa več deležnikov opozarja Komisijo, da naj se izogne podvajanju, nasprotujočim si obveznostim in pretirani regulaciji. V številnih pripombah je bil poudarjen pomen tehnološko nevtralnega in sorazmernega regulativnega okvira.

Deležniki so večinoma zahtevali ozko, jasno in natančno opredelitev umetne inteligence. Deležniki so tudi poudarili, da je poleg pojasnitve pojma umetne inteligence pomembno opredeliti pojme „tveganje“, „veliko tveganje“, „majhno tveganje“, „biometrična identifikacija na daljavo“ in „škoda“.

Večina anketirancev izrecno podpira pristop, ki temelji na tveganju. Uporaba okvira, ki temelji na tveganju, je bila ocenjena kot boljša možnost kot splošna ureditev vseh umetnointeligenčnih sistemov. Vrste tveganj in groženj bi morale temeljiti na pristopu za vsak sektor posebej in za vsak primer posebej. Tveganja je treba izračunati tudi ob upoštevanju vpliva na pravice in varnost.

Regulativni peskovniki bi lahko bili zelo koristni za spodbujanje umetne inteligence in jih pozdravljajo nekateri deležniki, zlasti poslovna združenja.

Med tistimi, ki so oblikovali svoje mnenje o modelih izvrševanja, jih je več kot 50 %, zlasti iz poslovnih združenj, podprlo kombinacijo predhodne samoocene tveganja in naknadnega izvrševanja za umetnointeligenčne sisteme velikega tveganja.

3.2. Zbiranje in uporaba strokovnega znanja

Predlog temelji na dveletni analizi in tesnem sodelovanju deležnikov, vključno z akademiki, podjetji, socialnimi partnerji, nevladnimi organizacijami, državami članicami in državljani. Pripravljalno delo se je začelo leta 2018 z ustanovitvijo **strokovne skupine na visoki ravni za umetno inteligenco**, ki je imela vključujočo in široko sestavo 52 znanih strokovnjakov, katerih naloga je bila svetovati Komisiji pri izvajanju strategije Komisije o umetni inteligenci. Komisija je aprila 2019 podprla[23] ključne zahteve iz etičnih smernic strokovne skupine na visoki ravni za umetno inteligenco za zaupanja vredno umetno inteligenco[24], ki so bile revidirane ob upoštevanju več kot 500 predlogov deležnikov. Ključne zahteve odražajo široko razširjen in skupen pristop, kar dokazujejo številni etični kodeksi in načela, ki so jih razvile številne zasebne in javne organizacije v Evropi in zunaj nje, da bi morala razvoj in uporaba

[23] Evropska komisija, *Krepitev zaupanja v umetno inteligenco, osredotočeno na človeka*, COM(2019) 168.

[24] Strokovna skupina na visoki ravni za umetno inteligenco, *Ethics Guidelines for Trustworthy AI* (Etične smernice za zaupanja vredno umetno inteligenco), 2019.

umetne inteligence temeljiti na nekaterih bistvenih vrednotno usmerjenih načelih. Na podlagi ocenjevalnega seznama za zaupanja vredno umetno inteligenco[25] so te zahteve začele delovati v pilotnem postopku z več kot 350 organizacijami.

Poleg tega je bilo ustanovljeno **zavezništvo za umetno inteligenco**[26], v kateri približno 4 000 deležnikov razpravlja o tehnoloških in družbenih posledicah umetne inteligence, ki doseže vrhunec na letni skupščini za umetno inteligenco.

Bela knjiga o umetni inteligenci je ta vključujoči pristop še nadgradila, saj je svoje pripombe dalo več kot 1 250 deležnikov, tudi z več kot 450 dodatnimi dokumenti o stališčih. Zato je Komisija objavila začetno oceno učinka, ki je prejela več kot 130 pripomb[27]. Organizirane so bile tudi **dodatne delavnice in dogodki za deležnike**, katerih rezultati podpirajo analizo v oceni učinka in politične odločitve, sprejete v tem predlogu[28]. Naročena je bila tudi **zunanja študija** za vključitev v oceno učinka.

3.3. Ocena učinka

Komisija je v skladu s svojo politiko za boljše pravno urejanje izvedla oceno učinka za ta predlog, ki jo je preučil odbor Komisije za regulativni nadzor. Dne 16. decembra 2020 je potekal sestanek z odborom za regulativni nadzor, ki mu je sledilo negativno mnenje. Odbor za regulativni nadzor je po temeljiti reviziji ocene učinka, ki je obravnavala pripombe, in ponovni predložitvi ocene učinka 21. marca 2021 izdal pozitivno mnenje. Mnenja odbora za regulativni nadzor, priporočila in pojasnilo, kako so bila ta upoštevana, so predstavljeni v Prilogi 1 k oceni učinka.

Komisija je preučila različne možnosti politike za uresničitev splošnega cilja predloga, ki je **zagotoviti pravilno delovanje enotnega trga** z ustvarjanjem pogojev za razvoj in uporabo zaupanja vredne umetne inteligence v Uniji.

Ocenjene so bile štiri možnosti politike z različnimi stopnjami regulativnega posredovanja:

- **možnost 1**: zakonodajni instrument EU o vzpostavitvi prostovoljnega sistema označevanja;
- **možnost 2**: sektorski *ad hoc* pristop;
- **možnost 3**: horizontalni zakonodajni instrument EU, ki temelji na sorazmernem pristopu na podlagi tveganja;
- **možnost 3+**: horizontalni zakonodajni instrument EU, ki temelji na sorazmernem pristopu na podlagi tveganja + kodeksi ravnanja za umetnointeligenčne sisteme, ki ne predstavljajo velikega tveganja;
- **možnost 4**: horizontalni zakonodajni instrument EU, ki določa obvezne zahteve za vse umetnointeligenčne sisteme ne glede na tveganje, ki ga predstavljajo.

---

25 Strokovna skupina na visoki ravni za umetno inteligenco, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment* (Ocenjevalni seznam za zaupanja vredno umetno inteligenco za samooceno), 2020.

26 Zavezništvo za umetno inteligenco je forum z več deležniki, ki je začel delovati junija 2018, Zavezništvo za umetno inteligenco https://ec.europa.eu/digital-single-market/en/european-ai-alliance

27 Evropska komisija, *Začetna ocena učinka predloga pravnega akta Evropskega parlamenta in Sveta, ki določa zahteve za umetno inteligenco*.

28 Za podrobnosti o vseh opravljenih posvetovanjih glej Prilogo 2 k oceni učinka.

V skladu z metodologijo Komisije je bila vsaka možnost politike ocenjena glede na gospodarske in družbene učinke s posebnim poudarkom na učinkih na temeljne pravice. Najprimernejša možnost je možnost 3+, tj. regulativni okvir samo za umetnointeligenčne sisteme velikega tveganja, pri čemer bi lahko vsi ponudniki umetnointeligenčnih sistemov, ki ne predstavljajo velikega tveganja, upoštevali kodeks ravnanja. Zahteve se bodo nanašale na podatke, dokumentacijo in sledljivost, zagotavljanje informacij in preglednost, človekov nadzor ter robustnost in točnost ter bodo obvezne za umetnointeligenčne sisteme velikega tveganja. Podjetja, ki uvedejo kodekse ravnanja za druge umetnointeligenčne sisteme, to storijo prostovoljno.

Prednostna možnost je bila ocenjena kot primerna za najučinkovitejšo obravnavo ciljev tega predloga. Z zahtevo po omejenem, a učinkovitem naboru ukrepov za razvijalce in uporabnike umetne inteligence prednostna možnost omejuje tveganja za kršitev temeljnih pravic in za varnost ljudi ter spodbuja učinkovit nadzor in izvrševanje, tako da zahteve usmerja le na sisteme, pri katerih obstaja veliko tveganje, da bi do takih kršitev lahko prišlo. S to možnostjo se stroški usklajevanja posledično zmanjšajo na minimum, s čimer se prepreči nepotrebna upočasnitev uvajanja zaradi višjih cen in stroškov izpolnjevanja obveznosti. Za odpravo morebitnih pomanjkljivosti za MSP ta možnost vključuje več določb za podporo njihovi skladnosti in zmanjšanje njihovih stroškov, vključno z vzpostavitvijo regulativnih peskovnikov in obveznostjo upoštevanja interesov MSP pri določanju pristojbin, povezanih z ugotavljanjem skladnosti.

Prednostna možnost bo povečala zaupanje ljudi v umetno inteligenco, podjetja bodo pridobila na pravni varnosti, države članice pa ne bodo videle razloga za enostransko ukrepanje, ki bi lahko razdrobilo enotni trg. Kot posledica večjega povpraševanja zaradi večjega zaupanja, več razpoložljivih ponudb zaradi pravne varnosti in odsotnosti ovir za čezmejni pretok umetnointeligenčnih sistemov bo enotni trg za umetno inteligenco verjetno cvetel. Evropska unija bo še naprej razvijala hitro rastoč umetnointeligenčni ekosistem inovativnih storitev in proizvodov, ki vključujejo tehnologijo umetne inteligence ali samostojne umetnointeligenčne sisteme, kar bo povečalo digitalno avtonomijo.

Podjetja ali javni organi, ki razvijajo ali uporabljajo umetno inteligenco v namene, ki predstavljajo veliko tveganje za varnost ali temeljne pravice državljanov, bi morali izpolnjevati posebne zahteve in obveznosti. Skladnost s temi zahtevami bi pomenila stroške v višini približno 6 000 do 7 000 EUR za dobavo povprečnega umetnointeligenčnega sistema velikega tveganja v višini približno 170 000 EUR do leta 2025. Za uporabnike umetne inteligence bi nastali tudi letni stroški za čas, porabljen za zagotavljanje človekovega nadzora, kadar je to primerno, odvisno od primera uporabe. Ti so ocenjeni na približno 5 000 EUR do 8 000 EUR na leto. Za dobavitelje umetne inteligence velikega tveganja bi lahko stroški preverjanja znašali od dodatnih 3 000 EUR do 7 500 EUR. Podjetja ali javni organi, ki razvijajo ali uporabljajo umetno inteligenco v namene, ki niso razvrščeni kot veliko tveganje, bi imeli le minimalne obveznosti obveščanja. Lahko pa se pridružijo drugim in skupaj sprejmejo kodeks ravnanja, da bi upoštevali ustrezne zahteve in zagotovili, da so njihovi umetnointeligenčni sistemi zaupanja vredni. V tem primeru bi bili stroški kvečjemu tako visoki kot pri sistemih umetne inteligence velikega tveganja, najverjetneje pa nižji.

Učinki možnosti politike na različne kategorije deležnikov (gospodarske subjekte/podjetja; organi za ugotavljanje skladnosti, organi za standardizacijo in drugi javni organi; posamezniki/državljani; raziskovalci) so podrobno pojasnjeni v Prilogi 3 k oceni učinka, ki podpira ta predlog.

3.4. Ustreznost in poenostavitev ureditve

Ta predlog določa obveznost, ki se bo uporabljala za ponudnike in uporabnike umetnointeligenčnih sistemov velikega tveganja. Za ponudnike, ki razvijajo in dajejo take sisteme na trg Unije, bo ustvarila pravno varnost ter zagotovila, da ne bodo nastajale ovire za čezmejno zagotavljanje storitev in proizvodov, povezanih z umetno inteligenco. Za podjetja, ki uporabljajo umetno inteligenco, bo spodbujala zaupanje pri njihovih strankah. Za nacionalne javne uprave bo spodbudila zaupanje javnosti v uporabo umetne inteligence in okrepila mehanizme izvrševanja (z uvedbo evropskega usklajevalnega mehanizma, zagotavljanjem ustreznih zmogljivosti in olajšanjem revizij umetnointeligenčnih sistemov z novimi zahtevami glede dokumentacije, sledljivosti in preglednosti). Poleg tega bodo v okviru predvideni posebni ukrepi za podporo inovacijam, vključno z regulativnimi peskovniki ter posebnimi ukrepi za podporo malim uporabnikom in ponudnikom umetnointeligenčnih sistemov velikega tveganja za uskladitev z novimi pravili.

Namen predloga je tudi okrepiti konkurenčnost in evropsko industrijsko bazo na področju umetne inteligence. Zagotovljena je popolna skladnost z obstoječo sektorsko zakonodajo Unije, ki se uporablja za umetnointeligenčne sisteme (npr. za proizvode in storitve), kar bo prineslo dodatno jasnost in poenostavilo izvrševanje novih pravil.

3.5. Temeljne pravice

Uporaba umetne inteligence s svojimi posebnimi značilnostmi (npr. neprepustnost, kompleksnost, odvisnost od podatkov, avtonomno vedenje) ima lahko škodljiv učinek na številne temeljne pravice iz Listine EU o temeljnih pravicah (v nadaljnjem besedilu: Listina). Namen tega predloga je zagotoviti visoko raven varstva teh temeljnih pravic in obravnavati različne vire tveganj z jasno opredeljenim pristopom, ki temelji na tveganju. S sklopom zahtev za zaupanja vredno umetno inteligenco in sorazmernimi obveznostmi za vse udeležence v vrednostni verigi bo predlog okrepil in spodbujal varstvo pravic, ki jih varuje Listina: pravico do človekovega dostojanstva (člen 1), spoštovanje zasebnega življenja in varstvo osebnih podatkov (člena 7 in 8), prepoved diskriminacije (člen 21) ter enakost žensk in moških (člen 23). Namen predloga je preprečiti hromitev pravic do svobode izražanja (člen 11) in svobode zbiranja (člen 12), zagotoviti varstvo pravice do učinkovitega pravnega sredstva in nepristranskega sodišča, pravice do obrambe in domneve nedolžnosti (člena 47 in 48) ter splošnega načela dobrega upravljanja. Poleg tega bo predlog, kot se uporablja na nekaterih področjih, pozitivno vplival na pravice številnih posebnih skupin, kot so pravice delavcev do poštenih in pravičnih delovnih pogojev (člen 31), visoka raven varstva potrošnikov (člen 28), pravice otroka (člen 24) in vključenost invalidov (člen 26). Prav tako je pomembna pravica do visoke ravni varstva okolja in izboljšanja kakovosti okolja (člen 37), tudi v zvezi z zdravjem in varnostjo ljudi. Obveznosti predhodnega testiranja, obvladovanja tveganja in človekovega nadzora bodo prav tako olajšale spoštovanje drugih temeljnih pravic z zmanjšanjem tveganja napačnih ali pristranskih odločitev, izvedenih s pomočjo umetne inteligence, na kritičnih področjih, kot so izobraževanje in usposabljanje, zaposlovanje, pomembne storitve, preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in sodstvo. Če se bodo kršitve temeljnih pravic še vedno dogajale, bodo izpostavljene osebe imele možnost učinkovitega sodnega varstva z zagotavljanjem preglednosti in sledljivosti umetnointeligenčnih sistemov skupaj z močnim naknadnim nadzorom.

Ta predlog uvaja nekatere omejitve svobode gospodarske pobude (člen 16) ter svobode umetnosti in znanosti (člen 13), da se zagotovi skladnost s prevladujočimi razlogi javnega interesa, kot so zdravje, varnost, varstvo potrošnikov in varstvo drugih temeljnih pravic („odgovorne inovacije“) pri razvoju in uporabi tehnologije umetne inteligence velikega

tveganja. Te omejitve so sorazmerne in omejene na minimum, potreben za preprečitev in zmanjševanje hudih varnostnih tveganj in verjetnih kršitev temeljnih pravic.

Povečane obveznosti glede preglednosti tudi ne bodo nesorazmerno vplivale na pravico do varstva intelektualne lastnine (člen 17(2)), saj bodo omejene le na minimalne informacije, ki jih posamezniki potrebujejo za uveljavljanje svoje pravice do učinkovitega pravnega sredstva, ter na potrebno preglednost za nadzorne in izvršilne organe v skladu z njihovimi pooblastili. Vsako razkritje informacij bo v skladu z ustrezno zakonodajo na tem področju, vključno z Direktivo (EU) 2016/943 o varstvu nerazkritega strokovnega znanja in izkušenj ter poslovnih informacij (poslovnih skrivnosti) pred njihovo protipravno pridobitvijo, uporabo in razkritjem. Kadar je treba javnim organom in priglašenim organom omogočiti dostop do zaupnih informacij ali izvorne kode, da bi preverili skladnost z bistvenimi obveznostmi, zanje veljajo zavezujoče obveznosti glede zaupnosti.

4. PRORAČUNSKE POSLEDICE

Države članice bodo morale imenovati nadzorne organe, pristojne za izvajanje zakonodajnih zahtev. Njihova nadzorna funkcija bi lahko temeljila na obstoječih ureditvah, na primer v zvezi z organi za ugotavljanje skladnosti ali nadzorom trga, vendar bi potrebovali dovolj tehnološkega znanja ter človeških in finančnih virov. Odvisno od obstoječe strukture v posamezni državi članici bi to lahko znašalo od 1 do 25 ekvivalentov polnega delovnega časa na državo članico.

Podroben pregled zadevnih stroškov je na voljo v „finančnem poročilu“, povezanem s tem predlogom.

5. DRUGI ELEMENTI

5.1. Izvedbeni načrti ter ureditve spremljanja, ocenjevanja in poročanja

Zagotavljanje robustnega mehanizma spremljanja in ocenjevanja je ključnega pomena za zagotovitev, da bo predlog učinkovit pri doseganju svojih posebnih ciljev. Komisija bo odgovorna za spremljanje učinkov predloga. Vzpostavila bo sistem za registracijo samostojne uporabe umetne inteligence velikega tveganja v javno podatkovno zbirko po vsej EU. Ta registracija bo pristojnim organom, uporabnikom in drugim zainteresiranim osebam omogočila tudi, da preverijo, ali je umetnointeligenčni sistem velikega tveganja skladen z zahtevami iz predloga, ter izvajajo okrepljen nadzor nad umetnointeligenčni sistemi, ki predstavljajo veliko tveganje za temeljne pravice. Za polnjenje te podatkovne zbirke bodo morali ponudniki umetne inteligence zagotoviti smiselne informacije o svojih sistemih in o opravljenem ugotavljanju skladnosti teh sistemov.

Poleg tega bodo morali ponudniki umetne inteligence obvestiti pristojne nacionalne organe o hudih incidentih ali okvarah, ki pomenijo kršitev obveznosti v zvezi s temeljnimi pravicami, takoj ko bodo zanje izvedeli, ter o vseh preklicih ali umikih umetnointeligenčnih sistemov s trga. Pristojni nacionalni organi bodo nato raziskali incidente ali okvare, zbrali vse potrebne informacije in jih redno pošiljali Komisiji z ustreznimi metapodatki. Komisija bo te informacije o incidentih dopolnila s celovito analizo celotnega trga za umetno inteligenco.

Komisija bo objavila poročilo o oceni in pregledu predlaganega okvira za umetno inteligenco pet let po datumu začetku njegove uporabe.

5.2. Podrobna obrazložitev konkretnih določb predloga

5.2.1. PODROČJE UPORABE IN OPREDELITEV POJMOV (NASLOV I)

Naslov I opredeljuje predmet uredbe in področje uporabe novih pravil, ki zajemajo dajanje na trg, v obratovanje in uporabo umetnointeligenčnih sistemov. Določa tudi opredelitve pojmov, ki se uporabljajo v celotnem instrumentu. Opredelitev umetnointeligenčnega sistema v pravnem okviru naj bi bila čim bolj tehnološko nevtralna in čim bolj primerna za prihodnost, ob upoštevanju hitrega tehnološkega in tržnega razvoja, povezanega z umetno inteligenco. Za zagotovitev potrebne pravne varnosti naslov I dopolnjuje Priloga I, ki vsebuje podroben seznam pristopov in tehnik za razvoj umetne inteligence, ki jih bo Komisija prilagodila v skladu z novim tehnološkim razvojem. Jasno so opredeljeni tudi ključni udeleženci v vrednostni verigi umetne inteligence, kot so ponudniki in uporabniki umetnointeligenčnih sistemov, ki zajemajo javne in zasebne operaterje, da se zagotovijo enaki konkurenčni pogoji.

5.2.2. PREPOVEDANE PRAKSE UMETNE INTELIGENCE (NASLOV II)

Naslov II določa seznam prepovedane uporabe umetne inteligence. Uredba temelji na pristopu na podlagi tveganja in razlikuje med uporabami umetne inteligence, ki ustvarjajo (i) nesprejemljivo tveganje, (ii) veliko tveganje in (iii) majhno ali minimalno tveganje. Seznam prepovedanih praks iz naslova II zajema vse tiste umetnointeligenčne sisteme, katerih uporaba se šteje za nesprejemljivo, saj so v nasprotju z vrednotami Unije, na primer s kršenjem temeljnih pravic. Prepovedi zajemajo prakse, ki imajo znaten potencial za manipulacijo oseb s subliminalnimi tehnikami, ki presegajo njihovo zavest, ali za izkoriščanje šibkih točk posebnih ranljivih skupin, kot so otroci ali invalidi, da bi materialno izkrivili njihovo vedenje na način, ki bi njim ali drugi osebi lahko povzročil psihično ali fizično škodo. Obstoječa zakonodaja o varstvu podatkov, varstvu potrošnikov in digitalnih storitvah, ki zagotavlja, da so fizične osebe ustrezno obveščene in da imajo prosto izbiro, da ne bodo predmet profiliranja ali drugih praks, ki bi lahko vplivale na njihovo vedenje, bi lahko zajela tudi druge manipulativne ali izkoriščevalske prakse, ki vplivajo na odrasle in bi jih lahko umetnointeligenčni sistemi olajšali. Predlog prepoveduje tudi družbeno točkovanje na podlagi umetne inteligence za splošne namene, ki jih izvajajo javni organi. Nazadnje je prepovedana tudi uporaba sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, razen če veljajo nekatere omejene izjeme.

5.2.3. UMETNOINTELIGENČNI SISTEMI VELIKEGA TVEGANJA (NASLOV III)

Naslov III vsebuje posebna pravila za umetnointeligenčne sisteme, ki predstavljajo veliko tveganje za zdravje in varnost ali temeljne pravice fizičnih oseb. V skladu s pristopom, ki temelji na tveganju, so navedeni umetnointeligenčni sistemi velikega tveganja dovoljeni na evropskem trgu, če izpolnjujejo nekatere obvezne zahteve in predhodno ugotavljanje skladnosti. Razvrstitev umetnointeligenčnega sistema kot sistema velikega tveganja temelji na predvidenem namenu umetnointeligenčnega sistema v skladu z veljavno zakonodajo o varnosti proizvodov. Zato razvrstitev med sisteme velikega tveganja ni odvisna le od funkcije, ki jo opravlja umetnointeligenčni sistem, ampak tudi od posebnega namena in načinov, za katere se ta sistem uporablja.

Poglavje 1 naslova III določa pravila za razvrščanje in opredeljuje dve glavni kategoriji umetnointeligenčnih sistemov velikega tveganja:

- umetnointeligenčni sistemi, namenjeni uporabi kot varnostna komponenta proizvodov, ki so predmet predhodnega ugotavljanja skladnosti s strani tretjih oseb;

- drugi samostojni umetnointeligenčni sistemi, ki vplivajo predvsem na temeljne pravice in so izrecno navedeni v Prilogi III.

Ta seznam umetnointeligenčnih sistemov velikega tveganja iz Priloge III vsebuje omejeno število umetnointeligenčnih sistemov, katerih tveganja so se že uresničila ali se bodo verjetno uresničila v bližnji prihodnosti. Da bi zagotovili, da se bo uredba lahko prilagodila nastajajočim uporabam umetne inteligence, lahko Komisija razširi seznam umetnointeligenčnih sistemov velikega tveganja, ki se uporabljajo na nekaterih vnaprej določenih področjih, in sicer z uporabo sklopa meril in metodologije za ugotavljanje tveganja.

Poglavje 2 določa pravne zahteve za umetnointeligenčne sisteme velikega tveganja v zvezi s podatki in upravljanjem podatkov, vodenjem dokumentacije in evidenc, preglednostjo in zagotavljanjem informacij uporabnikom, človekovim nadzorom, robustnostjo, točnostjo in varnostjo. Predlagane minimalne zahteve za mnoge vestne operaterje že pomenijo najsodobnejše stanje in so rezultat dveletnega pripravljalnega dela, ki izhaja iz etičnih smernic strokovne skupine na visoki ravni za umetno inteligenco[29], ki jih je pilotno izvajalo več kot 350 organizacij[30]. Prav tako so v veliki meri skladne z drugimi mednarodnimi priporočili in načeli, kar zagotavlja, da je predlagani okvir za umetno inteligenco združljiv s tistimi, ki so jih sprejeli mednarodni trgovinski partnerji EU. Natančne tehnične rešitve za doseganje skladnosti s temi zahtevami se lahko določijo s standardi ali drugimi tehničnimi specifikacijami ali pa se drugače razvijejo v skladu s splošnim inženirskim ali znanstvenim znanjem po presoji ponudnika umetnointeligenčnega sistema. Ta prožnost je še zlasti pomembna, ker ponudnikom umetnointeligenčnih sistemov omogoča, da izberejo način izpolnjevanja svojih zahtev, pri čemer upoštevajo najsodobnejše stanje ter tehnološki in znanstveni napredek na tem področju.

Poglavje 3 določa jasen sklop horizontalnih obveznosti za ponudnike umetnointeligenčnih sistemov velikega tveganja. Sorazmerne obveznosti so naložene tudi uporabnikom in drugim udeležencem v vrednostni verigi umetne inteligence (npr. uvoznikom, distributerjem, pooblaščenim zastopnikom).

Poglavje 4 določa okvir za sodelovanje priglašenih organov kot neodvisnih tretjih oseb v postopkih ugotavljanja skladnosti, poglavje 5 pa podrobno pojasnjuje postopke ugotavljanja skladnosti, ki jih je treba upoštevati za vsako vrsto umetnointeligenčnega sistema velikega tveganja. Cilj pristopa za ugotavljanje skladnosti je čim bolj zmanjšati breme za gospodarske subjekte in tudi priglašene organe, katerih zmogljivosti je treba sčasoma postopoma povečati. Za umetnointeligenčne sisteme, namenjene uporabi kot varnostne komponente proizvodov, ki jih ureja zakonodaja novega zakonodajnega okvira (npr. stroji, igrače, medicinski pripomočki), bodo veljali enaki predhodni in naknadni mehanizmi skladnosti in izvrševanja za proizvode, katerih komponente so. Ključna razlika je v tem, da bodo predhodni in naknadni mehanizmi zagotovili skladnost ne le z zahtevami sektorske zakonodaje, ampak tudi z zahtevami iz te uredbe.

Kar zadeva samostojne umetnointeligenčne sisteme velikega tveganja iz Priloge III, bo vzpostavljen nov sistem skladnosti in izvrševanja. To sledi modelu zakonodaje novega zakonodajnega okvira, ki se izvaja s preverjanji notranje kontrole s strani ponudnikov, razen sistemov za biometrično identifikacijo na daljavo, za katere bi veljalo ugotavljanje skladnosti s strani tretjih oseb. Celovito predhodno ugotavljanje skladnosti z notranjimi pregledi v

[29] Strokovna skupina na visoki ravni za umetno inteligenco, *Ethics Guidelines for Trustworthy AI* (Etične smernice za zaupanja vredno umetno inteligenco), 2019.

[30] Podprla jih je tudi Komisija v svojem sporočilu iz leta 2019 o humanocentričnem pristopu k umetni inteligenci.

kombinaciji s strogim naknadnim izvrševanjem bi lahko bila učinkovita in razumna rešitev za te sisteme glede na zgodnjo fazo regulativnega posega in dejstvo, da je sektor umetne inteligence zelo inovativen, strokovno znanje za revizijo pa se šele zbira. Ocena z notranjimi pregledi za „samostojne“ umetnointeligenčne sisteme velikega tveganja bi zahtevala popolno, učinkovito in ustrezno dokumentirano predhodno skladnost z vsemi zahtevami uredbe ter skladnost z robustnimi sistemi kakovosti in obvladovanja tveganja ter spremljanja po dajanju na trg. Ko ponudnik opravi ustrezno ugotavljanje skladnosti, bi moral te samostojne umetnointeligenčne sisteme velikega tveganja registrirati v podatkovni zbirki EU, ki jo bo upravljala Komisija, da bi povečala javno preglednost in nadzor ter okrepila naknadni nadzor s strani pristojnih organov. Zaradi skladnosti z obstoječo zakonodajo o varnosti proizvodov pa bo ugotavljanje skladnosti umetnointeligenčnih sistemov, ki so varnostne komponente proizvodov, potekalo po sistemu s postopki ugotavljanja skladnosti s strani tretjih oseb, ki so že vzpostavljeni v skladu z ustrezno sektorsko zakonodajo o varnosti proizvodov. V primeru bistvenih sprememb umetnointeligenčnih sistemov (in zlasti sprememb, ki presegajo tisto, kar je ponudnik vnaprej določil v svoji tehnični dokumentaciji in kar je bilo preverjeno ob predhodnem ugotavljanju skladnosti) bodo potrebna nova predhodna ponovna ugotavljanja skladnosti.

5.2.4. OBVEZNOSTI GLEDE PREGLEDNOSTI ZA NEKATERE UMETNOINTELIGENČNE SISTEME (NASLOV IV)

Naslov IV se nanaša na nekatere umetnointeligenčne sisteme, da se upoštevajo posebna tveganja manipulacije, ki jih predstavljajo. Obveznosti glede preglednosti bodo veljale za sisteme, ki (i) imajo stik z ljudmi, (ii) se uporabljajo za zaznavanje čustev ali določanje pripadnosti (družbenim) kategorijam na podlagi biometričnih podatkov ali (iii) ustvarjajo ali manipulirajo z vsebino („globoki ponaredki“). Kadar so osebe v stiku s sistemom umetne inteligence ali se njihova čustva ali značilnosti prepoznavajo z avtomatiziranimi sredstvi, jih je treba o tem obvestiti. Če se umetnointeligenčni sistem uporablja za ustvarjanje ali manipulacijo slikovne, zvočne ali videovsebine, ki je v znatni meri podobna verodostojni vsebini, bi morala obstajati obveznost razkritja, da je vsebina ustvarjena z avtomatiziranimi sredstvi, ob upoštevanju izjem za zakonite namene (preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, svoboda izražanja). To osebam omogoča, da sprejemajo informirane odločitve ali se umaknejo iz določene situacije.

5.2.5. UKREPI V PODPORO INOVACIJAM (NASLOV V)

Naslov V prispeva k cilju oblikovanja pravnega okvira, ki je inovacijam prijazen, primeren za prihodnost in odporen na motnje. V ta namen spodbuja pristojne nacionalne organe, da vzpostavijo regulativne peskovnike, ter določa osnovni okvir v smislu upravljanja, nadzora in odgovornosti. Regulativni peskovniki za umetno inteligenco vzpostavljajo nadzorovano okolje za testiranje inovativnih tehnologij za omejen čas na podlagi načrta testiranja, dogovorjenega s pristojnimi organi. Naslov V vsebuje tudi ukrepe za zmanjšanje regulativnega bremena za MSP in zagonska podjetja.

5.2.6. UPRAVLJANJE IN IZVAJANJE (NASLOVI VI, VII IN VIII)

Naslov VI določa sisteme upravljanja na ravni Unije in nacionalni ravni. Na ravni Unije se s predlogom ustanavlja Evropski odbor za umetno inteligenco (v nadaljnjem besedilu: odbor), ki ga sestavljajo predstavniki držav članic in Komisije. Odbor bo olajšal nemoteno, učinkovito in harmonizirano izvajanje te uredbe s prispevanjem k učinkovitemu sodelovanju nacionalnih nadzornih organov in Komisije ter z zagotavljanjem svetovanja in strokovnega znanja Komisiji. Prav tako bo zbiral in izmenjeval najboljše prakse med državami članicami.

Države članice bodo morale na nacionalni ravni imenovati enega ali več pristojnih nacionalnih organov ter med njimi nacionalni nadzorni organ za nadzor uporabe in izvajanja uredbe. Evropski nadzornik za varstvo podatkov bo deloval kot pristojni organ za nadzor institucij, agencij in organov Unije, kadar spadajo na področje uporabe te uredbe.

Namen **naslova VII** je olajšati spremljanje dela Komisije in nacionalnih organov z vzpostavitvijo podatkovne zbirke na ravni EU za samostojne umetnointeligenčne sisteme velikega tveganja, ki vplivajo predvsem na temeljne pravice. Podatkovno zbirko bo upravljala Komisija, podatke pa bodo zagotovili ponudniki umetnointeligenčnih sistemov, ki bodo morali svoje sisteme registrirati, preden jih dajo na trg ali kako drugače v uporabo.

Naslov VIII določa obveznosti spremljanja in poročanja za ponudnike umetnointeligenčnih sistemov v zvezi s spremljanjem po dajanju na trg in poročanjem ter preiskovanjem incidentov in okvar v zvezi z umetno inteligenco. Organi za nadzor trga bi prav tako nadzorovali trg ter preverjali skladnost z obveznostmi in zahtevami za vse umetnointeligenčne sisteme velikega tveganja, ki so že dani na trg. Organi za nadzor trga bi imeli vsa pooblastila iz Uredbe (EU) 2019/1020 o nadzoru trga. Naknadno izvrševanje bi moralo zagotoviti, da imajo javni organi po dajanju umetnointeligenčnega sistema na trg pooblastila in sredstva za posredovanje, če umetnointeligenčni sistemi povzročijo nepričakovana tveganja, ki zahtevajo hitro ukrepanje. Prav tako bodo spremljali, ali operaterji izpolnjujejo ustrezne obveznosti iz uredbe. Predlog ne predvideva samodejne ustanovitve dodatnih teles ali organov na ravni držav članic. Države članice lahko zato imenujejo obstoječe sektorske organe (in uporabijo njihovo strokovno znanje), ki bi bili pooblaščeni tudi za spremljanje in izvrševanje določb uredbe.

Vse to ne posega v obstoječi sistem in dodelitev pristojnosti za naknadno izvrševanje obveznosti v zvezi s temeljnimi pravicami v državah članicah. Kadar je to potrebno za njihove naloge, bodo obstoječi nadzorni in izvršilni organi imeli tudi pooblastila, da po potrebi zahtevajo dokumentacijo, ki se hrani v skladu s to uredbo, in dostopajo do nje ter po potrebi od organov za nadzor trga zahtevajo, da s tehničnimi sredstvi organizirajo testiranje umetnointeligenčnega sistema velikega tveganja.

5.2.7. KODEKSI RAVNANJA (NASLOV IX)

Naslov IX vzpostavlja okvir za oblikovanje kodeksov ravnanja, katerih cilj je spodbuditi ponudnike umetnointeligenčnih sistemov, ki ne predstavljajo velikega tveganja, k prostovoljni uporabi obveznih zahtev za umetnointeligenčne sisteme velikega tveganja (kot je določeno v naslovu III). Ponudniki umetnointeligenčnih sistemov, ki ne predstavljajo velikega tveganja, lahko sami oblikujejo in izvajajo kodekse ravnanja. Ti kodeksi lahko vključujejo tudi prostovoljne zaveze, povezane na primer z okoljsko trajnostjo, dostopnostjo za invalide, sodelovanjem deležnikov pri snovanju in razvoju umetnointeligenčnih sistemov ter raznolikostjo razvojnih skupin.

5.2.8. KONČNE DOLOČBE (NASLOVI X, XI IN XII)

Naslov X poudarja obveznost vseh strani, da spoštujejo zaupnost informacij in podatkov, ter določa pravila za izmenjavo informacij, pridobljenih med izvajanjem uredbe. Naslov X vključuje tudi ukrepe za zagotovitev učinkovitega izvajanja uredbe z učinkovitimi, sorazmernimi in odvračilnimi kaznimi za kršitve določb.

Naslov XI določa pravila za izvajanje delegiranih in izvedbenih pooblastil. Predlog pooblašča Komisijo, da po potrebi sprejme izvedbene akte za zagotovitev enotne uporabe uredbe ali delegiranih aktov za posodobitev ali dopolnitev seznamov iz prilog I do VII.

Naslov XII vsebuje obveznost Komisije, da redno ocenjuje potrebo po posodobitvi Priloge III ter pripravlja redna poročila o oceni in pregledu uredbe. Določa tudi končne določbe,

vključno z diferenciranim prehodnim obdobjem za začetni datum uporabe uredbe, da se olajša nemoteno izvajanje za vse zadevne strani.

2021/0106 (COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

O DOLOČITVI HARMONIZIRANIH PRAVIL O UMETNI INTELIGENCI (AKT O UMETNI INTELIGENCI) IN SPREMEMBI NEKATERIH ZAKONODAJNIH AKTOV UNIJE

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije ter zlasti členov 16 in 114 Pogodbe,

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora[31],

ob upoštevanju mnenja Odbora regij[32],

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

(1) Namen te uredbe je izboljšati delovanje notranjega trga z določitvijo enotnega pravnega okvira, zlasti za razvoj, trženje in uporabo umetne inteligence v skladu z vrednotami Unije. Ta uredba uresničuje številne nujne razloge javnega interesa, kot so visoka raven varovanja zdravja, varnosti in temeljnih pravic, ter zagotavlja prosti čezmejni pretok blaga in storitev, ki temeljijo na umetni inteligenci, s čimer državam članicam preprečuje, da bi uvedle omejitve za razvoj, trženje in uporabo umetnointeligenčnih sistemov, razen če je to izrecno dovoljeno s to uredbo.

(2) Umetnointeligenčne sisteme je mogoče zlahka uporabljati v več gospodarskih in družbenih sektorjih, tudi čezmejno, in lahko krožijo po vsej Uniji. Nekatere države članice so že preučile možnost sprejetja nacionalnih predpisov, s katerimi bi zagotovile, da je umetna inteligenca varna ter da se razvija in uporablja v skladu z obveznostmi glede temeljnih pravic. Različna nacionalna pravila lahko povzročijo razdrobljenost notranjega trga in zmanjšajo pravno varnost za operaterje, ki razvijajo ali uporabljajo umetnointeligenčne sisteme. Zato bi bilo treba zagotoviti dosledno in visoko raven varstva po vsej Uniji, hkrati pa preprečiti razlike, ki ovirajo prost pretok umetnointeligenčnih sistemov ter z njimi povezanih proizvodov in storitev na notranjem trgu, in sicer z določitvijo enotnih obveznosti za operaterje ter zagotovitvijo enotnega varstva prevladujočih razlogov javnega interesa in pravic oseb na notranjem trgu na podlagi člena 114 Pogodbe o delovanju Evropske unije (v nadaljnjem besedilu: PDEU). Ker ta uredba vsebuje nekatera posebna pravila o varstvu posameznikov pri obdelavi osebnih podatkov v zvezi z omejitvami uporabe umetnointeligenčnih sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, je

[31] UL C […], […], str. […].
[32] UL C […], […], str. […].

primerno, da se ta uredba, kar zadeva navedena posebna pravila, opira na člen 16 PDEU. Glede na ta posebna pravila in uporabo člena 16 PDEU se je primerno posvetovati z Evropskim odborom za varstvo podatkov.

(3) Umetna inteligenca je hitro razvijajoča se skupina tehnologij, ki lahko prispevajo k številnim gospodarskim in družbenim koristim v celotnem spektru panog in družbenih dejavnosti. Uporaba umetne inteligence lahko z izboljšanjem napovedi, optimizacijo delovanja in dodeljevanja virov ter po meri prilagojenimi digitalnimi rešitvami, ki so na voljo za posameznike in organizacije, zagotavlja ključne konkurenčne prednosti za podjetja ter podpira družbeno in okoljsko koristne rezultate, na primer na področju zdravstvenega varstva, kmetijstva, izobraževanja in usposabljanja, upravljanja infrastrukture, energije, prometa in logistike, javnih storitev, varnosti, pravosodja, učinkovite rabe virov in energije ter ublažitve podnebnih sprememb in prilagajanja nanje.

(4) Hkrati lahko umetna inteligenca glede na okoliščine v zvezi z njenim posebnim namenom uporabe povzroča tveganja ter škoduje javnim interesom in pravicam, ki jih varuje pravo Unije. Ta škoda je lahko materialna ali nematerialna.

(5) Zato je potreben pravni okvir Unije, ki bo določal harmonizirana pravila o umetni inteligenci, da bi spodbudil razvoj, uporabo in uvajanje umetne inteligence na notranjem trgu, ki bo hkrati zagotavljal visoko raven zaščite javnih interesov, kot so zdravje in varnost ter varstvo temeljnih pravic, kot jih priznava in varuje pravo Unije. Za dosego tega cilja bi bilo treba določiti pravila, ki urejajo dajanje na trg in v uporabo nekaterih umetnointeligenčnih sistemov, s čimer bi zagotovili nemoteno delovanje notranjega trga in omogočili, da ti sistemi izkoristijo načelo prostega pretoka blaga in storitev. Z določitvijo teh pravil ta uredba podpira cilj, da Unija postane vodilna v svetu pri razvoju varne, zaupanja vredne in etične umetne inteligence, kot je navedel Evropski svet[33], ter zagotavlja zaščito etičnih načel, kot je izrecno zahteval Evropski parlament[34].

(6) Pojem umetnointeligenčnega sistema bi moral biti jasno opredeljen, da se zagotovita pravna varnost in hkrati prožnost, ki bo omogočala prilagajanje prihodnjemu tehnološkemu razvoju. Opredelitev bi morala temeljiti na ključnih funkcionalnih značilnostih programske opreme, zlasti na zmožnosti, da za določen sklop ciljev, ki jih opredeli človek, ustvarja izhodne podatke, kot so vsebine, napovedi, priporočila ali odločitve, ki vplivajo na okolje, s katerim je sistem v interakciji, bodisi v fizični bodisi v digitalni razsežnosti. Umetnointeligenčni sistemi so lahko zasnovani tako, da delujejo z različnimi stopnjami avtonomije in se uporabljajo samostojno ali kot komponenta proizvoda, ne glede na to, ali je sistem fizično integriran v proizvod (vgrajen) ali služi funkcionalnosti proizvoda, ne da bi bil vanj integriran (nevgrajen). Opredelitev umetnointeligenčnega sistema bi bilo treba dopolniti s seznamom posebnih tehnik in pristopov, ki se uporabljajo za njegov razvoj, ta seznam pa bi bilo treba posodabljati glede na tržni in tehnološki razvoj, tako da Komisija sprejme delegirane akte za spremembo tega seznama.

(7) Pojem biometričnih podatkov, uporabljen v tej uredbi, je skladen s pojmom biometričnih podatkov, kot je opredeljen v členu 4(14) Uredbe (EU) 2016/679

---

33 Evropski svet, izredno zasedanje Evropskega sveta (1. in 2. oktobra 2020) – sklepi, EUCO 13/20, 2020, str. 6.

34 Resolucija Evropskega parlamenta z dne 20. oktobra 2020 s priporočili Komisiji o okviru etičnih vidikov umetne inteligence, robotike in sorodnih tehnologij, 2020/2012(INL).

Evropskega parlamenta in Sveta[35], členu 3(18) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta[36] ter členu 3(13) Direktive (EU) 2016/680 Evropskega parlamenta in Sveta[37], ter bi ga bilo treba razlagati dosledno.

(8) Pojem sistema za biometrično identifikacijo na daljavo, kot se uporablja v tej uredbi, bi bilo treba opredeliti funkcionalno kot umetnointeligenčni sistem, namenjen identifikaciji fizičnih oseb na daljavo s primerjavo biometričnih podatkov osebe z biometričnimi podatki iz referenčne podatkovne zbirke in ne da bi bilo vnaprej znano, ali bo ciljna oseba prisotna in ali jo bo mogoče identificirati, ne glede na uporabljeno tehnologijo, procese ali vrste biometričnih podatkov. Glede na različne značilnosti in načine uporabe ter različna tveganja je treba razlikovati med sistemi za biometrično identifikacijo na daljavo v realnem času in sistemi za naknadno biometrično identifikacijo na daljavo. Pri sistemih „v realnem času“ se zajemanje biometričnih podatkov, primerjava in identifikacija izvedejo takoj, skoraj trenutno ali v vsakem primeru brez večje zamude. V zvezi s tem ne bi smelo biti prostora za izogibanje pravilom te uredbe o uporabi zadevnih umetnointeligenčnih sistemov v realnem času s tem, da bi poskrbeli za manjše zamude. Sistemi „v realnem času“ vključujejo uporabo gradiva „v živo“ ali „skoraj v živo“, kot je videoposnetek, ki ga ustvari kamera ali druga naprava s podobno funkcionalnostjo. Pri „naknadnih“ sistemih so bili biometrični podatki že zajeti, primerjava in identifikacija pa se izvedeta šele po daljšem času. To vključuje gradivo, kot so slike ali videoposnetki, ki jih ustvarjajo kamere televizije zaprtega kroga ali zasebne naprave, ki je bilo ustvarjeno pred uporabo sistema v zvezi z zadevnimi fizičnimi osebami.

(9) V tej uredbi je treba pojem javno dostopnega prostora razumeti tako, da se nanaša na vsak fizični prostor, dostopen javnosti, ne glede na to, ali je ta prostor v zasebni ali javni lasti. Zato pojem ne zajema prostorov, ki so zasebne narave in običajno niso prosto dostopni tretjim osebam, vključno z organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, razen če so bile te osebe posebej povabljene ali pooblaščene, kot so domovi, zasebni klubi, pisarne, skladišča in tovarne. Spletni prostori prav tako niso zajeti, saj niso fizični prostori. Vendar pa zgolj dejstvo, da lahko za dostop do določenega prostora veljajo določeni pogoji, kot so vstopnice ali starostne omejitve, ne pomeni, da prostor ni javno dostopen v smislu te uredbe. Zato so poleg javnih prostorov, kot so ulice, ustrezni deli vladnih stavb in večina prometne infrastrukture, običajno javno dostopni tudi prostori, kot so kinodvorane, gledališča, trgovine in nakupovalna središča. Vendar je za vsak primer posebej treba ugotoviti, ali je določen prostor dostopen javnosti, ob upoštevanju posebnosti posamezne situacije.

(10) Za zagotovitev enakih konkurenčnih pogojev ter učinkovitega varstva pravic in svoboščin posameznikov po vsej Uniji bi se morala pravila iz te uredbe uporabljati za

---

35 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).

36 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 razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

37 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 (direktiva o kazenskem pregonu) (UL L 119, 4.5.2016, str. 89).

ponudnike umetnointeligenčnih sistemov na nediskriminatoren način, ne glede na to, ali imajo sedež v Uniji ali v tretji državi, in za uporabnike umetnointeligenčnih sistemov s sedežem v Uniji.

(11) Zaradi svoje digitalne narave bi morali nekateri umetnointeligenčni sistemi spadati na področje uporabe te uredbe, tudi če niso dani na trg, v obratovanje ali uporabo v Uniji. To velja na primer za operaterja s sedežem v Uniji, ki določene storitve naroča pri operaterju s sedežem zunaj Unije v zvezi z dejavnostjo, ki jo bo izvajal umetnointeligenčni sistem, ki bi bil opredeljen kot sistem velikega tveganja in katerega učinki vplivajo na fizične osebe s sedežem v Uniji. V teh okoliščinah bi lahko umetnointeligenčni sistem, ki ga uporablja operater zunaj Unije, obdeloval podatke, ki se zakonito zbirajo v Uniji in prenašajo iz nje, ter naročniku v Uniji zagotovil izhodne podatke navedenega umetnointeligenčnega sistema, ki izhajajo iz te obdelave, ne da bi bil ta umetnointeligenčni sistem dan na trg, v obratovanje ali uporabo v Uniji. Da bi preprečili izogibanje določbam te uredbe in zagotovili učinkovito varstvo fizičnih oseb v Uniji, bi se morala ta uredba uporabljati tudi za ponudnike in uporabnike umetnointeligenčnih sistemov s sedežem v tretji državi, če se izhodni podatki, ki jih ti sistemi ustvarijo, uporabljajo v Uniji. Kljub temu se zaradi upoštevanja obstoječih ureditev in posebnih potreb po sodelovanju s tujimi partnerji, s katerimi se izmenjujejo informacije in dokazi, ta uredba ne bi smela uporabljati za javne organe tretje države in mednarodne organizacije, kadar delujejo v okviru mednarodnih sporazumov, sklenjenih na nacionalni ali evropski ravni za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter pravosodja z Unijo ali njenimi državami članicami. Taki sporazumi so bili sklenjeni dvostransko med državami članicami in tretjimi državami ali med Evropsko unijo, Europolom in drugimi agencijami EU ter tretjimi državami in mednarodnimi organizacijami.

(12) Ta uredba bi se morala uporabljati tudi za institucije, urade, organe in agencije Unije, kadar delujejo kot ponudniki ali uporabniki umetnointeligenčnega sistema. Umetnointeligenčne sisteme, ki se razvijajo ali uporabljajo izključno v vojaške namene, bi bilo treba izključiti iz področja uporabe te uredbe, če ta uporaba spada v izključno pristojnost skupne zunanje in varnostne politike, ki jo ureja naslov V Pogodbe o Evropski uniji (v nadaljnjem besedilu: PEU). Ta uredba ne bi smela posegati v določbe o odgovornosti posrednih ponudnikov storitev iz Direktive 2000/31/ES Evropskega parlamenta in Sveta [kakor je bila spremenjena z aktom o digitalnih storitvah].

(13) Da bi zagotovili dosledno in visoko raven zaščite javnih interesov v zvezi z zdravjem, varnostjo in temeljnimi pravicami, bi bilo treba določiti skupne normativne standarde za vse umetnointeligenčne sisteme velikega tveganja. Ti standardi bi morali biti skladni z Listino Evropske unije o temeljnih pravicah (v nadaljnjem besedilu: Listina) ter nediskriminatorni in v skladu z mednarodnimi trgovinskimi zavezami Unije.

(14) Za uvedbo sorazmernega in učinkovitega sklopa zavezujočih pravil za umetnointeligenčne sisteme bi bilo treba uporabiti jasno opredeljen pristop, ki temelji na tveganju. Ta pristop bi moral vrsto in vsebino takih pravil prilagoditi intenzivnosti in obsegu tveganj, ki jih lahko ustvarijo umetnointeligenčni sistemi. Zato je treba prepovedati nekatere prakse umetne inteligence, določiti zahteve za umetnointeligenčne sisteme velikega tveganja in obveznosti za zadevne operaterje ter določiti obveznosti glede preglednosti za nekatere umetnointeligenčne sisteme.

(15) Poleg številnih koristnih uporab umetne inteligence je mogoče to tehnologijo tudi zlorabiti, tako da bi nastala nova in močna orodja za prakse manipulacije, izkoriščanja

in družbenega nadzora. Take prakse so še posebej škodljive in bi jih bilo treba prepovedati, ker so v nasprotju z vrednotami Unije glede spoštovanja človekovega dostojanstva, svobode, enakosti, demokracije in pravne države ter temeljnimi pravicami Unije, vključno s pravico do nediskriminacije, varstva podatkov in zasebnosti ter pravicami otroka.

(16) Prepovedati bi bilo treba dajanje na trg, v obratovanje ali uporabo nekaterih umetnointeligenčnih sistemov, namenjenih izkrivljanju človekovega vedenja, pri katerem obstaja verjetnost pojava fizične ali psihične škode. Taki umetnointeligenčni sistemi uporabljajo subliminalne komponente, ki jih posamezniki ne morejo zaznati, ali izkoriščajo šibke točke otrok in ljudi zaradi njihove starosti, telesne ali duševne nezmožnosti. To počnejo z namenom, da bi bistveno izkrivili vedenje osebe, in na način, ki tej ali drugi osebi povzroči ali bi ji lahko povzročil škodo. Namena ni mogoče predpostavljati, če je izkrivljanje človekovega vedenja posledica dejavnikov zunaj umetnointeligenčnega sistema in na katere ponudnik ali uporabnik ne more vplivati. Prepoved ne bi smela ovirati raziskav za zakonite namene v zvezi s takimi umetnointeligenčnimi sistemi, če take raziskave ne pomenijo uporabe umetnointeligenčnega sistema v odnosih med človekom in strojem, ki bi fizične osebe izpostavila škodi, ter če se take raziskave izvajajo v skladu s priznanimi etičnimi standardi za znanstvene raziskave.

(17) Umetnointeligenčni sistemi, ki zagotavljajo družbeno točkovanje fizičnih oseb za splošne namene s strani javnih organov ali v njihovem imenu, lahko vodijo do diskriminatornih rezultatov in izključitve nekaterih skupin. Lahko kršijo pravico do dostojanstva in nediskriminacije ter vrednote enakosti in pravičnosti. Taki umetnointeligenčni sistemi ocenjujejo ali razvrščajo zanesljivost fizičnih oseb na podlagi njihovega družbenega vedenja v več kontekstih ali znanih ali predvidenih osebnih ali osebnostnih značilnostih. Število družbenih točk, pridobljenih s takimi umetnointeligenčni sistemi, lahko vodi do škodljivega ali neugodnega obravnavanja fizičnih oseb ali njihovih celotnih skupin v družbenih kontekstih, ki niso povezani s kontekstom, v katerem so bili podatki prvotno ustvarjeni ali zbrani, ali do škodljivega obravnavanja, ki je nesorazmerno ali neupravičeno glede na resnost njihovega družbenega vedenja. Take umetnointeligenčne sisteme bi bilo zato treba prepovedati.

(18) Uporaba umetnointeligenčnih sistemov za biometrično identifikacijo fizičnih oseb na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj velja za posebno hudo poseganje v pravice in svoboščine zadevnih oseb, če lahko vpliva na zasebno življenje velikega dela prebivalstva, vzbuja občutek stalnega nadzora ter posredno odvrača od uresničevanja svobode zbiranja in drugih temeljnih pravic. Poleg tega se zaradi takojšnjega učinka in omejenih možnosti za nadaljnja preverjanja ali popravke v zvezi z uporabo takih sistemov, ki delujejo v „realnem času“, povečujejo tveganja za pravice in svoboščine oseb, ki jih zadevajo dejavnosti preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.

(19) Zato bi bilo treba prepovedati uporabo teh sistemov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, razen v treh izčrpno naštetih in ozko opredeljenih primerih, ko je uporaba nujno potrebna za dosego pomembnega javnega interesa, katerega pomen prevlada nad tveganji. V teh primerih gre za iskanje morebitnih žrtev kaznivih dejanj, vključno s pogrešanimi otroki; nekatere nevarnosti za življenje ali fizično varnost oseb ali varnost pred terorističnim napadom ter

odkrivanje, lokalizacijo, identifikacijo ali pregon storilcev ali osumljencev kaznivih dejanj iz Okvirnega sklepa Sveta 2002/584/PNZ[38], če se ta kazniva dejanja v zadevni državi članici kaznujejo z zaporno kaznijo ali ukrepom, vezanim na odvzem prostosti najmanj treh let, in so opredeljena v zakonodaji te države članice. Tak prag za zaporno kazen ali ukrep, vezan na odvzem prostosti, v skladu z nacionalnim pravom prispeva k zagotavljanju, da je kaznivo dejanje dovolj hudo, da bi lahko upravičilo uporabo sistemov za biometrično identifikacijo na daljavo v realnem času. Poleg tega bodo nekatera od 32 kaznivih dejanj, navedenih v Okvirnem sklepu Sveta 2002/584/PNZ, v praksi verjetno pomembnejša od drugih, saj bo uporaba biometrične identifikacije na daljavo v realnem času predvidoma potrebna in sorazmerna v zelo različnem obsegu za praktično odkrivanje, lokalizacijo, identifikacijo ali pregon storilca ali osumljenca različnih navedenih kaznivih dejanj ter ob upoštevanju verjetnih razlik v resnosti, verjetnosti in obsegu škode ali možnih negativnih posledic.

(20) Za zagotovitev odgovorne in sorazmerne uporabe teh sistemov je pomembno tudi določiti, da bi bilo treba v vsakem od teh treh izčrpno naštetih in ozko opredeljenih primerov upoštevati nekatere elemente, zlasti glede narave razmer, zaradi katerih je bila zahteva vložena, ter posledic uporabe za pravice in svoboščine vseh zadevnih oseb ter zaščitnih ukrepov in pogojev, predvidenih z uporabo. Poleg tega bi bilo treba za uporabo sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj določiti ustrezne časovne in prostorske omejitve, zlasti ob upoštevanju dokazov ali znamenj glede groženj, žrtev ali storilca. Referenčna podatkovna zbirka o osebah bi morala biti primerna za vsak primer uporabe v vsakem od treh zgoraj navedenih primerov.

(21) Za vsako uporabo sistema za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj bi bilo treba pridobiti izrecno in posebno dovoljenje pravosodnega organa ali neodvisnega upravnega organa države članice. Tako dovoljenje bi bilo treba načeloma pridobiti pred uporabo, razen v ustrezno utemeljenih nujnih primerih, tj. primerih, ko je potreba po uporabi zadevnih sistemov taka, da je dejansko in objektivno nemogoče pridobiti dovoljenje pred začetkom uporabe. V takih nujnih primerih bi bilo treba uporabo omejiti na absolutni minimum, zanjo pa bi morali veljati ustrezni zaščitni ukrepi in pogoji, kot jih določa nacionalno pravo ter kot jih v okviru vsakega posameznega primera nujne uporabe določi organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Poleg tega bi si moral organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v takih primerih prizadevati za čimprejšnjo pridobitev dovoljenja in hkrati podati razloge, zakaj ga ni mogel zahtevati prej.

(22) Poleg tega je v izčrpnem okviru, določenem s to uredbo, primerno določiti, da bi morala biti taka uporaba na ozemlju države članice v skladu s to uredbo mogoča le, kadar in v kolikor se je zadevna država članica odločila izrecno predvideti možnost odobritve take uporabe v svojih podrobnih pravilih nacionalnega prava. Zato imajo države članice v skladu s to uredbo še naprej možnost, da take možnosti sploh ne predvidijo ali da jo predvidijo le za nekatere cilje, ki lahko upravičijo dovoljeno uporabo, opredeljeno v tej uredbi.

---

[38] Okvirni sklep Sveta 2002/584/PNZ z dne 13. junija 2002 o evropskem nalogu za prijetje in postopkih predaje med državami članicami (UL L 190, 18.7.2002, str. 1).

(23) Uporaba umetnointeligenčnih sistemov za biometrično identifikacijo fizičnih oseb na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj nujno vključuje obdelavo biometričnih podatkov. Pravila te uredbe, ki ob upoštevanju nekaterih izjem prepovedujejo tako uporabo, ki temelji na členu 16 PDEU, bi se morala uporabljati kot *lex specialis* v zvezi s pravili o obdelavi biometričnih podatkov iz člena 10 Direktive (EU) 2016/680, tako da bi izčrpno urejala tako uporabo in obdelavo zadevnih biometričnih podatkov. Zato bi morali biti taki uporaba in obdelava mogoči le, če sta združljivi z okvirom iz te uredbe, ne da bi zunaj tega okvira obstajalo področje uporabe za pristojne organe, kadar delujejo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, za uporabo takih sistemov in obdelavo takih podatkov v zvezi z njimi na podlagi razlogov iz člena 10 Direktive (EU) 2016/680. V tem smislu ta uredba ni namenjena zagotavljanju pravne podlage za obdelavo osebnih podatkov v skladu s členom 8 Direktive (EU) 2016/680. Vendar uporaba sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene, ki niso preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, tudi s strani pristojnih organov, ne bi smela biti zajeta v posebni okvir v zvezi s tako uporabo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, določene s to uredbo. Za tako uporabo za namene, ki niso preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, zato ne bi smela veljati zahteva po dovoljenju v skladu s to uredbo in veljavnimi podrobnimi pravili nacionalnega prava, ki jo lahko uveljavljajo.

(24) Pri vsaki obdelavi biometričnih podatkov in drugih osebnih podatkov, povezanih z uporabo umetnointeligenčnih sistemov za biometrično identifikacijo, razen v povezavi z uporabo sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, kot jo ureja ta uredba, tudi kadar te sisteme uporabljajo pristojni organi v javno dostopnih prostorih za druge namene kot za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, bi morale biti še naprej izpolnjene vse zahteve, ki izhajajo iz člena 9(1) Uredbe (EU) 2016/679, člena 10(1) Uredbe (EU) 2018/1725 in člena 10 Direktive (EU) 2016/680, kot je ustrezno.

(25) V skladu s členom 6a Protokola št. 21 o stališču Združenega kraljestva in Irske v zvezi z območjem svobode, varnosti in pravice, ki je priložen k PEU in k PDEU, pravila iz člena 5(1), točke (d), (2) in (3) te uredbe, sprejeta na podlagi člena 16 PDEU, ki se nanašajo na obdelavo osebnih podatkov s strani držav članic, kadar izvajajo dejavnosti, ki spadajo na področje uporabe poglavja 4 ali 5 naslova V tretjega dela PDEU, za Irsko niso zavezujoča, če je ne zavezujejo pravila, ki urejajo oblike pravosodnega sodelovanja v kazenskih zadevah ali policijskega sodelovanja, v okviru katerih je treba upoštevati določbe predpisov, sprejetih na podlagi člena 16 PDEU.

(26) V skladu s členoma 2 in 2a Protokola št. 22 o stališču Danske, ki je priložen PEU in PDEU, Danske ne zavezujejo in se zanjo ne uporabljajo pravila, ki so določena v členu 5(1), točki (d), (2) in (3) te uredbe, sprejeta na podlagi člena 16 PDEU in se nanašajo na obdelavo osebnih podatkov s strani držav članic, kadar izvajajo dejavnosti, ki spadajo na področje uporabe poglavja 4 ali 5 naslova V tretjega dela PDEU.

(27) Umetnointeligenčne sisteme velikega tveganja bi bilo treba dati na trg Unije ali v uporabo le, če izpolnjujejo nekatere obvezne zahteve. Navedene zahteve bi morale zagotoviti, da umetnointeligenčni sistemi velikega tveganja, ki so na voljo v Uniji ali katerih izhodni podatki se drugače uporabljajo v Uniji, ne predstavljajo nesprejemljivega tveganja za pomembne javne interese Unije, kot jih priznava in

varuje pravo Unije. Umetnointeligenčni sistemi, določeni za sisteme velikega tveganja, bi morali biti omejeni na tiste, ki imajo znaten škodljiv vpliv na zdravje, varnost in temeljne pravice oseb v Uniji, taka omejitev pa bi morala čim bolj zmanjšati morebitno omejevanje mednarodne trgovine.

(28) Umetnointeligenčni sistemi bi lahko imeli škodljiv učinek na zdravje in varnost ljudi, zlasti kadar taki sistemi delujejo kot komponente proizvodov. V skladu s cilji harmonizacijske zakonodaje Unije, da se olajša prosti pretok proizvodov na notranjem trgu ter zagotovi, da na trg pridejo le varni in skladni proizvodi, je pomembno, da se ustrezno preprečijo in zmanjšajo varnostna tveganja, ki jih lahko povzroči proizvod kot celota zaradi svojih digitalnih komponent, vključno z umetnointeligenčnimi sistemi. Na primer vse bolj avtonomni roboti, ki se uporabljajo v proizvodnji ali za osebno pomoč in oskrbo, bi morali biti sposobni varno delovati in opravljati svoje funkcije v zapletenih okoljih. Podobno bi morali biti v zdravstvenem sektorju, v katerem je tveganje za življenje in zdravje še posebej veliko, vse bolj izpopolnjeni diagnostični sistemi in sistemi, ki podpirajo človeške odločitve, zanesljivi in točni. Pri razvrstitvi umetnointeligenčnega sistema kot sistema velikega tveganja je zlasti pomemben obseg škodljivega vpliva umetnointeligenčnega sistema na temeljne pravice, varovane z listino. Te pravice vključujejo pravico do človekovega dostojanstva, spoštovanja zasebnega in družinskega življenja, varstva osebnih podatkov, svobode izražanja in obveščanja, svobode zbiranja in združevanja ter nediskriminacije, varstva potrošnikov, pravic delavcev, pravic invalidov, pravice do učinkovitega pravnega sredstva in nepristranskega sodišča, pravice do obrambe in domneve nedolžnosti ter pravice do dobrega upravljanja. Poleg teh pravic je treba poudariti, da imajo otroci posebne pravice, zapisane v členu 24 Listine EU in Konvenciji Združenih narodov o otrokovih pravicah (v zvezi z digitalnim okoljem so podrobneje opredeljene v splošni pripombi št. 25 KOP), ki zahtevata upoštevanje šibkih točk otrok ter zagotavljanje zaščite in varstva, ki sta potrebna za njihovo dobro počutje. Pri ocenjevanju resnosti škode, ki jo lahko povzroči umetnointeligenčni sistem, je treba upoštevati tudi temeljno pravico do visoke ravni varstva okolja, ki je zapisana v Listini in se izvaja v politikah Unije, tudi v zvezi z zdravjem in varnostjo oseb.

(29) Kar zadeva umetnointeligenčne sisteme velikega tveganja, ki so varnostne komponente proizvodov ali sistemov ali ki so sami proizvodi ali sistemi s področja uporabe Uredbe (ES) št. 300/2008 Evropskega parlamenta in Sveta[39], Uredbe (EU) št. 167/2013 Evropskega parlamenta in Sveta[40], Uredbe (EU) št. 168/2013 Evropskega parlamenta in Sveta[41], Direktive 2014/90/EU Evropskega parlamenta in Sveta[42], Direktive (EU) 2016/797 Evropskega parlamenta in Sveta[43], Uredbe (EU) 2018/858

---

39 Uredba (ES) št. 300/2008 Evropskega parlamenta in Sveta z dne 11. marca 2008 o skupnih pravilih na področju varovanja civilnega letalstva in o razveljavitvi Uredbe (ES) št. 2320/2002 (UL L 97, 9.4.2008, str. 72).

40 Uredba (EU) št. 167/2013 Evropskega parlamenta in Sveta z dne 5. februarja 2013 o odobritvi in tržnem nadzoru kmetijskih in gozdarskih vozil (UL L 60, 2.3.2013, str. 1).

41 Uredba (EU) št. 168/2013 Evropskega parlamenta in Sveta z dne 15. januarja 2013 o odobritvi in tržnem nadzoru dvo- ali trikolesnih vozil in štirikolesnikov (UL L 60, 2.3.2013, str. 52).

42 Direktiva 2014/90/EU Evropskega parlamenta in Sveta z dne 23. julija 2014 o pomorski opremi in razveljavitvi Direktive Sveta 96/98/ES (UL L 257, 28.8.2014, str. 146).

43 Direktiva (EU) 2016/797 Evropskega parlamenta in Sveta z dne 11. maja 2016 o interoperabilnosti železniškega sistema v Evropski uniji (UL L 138, 26.5.2016, str. 44).

Evropskega parlamenta in Sveta[44], Uredbe (EU) 2018/1139 Evropskega parlamenta in Sveta[45] in Uredbe (EU) 2019/2144 Evropskega parlamenta in Sveta[46], je primerno navedene akte spremeniti, da se zagotovi, da Komisija na podlagi tehničnih in regulativnih posebnosti vsakega sektorja ter brez poseganja v obstoječe mehanizme in organe upravljanja, ugotavljanja skladnosti in izvrševanja, vzpostavljene v teh sektorjih, pri sprejemanju vseh ustreznih prihodnjih delegiranih ali izvedbenih aktov na podlagi navedenih aktov upošteva obvezne zahteve za umetnointeligenčne sisteme velikega tveganja, določene v tej uredbi.

(30) Kar zadeva umetnointeligenčne sisteme, ki so varnostne komponente proizvodov ali ki so sami proizvodi s področja uporabe določene harmonizacijske zakonodaje Unije, jih je primerno v skladu s to uredbo razvrstiti kot sisteme velikega tveganja, če je zadevni proizvod v postopku ugotavljanja skladnosti pri organu, ki kot tretja stran izvaja ugotavljanje skladnosti v skladu z ustrezno harmonizacijsko zakonodajo Unije. Taki proizvodi so zlasti stroji, igrače, dvigala, oprema in zaščitni sistemi za uporabo v potencialno eksplozivnih atmosferah, radijska oprema, tlačna oprema, oprema za plovila za rekreacijo, žičniške naprave, naprave, v katerih zgoreva plinasto gorivo, medicinski pripomočki ter in vitro diagnostični medicinski pripomočki.

(31) Razvrstitev umetnointeligenčnega sistema kot sistema velikega tveganja v skladu s to uredbo ne bi smela nujno pomeniti, da se proizvod, katerega varnostna komponenta je umetnointeligenčni sistem, ali sam umetnointeligenčni sistem kot proizvod šteje za „sistem velikega tveganja“ v skladu z merili iz ustrezne harmonizacijske zakonodaje Unije, ki se uporablja za proizvod. To velja zlasti za Uredbo (EU) 2017/745 Evropskega parlamenta in Sveta[47] ter Uredbo (EU) 2017/746 Evropskega parlamenta in Sveta[48], kadar je za proizvode srednjega in velikega tveganja predvideno ugotavljanje skladnosti s strani tretjih oseb.

---

44 Uredba (EU) 2018/858 Evropskega parlamenta in Sveta z dne 30. maja 2018 o odobritvi in tržnem nadzoru motornih vozil in njihovih priklopnikov ter sistemov, sestavnih delov in samostojnih tehničnih enot, namenjenih za taka vozila, spremembi uredb (ES) št. 715/2007 in (ES) št. 595/2009 ter razveljavitvi Direktive 2007/46/ES (UL L 151, 14.6.2018, str. 1).

45 Uredba (EU) 2018/1139 Evropskega parlamenta in Sveta z dne 4. julija 2018 o skupnih pravilih na področju civilnega letalstva in ustanovitvi Agencije Evropske unije za varnost v letalstvu ter spremembi uredb (ES) št. 2111/2005, (ES) št. 1008/2008, (EU) št. 996/2010, (EU) št. 376/2014 ter direktiv 2014/30/EU in 2014/53/EU Evropskega parlamenta in Sveta ter razveljavitvi uredb (ES) št. 552/2004 in (ES) št. 216/2008 Evropskega parlamenta in Sveta ter Uredbe Sveta (EGS) št. 3922/91 (UL L 212, 22.8.2018, str. 1).

46 Uredba (EU) 2019/2144 Evropskega parlamenta in Sveta z dne 27. novembra 2019 o zahtevah za homologacijo motornih vozil in njihovih priklopnikov ter sistemov, sestavnih delov in samostojnih tehničnih enot, namenjenih za taka vozila, v zvezi z njihovo splošno varnostjo in zaščito potnikov v vozilu ter izpostavljenih udeležencev v cestnem prometu in o spremembi Uredbe (EU) 2018/858 Evropskega parlamenta in Sveta ter razveljavitvi uredb (ES) št. 78/2009, (ES) št. 79/2009 in (ES) št. 661/2009 Evropskega parlamenta in Sveta in uredb Komisije (ES) št. 631/2009, (EU) št. 406/2010, (EU) št. 672/2010, (EU) št. 1003/2010, (EU) št. 1005/2010, (EU) št. 1008/2010, (EU) št. 1009/2010, (EU) št. 19/2011, (EU) št. 109/2011, (EU) št. 458/2011, (EU) št. 65/2012, (EU) št. 130/2012, (EU) št. 347/2012, (EU) št. 351/2012, (EU) št. 1230/2012 in (EU) 2015/166 (UL L 325, 16.12.2019, str. 1).

47 Uredba (EU) 2017/745 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o medicinskih pripomočkih, spremembi Direktive 2001/83/ES, Uredbe (ES) št. 178/2002 in Uredbe (ES) št. 1223/2009 ter razveljavitvi direktiv Sveta 90/385/EGS in 93/42/EGS (UL L 117, 5.5.2017, str. 1).

48 Uredba (EU) 2017/746 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o in vitro diagnostičnih medicinskih pripomočkih ter razveljavitvi Direktive 98/79/ES in Sklepa Komisije 2010/227/EU (UL L 117, 5.5.2017, str. 176).

(32) Kar zadeva samostojne umetnointeligenčne sisteme, tj. umetnointeligenčne sisteme velikega tveganja, razen tistih, ki so varnostne komponente proizvodov ali ki so sami proizvodi, jih je primerno razvrstiti kot sisteme velikega tveganja, če glede na svoj predvideni namen predstavljajo veliko tveganje škode za zdravje in varnost ali temeljne pravice oseb, ob upoštevanju resnosti možne škode in verjetnosti njenega nastanka, ter se uporabljajo na več posebej vnaprej opredeljenih področjih, določenih v Uredbi. Določitev teh sistemov temelji na enaki metodologiji in merilih, predvidenih tudi za morebitne prihodnje spremembe seznama umetnointeligenčnih sistemov velikega tveganja.

(33) Tehnične netočnosti umetnointeligenčnih sistemov, namenjenih za biometrično identifikacijo fizičnih oseb na daljavo, lahko vodijo do pristranskih rezultatov in diskriminatornih učinkov. To velja zlasti za starost, etnično pripadnost, spol ali invalidnost. Zato bi bilo treba sisteme za biometrično identifikacijo na daljavo v realnem času in sisteme za naknadno biometrično identifikacijo na daljavo razvrstiti med sisteme velikega tveganja. Zaradi tveganj, ki jih predstavljata, bi morale za obe vrsti sistemov za biometrično identifikacijo na daljavo veljati posebne zahteve glede zmogljivosti vodenja dnevnikov in človekovega nadzora.

(34) V zvezi z upravljanjem in delovanjem kritične infrastrukture je primerno, da se umetnointeligenčni sistemi, namenjeni uporabi kot varnostne komponente pri upravljanju in delovanju cestnega prometa ter oskrbi z vodo, plinom, ogrevanjem in električno energijo, razvrstijo kot sistemi velikega tveganja, saj lahko njihovo nedelovanje ali okvara delovanja ogrozijo življenje in zdravje ljudi v velikem obsegu ter povzročijo občutne motnje v rednem izvajanju družbenih in gospodarskih dejavnosti.

(35) Umetnointeligenčne sisteme, ki se uporabljajo v izobraževanju ali poklicnem usposabljanju, zlasti za določanje dostopa ali razvrščanje oseb v izobraževalne ustanove in ustanove za poklicno usposabljanje ali za ocenjevanje oseb na testih, ki so del izobraževanja ali predpogoj zanj, bi bilo treba obravnavati kot sisteme velikega tveganja, saj lahko določajo izobraževalni in poklicni potek življenja osebe ter tako vplivajo na sposobnost zagotavljanja preživetja te osebe. Če se taki sistemi neustrezno zasnujejo in uporabljajo, lahko kršijo pravico do izobraževanja in usposabljanja ter pravico do nediskriminacije in ohranjajo vzorce diskriminacije iz preteklosti.

(36) Umetnointeligenčne sisteme, ki se uporabljajo pri zaposlovanju, upravljanju delavcev in dostopu do samozaposlitve, zlasti za zaposlovanje in izbiro oseb, za sprejemanje odločitev o napredovanju in prenehanju zaposlitve ter za dodeljevanje nalog, spremljanje ali ocenjevanje oseb v pogodbenih delovnih razmerjih, bi bilo treba prav tako razvrstiti med sisteme velikega tveganja, saj lahko ti sistemi občutno vplivajo na prihodnje poklicne možnosti in možnosti preživljanja teh oseb. Ustrezna pogodbena delovna razmerja bi morala vključevati zaposlene in osebe, ki zagotavljajo storitve preko platform, kot so navedene v delovnem programu Komisije za leto 2021. Take osebe se načeloma ne bi smele šteti za uporabnike v smislu te uredbe. V celotnem postopku zaposlovanja in pri ocenjevanju, napredovanju ali ohranjanju oseb v pogodbenih delovnih razmerjih lahko taki sistemi ohranjajo vzorce diskriminacije iz preteklosti, na primer nad ženskami, določenimi starostnimi skupinami, invalidi ali osebami določenega rasnega ali etničnega porekla ali spolne usmerjenosti. Tudi umetnointeligenčni sistemi, ki se uporabljajo za spremljanje zmogljivosti in vedenja teh oseb, lahko vplivajo na njihove pravice do varstva podatkov in zasebnosti.

(37) Drugo področje, na katerem je treba posebno pozornost nameniti uporabi umetnointeligenčnih sistemov, je dostop do nekaterih bistvenih zasebnih in javnih storitev ter koristi, ki jih ljudje potrebujejo za polno udeležbo v družbi ali izboljšanje življenjskega standarda. Zlasti umetnointeligenčne sisteme, ki se uporabljajo za ocenjevanje kreditne ocene ali kreditne sposobnosti fizičnih oseb, bi bilo treba uvrstiti med umetnointeligenčne sisteme velikega tveganja, saj določajo dostop teh oseb do finančnih sredstev ali bistvenih storitev, kot so stanovanje, električna energija in telekomunikacijske storitve. Umetnointeligenčni sistemi, ki se uporabljajo v ta namen, lahko pripeljejo do diskriminacije oseb ali skupin in ohranijo vzorce diskriminacije iz preteklosti, na primer na podlagi rasnega ali etničnega porekla, invalidnosti, starosti, spolne usmerjenosti, ali ustvarijo nove oblike diskriminatornih vplivov. Glede na zelo omejen obseg vpliva in razpoložljivih alternativ na trgu je primerno izvzeti umetnointeligenčne sisteme za namene ocenjevanja kreditne sposobnosti in kreditnega točkovanja, kadar jih v uporabo dajejo mali ponudniki za lastno uporabo. Fizične osebe, ki zaprosijo za ugodnosti in storitve javne pomoči ali jih prejemajo od javnih organov, so po navadi odvisne od teh ugodnosti in storitev ter so v ranljivem položaju v odnosu do odgovornih organov. Če se umetnointeligenčni sistemi uporabljajo za določanje, ali naj organi take ugodnosti in storitve zavrnejo, zmanjšajo, prekličejo ali zahtevajo povračilo, lahko pomembno vplivajo na preživljanje oseb in kršijo njihove temeljne pravice, kot so pravica do socialne zaščite, nediskriminacije, človekovega dostojanstva ali učinkovitega pravnega sredstva. Zato bi bilo treba te sisteme uvrstiti med sisteme velikega tveganja. Kljub temu ta uredba ne bi smela ovirati razvoja in uporabe inovativnih pristopov v javni upravi, ki bi imela koristi od širše uporabe skladnih in varnih umetnointeligenčnih sistemov, če ti sistemi ne pomenijo velikega tveganja za pravne in fizične osebe. Nazadnje bi bilo treba tudi umetnointeligenčne sisteme, ki se uporabljajo za pošiljanje ali določanje prednosti pri napotitvi služb za ukrepanje ob nesrečah, razvrstiti med sisteme velikega tveganja, saj sprejemajo odločitve v zelo kritičnih razmerah za življenje in zdravje oseb ter njihovo premoženje.

(38) Za ukrepe organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ki vključujejo nekatere uporabe umetnointeligenčnih sistemov, je značilna precejšnja stopnja neravnovesja moči, kar lahko vodi do nadzora, prijetja ali odvzema prostosti fizične osebe ter drugih škodljivih učinkov na temeljne pravice, ki jih zagotavlja Listina. Zlasti če se umetnointeligenčni sistem ne uči z visokokakovostnimi podatki, ne izpolnjuje ustreznih zahtev glede točnosti ali robustnosti ali ni ustrezno zasnovan in testiran, preden je dan na trg ali na kakšen drug način v uporabo, lahko ljudi izloči na diskriminatoren ali kako drugače napačen ali nepravičen način. Poleg tega bi lahko bilo ovirano uveljavljanje pomembnih procesnih temeljnih pravic, kot so pravica do učinkovitega pravnega sredstva in nepristranskega sodišča ter pravica do obrambe in domneve nedolžnosti, zlasti, kadar taki umetnointeligenčni sistemi niso dovolj pregledni, obrazložljivi in dokumentirani. Zato je primerno, da se številni umetnointeligenčni sistemi, namenjeni uporabi v okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, razvrstijo kot sistemi velikega tveganja, kjer so točnost, zanesljivost in preglednost zlasti pomembni, da se preprečijo škodljivi učinki, ohrani zaupanje javnosti ter zagotovita odgovornost in učinkovito sodno varstvo. Glede na naravo zadevnih dejavnosti in z njimi povezanih tveganj bi morali ti umetnointeligenčni sistemi velikega tveganja vključevati zlasti umetnointeligenčne sisteme, namenjene uporabi s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj za individualne ocene tveganja, poligrafe in podobna orodja ali za zaznavanje čustvenega stanja fizične osebe, za odkrivanje „globokih

ponaredkov“, za oceno zanesljivosti dokazov v postopkih preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, za napovedovanje nastanka ali ponovitve dejanskega ali potencialnega kaznivega dejanja na podlagi profiliranja fizičnih oseb ali ocenjevanja osebnostnih lastnosti in značilnosti ali preteklih kaznivih dejanj fizičnih oseb ali skupin, za profiliranje pri odkrivanju, preiskovanju ali pregonu kaznivih dejanj ter za analize kaznivih dejanj v zvezi s fizičnimi osebami. Umetnointeligenčni sistemi, posebej namenjeni uporabi v upravnih postopkih s strani davčnih in carinskih organov, se ne bi smeli šteti za umetnointeligenčne sisteme velikega tveganja, ki jih uporabljajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj za namene preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj.

(39) Umetnointeligenčni sistemi, ki se uporabljajo pri upravljanju migracij, azila in nadzora meje, vplivajo na ljudi, ki so pogosto v posebej ranljivem položaju ter so odvisni od izida ukrepov pristojnih javnih organov. Točnost, nediskriminatorna narava in preglednost umetnointeligenčnih sistemov, ki se uporabljajo v teh kontekstih, so zato zlasti pomembni za zagotavljanje spoštovanja temeljnih pravic izpostavljenih oseb, zlasti njihovih pravic do prostega gibanja, nediskriminacije, varstva zasebnega življenja in osebnih podatkov, mednarodnega varstva in dobrega upravljanja. Zato je primerno, da se umetnointeligenčni sistemi za uporabo s strani pristojnih javnih organov, zadolženih za naloge na področju upravljanja migracij, azila in nadzora mej, kot so poligrafi in podobna orodja, ali za zaznavanje čustvenega stanja fizične osebe, uvrstijo med sisteme velikega tveganja; za ocenjevanje nekaterih tveganj, ki jih predstavljajo fizične osebe, ki vstopajo na ozemlje države članice ali zaprosijo za vizum ali azil; za preverjanje verodostojnosti ustreznih dokumentov fizičnih oseb; za pomoč pristojnim javnim organom pri obravnavi prošenj za azil, vizume in dovoljenja za prebivanje ter s tem povezanih pritožb, da se ugotovi upravičenost fizičnih oseb, ki zaprosijo za status. Umetnointeligenčni sistemi na področju upravljanja migracij, azila in nadzora mej, ki jih zajema ta uredba, bi morali biti skladni z ustreznimi postopkovnimi zahtevami iz Direktive 2013/32/EU Evropskega parlamenta in Sveta[49], Uredbe (ES) št. 810/2009 Evropskega parlamenta in Sveta[50] in druge ustrezne zakonodaje.

(40) Nekatere umetnointeligenčne sisteme, namenjene upravljanju pravosodja in demokratičnih procesov, bi bilo treba uvrstiti med sisteme velikega tveganja ob upoštevanju njihovega potencialno pomembnega vpliva na demokracijo, pravno državo, osebne svoboščine ter pravico do učinkovitega pravnega sredstva in nepristranskega sodišča. Zlasti za obravnavanje tveganj morebitnih pristranskosti, napak in neprepustnosti je primerno, da se umetnointeligenčni sistemi, namenjeni pomoči pravosodnim organom pri raziskovanju in razlagi dejstev in prava ter pri uporabi prava za konkreten sklop dejstev, opredelijo kot sistemi velikega tveganja. Take kvalifikacije pa se ne bi smele razširiti na umetnointeligenčne sisteme, namenjene izključno pomožnim upravnim dejavnostim, ki ne vplivajo na dejansko pravosodje v posameznih primerih, kot so anonimizacija ali psevdonimizacija sodnih odločb, dokumentov ali podatkov, komunikacija med osebjem, upravne naloge ali dodeljevanje virov.

---

[49] Direktiva 2013/32/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o skupnih postopkih za priznanje ali odvzem mednarodne zaščite (UL L 180, 29.6.2013, str. 60).

[50] Uredba (ES) št. 810/2009 Evropskega parlamenta in Sveta z dne 13. julija 2009 o vizumskem zakoniku Skupnosti (Vizumski zakonik) (UL L 243, 15.9.2009, str. 1).

(41) Dejstvo, da je umetnointeligenčni sistem v skladu s to uredbo razvrščen kot sistem velikega tveganja, ne bi smelo pomeniti, da je uporaba sistema nujno zakonita v skladu z drugimi akti prava Unije ali v skladu z nacionalnim pravom, združljivim s pravom Unije, kot so varstvo osebnih podatkov, uporaba poligrafov in podobnih orodij ali drugih sistemov za zaznavanje čustvenega stanja fizičnih oseb. Vsaka taka uporaba bi se morala še naprej izvajati izključno v skladu z veljavnimi zahtevami, ki izhajajo iz Listine ter iz veljavnih aktov sekundarnega prava Unije in nacionalnega prava. Te uredbe ne bi smeli razumeti kot pravne podlage za obdelavo osebnih podatkov, vključno s posebnimi vrstami osebnih podatkov, kadar je to ustrezno.

(42) Za zmanjševanje tveganj, ki jih za uporabnike in izpostavljene osebe predstavljajo umetnointeligenčni sistemi velikega tveganja, ki so dani na trg ali kako drugače dani v uporabo na trgu Unije, bi bilo treba uporabljati nekatere obvezne zahteve ob upoštevanju predvidenega namena uporabe sistema in v skladu s sistemom obvladovanja tveganja, ki ga vzpostavi ponudnik.

(43) Za umetnointeligenčne sisteme velikega tveganja bi morale veljati zahteve glede kakovosti uporabljenih naborov podatkov, tehnične dokumentacije in vodenja evidenc, preglednosti in zagotavljanja informacij uporabnikom, človekovega nadzora ter robustnosti, točnosti in kibernetske varnosti. Navedene zahteve so potrebne za učinkovito zmanjševanje tveganj za zdravje, varnost in temeljne pravice, kot se uporabljajo glede na predvideni namen sistema, in ni drugih manj omejevalnih ukrepov za trgovino, ki bi bili razumno na voljo, s čimer bi se izognili neupravičenim omejitvam trgovine.

(44) Visoka kakovost podatkov je bistvena za zmogljivost številnih umetnointeligenčnih sistemov, zlasti kadar se uporabljajo tehnike, ki vključujejo učenje modelov, s katerim bi zagotovili, da bo umetnointeligenčni sistem velikega tveganja deloval, kot je predvideno, in varno ter da ne bo postane vir diskriminacije, ki je prepovedana s pravom Unije. Za visokokakovostne nabore učnih in testnih podatkov ter podatkov za potrditev je treba izvajati ustrezne prakse vodenja in upravljanja podatkov. Nabori učnih in testnih podatkov ter podatkov za potrditev bi morali biti dovolj ustrezni, reprezentativni in brez napak ter popolni glede na predvideni namen sistema. Imeti bi morali tudi ustrezne statistične lastnosti, tudi v zvezi z osebami ali skupinami oseb, na katerih naj bi se uporabljal umetnointeligenčni sistem velikega tveganja. Nabori učnih in testnih podatkov ter podatkov za potrditev bi morali v obsegu, ki se zahteva glede na njihov predvideni namen, upoštevati zlasti lastnosti, značilnosti ali elemente, ki so značilni za konkretno geografsko, vedenjsko ali funkcionalno okolje ali kontekst, v katerem naj bi se uporabljal umetnointeligenčni sistem. Da bi zaščitili pravico drugih pred diskriminacijo, ki bi lahko bila posledica pristranskosti v sistemih umetne inteligence, bi morali ponudniki imeti možnost, da zaradi pomembnega javnega interesa obdelujejo tudi posebne kategorije osebnih podatkov, da se zagotovijo spremljanje, odkrivanje in odpravljanje pristranskosti v zvezi z umetnointeligenčnimi sistemi velikega tveganja.

(45) Za razvoj umetnointeligenčnih sistemov velikega tveganja bi morali imeti nekateri akterji, kot so ponudniki, priglašeni organi in drugi ustrezni subjekti, kot so vozlišča digitalnih inovacij, centri za testiranje in eksperimentiranje in raziskovalci, možnost dostopa do visokokakovostnih naborov podatkov in njihove uporabe na ustreznih področjih dejavnosti, povezanih s to uredbo. Evropski skupni podatkovni prostori, ki jih je vzpostavila Komisija, ter olajšanje souporabe podatkov med podjetji in z vlado v javnem interesu bodo bistveni za zagotavljanje zaupanja vrednega, odgovornega in nediskriminatornega dostopa do visokokakovostnih podatkov za učenje, potrjevanje in

testiranje umetnointeligenčnih sistemov. Evropski zdravstveni podatkovni prostor bo na primer na področju zdravja olajšal nediskriminatoren dostop do zdravstvenih podatkov in učenje algoritmov umetne inteligence na teh naborih podatkov na varen, pravočasen, pregleden in zaupanja vreden način ter z ustreznim institucionalnim upravljanjem. Ustrezni pristojni organi, vključno s sektorskimi, ki zagotavljajo ali podpirajo dostop do podatkov, lahko podpirajo tudi zagotavljanje visokokakovostnih podatkov za učenje, potrditev in testiranje umetnointeligenčnih sistemov.

(46) Informacije o tem, kako so bili umetnointeligenčni sistemi velikega tveganja razviti in kako delujejo v svojem življenjskem ciklu, so bistvene za preverjanje skladnosti z zahtevami iz te uredbe. To zahteva vodenje evidenc in razpoložljivost tehnične dokumentacije, ki vsebuje informacije, potrebne za oceno skladnosti umetnointeligenčnega sistema z ustreznimi zahtevami. Take informacije bi morale vključevati splošne značilnosti, zmogljivosti in omejitve sistema, uporabljene algoritme, podatke, postopke učenja, testiranja in potrjevanja ter dokumentacijo o ustreznem sistemu obvladovanja tveganja. Tehnično dokumentacijo je treba posodabljati.

(47) Za odpravo neprepustnosti, zaradi katere so nekateri umetnointeligenčni sistemi fizičnim osebam morda nerazumljivi ali zanje preveč zapleteni, bi bilo treba za umetnointeligenčne sisteme velikega tveganja zahtevati določeno stopnjo preglednosti. Uporabniki bi morali biti sposobni interpretirati izhodne podatke sistema in jih ustrezno uporabiti. Sistemom umetne inteligence velikega tveganja bi bilo zato treba priložiti ustrezno dokumentacijo in navodila za uporabo ter vključiti jedrnate in jasne informacije, vključno z morebitnimi tveganji za temeljne pravice in diskriminacijo, kjer je to primerno.

(48) Umetnointeligenčni sistemi velikega tveganja bi morali biti zasnovani in razviti tako, da lahko fizične osebe nadzorujejo njihovo delovanje. V ta namen bi moral ponudnik sistema pred dajanjem sistema na trg ali v uporabo določiti ustrezne ukrepe za človekov nadzor. Zlasti bi morali taki ukrepi, kadar je to primerno, zagotavljati, da za sistem veljajo vgrajene operativne omejitve, ki jih sistem sam ne more razveljaviti in se odziva na človeškega operaterja, ter da imajo fizične osebe, ki jim je bil dodeljen človekov nadzor, potrebno pristojnost, usposobljenost in pooblastila za opravljanje te vloge.

(49) Umetnointeligenčni sistemi velikega tveganja bi morali v svojem celotnem življenjskem ciklu delovati dosledno ter izpolnjevati ustrezno raven točnosti, robustnosti in kibernetske varnosti v skladu s splošno priznanim stanjem tehnike. O ravni točnosti in metrikah točnosti bi bilo treba obvestiti uporabnike.

(50) Tehnična robustnost je ključna zahteva za umetnointeligenčne sisteme velikega tveganja. Odporni morajo biti proti tveganjem, povezanim z omejitvami sistema (npr. napake, okvare, nedoslednosti, nepričakovane situacije), pa tudi proti zlonamernim dejanjem, ki lahko ogrozijo varnost umetnointeligenčnega sistema in povzročijo škodljivo ali drugače nezaželeno vedenje. Neuspešna zaščita pred temi tveganji bi lahko imela varnostne posledice ali negativno vplivala na temeljne pravice, na primer zaradi napačnih odločitev ali napačnih ali pristranskih izhodnih podatkov, ki jih ustvari umetnointeligenčni sistem.

(51) Kibernetska varnost ima ključno vlogo pri zagotavljanju odpornosti umetnointeligenčnih sistemov proti poskusom spreminjanja njihove uporabe, vedenja, zmogljivosti ali ogrožanja njihovih varnostnih lastnosti s strani zlonamernih tretjih oseb, ki izkoriščajo šibke točke sistema. Kibernetski napadi na umetnointeligenčne

sisteme lahko izkoristijo posebna sredstva umetne inteligence, kot so nabori učnih podatkov (npr. zastrupitev podatkov) ali naučeni modeli (npr. nasprotovalni napadi), ali pa izkoristijo šibke točke digitalnih sredstev umetnointeligenčnega sistema ali osnovne infrastrukture IKT. Da bi zagotovili raven kibernetske varnosti, ki ustreza tveganjem, bi morali ponudniki umetnointeligenčnih sistemov velikega tveganja sprejeti ustrezne ukrepe in pri tem ustrezno upoštevati tudi osnovno infrastrukturo IKT.

(52) Kot del harmonizacijske zakonodaje Unije bi bilo treba pravila, ki veljajo za dajanje na trg, v obratovanje in uporabo umetnointeligenčnih sistemov velikega tveganja, določiti skladno z Uredbo (ES) št. 765/2008 Evropskega parlamenta in Sveta[51] o določitvi zahtev za akreditacijo in nadzor trga proizvodov, Sklepom št. 768/2008/ES Evropskega parlamenta in Sveta[52] o skupnem okviru za trženje proizvodov in Uredbo (EU) 2019/1020 Evropskega parlamenta in Sveta[53] o nadzoru trga in skladnosti proizvodov („novi zakonodajni okvir za trženje proizvodov“).

(53) Primerno je, da določena fizična ali pravna oseba, opredeljena kot ponudnik, prevzame odgovornost za dajanje umetnointeligenčnega sistema velikega tveganja na trg ali v uporabo, ne glede na to, ali je ta fizična ali pravna oseba tista, ki je zasnovala ali razvila sistem.

(54) Ponudnik bi moral vzpostaviti zanesljiv sistem upravljanja kakovosti, zagotoviti izvedbo zahtevanega postopka ugotavljanja skladnosti, pripraviti ustrezno dokumentacijo in vzpostaviti robusten sistem spremljanja po dajanju na trg. Javni organi, ki umetnointeligenčne sisteme velikega tveganja dajejo v uporabo za lastno uporabo, lahko sprejmejo in izvajajo pravila za sistem upravljanja kakovosti kot del sistema upravljanja kakovosti, sprejetega na nacionalni oziroma regionalni ravni ob upoštevanju posebnosti sektorja ter pristojnosti in organizacije zadevnega javnega organa.

(55) Kadar umetnointeligenčni sistem velikega tveganja, ki je varnostna komponenta proizvoda, ki ga zajema ustrezna sektorska zakonodaja novega zakonodajnega okvira, ni dan na trg ali v uporabo neodvisno od proizvoda, bi moral proizvajalec končnega proizvoda, kot je opredeljen v ustrezni zakonodaji novega zakonodajnega okvira, izpolnjevati obveznosti ponudnika iz te uredbe in zlasti zagotoviti, da umetnointeligenčni sistem, vgrajen v končni proizvod, izpolnjuje zahteve te uredbe.

(56) Da se omogoči izvajanje te uredbe in ustvarijo enaki konkurenčni pogoji za operaterje ter ob upoštevanju različnih oblik dajanja digitalnih proizvodov na voljo, je pomembno zagotoviti, da lahko oseba s sedežem v Uniji v vseh okoliščinah organom zagotovi vse potrebne informacije o skladnosti umetnointeligenčnega sistema. Zato ponudniki s sedežem zunaj Unije pred dajanjem svojih umetnointeligenčnih sistemov na voljo v Uniji, kadar ni mogoče ugotoviti, kdo je uvoznik, s pisnim pooblastilom imenujejo pooblaščenega zastopnika s sedežem v Uniji.

---

51 Uredba (ES) št. 765/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o določitvi zahtev za akreditacijo in nadzor trga v zvezi s trženjem proizvodov ter razveljavitvi Uredbe (EGS) št. 339/93 (UL L 218, 13.8.2008, str. 30).

52 Sklep št. 768/2008/ES Evropskega parlamenta in Sveta z dne 9. julija 2008 o skupnem okviru za trženje proizvodov in razveljavitvi Sklepa Sveta 93/465/EGS (UL L 218, 13.8.2008, str. 82).

53 Uredba (EU) 2019/1020 Evropskega parlamenta in Sveta z dne 20. junija 2019 o nadzoru trga in skladnosti proizvodov ter spremembi Direktive 2004/42/ES in uredb (ES) št. 765/2008 in (EU) št. 305/2011 (Besedilo velja za EGP) (UL L 169, 25.6.2019, str. 1).

(57) V skladu z načeli novega zakonodajnega okvira je treba določiti posebne obveznosti za zadevne gospodarske subjekte, kot so uvozniki in distributerji, da se zagotovi pravna varnost in olajša izpolnjevanje predpisov s strani teh zadevnih subjektov.

(58) Glede na naravo umetnointeligenčnih sistemov ter tveganja za varnost in temeljne pravice, ki so morda povezana z njihovo uporabo, vključno s potrebo po zagotovitvi ustreznega spremljanja zmogljivosti umetnointeligenčnega sistema v realnem življenju, je primerno določiti posebne odgovornosti za uporabnike. Uporabniki bi morali umetnointeligenčne sisteme velikega tveganja uporabljati zlasti v skladu z navodili za uporabo, pri čemer bi bilo treba določiti nekatere druge obveznosti v zvezi s spremljanjem delovanja umetnointeligenčnih sistemov in po potrebi v zvezi z vodenjem evidenc.

(59) Primerno je predvideti, da je uporabnik umetnointeligenčnega sistema fizična ali pravna oseba, javni organ, agencija ali drug organ, pod čigar nadzorom deluje umetnointeligenčni sistem, razen kadar se uporablja v okviru osebne nepoklicne dejavnosti.

(60) Zaradi kompleksnosti vrednostne verige umetne inteligence bi morale ustrezne tretje osebe, zlasti tiste, ki so vključene v prodajo in dobavo programske opreme, programskih orodij in komponent, prednaučenih modelov in podatkov, ali ponudniki omrežnih storitev, po potrebi sodelovati s ponudniki in uporabniki, da jim omogočijo izpolnjevanje obveznosti iz te uredbe, ter s pristojnimi organi, ustanovljenimi na podlagi te uredbe.

(61) Standardizacija bi morala imeti ključno vlogo pri zagotavljanju tehničnih rešitev za ponudnike, da se zagotovi skladnost s to uredbo. Sredstvo, s katerim ponudniki dokazujejo skladnost z zahtevami iz te uredbe, bi morala biti skladnost s harmoniziranimi standardi, kot so opredeljeni v Uredbi (EU) št. 1025/2012 Evropskega parlamenta in Sveta[54]. Vendar bi lahko Komisija sprejela skupne tehnične specifikacije na področjih, na katerih harmonizirani standardi ne obstajajo ali kjer so nezadostni.

(62) Da bi zagotovili visoko raven zaupanja v umetnointeligenčne sisteme velikega tveganja, bi bilo treba za te sisteme pred dajanjem na trg ali v uporabo opraviti ugotavljanje skladnosti.

(63) Da bi čim bolj zmanjšali breme za operaterje in se izognili morebitnemu podvajanju, je primerno, da se za umetnointeligenčne sisteme velikega tveganja, povezane s proizvodi, za katere velja obstoječa harmonizacijska zakonodaja Unije v skladu s pristopom novega zakonodajnega okvira, skladnost teh umetnointeligenčnih sistemov z zahtevami te uredbe oceni kot del ugotavljanja skladnosti, ki ga že predvideva navedena zakonodaja. Uporaba zahtev iz te uredbe tako ne bi smela vplivati na posebno logiko, metodologijo ali splošno strukturo ugotavljanja skladnosti v skladu z ustrezno posebno zakonodajo novega zakonodajnega okvira. Ta pristop se v celoti odraža v medsebojnem delovanju te uredbe in [uredbe o strojih]. Medtem ko zahteve iz te uredbe rešujejo varnostna tveganja umetnointeligenčnih sistemov, ki zagotavljajo varnostne funkcije v strojih, bodo nekatere posebne zahteve iz [uredbe o strojih]

[54] Uredba (EU) št. 1025/2012 Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv Sveta 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega parlamenta in Sveta ter razveljavitvi Sklepa Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in Sveta (UL L 316, 14.11.2012, str. 12).

zagotovile varno vključitev umetnointeligenčnega sistema v stroje na splošno, da ne bo ogrožena varnost strojev kot celote. [Uredba o strojih] uporablja enako opredelitev umetnointeligenčnega sistema kot ta uredba.

(64) Glede na obsežnejše izkušnje poklicnih izdajateljev potrdil pred dajanjem na trg na področju varnosti proizvodov in različno naravo zadevnih tveganj je primerno, da se vsaj v začetni fazi uporabe te uredbe omeji področje uporabe ugotavljanja skladnosti s strani tretjih oseb za umetnointeligenčne sisteme velikega tveganja, ki niso povezani s proizvodi. Zato bi moral ugotavljanje skladnosti takih sistemov praviloma opraviti ponudnik na lastno odgovornost, z edino izjemo umetnointeligenčnih sistemov, namenjenih uporabi za biometrično identifikacijo oseb na daljavo, za katere bi bilo treba predvideti sodelovanje priglašenega organa pri ugotavljanju skladnosti, če to ni prepovedano.

(65) Za izvajanje ugotavljanja skladnosti umetnointeligenčnih sistemov, namenjenih uporabi za biometrično identifikacijo oseb na daljavo, s strani tretjih oseb, bi morali pristojni nacionalni organi v skladu s to uredbo imenovati priglašene organe, če izpolnjujejo vrsto zahtev, zlasti glede neodvisnosti, pristojnosti in neobstoja navzkrižja interesov.

(66) V skladu s skupno uveljavljenim pojmom bistvene spremembe za proizvode, ki jih ureja harmonizacijska zakonodaja Unije, je primerno, da se za umetnointeligenčni sistem ob vsaki spremembi, ki bi lahko vplivala na skladnost sistema s to uredbo ali ko se spremeni predvideni namen sistema, izvede novo ugotavljanje skladnosti. Poleg tega je treba v zvezi z umetnointeligenčnimi sistemi, ki se po dajanju na trg ali v uporabo še naprej „učijo“ (tj. samodejno prilagajajo način izvajanja funkcij), določiti pravila, ki določajo, da spremembe algoritma in njegove zmogljivosti, ki jih je ponudnik vnaprej določil in ocenil ob ugotavljanju skladnosti, ne bi smele pomeniti bistvene spremembe.

(67) Umetnointeligenčni sistemi velikega tveganja bi morali imeti oznako CE, ki označuje njihovo skladnost s to uredbo, da se lahko prosto gibljejo na notranjem trgu. Države članice ne bi smele neupravičeno ovirati dajanja na trg ali v uporabo umetnointeligenčnih sistemov velikega tveganja, ki izpolnjujejo zahteve iz te uredbe in nosijo oznako CE.

(68) Pod določenimi pogoji je lahko hitra razpoložljivost inovativnih tehnologij ključnega pomena za zdravje in varnost ljudi ter za družbo kot celoto. Zato je primerno, da lahko države članice iz izjemnih razlogov javne varnosti ali varstva življenja in zdravja fizičnih oseb ter varstva industrijske in poslovne lastnine dovolijo dajanje na trg ali v uporabo umetnointeligenčnih sistemov, za katere ni bilo opravljeno ugotavljanje skladnosti.

(69) Za olajšanje dela Komisije in držav članic na področju umetne inteligence ter povečanje preglednosti za javnost bi bilo treba od ponudnikov umetnointeligenčnih sistemov velikega tveganja, razen tistih, povezanih s proizvodi, ki spadajo na področje uporabe ustrezne obstoječe harmonizacijske zakonodaje Unije, zahtevati, da svoje umetnointeligenčne sisteme velikega tveganja registrirajo v podatkovni zbirki EU, ki jo vzpostavi in upravlja Komisija. Komisija bi morala biti upravljavec navedene zbirke

podatkov v skladu z Uredbo (EU) 2018/1725 Evropskega parlamenta in Sveta[55]. Za zagotovitev popolne funkcionalnosti podatkovne zbirke ob njeni uvedbi bi moral postopek za vzpostavitev zbirke podatkov vključevati pripravo funkcionalnih specifikacij s strani Komisije in neodvisno revizijsko poročilo.

(70) Nekateri umetnointeligenčni sistemi, namenjeni stikom s fizičnimi osebami ali ustvarjanju vsebine, lahko predstavljajo posebna tveganja za izdajanje za drugo osebo ali zavajanje, ne glede na to, ali se uvrščajo med sisteme velikega tveganja ali ne. V določenih okoliščinah bi zato za uporabo teh sistemov morale veljati posebne obveznosti glede preglednosti brez poseganja v zahteve in obveznosti za umetnointeligenčne sisteme velikega tveganja. Zlasti fizične osebe bi morale biti obveščene, da so v stiku s sistemom umetne inteligence, razen če je to razvidno iz okoliščin in konteksta uporabe. Poleg tega bi morale biti fizične osebe obveščene, kadar so izpostavljene sistemu za prepoznavanje čustev ali sistemu za biometrično kategorizacijo. Take informacije in obvestila bi bilo treba zagotoviti v oblikah, dostopnih za invalide. Poleg tega bi morali uporabniki, ki uporabljajo umetnointeligenčni sistem za ustvarjanje ali manipulacijo slikovne, zvočne ali videovsebine, ki v znatni meri spominja na obstoječe osebe, kraje ali dogodke in bi se osebi zdela verodostojna, čeprav ni, razkriti, da je bila vsebina umetno ustvarjena ali manipulirana, tako da ustrezno označijo izhodne podatke umetne inteligence in razkrijejo njihov umetni izvor.

(71) Umetna inteligenca je hitro razvijajoča se skupina tehnologij, ki zahteva nove oblike regulativnega nadzora in varen prostor za eksperimentiranje, hkrati pa zagotavlja odgovorne inovacije ter vključevanje ustreznih zaščitnih ukrepov in ukrepov za zmanjševanje tveganja. Da bi zagotovili pravni okvir, ki je prijazen do inovacij, primeren za prihodnost in odporen na motnje, bi bilo treba pristojne nacionalne organe iz ene ali več držav članic spodbuditi k vzpostavitvi regulativnih peskovnikov za umetno inteligenco, da bi omogočili razvoj in testiranje inovativnih umetnointeligenčnih sistemov pod strogim regulativnim nadzorom, preden se ti sistemi dajo na trg ali kako drugače v uporabo.

(72) Cilji regulativnih peskovnikov bi morali biti spodbujati inovacije na področju umetne inteligence z vzpostavitvijo nadzorovanega testnega okolja in okolja za eksperimentiranje v fazi razvoja ter pred trženjem, da se zagotovi skladnost inovativnih umetnointeligenčnih sistemov s to uredbo ter drugo ustrezno zakonodajo Unije in držav članic; povečati pravno varnost za inovatorje ter nadzor in razumevanje priložnosti, nastajajočih tveganj in učinkov uporabe umetne inteligence s strani pristojnih organov ter pospešiti dostop do trgov, tudi z odpravo ovir za mala in srednja podjetja (MSP) ter zagonska podjetja. Za zagotovitev enotnega izvajanja po vsej Uniji in ekonomije obsega je primerno določiti skupna pravila za izvajanje regulativnih peskovnikov in okvir za sodelovanje med ustreznimi organi, vključenimi v nadzor peskovnikov. Ta uredba bi morala zagotoviti pravno podlago za uporabo osebnih podatkov, zbranih za druge namene za razvoj nekaterih umetnointeligenčnih sistemov v javnem interesu v regulativnem peskovniku za umetno inteligenco v skladu s členom 6(4) Uredbe (EU) 2016/679 in členom 6 Uredbe (EU) 2018/1725 ter brez poseganja v člen 4(2) Direktive (EU) 2016/680. Udeleženci v peskovniku bi morali zagotoviti ustrezne zaščitne ukrepe in sodelovati s pristojnimi organi, tudi z

[55] 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).

upoštevanjem njihovih smernic ter hitrim in dobronamernim ukrepanjem, da bi zmanjšali vsa velika tveganja za varnost in temeljne pravice, ki se lahko pojavijo med razvojem in eksperimentiranjem v peskovniku. Ravnanje udeležencev v peskovniku bi bilo treba upoštevati, ko se pristojni organi odločijo, ali bodo naložili upravno globo v skladu s členom 83(2) Uredbe 2016/679 in členom 57 Direktive 2016/680.

(73) Za spodbujanje in zaščito inovacij je pomembno, da se upoštevajo zlasti interesi malih ponudnikov in uporabnikov umetnointeligenčnih sistemov. V ta namen bi morale države članice razviti pobude, namenjene tem operaterjem, vključno z ozaveščanjem in sporočanjem informacij. Poleg tega se pri določanju pristojbin s strani priglašenih organov za ugotavljanje skladnosti upoštevajo posebni interesi in potrebe malih ponudnikov. Stroški prevajanja, povezani z obvezno dokumentacijo in komuniciranjem z organi, lahko predstavljajo znaten strošek za ponudnike in druge operaterje, zlasti tiste manjšega obsega. Države članice bi morale po možnosti zagotoviti, da je eden od jezikov, ki jih določijo in sprejmejo za dokumentacijo zadevnih ponudnikov in za komunikacijo z operaterji, jezik, ki ga na splošno razume največje možno število čezmejnih uporabnikov.

(74) Da bi čim bolj zmanjšali tveganja za izvajanje, ki so posledica pomanjkanja znanja in strokovnega znanja na trgu, ter da bi ponudnikom in priglašenim organom olajšali izpolnjevanje njihovih obveznosti iz te uredbe, bi morali platforma za umetno inteligenco na zahtevo, evropska vozlišča digitalnih inovacij ter centri za testiranje in eksperimentiranje, ki so jih vzpostavile Komisija in države članice na nacionalni ravni ali ravni EU, po možnosti prispevati k izvajanju te uredbe. V okviru svojih nalog in področij pristojnosti lahko ponudnikom in priglašenim organom zagotavljajo zlasti tehnično in znanstveno podporo.

(75) Primerno je, da Komisija organom, skupinam ali laboratorijem, ustanovljenim ali akreditiranim v skladu z ustrezno harmonizacijsko zakonodajo Unije, ki izpolnjujejo naloge v okviru ugotavljanja skladnosti proizvodov ali pripomočkov, zajetih v navedeni harmonizacijski zakonodaji Unije, čim bolj olajša dostop do centrov za testiranje in eksperimentiranje. To velja zlasti za strokovne odbore, strokovne laboratorije in referenčne laboratorije na področju medicinskih pripomočkov v skladu z Uredbo (EU) 2017/745 in Uredbo (EU) 2017/746.

(76) Za lažje nemoteno, učinkovito in harmonizirano izvajanje te uredbe bi bilo treba ustanoviti Evropski odbor za umetno inteligenco. Odbor bi moral biti odgovoren za številne svetovalne naloge, med drugim za izdajanje mnenj, priporočil, nasvetov ali smernic o zadevah, povezanih z izvajanjem te uredbe, vključno s tehničnimi specifikacijami ali obstoječimi standardi v zvezi z zahtevami iz te uredbe, ter svetovanje in pomoč Komisiji pri posebnih vprašanjih v zvezi z umetno inteligenco.

(77) Države članice imajo ključno vlogo pri uporabi in izvrševanju te uredbe. V zvezi s tem bi morala vsaka država članica imenovati enega ali več pristojnih nacionalnih organov za nadzor uporabe in izvajanja te uredbe. Da bi se povečala učinkovitost organizacije s strani držav članic ter vzpostavila uradna kontaktna točka za stike z javnostjo in drugimi partnerji na ravni držav članic in Unije, bi bilo treba v vsaki državi članici en nacionalni organ imenovati za nacionalni nadzorni organ.

(78) Da bi zagotovili, da lahko ponudniki umetnointeligenčnih sistemov velikega tveganja upoštevajo izkušnje pri uporabi umetnointeligenčnih sistemov velikega tveganja za izboljšanje svojih sistemov ter postopka zasnove in razvoja ali da lahko pravočasno izvedejo morebitne popravne ukrepe, bi morali imeti vsi ponudniki vzpostavljen sistem spremljanja po dajanju na trg. Ta sistem je tudi ključen za zagotovitev

učinkovitejše in bolj pravočasne obravnave morebitnih tveganj, ki izhajajo iz umetnointeligenčnih sistemov, ki se po dajanju na trg ali v uporabo še naprej „učijo“. V zvezi s tem bi bilo treba od ponudnikov zahtevati tudi, da imajo vzpostavljen sistem za poročanje ustreznim organom o vseh hudih incidentih ali kršitvah nacionalne zakonodaje in zakonodaje Unije o varstvu temeljnih pravic, ki so posledica uporabe njihovih umetnointeligenčnih sistemov.

(79) Za zagotovitev ustreznega in učinkovitega izvrševanja zahtev in obveznosti iz te uredbe, ki je harmonizacijska zakonodaja Unije, bi bilo treba v celoti uporabljati sistem nadzora trga in skladnosti proizvodov, vzpostavljen z Uredbo (EU) 2019/1020. Kadar je to potrebno za njihove naloge, bi morali imeti nacionalni javni organi, ki nadzorujejo uporabo prava Unije o varstvu temeljnih pravic, vključno z organi za enakost, tudi dostop do kakršne koli dokumentacije, pripravljene v skladu s to uredbo.

(80) Zakonodaja Unije o finančnih storitvah vključuje pravila in zahteve glede notranjega upravljanja in obvladovanja tveganj, ki veljajo za regulirane finančne institucije v postopku opravljanja teh storitev, tudi kadar uporabljajo umetnointeligenčne sisteme. Za zagotovitev usklajene uporabe in izvrševanja obveznosti iz te uredbe ter ustreznih pravil in zahtev zakonodaje Unije o finančnih storitvah bi bilo treba organe, pristojne za nadzor in izvrševanje zakonodaje o finančnih storitvah, vključno z Evropsko centralno banko, kadar je to primerno, določiti kot pristojne organe za nadzor izvajanja te uredbe, vključno z dejavnostmi nadzora trga, v zvezi z umetnointeligenčnimi sistemi, ki jih dajejo na voljo ali uporabljajo regulirane in nadzorovane finančne institucije. Za nadaljnjo krepitev skladnosti med to uredbo in pravili, ki se uporabljajo za kreditne institucije, ki jih ureja Direktiva 2013/36/EU Evropskega parlamenta in Sveta[56], je primerno v obstoječe obveznosti in postopke iz Direktive 2013/36/EU vključiti tudi postopek ugotavljanja skladnosti in nekatere postopkovne obveznosti ponudnikov v zvezi z obvladovanjem tveganja, spremljanjem po dajanju na trg ter dokumentacijo. Da bi se izognili prekrivanju, bi bilo treba predvideti tudi omejena odstopanja v zvezi s sistemom upravljanja kakovosti ponudnikov in obveznostjo spremljanja za uporabnike umetnointeligenčnih sistemov velikega tveganja, kolikor se ti uporabljajo za kreditne institucije, ki jih ureja Direktiva 2013/36/EU.

(81) Razvoj umetnointeligenčnih sistemov, ki niso umetnointeligenčni sistemi velikega tveganja, v skladu z zahtevami iz te uredbe lahko pripelje do večje uporabe zaupanja vredne umetne inteligence v Uniji. Ponudnike umetnointeligenčnih sistemov, ki ne predstavljajo velikega tveganja, bi bilo treba spodbujati k oblikovanju kodeksov ravnanja, namenjenih spodbujanju prostovoljne uporabe obveznih zahtev, ki veljajo za umetnointeligenčne sisteme velikega tveganja. Ponudnike bi bilo treba spodbujati tudi k prostovoljni uporabi dodatnih zahtev, povezanih na primer z okoljsko trajnostjo, dostopnostjo za invalide, sodelovanjem deležnikov pri snovanju in razvoju umetnointeligenčnih sistemov ter raznolikostjo razvojnih skupin. Komisija lahko razvije pobude, vključno s sektorskimi, da se olajša zmanjšanje tehničnih ovir za čezmejno izmenjavo podatkov za razvoj umetne inteligence, vključno z infrastrukturo za dostop do podatkov, semantično in tehnično interoperabilnostjo različnih vrst podatkov.

---

[56] Direktiva 2013/36/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij in investicijskih podjetij, spremembi Direktive 2002/87/ES in razveljavitvi direktiv 2006/48/ES in 2006/49/ES (UL L 176, 27.6.2013, str. 338).

(82) Pomembno je, da so umetnointeligenčni sistemi, povezani s proizvodi brez velikega tveganja v skladu s to uredbo, in jim zato ni treba izpolnjevati zahtev iz te uredbe, kljub temu varni, ko so dani na trg ali v uporabo. Da bi prispevali k temu cilju, bi se Direktiva 2001/95/ES Evropskega parlamenta in Sveta[57] uporabljala kot varnostna mreža.

(83) Za zagotovitev zaupanja vrednega in konstruktivnega sodelovanja pristojnih organov na ravni Unije in nacionalni ravni bi morale vse strani, vključene v uporabo te uredbe, spoštovati zaupnost informacij in podatkov, pridobljenih pri opravljanju svojih nalog.

(84) Države članice bi morale sprejeti vse potrebne ukrepe za zagotovitev izvajanja določb iz te uredbe ter določiti učinkovite, sorazmerne in odvračilne kazni za kršitve teh določb. Za nekatere posebne kršitve bi morale države članice upoštevati meje in merila iz te uredbe. Evropski nadzornik za varstvo podatkov bi moral biti pooblaščen za nalaganje glob institucijam, agencijam in organom Unije, ki spadajo na področje uporabe te uredbe.

(85) Za zagotovitev, da se regulativni okvir lahko po potrebi prilagodi, bi bilo treba na Komisijo prenesti pooblastilo, da v skladu s členom 290 PDEU sprejme akte za spremembo tehnik in pristopov iz Priloge I za opredelitev umetnointeligenčnih sistemov, harmonizacijske zakonodaje Unije iz Priloge II, umetnointeligenčnih sistemov velikega tveganja iz Priloge III, določb v zvezi s tehnično dokumentacijo iz Priloge IV, vsebine izjave EU o skladnosti iz Priloge V, določb v zvezi s postopki ugotavljanja skladnosti iz prilog VI in VII ter določb o vzpostavitvi umetnointeligenčnih sistemov velikega tveganja, za katere bi se moral uporabljati postopek ugotavljanja skladnosti na podlagi ocene sistema upravljanja kakovosti in ocene tehnične dokumentacije. Zlasti je pomembno, da se Komisija pri svojem pripravljalnem delu ustrezno posvetuje, vključno na ravni strokovnjakov, in da se to posvetovanje izvede v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje[58]. Za zagotovitev enakopravnega sodelovanja pri pripravi delegiranih aktov Evropski parlament in Svet prejmeta zlasti vse dokumente sočasno s strokovnjaki iz držav članic, njuni strokovnjaki pa se lahko sistematično udeležujejo sestankov strokovnih skupin Komisije, ki zadevajo pripravo delegiranih aktov.

(86) Za zagotovitev enotnih pogojev izvajanja te uredbe bi bilo treba na Komisijo prenesti izvedbena pooblastila. Navedena pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta[59].

(87) Ker cilja te uredbe države članice ne morejo zadovoljivo doseči in se zaradi obsega ali učinka ukrepa lažje dosežejo na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 PEU. V skladu z načelom sorazmernosti iz navedenega člena ta uredba ne presega tistega, kar je potrebno za doseganje navedenega cilja.

(88) Ta uredba bi se morala uporabljati od … [*Urad za publikacije – vstavite datum iz člena 85*]. Vendar bi morala infrastruktura, povezana z upravljanjem in sistemom

---

57 Direktiva 2001/95/ES Evropskega parlamenta in Sveta z dne 3. decembra 2001 o splošni varnosti proizvodov (UL L 11, 15.1.2002, str. 4).

58 UL L 123, 12.5.2016, str. 1.

59 Uredba (EU) št. 182/2011 Evropskega parlamenta in Sveta z dne 16. februarja 2011 o določitvi splošnih pravil in načel, na podlagi katerih države članice nadzirajo izvajanje izvedbenih pooblastil Komisije (UL L 55, 28.2.2011, str. 13).

ugotavljanja skladnosti, začeti delovati pred navedenim datumom, zato bi se morale določbe o priglašenih organih in strukturi upravljanja uporabljati od … [Urad za publikacije – *vstavite datum – tri mesece po začetku veljavnosti te uredbe*]. Poleg tega bi morale države članice določiti pravila o kaznih, vključno z upravnimi globami bodo učinkovito izvajale do datuma začetka uporabe te uredbe. Zato bi se morale določbe o kaznih uporabljati od [Urad za publikacije – *vstavite datum – dvanajst mesecev po začetku veljavnosti te uredbe*].

(89) V skladu s členom 42(2) Uredbe (EU) 2018/1725 je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov in Evropskim odborom za varstvo podatkov, ki sta mnenje podala [...] –

SPREJELA NASLEDNJO UREDBO:

NASLOV I

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja

Ta uredba določa:

(a) harmonizirana pravila za dajanje na trg, v obratovanje in uporabo umetnointeligenčnih sistemov v Uniji;

(a) prepovedi nekaterih praks umetne inteligence;

(b) posebne zahteve za umetnointeligenčne sisteme velikega tveganja in obveznosti za operaterje takih sistemov;

(c) harmonizirana pravila o preglednosti za umetnointeligenčne sisteme, namenjene stikom s fizičnimi osebami, sisteme za prepoznavanje čustev in sisteme za biometrično kategorizacijo ter umetnointeligenčne sisteme, ki se uporabljajo za ustvarjanje ali manipulacijo slikovne, zvočne ali videovsebine;

(d) pravila o spremljanju in nadzoru trga.

Člen 2

Področje uporabe

1. Ta uredba se uporablja za:

(a) ponudnike, ki dajejo na trg ali v uporabo umetnointeligenčne sisteme v Uniji, ne glede na to, ali imajo ti ponudniki sedež v Uniji ali v tretji državi;

(b) uporabnike umetnointeligenčnih sistemov v Uniji;

(c) ponudnike in uporabnike umetnointeligenčnih sistemov v tretji državi, kadar se izhodni podatki, ki jih sistem ustvari, uporabljajo v Uniji.

2. Za umetnointeligenčne sisteme velikega tveganja, ki so varnostne komponente proizvodov ali sistemov ali ki so sami proizvodi ali sistemi s področja uporabe naslednjih aktov, se uporablja samo člen 84 te uredbe:

(a) Uredba (ES) št. 300/2008;

(b) Uredba (EU) št. 167/2013;

(c) Uredba (EU) št. 168/2013;

(d) Direktiva 2014/90/EU;

(e) Direktiva (EU) 2016/797;

(f) Uredba (EU) 2018/858;

(g) Uredba (EU) 2018/1139;

(h) Uredba (EU) 2019/2144.

3. Ta uredba se ne uporablja za umetnointeligenčne sisteme, ki so bili razviti ali se uporabljajo izključno v vojaške namene.

4. Ta uredba se ne uporablja za javne organe v tretji državi ali mednarodne organizacije, ki spadajo na področje uporabe te uredbe v skladu z odstavkom 1, kadar ti organi ali organizacije uporabljajo umetnointeligenčne sisteme v okviru mednarodnih sporazumov za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter za sodelovanje na področju pravosodja z Unijo ali z eno ali več državami članicami.

5. Ta uredba ne bi smela vplivati na uporabo določb o odgovornosti posrednih ponudnikov storitev iz oddelka 4 poglavja II Direktive 2000/31/ES Evropskega parlamenta in Sveta[60] [*ki se nadomestijo z ustreznimi določbami akta o digitalnih storitvah*].

Člen 3

Opredelitve pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „umetnointeligenčni sistem“ pomeni programsko opremo, ki je razvita z eno ali več tehnikami in pristopi iz Priloge I ter lahko za določen sklop ciljev, ki jih opredeli človek, ustvarja izhodne podatke, kot so vsebine, napovedi, priporočila ali odločitve, ki vplivajo na okolje, s katerim so v stiku;

(1) „ponudnik“ pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki razvije umetnointeligenčni sistem ali ima umetnointeligenčni sistem, razvit za dajanje na trg ali v uporabo pod svojim imenom ali blagovno znamko, bodisi za plačilo bodisi brezplačno;

(3) „mali ponudnik“ pomeni ponudnika, ki je mikro ali malo podjetje v smislu Priporočila Komisije 2003/361/ES[61];

[60] Direktiva 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (direktiva o elektronskem poslovanju) (UL L 178, 17.7.2000, str. 1).

[61] Priporočilo Komisije z dne 6. maja 2003 o opredelitvi mikro, malih in srednje velikih podjetij (UL L 124, 20.5.2003, str. 36).

(4) „uporabnik“ pomeni vsako fizično ali pravno osebo, javni organ, agencijo ali drug organ, ki umetnointeligenčni sistem uporablja v svoji pristojnosti, razen kadar se umetnointeligenčni sistem uporablja v okviru osebne nepoklicne dejavnosti;

(5) „pooblaščeni zastopnik“ pomeni vsako fizično ali pravno osebo s sedežem v Uniji, ki jo je ponudnik umetnointeligenčnega sistema pisno pooblastil, da v njegovem imenu opravlja in izvaja obveznosti in postopke, določene s to uredbo;

(6) „uvoznik“ pomeni vsako fizično ali pravno osebo s sedežem v Uniji, ki da na trg ali v uporabo umetnointeligenčni sistem, ki nosi ime ali blagovno znamko fizične ali pravne osebe s sedežem zunaj Unije;

(7) „distributer“ pomeni vsako fizično ali pravno osebo v dobavni verigi, razen ponudnika ali uvoznika, ki omogoči dostop do umetnointeligenčnega sistema na trgu Unije, ne da bi vplivala na njegove lastnosti;

(8) „operater“ pomeni ponudnika, uporabnika, pooblaščenega zastopnika, uvoznika in distributerja;

(9) „dajanje na trg“ pomeni, da je umetnointeligenčni sistem prvič dostopen na trgu Unije;

(10) „omogočanje dostopnosti na trgu“ pomeni vsako dobavo umetnointeligenčnega sistema za distribucijo ali uporabo na trgu Unije v okviru gospodarske dejavnosti, bodisi za plačilo ali brezplačno;

(11) „dajanje v uporabo“ pomeni dobavo umetnointeligenčnega sistema za prvo uporabo neposredno uporabniku ali za lastno uporabo na trgu Unije za predvideni namen;

(12) „predvideni namen“ pomeni uporabo, za katero je ponudnik namenil umetnointeligenčni sistem, vključno s posebnim kontekstom in pogoji uporabe, kot je navedeno v informacijah, ki jih je ponudnik predložil v navodilih za uporabo, promocijskem ali prodajnem gradivu in izjavah ter v tehnični dokumentaciji;

(13) „razumno predvidljiva napačna uporaba“ pomeni uporabo umetnointeligenčnega sistema na način, ki sicer ni v skladu s predvidenim namenom, vendar je lahko posledica razumno predvidljivega človeškega vedenja ali stikov z drugimi sistemi;

(14) „varnostna komponenta proizvoda ali sistema“ pomeni komponento proizvoda ali sistema, ki opravlja varnostno funkcijo za ta proizvod ali sistem ali katerega nedelovanje ali okvara ogroža zdravje in varnost oseb ali premoženja;

(15) „navodila za uporabo“ pomenijo informacije, ki jih zagotovi ponudnik, da uporabnika obvesti zlasti o predvidenem namenu in pravilni uporabi umetnointeligenčnega sistema, vključno s posebnim geografskim, vedenjskim ali funkcionalnim okoljem, v katerem naj bi se umetnointeligenčni sistem velikega tveganja uporabljal;

(16) „preklic umetnointeligenčnega sistema“ pomeni vsak ukrep, namenjen vrnitvi umetnointeligenčnega sistema, ki je na voljo uporabnikom, ponudniku;

(17) „umik umetnointeligenčnega sistema“ pomeni vsak ukrep, namenjen preprečevanju distribucije, prikaza in ponudbe umetnointeligenčnega sistema;

(18) „zmogljivost umetnointeligenčnega sistema“ pomeni sposobnost umetnointeligenčnega sistema, da doseže svoj predvideni namen;

(19) „priglasitveni organ“ pomeni nacionalni organ, odgovoren za vzpostavitev in izvajanje potrebnih postopkov za ocenjevanje, imenovanje in priglasitev organov za ugotavljanje skladnosti ter za njihovo spremljanje;

(20) „ugotavljanje skladnosti“ pomeni postopek preverjanja, ali so izpolnjene zahteve iz poglavja 2 naslova III te uredbe v zvezi s sistemom umetne inteligence;

(21) „organ za ugotavljanje skladnosti“ pomeni organ, ki kot tretja stran izvaja dejavnosti ugotavljanja skladnosti, vključno s testiranjem, izdajanjem potrdil in inšpekcijskim pregledovanjem;

(22) „priglašeni organ“ pomeni organ za ugotavljanje skladnosti, imenovan v skladu s to uredbo in drugo ustrezno harmonizacijsko zakonodajo Unije;

(23) „bistvena sprememba“ pomeni spremembo umetnointeligenčnega sistema po dajanju na trg ali v uporabo, ki vpliva na skladnost umetnointeligenčnega sistema z zahtevami iz poglavja 2 naslova III te uredbe ali povzroči spremembo predvidenega namena, za katerega je bil umetnointeligenčni sistem ocenjen;

(24) „oznaka skladnosti“ (oznaka CE) pomeni oznako, s katero ponudnik izjavlja, da je umetnointeligenčni sistem skladen z zahtevami iz naslova III, poglavje 2 te uredbe in druge veljavne zakonodaje Unije o harmonizaciji pogojev za trženje proizvodov („harmonizacijska zakonodaja Unije“), ki določa njeno pritrditev;

(25) „spremljanje po dajanju na trg“ pomeni vse dejavnosti, ki jih izvajajo ponudniki umetnointeligenčnih sistemov, da bi proaktivno zbirali in pregledovali izkušnje, pridobljene z uporabo umetnointeligenčnih sistemov, ki jih dajo na trg ali v uporabo, da bi ugotovili, ali so potrebni takojšnji korektivni ali preventivni ukrepi;

(26) „organ za nadzor trga“ pomeni nacionalni organ, ki izvaja dejavnosti in sprejema ukrepe v skladu z Uredbo (EU) 2019/1020;

(27) „harmonizirani standard“ pomeni evropski standard, kakor je opredeljen v členu 2(1)(c) Uredbe (EU) št. 1025/2012;

(28) „skupne specifikacije“ pomeni dokument, ki ni standard ter vsebuje tehnične rešitve, ki zagotavljajo sredstva za izpolnjevanje nekaterih zahtev in obveznosti, določenih s to uredbo;

(29) „učni podatki“ pomeni podatke, ki se uporabljajo za učenje umetnointeligenčnega sistema s prilagajanjem njegovih učljivih parametrov, vključno z utežmi nevronske mreže;

(30) „podatki za potrditev“ pomeni podatke, ki se uporabljajo za ocenjevanje naučenega umetnointeligenčnega sistema ter za uravnavanje parametrov, ki se jih ne more naučiti, in učnega postopka sistema, med drugim za preprečevanje pretiranega prilagajanja; ker je lahko nabor podatkov za potrditev ločen nabor podatkov ali del nabora učnih podatkov, bodisi kot stalna ali spremenljiva delitev;

(31) „testni podatki“ pomeni podatke, ki se uporabljajo za zagotavljanje neodvisne ocene naučenega in potrjenega umetnointeligenčnega sistema za potrditev pričakovane zmogljivosti tega sistema pred dajanjem na trg ali v uporabo;

(32) „vhodni podatki“ pomeni podatke, ki se dajo na razpolago umetnointeligenčnemu sistemu ali jih ta neposredno pridobi in na podlagi katerih sistem ustvari izhodne podatke;

(33) „biometrični podatki“ pomeni osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi fizične osebe, ki omogočajo ali potrjujejo edinstveno identifikacijo te fizične osebe, kot so podobe obraza ali daktiloskopski podatki;

(34) „sistem za prepoznavanje čustev“ pomeni umetnointeligenčni sistem za prepoznavanje čustev ali sklepanje o čustvih ali namenih fizičnih oseb na podlagi njihovih biometričnih podatkov;

(35) „sistem za biometrično kategorizacijo“ pomeni umetnointeligenčni sistem za razvrščanje fizičnih oseb v posebne kategorije, kot so spol, starost, barva las, barva oči, tetovaže, etnično poreklo ali spolna ali politična usmerjenost, na podlagi njihovih biometričnih podatkov;

(36) „sistem za biometrično identifikacijo na daljavo“ pomeni umetnointeligenčni sistem za identifikacijo fizičnih oseb na daljavo s primerjavo biometričnih podatkov osebe z biometričnimi podatki iz referenčne podatkovne zbirke, pri čemer uporabnik umetnointeligenčnega sistema ne ve vnaprej, ali bo oseba prisotna in ali jo je mogoče identificirati;

(37) „sistem za biometrično identifikacijo na daljavo v realnem času“ pomeni sistem za biometrično identifikacijo na daljavo, pri katerem se zajemanje biometričnih podatkov, primerjava in identifikacija izvedejo brez večje zamude. To ne vključuje le takojšnje identifikacije, temveč tudi omejene kratke zamude, da bi se preprečilo izogibanje določbi.

(38) „sistem za naknadno biometrično identifikacijo na daljavo“ pomeni sistem za biometrično identifikacijo na daljavo, ki ni sistem za biometrično identifikacijo na daljavo v realnem času;

(39) „javno dostopni prostor“ pomeni vsak fizični prostor, ki je dostopen javnosti, ne glede na to, ali veljajo določeni pogoji za dostop;

(40) „organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj“ pomeni:

(a) kateri koli javni organ, ki je pristojen za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem; ali

(b) kateri koli drug organ ali subjekt, ki v skladu s pravom države članice lahko opravlja javne funkcije ali izvaja javna pooblastila za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem;

(41) „preprečevanje, odkrivanje in preiskovanje kaznivih dejanj“ pomeni dejavnosti, ki jih izvajajo organi za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem;

(42) „nacionalni nadzorni organ“ pomeni organ, ki mu država članica dodeli odgovornost za izvajanje in uporabo te uredbe, za usklajevanje dejavnosti, zaupanih tej državi članici, za delovanje kot enotna kontaktna točka za Komisijo in za zastopanje države članice v Evropskem odboru za umetno inteligenco;

(43) „pristojni nacionalni organ“ pomeni nacionalni nadzorni organ, priglasitveni organ in organ za nadzor trga;

(44) „hud incident“ pomeni vsak incident, ki neposredno ali posredno povzroči, je lahko povzročil ali bi lahko povzročil:

(a) smrt osebe ali hudo škodo za zdravje osebe, premoženje ali okolje,

(b) hude in nepopravljive motnje pri upravljanju in delovanju kritične infrastrukture.

Člen 4

Spremembe Priloge I

Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 73 za spremembo seznama tehnik in pristopov iz Priloge I, da se navedeni seznam posodobi glede na tržni in tehnološki razvoj na podlagi značilnosti, ki so podobne tam navedenim tehnikam in pristopom.

NASLOV II

PREPOVEDANE PRAKSE UMETNE INTELIGENCE

Člen 5

1. Prepovedane so naslednje prakse umetne inteligence:

(a) dajanje na trg, v uporabo ali v obratovanje umetnointeligenčnega sistema, ki uporablja subliminalne tehnike, ki presegajo zavest osebe, da bi bistveno izkrivili vedenje osebe na način, ki tej osebi ali drugi osebi povzroči ali bi ji lahko povzročil fizično ali psihično škodo;

(b) dajanje na trg, v uporabo ali v obratovanje umetnointeligenčnega sistema, ki izkorišča katere koli šibke točke določene skupine oseb zaradi njihove starosti, telesne ali duševne invalidnosti, da bi bistveno izkrivili vedenje osebe, ki spada v to skupino, na način, ki tej osebi ali drugi osebi povzroči ali bi ji lahko povzročil fizično ali psihično škodo;

(c) dajanje umetnointeligenčnih sistemov na trg, v uporabo ali v obratovanje s strani javnih organov ali v njihovem imenu za ocenjevanje ali razvrščanje fizičnih oseb po tem, koliko so vredne zaupanja, v določenem časovnem obdobju na podlagi njihovega družbenega vedenja ali znanih ali predvidenih osebnih ali osebnostnih značilnosti, pri čemer število družbenih točk vodi do ene ali obeh naslednjih možnosti:

(i) škodljiva ali neugodna obravnava nekaterih fizičnih oseb ali njihovih celotnih skupin v družbenih okoliščinah, ki niso povezane z okoliščinami, v katerih so bili podatki prvotno ustvarjeni ali zbrani;

(ii) škodljiva ali neugodna obravnava nekaterih fizičnih oseb ali njihovih celotnih skupin, ki je neupravičena ali nesorazmerna z njihovim družbenim vedenjem ali resnostjo njihovega družbenega vedenja;

(d) uporabo sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja

kaznivih dejanj, razen če je taka uporaba nujno potrebna za enega od naslednjih ciljev:

(i) usmerjeno iskanje določenih potencialnih žrtev kaznivih dejanj, vključno s pogrešanimi otroki;

(ii) preprečitev konkretne, znatne in neposredne nevarnosti za življenje ali fizično varnost fizičnih oseb ali preprečitev terorističnega napada;

(iii) odkrivanje, lokalizacijo, identifikacijo ali pregon storilca ali osumljenca kaznivega dejanja iz člena 2(2) Okvirnega sklepa Sveta 2002/584/PNZ[62], ki se v zadevni državi članici kaznuje z zaporno kaznijo ali ukrepom, vezanim na odvzem prostosti najmanj treh let, kot je določeno z zakonodajo te države članice.

2. Pri uporabi sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj za katerega koli od ciljev iz točke (d) odstavka 1 se upoštevajo naslednji elementi:

(a) narava razmer, ki povzročajo morebitno uporabo, zlasti resnost, verjetnost in obseg škode, povzročene v odsotnosti uporabe sistema;

(b) posledice uporabe sistema za pravice in svoboščine vseh zadevnih oseb, zlasti resnost, verjetnost in obseg teh posledic.

Poleg tega je uporaba sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj za katerega koli od ciljev iz točke (d) odstavka 1 skladna s potrebnimi in sorazmernimi zaščitnimi ukrepi in pogoji v zvezi z uporabo, zlasti glede časovnih, geografskih in osebnih omejitev.

3. V zvezi s točko (d) odstavka 1 in odstavkom 2 je za vsako posamezno uporabo sistema za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj treba pridobiti predhodno dovoljenje pravosodnega organa ali neodvisnega upravnega organa države članice, v kateri bo potekala uporaba, izdano na podlagi obrazložene zahteve in v skladu s podrobnimi pravili nacionalnega prava iz odstavka 4. Vendar se lahko v ustrezno utemeljenih nujnih primerih uporaba sistema začne brez dovoljenja, dovoljenje pa se lahko zahteva šele med uporabo ali po njej.

Pristojni sodni ali upravni organ izda dovoljenje le, če se na podlagi objektivnih dokazov ali jasnih navedb, ki so mu bili predloženi, prepriča, da je uporaba zadevnega sistema za biometrično identifikacijo na daljavo v realnem času potrebna in sorazmerna za doseganje enega od ciljev iz točke (d) odstavka 1, kot je opredeljeno v zahtevi. Pristojni sodni ali upravni organ pri odločanju o zahtevi upošteva elemente iz odstavka 2.

4. Država članica se lahko odloči, da v okviru omejitev in pod pogoji iz točke (d) odstavka 1 ter odstavkov 2 in 3 v celoti ali delno dovoli uporabo sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Ta država članica

[62] Okvirni sklep Sveta 2002/584/PNZ z dne 13. junija 2002 o evropskem nalogu za prijetje in postopkih predaje med državami članicami (UL L 190, 18.7.2002, str. 1).

v svoji nacionalni zakonodaji določi potrebna podrobna pravila za zahtevo, izdajo in izvajanje ter nadzor v zvezi z dovoljenji iz odstavka 3. Ta pravila poleg tega določajo, za katere od ciljev iz točke (d) odstavka 1, med drugim tudi, za katera kazniva dejanja iz točke (iii), se lahko pristojnim organom dovoli uporaba teh sistemov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.

NASLOV III

UMETNOINTELIGENČNI SISTEMI VELIKEGA TVEGANJA

POGLAVJE 1

RAZVRSTITEV UMETNOINTELIGENČNIH SISTEMOV MED SISTEME VELIKEGA TVEGANJA

Člen 6

Pravila razvrstitve za umetnointeligenčne sisteme velikega tveganja

1. Ne glede na to, ali je umetnointeligenčni sistem dan na trg ali v uporabo neodvisno od proizvodov iz točk (a) in (b), se ta umetnointeligenčni sistem šteje za sistem velikega tveganja, če sta izpolnjena oba naslednja pogoja:

   (a) umetnointeligenčni sistem je namenjen uporabi kot varnostna komponenta proizvoda ali pa je sam proizvod, ki ga zajema harmonizacijska zakonodaja Unije iz Priloge II;

   (b) za proizvod, katerega varnostna komponenta je umetnointeligenčni sistem, ali pa je sam umetnointeligenčni sistem kot proizvod, je treba opraviti ugotavljanje skladnosti s strani tretje osebe zaradi dajanja tega proizvoda na trg ali v uporabo v skladu s harmonizacijsko zakonodajo Unije iz Priloge II.

2. Poleg umetnointeligenčnih sistemov velikega tveganja iz odstavka 1 se za umetnointeligenčne sisteme velikega tveganja štejejo tudi umetnointeligenčni sistemi iz Priloge III .

Člen 7

Spremembe Priloge III

1. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 73 za posodobitev seznama iz Priloge III z dodajanjem umetnointeligenčnih sistemov velikega tveganja, če sta izpolnjena oba naslednja pogoja:

   (a) umetnointeligenčni sistemi so namenjeni uporabi na katerem koli območju iz točk 1 do 8 Priloge III;

   (b) umetnointeligenčni sistemi predstavljajo tveganje škode za zdravje in varnost ali tveganje škodljivega vpliva na temeljne pravice, ki je glede na resnost in verjetnost nastanka enako ali večje od tveganja škode ali škodljivega vpliva umetnointeligenčnih sistemov velikega tveganja, ki so že navedeni v Prilogi III.

2. Komisija pri ocenjevanju za namene odstavka 1, ali umetnointeligenčni sistem predstavlja tveganje škode za zdravje in varnost ali tveganje škodljivega vpliva na temeljne pravice, ki je enako ali večje od tveganja škode umetnointeligenčnih sistemov velikega tveganja, ki so že navedeni v Prilogi III, upošteva naslednja merila:

(a) predvideni namen umetnointeligenčnega sistema;

(b) obseg uporabe ali verjetnost uporabe umetnointeligenčnega sistema;

(c) obseg, v katerem je uporaba umetnointeligenčnega sistema že povzročila škodo za zdravje in varnost ali škodljiv vpliv na temeljne pravice ali povzročila resno zaskrbljenost glede uresničitve take škode ali škodljivega vpliva, kot je razvidno iz poročil ali dokumentiranih trditev, predloženih pristojnim nacionalnim organom;

(d) morebitni obseg take škode ali takega škodljivega vpliva, zlasti v smislu njene intenzivnosti in zmožnosti, da vpliva na pluralnost oseb;

(e) obseg, v katerem so potencialno oškodovane ali oškodovane osebe odvisne od izida, doseženega s sistemom umetne inteligence, zlasti ker iz praktičnih ali pravnih razlogov ni mogoče razumno odstopiti od tega izida;

(f) obseg, v katerem so potencialno oškodovane ali prizadete osebe v ranljivem položaju v odnosu do uporabnika umetnointeligenčnega sistema, zlasti zaradi neravnovesja moči, znanja, ekonomskih ali socialnih okoliščin ali starosti;

(g) obseg, v katerem je izid, ustvarjen s sistemom umetne inteligence, mogoče zlahka odpraviti, pri čemer se izidi, ki vplivajo na zdravje ali varnost oseb, ne štejejo za take, ki je mogoče zlahka odpraviti;

(h) obseg, v katerem obstoječa zakonodaja Unije določa:

(i) učinkovite ukrepe sodnega varstva v zvezi s tveganji, ki jih predstavlja umetnointeligenčni sistem, razen odškodninskih zahtevkov;

(ii) učinkovite ukrepe za preprečevanje ali bistveno zmanjšanje teh tveganj.

POGLAVJE 2

ZAHTEVE ZA UMETNOINTELIGENČNE SISTEME VELIKEGA TVEGANJA

Člen 8

Skladnost z zahtevami

1. Umetnointeligenčni sistemi velikega tveganja izpolnjujejo zahteve iz tega poglavja.

2. Predvideni namen umetnointeligenčnega sistema velikega tveganja in sistema obvladovanja tveganja iz člena 9 se upošteva pri zagotavljanju skladnosti z navedenimi zahtevami.

Člen 9

Sistem obvladovanja tveganja

1. V zvezi z umetnointeligenčnimi sistemi velikega tveganja se vzpostavi, izvaja, dokumentira in vzdržuje sistem obvladovanja tveganja.

2. Sistem obvladovanja tveganja je sestavljen iz neprekinjenega ponavljajočega se procesa, ki se izvaja med celotno življenjsko dobo umetnointeligenčnega sistema velikega tveganja in ga je treba redno sistematično posodabljati. Obsegati mora naslednje korake:

   (a) ugotovitev in analizo znanih in predvidljivih tveganj, povezanih z vsakim sistemom umetne inteligence velikega tveganja;

   (b) oceno in ovrednotenje tveganj, ki se lahko pojavijo pri uporabi umetnointeligenčnega sistema velikega tveganja v skladu s predvidenim namenom in v razmerah razumno predvidljive napačne uporabe;

   (c) ovrednotenje drugih morebitnih tveganj na podlagi analize podatkov, zbranih iz sistema spremljanja po dajanju na trg iz člena 61;

   (d) sprejetje ustreznih ukrepov za obvladovanje tveganja v skladu z določbami naslednjih odstavkov.

3. Pri ukrepih za obvladovanje tveganja iz točke (d) odstavka 2 se ustrezno upoštevajo učinki in možni medsebojni vplivi, ki izhajajo iz skupne uporabe zahtev iz tega poglavja 2. Upoštevajo splošno priznano stanje tehnike, vključno s tistim, kar se odraža v ustreznih harmoniziranih standardih ali skupnih specifikacijah.

4. Ukrepi za obvladovanje tveganja iz točke (d) odstavka 2 so taki, da se vsako preostalo tveganje, povezano z vsako nevarnostjo, in celotno preostalo tveganje umetnointeligenčnih sistemov velikega tveganja štejeta za sprejemljiva pod pogojem, da se umetnointeligenčni sistem velikega tveganja uporablja v skladu s predvidenim namenom ali v razmerah razumno predvidljive napačne uporabe. O teh preostalih tveganjih je treba obvestiti uporabnika.

   Pri določanju najustreznejših ukrepov za obvladovanje tveganja se zagotovi naslednje:

   (a) z ustrezno zasnovo in razvojem odpraviti tveganja ali jih kar najbolj zmanjšati;

   (b) po potrebi izvajati ustrezne ukrepe za blažitev in nadzor v zvezi s tveganji, ki jih ni mogoče odpraviti;

   (c) zagotoviti ustrezne informacije v skladu s členom 13, zlasti v zvezi s tveganji iz točke (b) odstavka 2 tega člena, in po potrebi zagotoviti usposabljanje uporabnikov.

   Pri odpravljanju ali zmanjševanju tveganj, povezanih z uporabo umetnointeligenčnega sistema velikega tveganja, se ustrezno upoštevajo tehnično znanje, izkušnje, izobraževanje, usposabljanje, ki ga lahko pričakuje uporabnik, in okolje, v katerem naj bi se sistem uporabljal.

5. Umetnointeligenčni sistemi velikega tveganja se testirajo, da se določijo najprimernejši ukrepi za obvladovanje tveganja. S testiranjem se zagotovi, da umetnointeligenčni sistemi velikega tveganja delujejo dosledno za predvideni namen in izpolnjujejo zahteve iz tega poglavja.

6. Postopki testiranja so primerni za doseganje predvidenega namena umetnointeligenčnega sistema in jim ni treba presegati tistega, kar je potrebno za doseganje navedenega namena.

7. Testiranje umetnointeligenčnih sistemov velikega tveganja se po potrebi izvede kadar koli v celotnem razvojnem procesu, vsekakor pa pred dajanjem na trg ali v uporabo. Testiranje se opravi na podlagi predhodno opredeljenih metrik in verjetnostnih pragov, ki ustrezajo predvidenemu namenu umetnointeligenčnega sistema velikega tveganja.

8. Pri izvajanju sistema obvladovanja tveganja iz odstavkov 1–7 se posebej preuči, ali je verjetno, da bodo do umetnointeligenčnega sistema velikega tveganja dostopali otroci oziroma ali bo sistem vplival nanje.

9. Za kreditne institucije, ki jih ureja Direktiva 2013/36/EU, so vidiki iz odstavkov 1–8 del postopkov obvladovanja tveganja, ki jih določijo navedene institucije v skladu s členom 74 navedene direktive.

Člen 10

Podatki in upravljanje podatkov

1. Umetnointeligenčni sistemi velikega tveganja, ki uporabljajo tehnike, ki vključujejo učenje modelov s podatki, se razvijejo na podlagi naborov učnih podatkov, podatkov za potrditev in testnih podatkov, ki izpolnjujejo merila kakovosti iz odstavkov 2–5.

2. Za nabore učnih in testnih podatkov ter podatkov za potrditev veljajo ustrezne prakse vodenja in upravljanja podatkov. Te prakse zadevajo zlasti:

   (a) ustrezne izbire zasnove;

   (b) zbiranje podatkov;

   (c) ustrezne postopke obdelave za pripravo podatkov, kot so dodajanje opomb, označevanje, čiščenje, obogatitev in združevanje;

   (d) oblikovanje ustreznih predpostavk, zlasti v zvezi z informacijami, ki naj bi jih podatki merili in predstavljali;

   (e) predhodno oceno razpoložljivosti, količine in primernosti potrebnih naborov podatkov;

   (f) preučitev morebitnih pristranskosti;

   (g) prepoznavanje morebitnih vrzeli ali pomanjkljivosti v podatkih ter način za odpravljanje teh vrzeli in pomanjkljivosti.

3. Nabori učnih in testnih podatkov ter podatkov za potrditev so ustrezni, reprezentativni, brez napak in popolni. Imeti morajo tudi ustrezne statistične lastnosti, tudi v zvezi z osebami ali skupinami oseb, kadar je primerno, na katerih naj bi se uporabljal umetnointeligenčni sistem velikega tveganja. Te značilnosti naborov podatkov se lahko izpolnijo na ravni posameznih naborov podatkov ali njihovih kombinacij.

4. Nabori učnih in testnih podatkov ter podatkov za potrditev morajo v obsegu, ki se zahteva glede na njihov predvideni namen, upoštevati značilnosti ali elemente, ki so značilni za posebno geografsko, vedenjsko ali funkcionalno okolje, v katerem naj bi se umetnointeligenčni sistem velikega tveganja uporabljal.

5. Če je to nujno potrebno za namene zagotavljanja spremljanja, odkrivanja in odpravljanja pristranskosti v zvezi z umetnointeligenčnimi sistemi velikega tveganja, lahko ponudniki takih sistemov obdelujejo posebne kategorije osebnih podatkov iz člena 9(1) Uredbe (EU) 2016/679, člena 10 Direktive (EU) 2016/680 in člena 10(1) Uredbe (EU) 2018/1725 ob upoštevanju ustreznih zaščitnih ukrepov za temeljne pravice in svoboščine fizičnih oseb, vključno s tehničnimi omejitvami ponovne uporabe in uporabe najsodobnejših varnostnih ukrepov in ukrepov za ohranjanje zasebnosti, kot je psevdonimizacija ali šifriranje, kadar lahko anonimizacija bistveno vpliva na želeni namen.

6. Za razvoj umetnointeligenčnih sistemov velikega tveganja, razen tistih, ki uporabljajo tehnike, ki vključujejo učenje modelov, se uporabljajo ustrezne prakse vodenja in upravljanja podatkov, da se zagotovi skladnost teh umetnointeligenčnih sistemov velikega tveganja z odstavkom 2.

Člen 11

Tehnična dokumentacija

1. Tehnična dokumentacija umetnointeligenčnega sistema velikega tveganja se pripravi pred dajanjem sistema na trg ali v uporabo in se posodablja.

   Tehnična dokumentacija se pripravi tako, da dokazuje, da je umetnointeligenčni sistem velikega tveganja skladen z zahtevami iz tega poglavja, ter pristojnim nacionalnim organom in priglašenim organom zagotovi vse potrebne informacije za ugotavljanje skladnosti umetnointeligenčnega sistema z navedenimi zahtevami. Vsebovati mora vsaj elemente iz Priloge IV.

2. Kadar je umetnointeligenčni sistem velikega tveganja, povezan s proizvodom, za katerega se uporabljajo pravni akti iz oddelka A Priloge II, dan na trg ali v uporabo, se pripravi enotna tehnična dokumentacija, ki vsebuje vse informacije iz Priloge IV in informacije, zahtevane v navedenih pravnih aktih.

3. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 73 za spremembo Priloge IV, kadar je to potrebno za zagotovitev, da tehnična dokumentacija glede na tehnični napredek zagotavlja vse potrebne informacije za ugotavljanje skladnosti sistema z zahtevami iz tega poglavja.

Člen 12

Vodenje evidenc

1. Umetnointeligenčni sistemi velikega tveganja so zasnovani in razviti z zmogljivostmi, ki omogočajo samodejno beleženje dogodkov („dnevniki“), med delovanjem umetnointeligenčnih sistemov velikega tveganja. Te zmogljivosti vodenja dnevnikov so v skladu s priznanimi standardi ali skupnimi specifikacijami.

2. Zmogljivosti vodenja dnevnikov zagotavljajo raven sledljivosti delovanja umetnointeligenčnega sistema v celotnem življenjskem ciklu, ki ustreza predvidenemu namenu sistema.

3. Zlasti zmogljivosti vodenja dnevnikov omogočajo spremljanje delovanja umetnointeligenčnega sistema velikega tveganja v zvezi s pojavom situacij, ki lahko povzročijo, da bi sistem umetne inteligence predstavljal tveganje v smislu

člena 65(1), pa se zaradi njih izvedejo bistvene spremembe, in olajšujejo spremljanje po dajanju na trg iz člena 61.

4. Za umetnointeligenčne sisteme velikega tveganja iz točke (a) odstavka 1 Priloge III zmogljivosti vodenja dnevnikov zagotavljajo najmanj:

(a) evidentiranje obdobja vsake uporabe sistema (datum in čas začetka ter datum in čas konca vsake uporabe);

(b) referenčno podatkovno zbirko, s katero je sistem preveril vhodne podatke;

(c) vhodne podatke, za katere je bilo pri iskanju najdeno ujemanje;

(d) identifikacijo fizičnih oseb, vključenih v preverjanje rezultatov iz člena 14(5).

Člen 13

Preglednost in zagotavljanje informacij uporabnikom

1. Umetnointeligenčni sistemi velikega tveganja so zasnovani in razviti tako, da je njihovo delovanje dovolj pregledno, da lahko uporabniki razlagajo izhodne podatke sistema in jih ustrezno uporabijo. Zagotovita se ustrezna vrsta in stopnja preglednosti, da se doseže skladnost z ustreznimi obveznostmi uporabnika in ponudnika iz poglavja 3 tega naslova.

2. Umetnointeligenčnim sistemom velikega tveganja so priložena navodila za uporabo v ustrezni digitalni obliki ali kako drugače, ki vključujejo jedrnate, popolne, pravilne in jasne informacije, ki so pomembne, dostopne in razumljive uporabnikom.

3. Informacije iz odstavka 2 določajo:

(a) istovetnost in kontaktne podatke ponudnika in njegovega pooblaščenega zastopnika, kadar ta obstaja;

(b) značilnosti, zmogljivosti in omejitve delovanja umetnointeligenčnega sistema velikega tveganja, ki vključujejo:

(i) njegov predvideni namen;

(ii) raven točnosti, robustnosti in kibernetske varnosti iz člena 15, na podlagi katere je bil umetnointeligenčni sistem velikega tveganja testiran ter potrjen in katero se lahko pričakuje, ter vse znane in predvidljive okoliščine, ki bi lahko vplivale na to pričakovano raven točnosti, robustnosti in kibernetske varnosti;

(iii) vse znane ali predvidljive okoliščine, povezane z uporabo umetnointeligenčnega sistema velikega tveganja v skladu s predvidenim namenom ali v razmerah razumno predvidljive napačne uporabe, ki lahko pripeljejo do tveganj za zdravje in varnost ali za temeljne pravice;

(iv) njegove zmogljivosti v zvezi z osebami ali skupinami oseb, na katerih naj bi se sistem uporabljal;

(v) kadar je to primerno, specifikacije za vhodne podatke ali katere koli druge ustrezne informacije v zvezi z uporabljenimi nabori učnih in testnih podatkov ter podatkov za potrditev, ob upoštevanju predvidenega namena umetnointeligenčnega sistema;

(c) morebitne spremembe umetnointeligenčnega sistema velikega tveganja in njegove zmogljivosti, ki jih je ponudnik vnaprej določil ob začetnem ugotavljanju skladnosti;

(d) ukrepe človekovega nadzora iz člena 14, vključno z vzpostavljenimi tehničnimi ukrepi, ki uporabnikom olajšajo razlago izhodnih podatkov umetnointeligenčnih sistemov;

(e) pričakovano življenjsko dobo umetnointeligenčnega sistema velikega tveganja ter vse potrebne vzdrževalne in negovalne ukrepe za zagotovitev pravilnega delovanja tega umetnointeligenčnega sistema, tudi v zvezi s posodobitvami programske opreme.

Člen 14

Človekov nadzor

1. Umetnointeligenčni sistemi velikega tveganja so zasnovani in razviti tako, da jih lahko fizične osebe v obdobju uporabe umetnointeligenčnega sistema učinkovito nadzorujejo, vključno z ustreznimi orodji za vmesnik med človekom in strojem.

2. Namen človekovega nadzora je preprečiti ali čim bolj zmanjšati tveganja za zdravje, varnost ali temeljne pravice, ki se lahko pojavijo pri uporabi umetnointeligenčnega sistema velikega tveganja v skladu s predvidenim namenom ali v razmerah razumno predvidljive napačne uporabe, zlasti če taka tveganja niso odpravljena kljub uporabi drugih zahtev iz tega poglavja.

3. Človekov nadzor se zagotovi z enim ali vsemi naslednjimi ukrepi:

(a) ponudnik ga je določil in vgradil, če je to tehnično izvedljivo, v umetnointeligenčni sistem velikega tveganja, preden je bil dan na trg ali v uporabo;

(b) ponudnik ga je določil pred dajanjem umetnointeligenčnega sistema velikega tveganja na trg ali v uporabo in je primeren za uporabo s strani uporabnika.

4. Ukrepi iz odstavka 3 posameznikom, ki jim je dodeljen človekov nadzor, omogočajo, da glede na okoliščine storijo naslednje:

(a) v celoti razumejo zmogljivosti in omejitve umetnointeligenčnega sistema velikega tveganja ter so sposobni ustrezno spremljati njegovo delovanje, da se lahko čim prej odkrijejo in odpravijo znaki nepravilnosti, motenj in nepričakovanega delovanja;

(b) se zavedajo morebitne težnje po samodejnem zanašanju ali prevelikem zanašanju na izhodne podatke umetnointeligenčnega sistema velikega tveganja („pristranskost zaradi avtomatizacije“), zlasti pri umetnointeligenčnih sistemih velikega tveganja, ki se uporabljajo za zagotavljanje informacij ali priporočil za odločitve, ki jih sprejemajo fizične osebe;

(c) so sposobni pravilno razlagati izhodne podatke umetnointeligenčnega sistema velikega tveganja, zlasti ob upoštevanju značilnosti sistema ter razpoložljivih orodij in metod za razlago;

(d) se lahko v vseh okoliščinah odločijo, da ne bodo uporabljali umetnointeligenčnega sistema velikega tveganja ali da bodo kako drugače

zanemarili, razveljavili ali obrnili izhodne podatke umetnointeligenčnega sistema velikega tveganja;

(e) so sposobni poseči v delovanje umetnointeligenčnega sistema velikega tveganja ali ga prekiniti s tipko „stop“ ali podobnim postopkom.

5. Za umetnointeligenčne sisteme velikega tveganja iz točke 1(a) Priloge III so ukrepi iz odstavka 3 taki, da zagotavljajo, da uporabnik poleg tega ne izvede nobenega dejanja ali ne sprejme nobenega ukrepa ali odločitve na podlagi identifikacije, ki izhaja iz sistema, razen če to preverita in potrdita vsaj dve fizični osebi.

Člen 15

Točnost, robustnost in kibernetska varnost

1. Umetnointeligenčni sistemi velikega tveganja so zasnovani in razviti tako, da glede na predvideni namen dosegajo ustrezno raven točnosti, robustnosti in kibernetske varnosti ter v teh vidikih delujejo dosledno v svojem celotnem življenjskem ciklu.

2. Ravni točnosti in ustrezna merila točnosti umetnointeligenčnih sistemov velikega tveganja se navedejo v priloženih navodilih za uporabo.

3. Umetnointeligenčni sistemi velikega tveganja so odporni na napake, okvare ali neskladnosti, ki se lahko pojavijo v sistemu ali okolju, v katerem sistem deluje, zlasti zaradi njihove interakcije s fizičnimi osebami ali drugimi sistemi.

4. Robustnost umetnointeligenčnih sistemov velikega tveganja se lahko doseže s tehničnimi redundantnimi rešitvami, ki lahko vključujejo rezervne načrte ali načrte varne odpovedi.

5. Umetnointeligenčne sisteme velikega tveganja, ki se po dajanju na trg ali v uporabo še naprej učijo, je treba razviti tako, da se morebitni pristranski izhodni podatki zaradi izhodnih podatkov, ki se uporabljajo kot vhodni podatki za prihodnje operacije („povratne zanke“), ustrezno obravnavajo s primernimi blažilnimi ukrepi.

6. Umetnointeligenčni sistemi velikega tveganja morajo biti odporni na poskuse nepooblaščenih tretjih oseb, da z izkoriščanjem šibkih točk sistema spremenijo njihovo uporabo ali zmogljivost.

Tehnične rešitve, namenjene zagotavljanju kibernetske varnosti umetnointeligenčnih sistemov velikega tveganja, ustrezajo ustreznim okoliščinam in tveganjem.

Tehnične rešitve za odpravljanje šibkih točk, značilnih za umetno inteligenco, po potrebi vključujejo ukrepe za preprečevanje in nadzor napadov, ki poskušajo manipulirati z naborom učnih podatkov („zastrupitev podatkov“), vhodne podatke, katerih namen je povzročiti napako modela („nasprotovalni primer“), ali pomanjkljivosti modela.

POGLAVJE 3

OBVEZNOSTI PONUDNIKOV IN UPORABNIKOV UMETNOINTELIGENČNIH SISTEMOV VELIKEGA TVEGANJA IN DRUGIH STRANK

Člen 16

Obveznosti ponudnikov umetnointeligenčnih sistemov velikega tveganja

Ponudniki umetnointeligenčnih sistemov velikega tveganja:

(a) zagotovijo, da so njihovi umetnointeligenčni sistemi velikega tveganja skladni z zahtevami iz poglavja 2 tega naslova;

(b) imajo vzpostavljen sistem upravljanja kakovosti, skladen s členom 17;

(c) pripravijo tehnično dokumentacijo umetnointeligenčnega sistema velikega tveganja;

(d) kadar je to pod njihovim nadzorom, hranijo dnevnike, ki jih samodejno ustvarijo njihovi umetnointeligenčni sistemi velikega tveganja;

(e) zagotovijo, da umetnointeligenčni sistem velikega tveganja pred dajanjem na trg ali v uporabo opravi ustrezen postopek ugotavljanja skladnosti;

(f) izpolnjujejo obveznosti registracije iz člena 51;

(g) sprejmejo potrebne popravne ukrepe, če umetnointeligenčni sistem velikega tveganja ni skladen z zahtevami iz poglavja 2 tega naslova;

(h) obvestijo pristojne nacionalne organe držav članic, v katerih so dali umetnointeligenčni sistem na voljo ali v uporabo, ter, kadar je to primerno, obvestijo priglašeni organ o neskladnosti in sprejetih popravnih ukrepih;

(i) namestijo oznako CE na svoje umetnointeligenčne sisteme velikega tveganja, da v skladu s členom 49 označijo skladnost s to uredbo;

(j) na zahtevo pristojnega nacionalnega organa dokažejo skladnost umetnointeligenčnega sistema velikega tveganja z zahtevami iz poglavja 2 tega naslova.

Člen 17

Sistem upravljanja kakovosti

1. Ponudniki umetnointeligenčnih sistemov velikega tveganja vzpostavijo sistem upravljanja kakovosti, ki zagotavlja skladnost s to uredbo. Ta sistem se sistematično in urejeno dokumentira v obliki pisnih politik, postopkov in navodil ter vključuje vsaj naslednje vidike:

   (a) strategijo za skladnost z zakonodajo, tudi skladnost s postopki za ugotavljanje skladnosti in postopki za upravljanje sprememb umetnointeligenčnega sistema velikega tveganja;

   (b) tehnike, postopke in sistematične ukrepe, ki se uporabljajo za zasnovo, nadzor zasnove in preverjanje zasnove umetnointeligenčnega sistema velikega tveganja;

(c) tehnike, postopke in sistematične ukrepe, ki se uporabljajo za razvoj, nadzor kakovosti in zagotavljanje kakovosti umetnointeligenčnega sistema velikega tveganja;

(d) postopke pregledovanja, testiranja in postopke za potrditev, ki se izvedejo pred razvojem umetnointeligenčnega sistema velikega tveganja, med njim in po njem, ter pogostost njihovega izvajanja;

(e) tehnične specifikacije, vključno s standardi, ki jih je treba uporabiti, in, kadar se ustrezni harmonizirani standardi ne uporabljajo v celoti, sredstva, ki se uporabljajo za zagotovitev, da je umetnointeligenčni sistem velikega tveganja skladen z zahtevami iz poglavja 2 tega naslova;

(f) sisteme in postopke za upravljanje podatkov, vključno z zbiranjem podatkov, analizo podatkov, označevanjem podatkov, shranjevanjem podatkov, filtriranjem podatkov, podatkovnim rudarjenjem, združevanjem podatkov, hrambo podatkov ter vsemi drugimi postopki v zvezi s podatki, ki se izvajajo pred dajanjem na trg ali v uporabo in za namene dajanja na trg ali v uporabo umetnointeligenčnih sistemov velikega tveganja;

(g) sistem obvladovanja tveganja iz člena 9;

(h) vzpostavitev, izvajanje in vzdrževanje sistema za spremljanje po dajanju na trg v skladu s členom 61;

(i) postopke v zvezi s poročanjem o hudih incidentih in okvarah v skladu s členom 62;

(j) vodenje komunikacije s pristojnimi nacionalnimi organi, pristojnimi organi, vključno s sektorskimi, ki zagotavljajo ali podpirajo dostop do podatkov, priglašenimi organi, drugimi operaterji, strankami ali drugimi zainteresiranimi stranmi;

(k) sisteme in postopke za vodenje evidenc vse ustrezne dokumentacije in informacij;

(l) upravljanje virov, vključno z ukrepi, povezanimi z zanesljivostjo oskrbe;

(m) okvir odgovornosti, ki določa odgovornosti vodstva in drugega osebja v zvezi z vsemi vidiki iz tega odstavka.

2. Izvajanje vidikov iz odstavka 1 je sorazmerno z velikostjo organizacije ponudnika.

3. Za ponudnike, ki so kreditne institucije, ki jih ureja Direktiva 2013/36/EU, se šteje, da je obveznost vzpostavitve sistema upravljanja kakovosti izpolnjena z upoštevanjem pravil o ureditvah, procesih in mehanizmih notranjega upravljanja v skladu s členom 74 navedene direktive. V tem okviru se upoštevajo vsi harmonizirani standardi iz člena 40 te uredbe.

Člen 18

Obveznost priprave tehnične dokumentacije

1. Ponudniki umetnointeligenčnih sistemov velikega tveganja pripravijo tehnično dokumentacijo iz člena 11 v skladu s Prilogo IV.

2. Ponudniki, ki so kreditne institucije, ki jih ureja Direktiva 2013/36/EU, hranijo tehnično dokumentacijo kot del dokumentacije o ureditvah, procesih in mehanizmih notranjega upravljanja v skladu s členom 74 navedene direktive.

Člen 19

Ugotavljanje skladnosti

1. Ponudniki umetnointeligenčnih sistemov velikega tveganja zagotovijo, da njihovi sistemi pred dajanjem na trg ali v uporabo opravijo ustrezen postopek ugotavljanja skladnosti v skladu s členom 43. Kadar je bila po navedenem ugotavljanju skladnosti dokazana skladnost umetnointeligenčnih sistemov z zahtevami iz poglavja 2 tega naslova, ponudniki pripravijo izjavo EU o skladnosti v skladu s členom 48 in namestijo oznako skladnosti v skladu s členom 49.

2. Za umetnointeligenčne sisteme velikega tveganja iz točke 5(b) Priloge III, ki jih dajejo na trg ali v uporabo ponudniki, ki so kreditne institucije, urejene z Direktivo 2013/36/EU, se ugotavljanje skladnosti izvede kot del postopka iz členov 97 do 101 navedene direktive.

Člen 20

Samodejno ustvarjeni dnevniki

1. Ponudniki umetnointeligenčnih sistemov velikega tveganja vodijo dnevnike, ki jih samodejno ustvarijo njihovi umetnointeligenčni sistemi velikega tveganja, če so ti dnevniki pod njihovim nadzorom na podlagi pogodbenega dogovora z uporabnikom ali drugače po zakonu. Dnevniki se hranijo za obdobje, ki je primerno glede na predvideni namen umetnointeligenčnega sistema velikega tveganja in veljavne pravne obveznosti v skladu s pravom Unije ali nacionalnim pravom.

2. Ponudniki, ki so kreditne institucije, urejene z Direktivo 2013/36/EU, vodijo dnevnike, ki jih samodejno ustvarijo njihovi umetnointeligenčni sistemi velikega tveganja, kot del dokumentacije v skladu s členom 74 navedene direktive.

Člen 21

Popravni ukrepi

Ponudniki umetnointeligenčnih sistemov velikega tveganja, ki menijo ali utemeljeno domnevajo, da umetnointeligenčni sistem velikega tveganja, ki so ga dali na trg ali v uporabo, ni v skladu s to uredbo, nemudoma sprejmejo potrebne popravne ukrepe, da zagotovijo skladnost sistema ali pa ga po potrebi umaknejo ali prekličejo. O tem ustrezno obvestijo distributerje zadevnega umetnointeligenčnega sistema velikega tveganja ter po potrebi pooblaščenega zastopnika in uvoznike.

Člen 22

Dolžnost obveščanja

Kadar umetnointeligenčni sistem velikega tveganja predstavlja tveganje v smislu člena 65(1) in je to tveganje ponudniku sistema znano, ta ponudnik nemudoma obvesti pristojne nacionalne organe držav članic, v katerih je dal sistem na voljo, ter, kadar je to primerno, priglašeni organ, ki je izdal potrdilo za umetnointeligenčni sistem velikega tveganja, zlasti o neskladnosti in vseh sprejetih popravnih ukrepih.

Člen 23

Sodelovanje s pristojnimi organi

Ponudniki umetnointeligenčnih sistemov velikega tveganja na zahtevo pristojnega nacionalnega organa zagotovijo temu organu vse informacije in dokumentacijo, potrebne za dokazovanje skladnosti umetnointeligenčnega sistema velikega tveganja z zahtevami iz poglavja 2 tega naslova, v uradnem jeziku Unije, ki ga določi zadevna država članica. Ponudniki na podlagi obrazložene zahteve pristojnega nacionalnega organa temu organu omogočijo tudi dostop do dnevnikov, ki jih samodejno ustvari umetnointeligenčni sistem velikega tveganja, če so ti dnevniki pod njihovim nadzorom na podlagi pogodbenega dogovora z uporabnikom ali drugače po zakonu.

Člen 24

Obveznosti proizvajalcev proizvodov

Kadar je umetnointeligenčni sistem velikega tveganja, povezan s proizvodi, za katere se uporabljajo pravni akti iz oddelka A Priloge II, dan na trg ali v uporabo skupaj s proizvodom, proizvedenim v skladu s temi pravnimi akti in pod imenom proizvajalca proizvoda, proizvajalec proizvoda prevzame odgovornost za skladnost umetnointeligenčnega sistema s to uredbo ter ima, kar zadeva umetnointeligenčni sistem, enake obveznosti, kot jih ta uredba nalaga ponudniku.

Člen 25

Pooblaščeni zastopniki

1. Kadar ni mogoče ugotoviti, kdo je uvoznik, ponudniki s sedežem zunaj Unije pred dajanjem svojih sistemov na trg Unije s pisnim pooblastilom imenujejo pooblaščenega zastopnika s sedežem v Uniji.

2. Pooblaščeni zastopnik opravlja naloge, določene v pooblastilu, ki ga prejme od ponudnika. Pooblastilo omogoča pooblaščenemu zastopniku, da opravlja naslednje naloge:

   (a) hrani izvod izjave EU o skladnosti in tehnične dokumentacije, ki je na voljo pristojnim nacionalnim organom in nacionalnim organom iz člena 63(7);

   (b) pristojnemu nacionalnemu organu na podlagi obrazložene zahteve zagotovi vse informacije in dokumentacijo, potrebne za dokazovanje skladnosti umetnointeligenčnega sistema velikega tveganja z zahtevami iz poglavja 2 tega

naslova, vključno z dostopom do dnevnikov, ki jih samodejno ustvari umetnointeligenčni sistem velikega tveganja, če so ti dnevniki pod nadzorom ponudnika na podlagi pogodbenega dogovora z uporabnikom ali drugače po zakonu;

(c) na podlagi obrazložene zahteve sodeluje s pristojnimi nacionalnimi organi pri vseh ukrepih, ki jih slednji sprejmejo v zvezi z umetnointeligenčnim sistemom velikega tveganja.

Člen 26

Obveznosti uvoznikov

1. Pred dajanjem umetnointeligenčnega sistema velikega tveganja na trg uvozniki tega sistema zagotovijo:

   (a) da je ponudnik umetnointeligenčnega sistema velikega tveganja izvedel ustrezen postopek ugotavljanja skladnosti;

   (b) da je ponudnik pripravil tehnično dokumentacijo v skladu s Prilogo IV;

   (c) da je sistem opremljen z zahtevano oznako skladnosti ter mu je priložena zahtevana dokumentacija in navodila za uporabo.

2. Kadar uvoznik meni ali utemeljeno domneva, da umetnointeligenčni sistem velikega tveganja ni skladen s to uredbo, tega sistema ne da na trg, dokler ni zagotovljena skladnost tega umetnointeligenčnega sistema. Kadar umetnointeligenčni sistem velikega tveganja predstavlja tveganje v smislu člena 65(1), uvoznik o tem obvesti ponudnika umetnointeligenčnega sistema in organe za nadzor trga.

3. Uvozniki navedejo svoje ime, registrirano trgovsko ime ali registrirano blagovno znamko in naslov, na katerem so dosegljivi, v umetnointeligenčnem sistemu velikega tveganja ali, kadar to ni mogoče, na embalaži ali spremni dokumentaciji, kot je ustrezno.

4. Uvozniki zagotovijo, da v času, ko so odgovorni za umetnointeligenčni sistem velikega tveganja, pogoji skladiščenja ali prevoza ne ogrožajo skladnosti sistema z zahtevami iz poglavja 2 tega naslova, kadar je to primerno.

5. Uvozniki pristojnim nacionalnim organom na podlagi obrazložene zahteve zagotovijo vse informacije in dokumentacijo, potrebne za dokazovanje skladnosti umetnointeligenčnega sistema velikega tveganja z zahtevami iz poglavja 2 tega naslova, v jeziku, ki ga ta pristojni nacionalni organ zlahka razume, vključno z dostopom do dnevnikov, ki jih samodejno ustvari umetnointeligenčni sistem velikega tveganja, če so ti dnevniki pod nadzorom ponudnika na podlagi pogodbenega dogovora z uporabnikom ali drugače po zakonu. S temi organi sodelujejo tudi pri vseh ukrepih, ki jih pristojni nacionalni organ sprejme v zvezi s tem sistemom.

Člen 27

Obveznosti distributerjev

1. Preden omogočijo dostopnost umetnointeligenčnega sistema velikega tveganja na trgu, distributerji preverijo, ali je umetnointeligenčni sistem velikega tveganja opremljen z zahtevano oznako skladnosti, ali mu je priložena zahtevana

dokumentacija in navodila za uporabo ter ali je ponudnik oziroma uvoznik sistema izpolnil obveznosti iz te uredbe.

2. Kadar distributer meni ali utemeljeno domneva, da umetnointeligenčni sistem velikega tveganja ni skladen z zahtevami iz poglavja 2 tega naslova, za umetnointeligenčni sistem velikega tveganja ne omogoči dostopnosti na trgu, dokler ni zagotovljena skladnost tega sistema z navedenimi zahtevami. Kadar sistem predstavlja tveganje v smislu člena 65(1), distributer o tem obvesti ponudnika oziroma uvoznika sistema.

3. Distributerji zagotovijo, da v času, ko so odgovorni za umetnointeligenčni sistem velikega tveganja, pogoji skladiščenja ali prevoza ne ogrožajo skladnosti tega sistema z zahtevami iz poglavja 2 tega naslova, kadar je to primerno.

4. Distributer, ki meni ali utemeljeno domneva, da umetnointeligenčni sistem velikega tveganja, za katerega je omogočil dostopnost na trgu, ni skladen z zahtevami iz poglavja 2 tega naslova, sprejme popravne ukrepe, potrebne za uskladitev tega sistema z navedenimi zahtevami, ga umakne ali prekliče ali zagotovi, da te popravne ukrepe sprejme ponudnik, uvoznik ali kateri koli zadevni operater, kakor je ustrezno t. Kadar umetnointeligenčni sistem velikega tveganja predstavlja tveganje v smislu člena 65(1), distributer o tem nemudoma obvesti pristojne nacionalne organe držav članic, v katerih je dal proizvod na voljo, ter navede podrobnosti, zlasti o neskladnosti in vseh sprejetih popravnih ukrepih.

5. Distributerji umetnointeligenčnih sistemov velikega tveganja pristojnemu nacionalnemu organu na podlagi obrazložene zahteve zagotovijo vse informacije in dokumentacijo, potrebne za dokazovanje skladnosti umetnointeligenčnega sistema velikega tveganja z zahtevami iz poglavja 2 tega naslova. Distributerji s tem pristojnim nacionalnim organom sodelujejo tudi pri vseh ukrepih, ki jih sprejme ta organ.

Člen 28Obveznosti distributerjev, uvoznikov, uporabnikov ali katere koli druge tretje osebe

1. Vsak distributer, uvoznik, uporabnik ali druga tretja oseba se za namene te uredbe šteje za ponudnika in zanj veljajo obveznosti ponudnika iz člena 16 v kateri koli od naslednjih okoliščin:

   (a) umetnointeligenčni sistem velikega tveganja dajo na trg ali v uporabo pod svojim imenom ali blagovno znamko;

   (b) spremenijo predvideni namen umetnointeligenčnega sistema velikega tveganja, ki je že dan na trg ali v uporabo;

   (c) bistveno spremenijo umetnointeligenčni sistem velikega tveganja.

2. Kadar nastopijo okoliščine iz točke (b) ali (c) odstavka 1, se ponudnik, ki je prvotno dal umetnointeligenčni sistem velikega tveganja na trg ali v uporabo, za namene te uredbe ne šteje več za ponudnika.

Člen 29Obveznosti uporabnikov umetnointeligenčnih sistemov velikega tveganja

1. Uporabniki umetnointeligenčnih sistemov velikega tveganja uporabljajo take sisteme v skladu s priloženimi navodili za uporabo, v skladu z odstavkoma 2 in 5.

2. Obveznosti iz odstavka 1 ne posegajo v druge obveznosti uporabnikov v skladu s pravom Unije ali nacionalnim pravom ter v pravico uporabnika, da organizira lastna

sredstva in dejavnosti za izvajanje ukrepov za človekov nadzor, ki jih navede ponudnik.

3. Brez poseganja v odstavek 1 uporabnik, kolikor izvaja nadzor nad vhodnimi podatki, zagotovi, da so vhodni podatki ustrezni glede na predvideni namen umetnointeligenčnega sistema velikega tveganja.

4. Uporabniki spremljajo delovanje umetnointeligenčnega sistema velikega tveganja na podlagi navodil za uporabo. Kadar imajo razloge za domnevo, da lahko uporaba v skladu z navodili za uporabo povzroči, da umetnointeligenčni sistem predstavlja tveganje v smislu člena 65(1), o tem obvestijo ponudnika ali distributerja in začasno ustavijo uporabo sistema. Ponudnika ali distributerja obvestijo tudi, ko ugotovijo kakršen koli hud incident ali kakršno koli okvaro v smislu člena 62 in prekinejo uporabo umetnointeligenčnega sistema. Če uporabnik ne more priti v stik s ponudnikom, se smiselno uporablja člen 62.

5. Za uporabnike, ki so kreditne institucije, ki jih ureja Direktiva 2013/36/EU, se šteje, da je obveznost spremljanja iz prvega pododstavka izpolnjena z upoštevanjem pravil o ureditvah, procesih in mehanizmih notranjega upravljanja v skladu s členom 74 navedene direktive.

6. Uporabniki umetnointeligenčnih sistemov velikega tveganja vodijo dnevnike, ki jih samodejno ustvari ta umetnointeligenčni sistem velikega tveganja, če so ti dnevniki pod njihovim nadzorom. Dnevniki se hranijo za obdobje, ki je primerno glede na predvideni namen umetnointeligenčnega sistema velikega tveganja in veljavne pravne obveznosti v skladu s pravom Unije ali nacionalnim pravom.

   Uporabniki, ki so kreditne institucije, ki jih ureja Direktiva 2013/36/EU, hranijo dnevnike kot del dokumentacije o ureditvah, procesih in mehanizmih notranjega upravljanja v skladu s členom 74 navedene direktive.

7. Uporabniki umetnointeligenčnih sistemov velikega tveganja uporabijo informacije iz člena 13, da izpolnijo svojo obveznost izvedbe ocene učinka v zvezi z varstvom podatkov v skladu s členom 35 Uredbe (EU) 2016/679 ali členom 27 Direktive (EU) 2016/680, kadar je to primerno.

POGLAVJE 4

PRIGLASITVENI IN PRIGLAŠENI ORGANI

Člen 30

Priglasitveni organi

1. Vsaka država članica imenuje ali vzpostavi priglasitveni organ, odgovoren za vzpostavitev in izvajanje potrebnih postopkov za ocenjevanje, imenovanje in priglasitev organov za ugotavljanje skladnosti ter za njihovo spremljanje.

2. Države članice lahko za priglasitveni organ imenujejo nacionalni akreditacijski organ iz Uredbe (ES) št. 765/2008.

3. Priglasitveni organi se ustanovijo, organizirajo in delujejo tako, da ne pride do navzkrižja interesov z organi za ugotavljanje skladnosti ter da se zaščitita objektivnost in nepristranskost njihovih dejavnosti.

4. Priglasitveni organi so organizirani tako, da odločitve v zvezi s priglasitvijo organov za ugotavljanje skladnosti sprejemajo pristojne osebe, ki niso tiste, ki so izvedle ocenjevanje teh organov.

5. Priglasitveni organi ne ponujajo ali izvajajo nobenih dejavnosti, ki jih izvajajo organi za ugotavljanje skladnosti, ali kakršnih koli storitev svetovanja na komercialni ali konkurenčni podlagi.

6. Priglasitveni organi zagotavljajo zaupnost pridobljenih informacij.

7. Priglasitveni organi imajo na voljo zadostno število strokovnega osebja za pravilno izvajanje svojih nalog.

8. Priglasitveni organi zagotovijo, da se ugotavljanje skladnosti izvaja sorazmerno, pri čemer se izognejo nepotrebnim bremenom za ponudnike, ter da priglašeni organi izvajajo svoje dejavnosti ob ustreznem upoštevanju velikosti podjetja, sektorja, v katerem deluje, njegove strukture in stopnje zapletenosti zadevnega umetnointeligenčnega sistema.

Člen 31

Vloga organa za ugotavljanje skladnosti za priglasitev

1. Organi za ugotavljanje skladnosti predložijo vlogo za priglasitev priglasitvenemu organu države članice, v kateri imajo sedež.

2. Vlogi za priglasitev se priložijo opis dejavnosti ugotavljanja skladnosti, opis modula ali modulov za ugotavljanje skladnosti in opis umetnointeligenčnih tehnologij, za katere organ za ugotavljanje skladnosti trdi, da je pristojen, ter morebitno potrdilo o akreditaciji, ki ga izda nacionalni akreditacijski organ, ki potrjuje, da organ za ugotavljanje skladnosti izpolnjuje zahteve iz člena 33. Doda se vsak veljaven dokument v zvezi z obstoječimi imenovanji priglašenega organa vlagatelja v skladu s katero koli drugo harmonizacijsko zakonodajo Unije.

3. Kadar zadevni organ za ugotavljanje skladnosti ne more zagotoviti potrdila o akreditaciji, priglasitvenemu organu predloži vsa dokumentarna dokazila, potrebna za preverjanje, priznavanje in redno spremljanje njegove skladnosti z zahtevami iz člena 33. Za priglašene organe, imenovane v skladu s katero koli drugo harmonizacijsko zakonodajo Unije, se lahko vsi dokumenti in potrdila v zvezi s temi imenovanji po potrebi uporabijo za podporo njihovemu postopku imenovanja v skladu s to uredbo.

Člen 32

Postopek priglasitve

1. Priglasitveni organi lahko priglasijo samo tiste organe za ugotavljanje skladnosti, ki izpolnjujejo zahteve iz člena 33.

2. Priglasitveni organi obveščajo Komisijo in ostale države članice z uporabo elektronskega orodja za priglasitev, ki ga je razvila in ga upravlja Komisija.

3. Priglasitev vključuje vse podrobnosti o dejavnostih za ugotavljanje skladnosti, modul ali module za ugotavljanje skladnosti in zadevne umetnointeligenčne tehnologije.

4. Zadevni organ za ugotavljanje skladnosti lahko izvaja dejavnosti priglašenega organa le, če Komisija ali druge države članice ne vložijo ugovora v enem mesecu od priglasitve.

5. Priglasitveni organi obvestijo Komisijo in druge države članice o vseh poznejših zadevnih spremembah priglasitve.

Člen 33

Priglašeni organi

1. Priglašeni organi preverijo skladnost umetnointeligenčnega sistema velikega tveganja v skladu s postopki ugotavljanja skladnosti iz člena 43.

2. Priglašeni organi izpolnjujejo organizacijske zahteve, zahteve glede upravljanja kakovosti, virov in procesov, potrebnih za izpolnjevanje njihovih nalog.

3. Organizacijska struktura, dodelitev pristojnosti, poročanje in delovanje priglašenih organov so taki, da zagotavljajo zaupanje v učinkovitost priglašenih organov in v rezultate dejavnosti ugotavljanja skladnosti, ki jih izvajajo.

4. Priglašeni organi so neodvisni od ponudnika umetnointeligenčnega sistema velikega tveganja, v zvezi s katerim izvajajo dejavnosti ugotavljanja skladnosti. Priglašeni organi so neodvisni tudi od vseh drugih operaterjev, ki imajo gospodarski interes pri ocenjevanem umetnointeligenčnem sistemu velikega tveganja, in od vseh konkurentov ponudnika.

5. Priglašeni organi s svojo organizacijo in delovanjem zagotavljajo neodvisnost, objektivnost in nepristranskost pri izvajanju svojih dejavnosti. Priglašeni organi dokumentirajo in izvajajo strukturo in postopke za zagotovitev nepristranskosti ter za spodbujanje in uporabo načel nepristranskosti v svoji organizaciji, med osebjem in v dejavnostih ocenjevanja.

6. Priglašeni organi vzpostavijo dokumentirane postopke za zagotovitev, da njihovo osebje, odbori, odvisne družbe, podizvajalci, kateri koli povezan organ ali osebje zunanjih organov spoštuje zaupnost informacij, pridobljenih med opravljanjem dejavnosti ugotavljanja skladnosti, razen kadar njihovo razkritje zahteva zakon. Osebje priglašenih organov je zavezano k varovanju poklicnih skrivnosti v zvezi z vsemi informacijami, pridobljenimi med izvajanjem nalog v skladu s to uredbo, razen v zvezi s priglasitvenimi organi države članice, v kateri izvajajo svoje dejavnosti.

7. Priglašeni organi imajo postopke za izvajanje dejavnosti, pri katerih se ustrezno upoštevajo velikost podjetja, sektor, v katerem deluje, njegova struktura in stopnja zahtevnosti zadevnega umetnointeligenčnega sistema.

8. Priglašeni organi sklenejo zavarovanje odgovornosti za svoje dejavnosti ugotavljanja skladnosti, razen če odgovornost prevzame zadevna država članica v skladu z nacionalnim pravom ali če je ta država članica neposredno pristojna za ugotavljanje skladnosti.

9. Priglašeni organi so sposobni izvajati vse naloge, ki jim pripadajo v skladu s to uredbo, z najvišjo stopnjo profesionalne integritete in potrebnimi kompetencami na določenem področju, ne glede na to, ali navedene naloge izvajajo priglašeni organi sami ali se izvajajo v njihovem imenu in pod njihovo odgovornostjo.

10. Priglašeni organi imajo zadostne notranje kompetence, da lahko učinkovito ocenijo naloge, ki jih opravljajo zunanje stranke v njihovem imenu. V ta namen ima priglašeni organ vedno in za vsak postopek ugotavljanja skladnosti ter vsako vrsto umetnointeligenčnega sistema velikega tveganja, v zvezi s katerim so bili imenovani, na voljo dovolj upravnega, tehničnega in znanstvenega osebja, ki ima izkušnje in znanje v zvezi z ustreznimi umetnointeligenčnimi tehnologijami, podatki in računalniško obdelavo podatkov ter zahtevami iz poglavja 2 tega naslova.

11. Priglašeni organi sodelujejo v usklajevalnih dejavnostih iz člena 38. Sodelujejo tudi neposredno ali so zastopani v evropskih organizacijah za standardizacijo ali zagotavljajo, da so seznanjeni in na tekočem v zvezi z ustreznimi standardi.

12. Priglašeni organi dajo priglasitvenemu organu iz člena 30 na voljo ter mu na zahtevo predložijo vso zadevno dokumentacijo, vključno z dokumentacijo ponudnikov, da mu omogočijo izvajanje dejavnosti ocenjevanja, imenovanja, priglasitve, spremljanja in nadzora ter da se olajša ocenjevanje, opisano v tem poglavju.

Člen 34

Odvisne družbe in podizvajalci priglašenih organov

1. Kadar priglašeni organ za določene naloge, povezane z ugotavljanjem skladnosti, sklene pogodbo s podizvajalcem ali jih prenese na odvisno družbo, zagotovi, da podizvajalec ali odvisna družba izpolnjuje zahteve iz člena 33, ter o tem ustrezno obvesti priglasitveni organ.

2. Priglašeni organi so v celoti odgovorni za naloge, ki jih izvajajo podizvajalci ali odvisne družbe, ne glede na to, kje imajo ti podizvajalci ali te odvisne družbe sedež.

3. Dejavnosti se lahko prenesejo na podizvajalca ali odvisno družbo samo, če ponudnik s tem soglaša.

4. Priglašeni organi hranijo ter omogočajo priglasitvenemu organu dostop do zadevnih dokumentov v zvezi z ocenjevanjem usposobljenosti podizvajalca ali odvisne družbe ter nalogami, ki jih izvaja v skladu s to uredbo.

Člen 35

Identifikacijske številke in seznami priglašenih organov, imenovanih v skladu s to uredbo

1. Komisija priglašenim organom dodeli identifikacijsko številko. Vsakemu organu dodeli samo eno številko, tudi kadar je organ priglašen v skladu z več akti Unije.

2. Komisija javno objavi seznam organov, priglašenih v skladu s to uredbo, vključno z identifikacijskimi številkami, ki so jim bile dodeljene, in dejavnostmi, za katere so bili priglašeni. Komisija poskrbi za posodabljanje seznama.

Člen 36

Spremembe priglasitev

1. Kadar priglasitveni organ sumi ali je obveščen, da priglašeni organ ne izpolnjuje več zahtev iz člena 33 ali da ne izpolnjuje svojih obveznosti, zadevo brez odlašanja razišče z največjo skrbnostjo. V tem okviru obvesti zadevni priglašeni organ o

vloženih ugovorih in mu omogoči, da izrazi svoja stališča. Kadar priglasitveni organ ugotovi, da priglašeni organ, ki je predmet preiskave, ne izpolnjuje več zahtev iz člena 33 ali da ne izpolnjuje svojih obveznosti, priglasitveni organ omeji, začasno prekliče ali umakne priglasitev, kot je primerno glede na resnost kršitve. O tem tudi nemudoma ustrezno obvesti Komisijo in druge države članice.

2. V primeru omejitve, začasnega preklica ali umika priglasitve ali če je priglašeni organ prenehal z dejavnostjo, priglasitveni organ izvede ustrezne ukrepe za zagotovitev, da gradivo tega priglašenega organa prevzame drug priglašeni organ ali da je na voljo pristojnim priglasitvenim organom na njihovo zahtevo.

Člen 37

Izpodbijanje usposobljenosti priglašenih organov

1. Komisija po potrebi razišče vse primere, v katerih obstajajo razlogi za dvom, ali priglašeni organ izpolnjuje zahteve iz člena 33.

2. Priglasitveni organ Komisiji na zahtevo predloži vse ustrezne informacije v zvezi s priglasitvijo zadevnega priglašenega organa.

3. Komisija zagotovi, da se vse zaupne informacije, ki jih pridobi med preiskavami v skladu s tem členom, obravnavajo zaupno.

4. Kadar Komisija ugotovi, da priglašeni organ ne izpolnjuje ali ne izpolnjuje več zahtev iz člena 33, sprejme utemeljen sklep, s katerim zahteva od države članice priglasiteljice, da izvede potrebne popravne ukrepe, vključno z umikom priglasitve, če je to potrebno. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 74(2).

Člen 38

Usklajevanje priglašenih organov

1. Komisija zagotovi, da se v zvezi s področji, ki jih zajema ta uredba, vzpostavi ustrezno usklajevanje in sodelovanje med priglašenimi organi, dejavnimi v postopkih ugotavljanja skladnosti umetnointeligenčnih sistemov v skladu s to uredbo, in da pravilno delujejo v obliki sektorske skupine priglašenih organov**.**

2. Države članice zagotovijo, da organi, ki jih priglasijo, sodelujejo pri delu te skupine, neposredno ali preko pooblaščenih predstavnikov.

Člen 39

Organi za ugotavljanje skladnosti iz tretjih držav

Organi za ugotavljanje skladnosti, ustanovljeni v skladu s pravom tretje države, s katero je Unija sklenila sporazum, so lahko pooblaščeni za izvajanje dejavnosti priglašenih organov v skladu s to uredbo.

POGLAVJE 5

STANDARDI, UGOTAVLJANJE SKLADNOSTI, POTRDILA, REGISTRACIJA

Člen 40

Harmonizirani standardi

Za umetnointeligenčne sisteme velikega tveganja, ki so v skladu s harmoniziranimi standardi ali njihovimi deli, katerih sklici so bili objavljeni v Uradnem listu Evropske unije, se domneva, da so skladni z zahtevami iz poglavja 2 tega naslova, kolikor ti standardi zajemajo te zahteve.

Člen 41

Skupne specifikacije

1. Kadar harmonizirani standardi iz člena 40 ne obstajajo ali kadar Komisija meni, da ustrezni harmonizirani standardi ne zadostujejo ali da je treba obravnavati posebne pomisleke glede varnosti ali temeljnih pravic, lahko Komisija z izvedbenimi akti sprejme skupne specifikacije v zvezi z zahtevami iz poglavja 2 tega naslova. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 74(2).
2. Komisija pri pripravi skupnih specifikacij iz odstavka 1 zbere mnenja ustreznih organov ali strokovnih skupin, ustanovljenih v skladu z ustreznim sektorskim pravom Unije.
3. Za umetnointeligenčne sisteme velikega tveganja, ki so v skladu s skupnimi specifikacijami iz odstavka 1, se domneva, da so skladni z zahtevami iz poglavja 2 tega naslova, kolikor te skupne specifikacije zajemajo te zahteve.
4. Kadar ponudniki ne izpolnjujejo skupnih specifikacij iz odstavka 1, ustrezno utemeljijo, da so sprejeli tehnične rešitve, ki so jim vsaj enakovredne.

Člen 42

Domneva o skladnosti z nekaterimi zahtevami

1. Ob upoštevanju predvidenega namena se za umetnointeligenčne sisteme velikega tveganja, ki so bili naučeni in testirani na podlagi podatkov o posebnem geografskem, vedenjskem in funkcionalnem okolju, v katerem naj bi se uporabljali, domneva, da izpolnjujejo zahteve iz člena 10(4).
2. Za umetnointeligenčne sisteme velikega tveganja, ki so prejeli potrdilo ali za katere je bila izdana izjava o skladnosti v okviru certifikacijske sheme za kibernetsko varnost v skladu z Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta[63] in sklici na katere so bili objavljeni v Uradnem listu Evropske unije, se domneva, da so

[63] Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 1).

skladni z zahtevami za kibernetsko varnost iz člena 15 te uredbe, kolikor potrdilo o kibernetski varnosti ali izjava o skladnosti ali njuni deli zajemajo te zahteve.

Člen 43

Ugotavljanje skladnosti

1. Za umetnointeligenčne sisteme velikega tveganja iz točke 1 Priloge III, pri katerih je ponudnik pri dokazovanju skladnosti umetnointeligenčnega sistema velikega tveganja z zahtevami iz poglavja 2 tega naslova uporabil harmonizirane standarde iz člena 40 ali, kadar je to primerno, skupne specifikacije iz člena 41, uporabi enega od naslednjih postopkov:

   (a) postopek ugotavljanja skladnosti na podlagi notranje kontrole iz Priloge VI;

   (b) postopek ugotavljanja skladnosti na podlagi ocenjevanja sistema upravljanja kakovosti in ocenjevanja tehnične dokumentacije s sodelovanjem priglašenega organa iz Priloge VII.

   Kadar ponudnik pri dokazovanju skladnosti umetnointeligenčnega sistema velikega tveganja z zahtevami iz poglavja 2 tega naslova ni uporabil harmoniziranih standardov iz člena 40 ali jih je uporabil le delno ali kadar taki harmonizirani standardi ne obstajajo in skupne specifikacije iz člena 41 niso na voljo, uporabi postopek ugotavljanja skladnosti iz Priloge VII.

   Za namen postopka ugotavljanja skladnosti iz Priloge VII lahko ponudnik izbere katerega koli od priglašenih organov. Kadar pa naj bi sistem dali v uporabo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organi, pristojni za priseljevanje, ali azilni organi ter institucije, organi ali agencije EU, kot priglašeni organ deluje organ za nadzor trga iz člena 63(5) ali (6), kot je ustrezno.

2. Za umetnointeligenčne sisteme velikega tveganja iz točk 2 do 8 Priloge III ponudniki upoštevajo postopek ugotavljanja skladnosti na podlagi notranje kontrole iz Priloge VI, ki ne predvideva sodelovanja priglašenega organa. Za umetnointeligenčne sisteme velikega tveganja iz točke 5(b) Priloge III, ki jih dajejo na trg ali v uporabo kreditne institucije, urejene z Direktivo 2013/36/EU, se ugotavljanje skladnosti izvede kot del postopka iz členov 97 do 101 navedene direktive.

3. Za umetnointeligenčne sisteme velikega tveganja, za katere se uporabljajo pravni akti iz oddelka A Priloge II, ponudnik upošteva ustrezno ugotavljanje skladnosti, kot se zahteva v navedenih pravnih aktih. Zahteve iz poglavja 2 tega naslova se uporabljajo za te umetnointeligenčne sisteme velikega tveganja in so del te ocene. Uporabljajo se tudi točke 4.3, 4.4, 4.5 in peti odstavek točke 4.6 Priloge VII.

   Za namene te ocene imajo priglašeni organi, ki so priglašeni na podlagi teh pravnih aktov, pravico nadzorovati skladnost umetnointeligenčnih sistemov velikega tveganja z zahtevami iz poglavja 2 tega naslova, če je bila skladnost teh priglašenih organov z zahtevami iz člena 33(4), (9) in (10) ocenjena v okviru priglasitvenega postopka v skladu s temi pravnimi akti.

   Kadar pravni akti iz oddelka A Priloge II proizvajalcu proizvoda omogočajo, da se odloči za izvzetje iz ugotavljanja skladnosti s strani tretje osebe, pod pogojem, da je ta proizvajalec uporabil vse harmonizirane standarde, ki zajemajo vse ustrezne zahteve, lahko ta proizvajalec uporabi to možnost le, če je uporabil harmonizirane

standarde ali, kadar je to primerno, skupne specifikacije iz člena 41, ki zajemajo zahteve iz poglavja 2 tega naslova.

4. Pri umetnointeligenčnih sistemih velikega tveganja se opravi nov postopek ugotavljanja skladnosti, kadar koli so bistveno spremenjeni, ne glede na to, ali je spremenjeni sistem namenjen nadaljnji distribuciji ali ga še naprej uporablja sedanji uporabnik.

   Za umetnointeligenčne sisteme velikega tveganja, ki se po dajanju na trg ali v uporabo še naprej učijo, spremembe umetnointeligenčnega sistema velikega tveganja in njegovega delovanja, ki jih je ponudnik vnaprej določil ob začetnem ugotavljanju skladnosti in so del informacij iz tehnične dokumentacije iz točke 2(f) Priloge IV, ne pomenijo bistvene spremembe.

5. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 73 za posodobitev prilog VI in VII za uvedbo elementov postopkov ugotavljanja skladnosti, ki postanejo potrebni zaradi tehničnega napredka.

6. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov za spremembo odstavkov 1 in 2, da se za umetnointeligenčne sisteme velikega tveganja iz točk 2 do 8 Priloge III uvede postopek ugotavljanja skladnosti iz Priloge VII ali njenih delov. Komisija sprejme take delegirane akte ob upoštevanju učinkovitosti postopka ugotavljanja skladnosti na podlagi notranje kontrole iz Priloge VI pri preprečevanju ali zmanjševanju tveganj za zdravje in varnost ter varstva temeljnih pravic, ki jih predstavljajo taki sistemi, ter razpoložljivosti ustreznih zmogljivosti in virov med priglašenimi organi.

Člen 44

Potrdila

1. Potrdila, ki jih izdajo priglašeni organi v skladu s Prilogo VII, so pripravljena v uradnem jeziku Unije, ki ga določi država članica, v kateri je sedež priglašenega organa, ali v uradnem jeziku Unije, sicer sprejemljivem za priglašeni organ.

2. Potrdila so veljavna za navedeno obdobje, ki ne presega pet let. Na predlog ponudnika se lahko veljavnost potrdila na podlagi ponovne ocene v skladu z veljavnimi postopki za ugotavljanje skladnosti podaljša za nadaljnja obdobja, ki ne presegajo pet let.

3. Če priglašeni organ ugotovi, da umetnointeligenčni sistem ne izpolnjuje več zahtev iz poglavja 2 tega naslova, ob upoštevanju načela sorazmernosti začasno prekliče ali umakne izdano potrdilo oziroma ga omeji, razen če se skladnost s temi zahtevami zagotovi z ustreznimi popravnimi ukrepi, ki jih je ponudnik sistema sprejel v ustreznem roku, ki ga določi priglašeni organ. Priglašeni organ obrazloži svojo odločitev.

Člen 45

Pritožba zoper odločitve priglašenih organov

Države članice zagotovijo, da je pritožbeni postopek zoper odločitve priglašenih organov na voljo strankam, ki imajo upravičen interes za to odločitev.

Člen 46

Obveznosti obveščanja za priglašene organe

1. Priglašeni organi obveščajo priglasitveni organ o:

   (a) vseh potrdilih Unije o oceni tehnične dokumentacije, vseh dodatkih k tem potrdilom, odobritvah sistema upravljanja kakovosti, izdanih v skladu z zahtevami iz Priloge VII;

   (b) vseh zavrnitvah, omejitvah, začasnem preklicu ali umiku potrdila Unije o oceni tehnične dokumentacije ali odobritvi sistema upravljanja kakovosti, izdanih v skladu z zahtevami iz Priloge VII;

   (c) vseh okoliščinah, ki vplivajo na obseg ali pogoje za priglasitev;

   (d) vseh zahtevah po informacijah, ki so jih prejeli od organov za nadzor trga, v zvezi z dejavnostmi ugotavljanja skladnosti;

   (e) dejavnostih ugotavljanja skladnosti, izvedenih v okviru njihove priglasitve, in o kakršnih koli drugih izvedenih dejavnostih, vključno s čezmejnimi dejavnostmi in sklepanjem pogodb s podizvajalci, če je to zahtevano.

2. Vsak priglašeni organ obvesti druge priglašene organe o:

   (a) odobritvah sistema upravljanja kakovosti, ki jih je zavrnil, začasno preklical ali umaknil, ter jih na zahtevo obvesti o odobritvah sistema kakovosti, ki jih je izdal;

   (b) potrdilih o oceni tehnične dokumentacije EU ali njihovih dodatkih, ki jih je zavrnil, začasno preklical ali umaknil ali drugače omejil, ter jih na zahtevo obvesti o potrdilih in/ali dodatkih, ki jih je izdal.

3. Vsak priglašeni organ drugim priglašenim organom, ki izvajajo podobne dejavnosti ugotavljanja skladnosti v zvezi z istimi umetnointeligenčnimi tehnologijami, predloži ustrezne informacije o vprašanjih v zvezi z negativnimi rezultati ugotavljanja skladnosti, na zahtevo pa tudi pozitivnimi rezultati ugotavljanja skladnosti.

Člen 47

Odstopanje od postopka ugotavljanja skladnosti

1. Z odstopanjem od člena 43 lahko kateri koli organ za nadzor trga dovoli dajanje na trg ali v uporabo posebnih umetnointeligenčnih sistemov velikega tveganja na ozemlju zadevne države članice iz izjemnih razlogov javne varnosti ali varstva življenja in zdravja ljudi, varstva okolja ter varstva ključnih industrijskih in infrastrukturnih sredstev. To dovoljenje velja za omejeno obdobje, dokler se izvajajo potrebni postopki ugotavljanja skladnosti, in preneha veljati, ko so ti postopki zaključeni. Ti postopki se zaključijo brez nepotrebnega odlašanja.

2. Dovoljenje iz odstavka 1 se izda le, če organ za nadzor trga ugotovi, da umetnointeligenčni sistem velikega tveganja izpolnjuje zahteve iz poglavja 2 tega naslova. Organ za nadzor trga obvesti Komisijo in druge države članice o vseh dovoljenjih, izdanih v skladu z odstavkom 1.

3. Če v 15 koledarskih dneh po prejemu informacij iz odstavka 2 država članica ali Komisija ne poda nobenega ugovora glede dovoljenja, ki ga je izdal organ za nadzor trga države članice v skladu z odstavkom 1, se šteje, da je dovoljenje upravičeno.

4. Če v 15 koledarskih dneh po prejemu priglasitve iz odstavka 2 država članica poda ugovore zoper dovoljenje, ki ga je izdal organ za nadzor trga druge države članice, ali če Komisija meni, da je dovoljenje v nasprotju s pravom Unije ali da je sklep držav članic glede skladnosti sistema iz odstavka 2 neutemeljen, se brez odlašanja posvetuje z zadevno državo članico; z zadevnimi operaterji se je treba posvetovati in ti morajo imeti možnost, da predstavijo svoja stališča. Glede na to Komisija odloči, ali je dovoljenje upravičeno ali ne. Komisija svojo odločitev naslovi na zadevno državo članico in ustreznega operaterja ali operaterje.

5. Če se dovoljenje šteje za neupravičeno, ga umakne organ za nadzor trga zadevne države članice.

6. Z odstopanjem od odstavkov 1 do 5 se za umetnointeligenčne sisteme velikega tveganja, ki so namenjeni uporabi kot varnostne komponente pripomočkov ali ki so sami pripomočki, zajeti v Uredbi (EU) 2017/745 in Uredbi (EU) 2017/746, uporabljata člen 59 Uredbe (EU) 2017/745 in člen 54 Uredbe (EU) 2017/746 tudi v zvezi z odstopanjem od ugotavljanja skladnosti z zahtevami iz poglavja 2 tega naslova.

Člen 48

Izjava EU o skladnosti

1. Ponudnik za vsak umetnointeligenčni sistem sestavi pisno izjavo EU o skladnosti in jo hrani za potrebe pristojnih nacionalnih organov ter jim jo daje na voljo še 10 let po tem, ko je bil umetnointeligenčni sistem dan na trg ali v uporabo. Izjava EU o skladnosti opredeljuje umetnointeligenčni sistem, za katerega je bila sestavljena. Na zahtevo se ustreznim pristojnim nacionalnim organom predloži izvod izjave EU o skladnosti.

2. Izjava EU o skladnosti navaja, da zadevni umetnointeligenčni sistem velikega tveganja izpolnjuje zahteve iz poglavja 2 tega naslova. Izjava EU o skladnosti vsebuje informacije iz Priloge V in se prevede v uradni jezik Unije ali jezike, ki jih zahteva država članica oziroma države članice, v katerih je umetnointeligenčni sistem velikega tveganja dostopen.

3. Kadar za umetnointeligenčne sisteme velikega tveganja velja druga harmonizacijska zakonodaja Unije, ki zahteva tudi izjavo EU o skladnosti, se pripravi enotna izjava EU o skladnosti za vse zakonodaje Unije, ki se uporabljajo za umetnointeligenčni sistem velikega tveganja. Ta izjava vsebuje vse informacije, potrebne za ugotovitev, na katero harmonizirano zakonodajo Unije se izjava nanaša.

4. S pripravo izjave EU o skladnosti ponudnik prevzame odgovornost za skladnost z zahtevami iz poglavja 2 tega naslova. Ponudnik izjavo EU o skladnosti ustrezno posodablja.

5. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 73 za posodobitev vsebine izjave EU o skladnosti iz Priloge V za uvedbo elementov, ki postanejo potrebni zaradi tehničnega napredka.

Člen 49

Oznaka skladnosti

1. Oznaka CE se vidno, čitljivo in neizbrisno namesti za umetnointeligenčne sisteme velikega tveganja. Kadar to ni mogoče ali ni upravičeno zaradi značilnosti umetnointeligenčnega sistema velikega tveganja, se oznaka namesti na embalažo ali spremno dokumentacijo, kot je ustrezno.
2. Za oznako CE iz odstavka 1 tega člena veljajo splošna načela, določena v členu 30 Uredbe (ES) št. 765/2008.
3. Oznaki CE po potrebi sledi identifikacijska številka priglašenega organa, odgovornega za postopke ugotavljanja skladnosti, določene v členu 43. Identifikacijska številka je navedena tudi v promocijskem gradivu, v katerem je navedeno, da umetnointeligenčni sistem velikega tveganja izpolnjuje zahteve za oznako CE.

Člen 50

Hramba dokumentov

Ponudnik še 10 let po tem, ko je bil umetnointeligenčni sistem dan na trg ali v uporabo, za pristojni nacionalni organ hrani:

(a) tehnično dokumentacijo iz člena 11;

(b) dokumentacijo v zvezi s sistemom upravljanja kakovosti iz člena 17;

(c) dokumentacijo o spremembah, ki so jih odobrili priglašeni organi, kjer je to primerno;

(d) odločitve in druge dokumente, ki so jih izdali priglašeni organi, kjer je to primerno;

(e) izjavo EU o skladnosti iz člena 48.

Člen 51

Registracija

Ponudnik ali, kjer je to ustrezno, pooblaščeni zastopnik pred dajanjem umetnointeligenčnega sistema velikega tveganja iz člena 6(2) na trg ali v uporabo ta sistem registrira v podatkovni zbirki EU iz člena 60.

NASLOV IV

OBVEZNOSTI GLEDE PREGLEDNOSTI ZA NEKATERE UMETNOINTELIGENČNE SISTEME

Člen 52

Obveznosti glede preglednosti za nekatere umetnointeligenčne sisteme

1. Ponudniki zagotovijo, da so umetnointeligenčni sistemi, namenjeni interakciji s fizičnimi osebami, zasnovani in razviti tako, da so fizične osebe obveščene, da so v stiku z umetnointeligenčnim sistemom, razen če je to razvidno iz okoliščin in konteksta uporabe. Ta obveznost se ne uporablja za umetnointeligenčne sisteme, ki so z zakonom pooblaščeni za odkrivanje, preprečevanje, preiskovanje in pregon kaznivih dejanj, razen če so ti sistemi na voljo javnosti za prijavo kaznivega dejanja.

2. Uporabniki sistema za prepoznavanje čustev ali sistema za biometrično kategorizacijo o delovanju sistema obvestijo fizične osebe, ki so jim bile izpostavljene. Ta obveznost se ne uporablja za umetnointeligenčne sisteme, ki se uporabljajo za biometrično kategorizacijo ter so z zakonom dovoljeni za odkrivanje, preprečevanje in preiskovanje kaznivih dejanj.

3. Uporabniki umetnointeligenčnega sistema, ki ustvarja ali manipulira slikovno, zvočno ali videovsebino, ki v znatni meri spominja na obstoječe osebe, predmete, kraje ali druge subjekte ali dogodke in bi se osebi lažno zdela verodostojna ali resnična („globoki ponaredek“), razkrijejo, da je bila vsebina umetno ustvarjena ali manipulirana.

   Vendar se prvi pododstavek ne uporablja, kadar je uporaba z zakonom dovoljena za odkrivanje, preprečevanje, preiskovanje in pregon kaznivih dejanj ali je potrebna za uresničevanje pravice do svobode izražanja in pravice do svobode umetnosti in znanosti, zagotovljene z Listino EU o temeljnih pravicah, ter ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine tretjih oseb.

4. Odstavki 1, 2 in 3 ne vplivajo na zahteve in obveznosti iz naslova III te uredbe.

NASLOV V

UKREPI V PODPORO INOVACIJAM

Člen 53

Regulativni peskovniki za umetno inteligenco

1. Regulativni peskovniki za umetno inteligenco, ki jih vzpostavijo pristojni organi ene ali več držav članic ali Evropski nadzornik za varstvo podatkov, zagotavljajo nadzorovano okolje, ki omogoča razvoj, testiranje in potrjevanje inovativnih umetnointeligenčnih sistemov za omejen čas pred dajanjem na trg ali v uporabo v skladu s posebnim načrtom. To se izvaja pod neposrednim nadzorom in smernicami pristojnih organov, da se zagotovi skladnost z zahtevami iz te uredbe ter po potrebi z drugo zakonodajo Unije in držav članic, ki se nadzoruje v peskovniku.

2. Države članice zagotovijo, da so nacionalni organi za varstvo podatkov in ti drugi nacionalni organi povezani z delovanjem regulativnega peskovnika za umetno inteligenco, če inovativni umetnointeligenčni sistemi vključujejo obdelavo osebnih podatkov ali kako drugače spadajo v nadzorno pristojnost drugih nacionalnih organov ali pristojnih organov, ki zagotavljajo ali podpirajo dostop do podatkov.

3. Regulativni peskovniki za umetno inteligenco ne vplivajo na pooblastila pristojnih organov za nadzor in popravne ukrepe. Vsa pomembna tveganja za zdravje in varnost ter temeljne pravice, ugotovljena med razvojem in testiranjem takih sistemov, je treba nemudoma zmanjšati, v nasprotnem primeru pa postopek razvoja in testiranja ustaviti, dokler ne pride do takega zmanjšanja.

4. Udeleženci v regulativnem peskovniku za umetno inteligenco so v skladu z veljavno zakonodajo Unije in držav članic o odgovornosti še naprej odgovorni za škodo, povzročeno tretjim osebam zaradi eksperimentov, ki se izvajajo v peskovniku.

5. Pristojni organi držav članic, ki so vzpostavili regulativne peskovnike za umetno inteligenco, usklajujejo svoje dejavnosti in sodelujejo v okviru Evropskega odbora za umetno inteligenco. Odboru in Komisiji predložijo letna poročila o rezultatih izvajanja navedenih shem, vključno z dobrimi praksami, pridobljenimi izkušnjami in priporočili o njihovi vzpostavitvi ter po potrebi o uporabi te uredbe in druge zakonodaje Unije, ki se nadzoruje v peskovniku.

6. Načini in pogoji delovanja regulativnih peskovnikov za umetno inteligenco, vključno z merili za upravičenost in postopkom za prijavo, izbiro, sodelovanje in izstop iz peskovnika, ter pravice in obveznosti udeležencev se določijo v izvedbenih aktih. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 74(2).

Člen 54

Nadaljnja obdelava osebnih podatkov za razvoj določenih umetnointeligenčnih sistemov v javnem interesu v regulativnem peskovniku za umetno inteligenco

1. V regulativnem peskovniku za umetno inteligenco se osebni podatki, zakonito zbrani za druge namene, obdelujejo za razvoj in testiranje nekaterih inovativnih umetnointeligenčnih sistemov v peskovniku pod naslednjimi pogoji:

   (a) inovativni umetnointeligenčni sistemi se razvijejo za zaščito bistvenega javnega interesa na enem ali več naslednjih področjih:

      (i) preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, pod nadzorom in odgovornostjo pristojnih organov. Obdelava temelji na pravu države članice ali pravu Unije;

      (ii) javne varnosti in javnega zdravja, vključno s preprečevanjem, nadzorom in zdravljenjem bolezni;

      (iii) visoke ravni varstva in izboljšanja kakovosti okolja;

   (b) obdelani podatki so potrebni za izpolnjevanje ene ali več zahtev iz poglavja 2 naslova III, kadar teh zahtev ni mogoče učinkovito izpolniti z obdelavo anonimiziranih, sintetičnih ali drugih neosebnih podatkov;

(c) obstajajo učinkoviti mehanizmi za spremljanje, s katerimi se ugotovi, ali se med eksperimentiranjem v peskovniku lahko pojavijo velika tveganja za temeljne pravice posameznikov, na katere se nanašajo osebni podatki, ter ali obstajajo mehanizmi za odzivanje, s katerimi se ta tveganja nemudoma zmanjšajo in po potrebi ustavi obdelava;

(d) vsi osebni podatki, ki se obdelujejo v okviru peskovnika, so v funkcionalno ločenem, izoliranem in zaščitenem okolju za obdelavo podatkov pod nadzorom udeležencev, dostop do teh podatkov pa imajo samo pooblaščene osebe;

(e) nobeni obdelani osebni podatki ne smejo biti posredovani, preneseni ali drugače dostopni drugim strankam;

(f) nobena obdelava osebnih podatkov v okviru peskovnika ne sme biti podlaga za sprejetje ukrepov ali odločitev, ki bi vplivali na posameznike, na katere se nanašajo osebni podatki;

(g) vsi osebni podatki, obdelani v okviru peskovnika, se izbrišejo, ko se sodelovanje v peskovniku konča ali ko se izteče obdobje hrambe osebnih podatkov;

(h) dnevniki obdelave osebnih podatkov v okviru peskovnika se hranijo ves čas trajanja sodelovanja v peskovniku in eno leto po njegovem zaključku, in sicer izključno za izpolnjevanje obveznosti glede odgovornosti in dokumentacije v skladu s tem členom ali drugo veljavno zakonodajo Unije ali držav članic, in le toliko časa, kolikor je potrebno za ta namen;

(i) celovit in podroben opis postopka in utemeljitev za učenje, testiranje in potrjevanje umetnointeligenčnega sistema se hranita skupaj z rezultati testiranja kot del tehnične dokumentacije v Prilogi IV;

(j) kratek povzetek projekta umetne inteligence, razvitega v peskovniku, njegovih ciljev in pričakovanih rezultatov, je objavljen na spletišču pristojnih organov.

2. Odstavek 1 ne posega v zakonodajo Unije ali držav članic, ki izključuje obdelavo za druge namene, kot so izrecno navedeni v navedeni zakonodaji.

Člen 55

Ukrepi za male ponudnike in uporabnike

1. Države članice sprejmejo naslednje ukrepe:

(a) malim ponudnikom in zagonskim podjetjem zagotovijo prednostni dostop do regulativnih peskovnikov za umetno inteligenco, če izpolnjujejo pogoje za upravičenost;

(b) organizirajo posebne dejavnosti ozaveščanja o uporabi te uredbe, prilagojene potrebam malih ponudnikov in uporabnikov;

(c) po potrebi vzpostavijo poseben kanal za komunikacijo z malimi ponudniki in uporabniki ter drugimi inovatorji, da zagotovijo smernice in odgovore na vprašanja o izvajanju te uredbe.

2. Pri določanju pristojbin za ugotavljanje skladnosti v skladu s členom 43 se upoštevajo posebni interesi in potrebe malih ponudnikov, pri čemer se te pristojbine znižajo sorazmerno z njihovo velikostjo in velikostjo trga.

NASLOV VI

UPRAVLJANJE

POGLAVJE 1

EVROPSKI ODBOR ZA UMETNO INTELIGENCO

Člen 56

Ustanovitev Evropskega odbora za umetno inteligenco

1. Ustanovi se Evropski odbor za umetno inteligenco (v nadaljnjem besedilu: Odbor).

2. Odbor svetuje in pomaga Komisiji, da:

   (a) prispeva k učinkovitemu sodelovanju nacionalnih nadzornih organov in Komisije v zvezi z zadevami, zajetimi s to uredbo;

   (b) usklajuje smernice in analize, ki jih pripravijo Komisija, nacionalni nadzorni organi in drugi pristojni organi v zvezi z vprašanji, ki se pojavijo na celotnem notranjem trgu v zvezi z zadevami, zajetimi s to uredbo, ter prispeva k navedenim smernicam in analizam;

   (c) pomaga nacionalnim nadzornim organom in Komisiji pri zagotavljanju dosledne uporabe te uredbe.

Člen 57

Struktura Odbora

1. Odbor sestavljajo nacionalni nadzorni organi, ki jih zastopa vodja ali enakovreden visoki uradnik tega organa, in Evropski nadzornik za varstvo podatkov. Na sestanke se lahko povabijo tudi drugi nacionalni organi, kadar so vprašanja, o katerih se razpravlja, pomembna zanje.

2. Odbor sprejme svoj poslovnik z navadno večino svojih članov po soglasju Komisije. Poslovnik vsebuje tudi operativne vidike, povezane z izvajanjem nalog Odbora iz člena 58. Odbor lahko po potrebi ustanovi podskupine za preučitev posebnih vprašanj.

3. Odboru predseduje Komisija. Komisija skliče sestanke in pripravi dnevni red v skladu z nalogami Odbora na podlagi te uredbe in v skladu s poslovnikom. Komisija zagotavlja upravno in analitično podporo dejavnostim odbora v skladu s to uredbo.

4. Odbor lahko na svoje seje povabi zunanje strokovnjake in opazovalce ter organizira izmenjavo informacij z zainteresiranimi tretjimi stranmi, da jih v ustreznem obsegu upošteva pri svojih dejavnostih. V ta namen lahko Komisija olajša izmenjave med Odborom in drugimi organi, uradi, agencijami in svetovalnimi skupinami Unije.

Člen 58

Naloge Odbora

Odbor pri svetovanju in pomoči Komisiji v smislu člena 56(2) zlasti:

(a) zbira in izmenjuje strokovno znanje in najboljše prakse med državami članicami;

(b) prispeva k enotnim upravnim praksam v državah članicah, tudi za delovanje regulativnih peskovnikov iz člena 53;

(c) izdaja mnenja, priporočila ali pisne prispevke o zadevah, povezanih z izvajanjem te uredbe, zlasti

(i) o tehničnih specifikacijah ali obstoječih standardih v zvezi z zahtevami iz poglavja 2 naslova III,

(ii) o uporabi harmoniziranih standardov ali skupnih specifikacij iz členov 40 in 41,

(iii) o pripravi smernic, vključno s smernicami za določanje upravnih glob iz člena 71.

POGLAVJE 2

PRISTOJNI NACIONALNI ORGANI

Člen 59

Imenovanje pristojnih nacionalnih organov

1. Pristojne nacionalne organe ustanovi ali imenuje vsaka država članica za zagotavljanje uporabe in izvajanja te uredbe. Pristojni nacionalni organi so organizirani tako, da zagotavljajo objektivnost in nepristranskost svojih dejavnosti.

2. Vsaka država članica izmed pristojnih nacionalnih organov imenuje nacionalni nadzorni organ. Nacionalni nadzorni organ deluje kot priglasitveni organ in organ za nadzor trga, razen če ima država članica organizacijske in upravne razloge za imenovanje več kot enega organa.

3. Države članice obvestijo Komisijo o svojem imenovanju ali imenovanjih in po potrebi o razlogih za imenovanje več kot enega organa.

4. Države članice zagotovijo, da imajo pristojni nacionalni organi na voljo ustrezne finančne in človeške vire za izpolnjevanje svojih nalog v skladu s to uredbo. Pristojni nacionalni organi imajo zlasti zadostno število stalno razpoložljivega osebja, katerega kompetence in strokovno znanje vključujeta poglobljeno razumevanje tehnologij umetne inteligence, podatkov in računalniške obdelave podatkov, temeljnih pravic, zdravstvenih in varnostnih tveganj ter poznavanje obstoječih standardov in pravnih zahtev.

5. Države članice Komisiji vsako leto poročajo o stanju finančnih in človeških virov pristojnih nacionalnih organov z oceno njihove ustreznosti. Komisija te informacije posreduje odboru v razpravo in morebitna priporočila.

6. Komisija olajša izmenjavo izkušenj med pristojnimi nacionalnimi organi.

7. Pristojni nacionalni organi lahko zagotovijo smernice in nasvete o izvajanju te uredbe, tudi malim ponudnikom. Kadar nameravajo pristojni nacionalni organi zagotoviti smernice in nasvete v zvezi z umetnointeligenčnim sistemom na področjih, ki jih zajema druga zakonodaja Unije, se po potrebi posvetujejo s pristojnimi nacionalnimi organi, ki delujejo v skladu s to zakonodajo Unije. Države članice lahko vzpostavijo tudi eno osrednjo kontaktno točko za komunikacijo z operaterji.

8. Kadar institucije, agencije in organi Unije spadajo na področje uporabe te uredbe, Evropski nadzornik za varstvo podatkov deluje kot pristojni organ za njihov nadzor.

NASLOV VII

PODATKOVNA ZBIRKA EU ZA SAMOSTOJNE UMETNOINTELIGENČNE SISTEME VELIKEGA TVEGANJA

Člen 60

Podatkovna zbirka EU za samostojne umetnointeligenčne sisteme velikega tveganja

1. Komisija v sodelovanju z državami članicami vzpostavi in vzdržuje podatkovno zbirko EU, ki vsebuje informacije iz odstavka 2 o umetnointeligenčnih sistemih velikega tveganja iz člena 6(2), registriranih v skladu s členom 51.

2. Podatke iz Priloge VIII v podatkovno zbirko EU vnašajo ponudniki. Komisija jim zagotovi tehnično in upravno podporo.

3. Informacije v podatkovni zbirki EU so dostopne javnosti.

4. Podatkovna zbirka EU vsebuje osebne podatke le, kolikor je to potrebno za zbiranje in obdelavo informacij v skladu s to uredbo. Te informacije vključujejo imena in kontaktne podatke fizičnih oseb, ki so odgovorne za registracijo sistema in imajo pravno pooblastilo za zastopanje ponudnika.

5. Komisija je upravljavec podatkovne zbirke EU. Ponudnikom zagotovi tudi ustrezno tehnično in upravno podporo.

NASLOV VIII

SPREMLJANJE PO DAJANJU NA TRG, SOUPORABA INFORMACIJ, NADZOR TRGA

POGLAVJE 1

SPREMLJANJE PO DAJANJU NA TRG

Člen 61

Spremljanje po dajanju na trg s strani ponudnikov in načrt spremljanja po dajanju na trg za umetnointeligenčne sisteme velikega tveganja

1. Ponudniki vzpostavijo in dokumentirajo sistem spremljanja po dajanju na trg na način, sorazmeren z naravo umetnointeligenčnih tehnologij in tveganji umetnointeligenčnega sistema velikega tveganja.

2. Sistem spremljanja po dajanju na trg aktivno in sistematično zbira, dokumentira in analizira ustrezne podatke o učinkovitosti umetnointeligenčnih sistemov velikega tveganja skozi celotno življenjsko dobo, ki jih zagotovijo uporabniki ali se zberejo preko drugih virov, ter ponudniku omogoča, da oceni stalno skladnost umetnointeligenčnih sistemov z zahtevami iz poglavja 2 naslova III.

3. Sistem spremljanja po dajanju na trg temelji na načrtu spremljanja po dajanju na trg. Načrt spremljanja po dajanju na trg je del tehnične dokumentacije iz Priloge IV. Komisija sprejme izvedbeni akt, v katerem določi podrobne določbe o predlogih za načrt spremljanja po dajanju na trg in seznam elementov, ki jih je treba vključiti v načrt.

4. Za umetnointeligenčne sisteme velikega tveganja, ki jih zajemajo pravni akti iz Priloge II, kadar sta sistem in načrt spremljanja po dajanju na trg že vzpostavljena v skladu z navedeno zakonodajo, se v ta sistem in načrt po potrebi vključijo elementi iz odstavkov 1, 2 in 3.

   Prvi pododstavek se uporablja tudi za umetnointeligenčne sisteme velikega tveganja iz točke 5(b) Priloge III, ki jih dajejo na trg ali v uporabo kreditne institucije, urejene z Direktivo 2013/36/EU.

POGLAVJE 2

SOUPORABA INFORMACIJ O INCIDENTIH IN OKVARAH

Člen 62

Poročanje o hudih incidentih in okvarah

1. Ponudniki umetnointeligenčnih sistemov velikega tveganja, ki so dani na trg Unije, sporočijo vsak hud incident ali kakršno koli okvaro teh sistemov, ki predstavlja kršitev obveznosti iz prava Unije, namenjenih zaščiti temeljnih pravic, organom za nadzor trga držav članic, v katerih je prišlo do tega incidenta ali kršitve.

Tako obvestilo se pošlje takoj, ko ponudnik vzpostavi vzročno zvezo med umetnointeligenčnim sistemom in incidentom ali okvaro ali razumno verjetnost take povezave, v vsakem primeru pa najpozneje 15 dni po tem, ko ponudnik izve za hud incident ali okvaro.

2. Organ za nadzor trga po prejemu obvestila o kršitvi obveznosti iz prava Unije, namenjenih zaščiti temeljnih pravic, obvesti nacionalne javne organe ali telesa iz člena 64(3). Komisija pripravi posebne smernice za lažje izpolnjevanje obveznosti iz odstavka 1. Te smernice se izdajo najpozneje 12 mesecev po začetku veljavnosti te uredbe.

3. Za umetnointeligenčne sisteme velikega tveganja iz točke 5(b) Priloge III, ki jih dajejo na trg ali v uporabo ponudniki, ki so kreditne institucije, urejene z Direktivo 2013/36/EU, in za umetnointeligenčne sisteme velikega tveganja, ki so varnostne komponente pripomočkov ali so sami pripomočki, zajeti v Uredbi (EU) 2017/745 in Uredbi (EU) 2017/746, je obveščanje o hudih incidentih ali okvarah omejeno na tiste, ki pomenijo kršitev obveznosti v skladu s pravom Unije za zaščito temeljnih pravic.

POGLAVJE 3

IZVRŠEVANJE

Člen 63

Nadzor trga in nadzor umetnointeligenčnih sistemov na trgu Unije

1. Za umetnointeligenčne sisteme, zajete s to uredbo, se uporablja Uredba (EU) 2019/1020. Vendar pa za učinkovito izvrševanje te uredbe velja naslednje:

   (a) vsako sklicevanje na gospodarski subjekt v skladu z Uredbo (EU) 2019/1020 se razume kot sklicevanje na vse operaterje, opredeljene v poglavju 3 naslova III te uredbe;

   (b) vsako sklicevanje na proizvod v skladu z Uredbo (EU) 2019/1020 se razume kot sklicevanje na vse umetnointeligenčne sisteme, ki spadajo na področje uporabe te uredbe.

2. Nacionalni nadzorni organ Komisiji redno poroča o izidih zadevnih dejavnosti nadzora trga. Nacionalni nadzorni organ Komisiji in zadevnim nacionalnim organom za varstvo konkurence brez odlašanja poroča o vseh informacijah, ugotovljenih med dejavnostmi nadzora trga, ki bi lahko zadevale uporabo prava Unije o pravilih konkurence.

3. Za umetnointeligenčne sisteme velikega tveganja, povezane s proizvodi, za katere se uporabljajo pravni akti iz oddelka A Priloge II, je organ za nadzor trga za namene te uredbe organ, odgovoren za dejavnosti nadzora trga, določene v navedenih pravnih aktih.

4. Za umetnointeligenčne sisteme, ki jih dajo na trg, v obratovanje ali jih uporabljajo finančne institucije, ki jih ureja zakonodaja Unije o finančnih storitvah, je organ za nadzor trga za namene te uredbe ustrezni organ, odgovoren za finančni nadzor teh institucij v skladu z navedeno zakonodajo.

5. Za umetnointeligenčne sisteme iz točke 1(a), če se sistemi uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj iz točk 6 in 7 Priloge III, države članice za namene te uredbe imenujejo organe za nadzor trga ali pristojne nadzorne organe za varstvo podatkov v skladu z Direktivo (EU) 2016/680 ali Uredbo 2016/679 ali pristojne nacionalne organe, ki nadzorujejo dejavnosti organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organov, pristojnih za priseljevanje, ali azilnih organov, ki dajejo v uporabo ali uporabljajo te sisteme.

6. Kadar institucije, agencije in organi Unije spadajo na področje uporabe te uredbe, Evropski nadzornik za varstvo podatkov deluje kot njihov organ za nadzor trga.

7. Države članice olajšajo usklajevanje med organi za nadzor trga, imenovanimi v skladu s to uredbo, in drugimi ustreznimi nacionalnimi organi ali telesi, ki nadzorujejo uporabo harmonizacijske zakonodaje Unije iz Priloge II ali druge zakonodaje Unije, ki bi lahko bila pomembna za umetnointeligenčne sisteme velikega tveganja iz Priloge III.

Člen 64

Dostop do podatkov in dokumentacije

1. V okviru svojih dejavnosti imajo organi za nadzor trga popoln dostop do naborov učnih in testnih podatkov ter podatkov za potrditev, ki jih uporablja ponudnik, tudi preko vmesnikov za aplikacijsko programiranje (API) ali drugih ustreznih sredstev in orodij, ki omogočajo oddaljeni dostop.

2. Organom za nadzor trga se na podlagi obrazložene zahteve omogoči tudi dostop do izvorne kode umetnointeligenčnega sistema, če je to potrebno za oceno skladnosti umetnointeligenčnega sistema velikega tveganja z zahtevami iz poglavja 2 naslova III.

3. Nacionalni javni organi, ki nadzorujejo ali uveljavljajo spoštovanje obveznosti iz prava Unije o varstvu temeljnih pravic v zvezi z uporabo umetnointeligenčnih sistemov velikega tveganja iz Priloge III, so pooblaščeni, da zahtevajo kakršno koli dokumentacijo, ustvarjeno ali hranjeno v skladu s to uredbo, in dostopajo do nje, kadar je dostop do te dokumentacije potreben za izvrševanje pristojnosti v okviru njihovih pooblastil v mejah njihove pristojnosti. Zadevni javni organ o vsaki taki zahtevi obvesti organ za nadzor trga zadevne države članice.

4. Vsaka država članica do treh mesecev po začetku veljavnosti te uredbe določi javne organe iz odstavka 3 in objavi seznam na spletišču nacionalnega nadzornega organa. Države članice o seznamu uradno obvestijo Komisijo in vse druge države članice ter seznam redno posodabljajo.

5. Kadar dokumentacija iz odstavka 3 ne zadošča za ugotovitev, ali je prišlo do kršitve obveznosti iz prava Unije, namenjene zaščiti temeljnih pravic, lahko javni organ iz odstavka 3 na podlagi obrazložene zahteve od organa za nadzor trga zahteva, da s tehničnimi sredstvi organizira testiranje umetnointeligenčnega sistema velikega tveganja. Organ za nadzor trga organizira testiranje ob tesnem sodelovanju javnega organa, ki je vložil zahtevo, v razumnem času po prejemu zahteve.

6. Vse informacije in dokumentacija, ki jih nacionalni javni organi ali telesa iz odstavka 3 pridobijo na podlagi določb tega člena, se obravnavajo v skladu z obveznostmi glede zaupnosti iz člena 70.

Člen 65

Postopek za obravnavo umetnointeligenčnih sistemov, ki predstavljajo tveganje na nacionalni ravni

1. Za umetnointeligenčne sisteme, ki predstavljajo tveganje, se šteje proizvod, ki predstavlja tveganje, opredeljen v točki 19 člena 3 Uredbe (EU) 2019/1020, kar zadeva tveganja za zdravje ali varnost ali varstvo temeljnih pravic oseb.

2. Kadar ima organ za nadzor trga države članice zadostne razloge, da meni, da umetnointeligenčni sistem predstavlja tveganje iz odstavka 1, opravi oceno zadevnega umetnointeligenčnega sistema glede njegove skladnosti z vsemi zahtevami in obveznostmi iz te uredbe. Ob prisotnosti tveganj za zaščito temeljnih pravic organ za nadzor trga obvesti tudi ustrezne nacionalne javne organe ali telesa iz člena 64(3). Zadevni operaterji po potrebi sodelujejo z organi za nadzor trga in drugimi nacionalnimi javnimi organi ali telesi iz člena 64(3).

   Kadar organ za nadzor trga med navedenim ocenjevanjem ugotovi, da umetnointeligenčni sistem ni skladen z zahtevami in obveznostmi iz te uredbe, od zadevnega operaterja brez odlašanja zahteva, da sprejme vse ustrezne popravne ukrepe, da zagotovi skladnost umetnointeligenčnega sistema, ga umakne s trga ali prekliče v razumnem roku, ki ga določi glede na naravo tveganja.

   Organ za nadzor trga o tem ustrezno obvesti zadevni priglašeni organ. Za ukrepe iz drugega pododstavka se uporablja člen 18 Uredbe (EU) 2019/1020.

3. Kadar organ za nadzor trga meni, da neskladnost ni omejena na njegovo nacionalno ozemlje, Komisijo in druge države članice obvesti o rezultatih ocenjevanja in ukrepih, ki jih je zahteval od operaterja.

4. Operater zagotovi izvedbo vseh ustreznih popravnih ukrepov glede vseh zadevnih umetnointeligenčnih sistemov, katerih dostopnost na trgu je omogočil po vsej Uniji.

5. Kadar operater umetnointeligenčnega sistema ne sprejme ustreznih popravnih ukrepov v roku iz odstavka 2, organ za nadzor trga sprejme vse ustrezne začasne ukrepe za prepoved ali omejitev dajanja umetnointeligenčnega sistema na nacionalni trg, za umik ali za preklic proizvoda z navedenega trga. Ta organ o teh ukrepih brez odlašanja obvesti Komisijo in druge države članice.

6. Informacije iz odstavka 5 vsebujejo vse razpoložljive podrobnosti, zlasti podatke, potrebne za identifikacijo neskladnega umetnointeligenčnega sistema, poreklo umetnointeligenčnega sistema, naravo domnevne neskladnosti in tveganja, naravo in trajanje sprejetih nacionalnih ukrepov ter argumente zadevnega operaterja. Organi za nadzor trga zlasti navedejo, ali je neskladnost posledica naslednjega:

   (a) umetnointeligenčni sistem ne izpolnjuje zahtev iz poglavja 2 naslova III;

   (b) pomanjkljivosti harmoniziranih standardov ali skupnih specifikacij iz členov 40 in 41, na katerih temelji domneva o skladnosti.

7. Organi za nadzor trga držav članic, ki niso organi za nadzor trga države članice, ki je začela postopek, brez odlašanja obvestijo Komisijo in druge države članice o vseh sprejetih ukrepih in vseh dodatnih informacijah, ki so jim na voljo v zvezi z neskladnostjo zadevnega umetnointeligenčnega sistema, ter v primeru nestrinjanja s priglašenim nacionalnim ukrepom o svojih ugovorih.

8. Kadar država članica ali Komisija v treh mesecih po prejemu informacij iz odstavka 5 ne poda ugovora glede začasnega ukrepa, ki ga je sprejela država članica, se šteje, da je ukrep upravičen. To ne posega v postopkovne pravice zadevnega operaterja v skladu s členom 18 Uredbe (EU) 2019/1020.

9. Organi za nadzor trga vseh držav članic zagotovijo takojšnje sprejetje ustreznih omejevalnih ukrepov v zvezi z zadevnim proizvodom, kot je umik proizvoda s trga.

Člen 66

Zaščitni postopek Unije

1. Kadar država članica v treh mesecih od prejema priglasitve iz člena 65(5) poda ugovor proti ukrepu, ki ga je sprejela druga država članica, ali kadar Komisija meni, da je ukrep v nasprotju s pravom Unije, se Komisija brez odlašanja posvetuje z zadevno državo članico in operaterjem ali operaterji ter oceni nacionalni ukrep. Komisija na podlagi rezultatov navedenega ocenjevanja odloči, ali je nacionalni ukrep upravičen ali ne v devetih mesecih od priglasitve iz člena 65(5), in o taki odločitvi uradno obvesti zadevno državo članico.

2. Če se nacionalni ukrep šteje za upravičenega, vse države članice sprejmejo ukrepe, potrebne za umik neskladnega umetnointeligenčnega sistema s svojega trga, in o tem ustrezno obvestijo Komisijo. Če se nacionalni ukrep šteje za neupravičenega, ga zadevna država članica umakne.

3. Kadar se nacionalni ukrep šteje za upravičenega, umetnointeligenčni sistem pa ni skladen zaradi pomanjkljivosti harmoniziranih standardov ali skupnih specifikacij iz členov 40 in 41 te uredbe, Komisija uporabi postopek iz člena 11 Uredbe (EU) št. 1025/2012.

Člen 67

Skladni umetnointeligenčni sistemi, ki predstavljajo tveganje

1. Kadar organ za nadzor trga države članice po opravljeni oceni iz člena 65 ugotovi, da je umetnointeligenčni sistem sicer v skladu s to direktivo, vendar pomeni tveganje za zdravje ali varnost oseb, skladnost z obveznostmi iz prava Unije ali nacionalnega prava, namenjenimi zaščiti temeljnih pravic ali drugih vidikov zaščite javnega interesa, od zadevnega operaterja zahteva, da sprejme vse ustrezne ukrepe, s katerimi zagotovi, da zadevni umetnointeligenčni sistem, ko je dan na trg ali v uporabo, ne predstavlja več navedenega tveganja, ali da ga umakne s trga ali prekliče v razumnem roku, ki ga določi glede na naravo tveganja.

2. Ponudnik ali drugi zadevni operaterji zagotovijo izvedbo popravnih ukrepov glede vseh zadevnih umetnointeligenčnih sistemov, katerih dostopnost na trgu so omogočili po vsej Uniji, v roku, ki ga predpiše organ za nadzor trga države članice iz odstavka 1.

3. Država članica o tem nemudoma obvesti Komisijo in druge države članice. Te informacije vključujejo vse razpoložljive podrobnosti, zlasti podatke, potrebne za identifikacijo zadevnega umetnointeligenčnega sistema, poreklo in dobavno verigo umetnointeligenčnega sistema, naravo tveganja ter naravo in trajanje sprejetih nacionalnih ukrepov.

4. Komisija se brez odlašanja posvetuje z državami članicami in ustreznimi operaterji ter oceni sprejete nacionalne ukrepe. Komisija na podlagi rezultatov ocenjevanja odloči, ali je ukrep upravičen ali ne, in po potrebi predlaga ustrezne ukrepe.

5. Komisija svojo odločitev naslovi na države članice.

Člen 68

Formalna neskladnost

1. Kadar organ za nadzor trga države članice ugotovi eno od naslednjih dejstev, od zadevnega ponudnika zahteva, naj zadevno neskladnost odpravi:

   (a) oznaka skladnosti ni nameščena v skladu s členom 49;

   (b) oznaka skladnosti ni nameščena;

   (c) izjava EU o skladnosti ni pripravljena;

   (d) izjava EU o skladnosti ni pravilno pripravljena;

   (e) identifikacijska številka morebitnega priglašenega organa, ki je vključen v postopek ugotavljanja skladnosti, ni nameščena.

2. Kadar se neskladnost iz odstavka 1 nadaljuje, zadevna država članica izvede vse ustrezne ukrepe za omejitev ali prepoved omogočanja dostopnosti umetnointeligenčnega sistema velikega tveganja na trgu ali pa zagotovi njegov preklic ali umik s trga.

NASLOV IX

KODEKSI RAVNANJA

Člen 69

Kodeksi ravnanja

1. Komisija in države članice spodbujajo in olajšujejo pripravo kodeksov ravnanja, namenjenih spodbujanju prostovoljne uporabe zahtev iz poglavja 2 naslova III za umetnointeligenčne sisteme, ki niso umetnointeligenčni sistemi velikega tveganja, na podlagi tehničnih specifikacij in rešitev, ki so ustrezna sredstva za zagotavljanje skladnosti s takimi zahtevami glede na predvideni namen sistemov.

2. Komisija in Odbor spodbujata in olajšujeta pripravo kodeksov ravnanja, namenjenih spodbujanju prostovoljne uporabe zahtev, povezanih na primer z okoljsko trajnostjo, dostopnostjo za invalide, sodelovanjem deležnikov pri oblikovanju in razvoju umetnointeligenčnih sistemov ter raznolikostjo razvojnih skupin na podlagi jasnih ciljev in ključnih kazalnikov uspešnosti za merjenje doseganja teh ciljev, za umetnointeligenčne sisteme.

3. Kodekse ravnanja lahko pripravijo posamezni ponudniki sistemov umetne inteligence ali organizacije, ki jih zastopajo, ali oboji, tudi z vključevanjem uporabnikov in vseh zainteresiranih strani ter njihovih predstavniških organizacij. Kodeksi ravnanja lahko zajemajo enega ali več umetnointeligenčnih sistemov ob upoštevanju podobnosti predvidenega namena zadevnih sistemov.

4. Komisija in odbor pri spodbujanju in olajševanju priprave kodeksov ravnanja upoštevata posebne interese in potrebe malih ponudnikov in zagonskih podjetij.

NASLOV X

ZAUPNOST IN KAZNI

Člen 70

Zaupnost

1. Pristojni nacionalni organi in priglašeni organi, vključeni v uporabo te uredbe, spoštujejo zaupnost informacij in podatkov, pridobljenih pri opravljanju svojih nalog in dejavnosti, tako da varujejo zlasti:

   (a) pravice intelektualne lastnine in zaupne poslovne informacije ali poslovne skrivnosti fizične ali pravne osebe, vključno z izvorno kodo, razen v primerih iz člena 5 Direktive (EU) 2016/943 o varstvu nerazkritega strokovnega znanja in izkušenj ter poslovnih informacij (poslovnih skrivnosti) pred njihovo protipravno pridobitvijo, uporabo in razkritjem;

   (b) učinkovito izvajanje te uredbe, zlasti za namene inšpekcijskih pregledov, preiskav ali revizij; (c) interese javne in nacionalne varnosti;

   (c) celovitost kazenskih ali upravnih postopkov.

2. Brez poseganja v odstavek 1 se informacije, ki se zaupno izmenjujejo med pristojnimi nacionalnimi organi ter med pristojnimi nacionalnimi organi in Komisijo, ne razkrijejo brez predhodnega posvetovanja z izvornim pristojnim nacionalnim organom in uporabnikom, kadar umetnointeligenčne sisteme velikega tveganja iz točk 1, 6 in 7 Priloge III uporabljajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organi, pristojni za priseljevanje, ali organi za presojo prošenj za azil, kadar bi tako razkritje ogrozilo javne in nacionalne varnostne interese.

   Kadar so organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organi, pristojni za priseljevanje, ali organi za presojo prošenj za azil ponudniki umetnointeligenčnih sistemov velikega tveganja iz točk 1, 6 in 7 Priloge III, ostane tehnična dokumentacija iz Priloge IV v prostorih teh organov. Ti organi zagotovijo, da lahko organi za nadzor trga iz člena 63(5) in (6), kot je ustrezno, na zahtevo nemudoma dostopajo do dokumentacije ali pridobijo njeno kopijo. Dostop do te dokumentacije ali njene kopije je dovoljen samo osebju organa za nadzor trga, ki ima ustrezno stopnjo varnostnega dovoljenja.

3. Odstavka 1 in 2 ne vplivata niti na pravice in obveznosti Komisije, držav članic in priglašenih organov v zvezi z izmenjavo informacij in razširjanjem opozoril niti na obveznost zadevnih strani, da zagotovijo podatke v skladu s kazenskim pravom držav članic.

4. Komisija in države članice lahko izmenjajo, kadar je to potrebno, zaupne informacije z regulativnimi organi tretjih držav, s katerimi so sklenile dvostranske ali večstranske dogovore o zaupnosti, ki zagotavljajo ustrezno raven zaupnosti.

Člen 71

Kazni

1. Države članice v skladu s pogoji iz te uredbe določijo pravila o kaznih, vključno z upravnimi globami, ki se uporabljajo za kršitve te uredbe, ter sprejmejo vse ukrepe, potrebne za zagotovitev, da se te pravilno in učinkovito izvajajo. Te kazni morajo biti učinkovite, sorazmerne in odvračilne. Upoštevajo zlasti interese malih ponudnikov in zagonskih podjetij ter njihovo ekonomsko sposobnost.

2. Države članice o teh pravilih uradno obvestijo Komisijo in jo brez odlašanja uradno obvestijo o vsakršni naknadni spremembi, ki nanje vpliva.

3. Za naslednje kršitve se naložijo upravne globe v višini do 30 000 000 EUR ali, če je kršitelj podjetje, do 6 % njegovega skupnega svetovnega letnega prometa za preteklo proračunsko leto, pri čemer se upošteva višji znesek:

   (a) neskladnost s prepovedmi praks umetne inteligence iz člena 5;

   (b) neskladnost umetnointeligenčnega sistema z zahtevami iz člena 10.

4. Če umetnointeligenčni sistem ne izpolnjuje zahtev ali obveznosti iz te uredbe, razen tistih iz členov 5 in 10, se kaznuje z upravnimi globami v višini do 20 000 000 EUR ali, če je kršitelj podjetje, do 4 % njegovega skupnega svetovnega letnega prometa za preteklo proračunsko leto, pri čemer se upošteva višji znesek.

5. Če se priglašenim organom in pristojnim nacionalnim organom v odgovor na zahtevo predložijo nepravilne, nepopolne ali zavajajoče informacije, se izreče upravna globa do 10 000 000 EUR ali, če je kršitelj podjetje, do 2 % njegovega skupnega svetovnega letnega prometa za preteklo proračunsko leto, pri čemer se upošteva višji znesek.

6. Pri odločanju o znesku upravne globe v vsakem posameznem primeru se upoštevajo vse zadevne okoliščine za konkretno situacijo, ustrezno pa se upošteva tudi naslednje:

   (a) vrsta, resnost in trajanje kršitve ter njene posledice;

   (b) ali so drugi organi za nadzor trga že naložili upravne globe istemu operaterju za isto kršitev.

   (c) velikost in tržni delež operaterja, ki je storil kršitev;

7. Vsaka država članica določi pravila o tem, ali in v kolikšni meri se lahko javnim organom in telesom s sedežem v zadevni državi članici naložijo upravne globe.

8. Glede na pravni sistem držav članic se lahko pravila o upravnih globah uporabljajo tako, da globe naložijo pristojna nacionalna sodišča ali drugi organi, kot velja v teh državah članicah. Uporaba takih pravil v teh državah članicah ima enakovreden učinek.

Člen 72

Upravne globe za institucije, agencije in organe Unije

1. Evropski nadzornik za varstvo lahko naloži upravne globe institucijam, agencijam in organom Unije, ki spadajo na področje uporabe te uredbe. Pri odločanju o naložitvi upravne globe in odločanju o znesku upravne globe v vsakem posameznem primeru

se upoštevajo vse zadevne okoliščine za konkretno situacijo, ustrezno pa se upošteva tudi naslednje:

(a) vrsta, resnost in trajanje kršitve ter njene posledice;

(b) sodelovanje z Evropskim nadzornikom za varstvo podatkov za odpravo kršitve in zmanjševanje morebitnih škodljivih učinkov kršitve, vključno z upoštevanjem katerega koli ukrepa, ki ga je Evropski nadzornik za varstvo podatkov predhodno odredil zoper zadevno institucijo ali agencijo ali organ Unije v zvezi z isto vsebino;

(c) vse podobne prejšnje kršitve institucije, agencije ali organa Unije;

2. Za naslednje kršitve se naložijo upravne globe do 500 000 EUR:

(a) neskladnost s prepovedmi praks umetne inteligence iz člena 5;

(b) neskladnost umetnointeligenčnega sistema z zahtevami iz člena 10.

3. Če umetnointeligenčni sistem ne izpolnjuje zahtev ali obveznosti iz te uredbe, razen tistih iz členov 5 in 10, se kaznuje z upravnimi globami do 250 000 EUR.

4. Evropski nadzornik za varstvo podatkov pred sprejetjem odločitev v skladu s tem členom instituciji, agenciji ali organu Unije, zaradi katerih je začel postopek, omogoči, da podajo izjavo o zadevi v zvezi z morebitno kršitvijo. Evropski nadzornik za varstvo podatkov svoje odločitve sprejme le na podlagi elementov in okoliščin, na katere so lahko zadevne strani podale pripombe. Pritožniki, če obstajajo, so v tesni povezavi s postopki.

5. Pravica do obrambe zadevnih strani se v postopkih v celoti spoštuje. Zagotovljena jim je pravica do vpogleda v spis Evropskega nadzornika za varstvo podatkov ob upoštevanju zakonitega interesa posameznikov ali podjetij za varstvo njihovih osebnih podatkov ali poslovnih skrivnosti.

6. Sredstva, zbrana z naložitvijo glob iz tega člena, so prihodek splošnega proračuna Unije.

NASLOV XI

PRENOS POOBLASTIL IN POSTOPEK V ODBORU

Člen 73

Izvajanje prenosa pooblastila

1. Pooblastilo za sprejemanje delegiranih aktov se prenese na Komisijo pod pogoji, določenimi v tem členu.

2. Pooblastilo iz člena 4, člena 7(1), člena 11(3), člena 43(5) in (6) ter člena 48(5) se prenese na Komisijo za nedoločen čas od [*datuma začetka veljavnosti te uredbe*].

3. Pooblastilo iz člena 4, člena 7(1), člena 11(3), člena 43(5) in (6) in člena 48(5) lahko kadar koli prekliče Evropski parlament ali Svet. S sklepom o preklicu preneha veljati prenos pooblastila iz navedenega sklepa. Sklep začne učinkovati dan po njegovi objavi v *Uradnem listu Evropske unije* ali na poznejši dan, ki je določen v navedenem sklepu. Ne vpliva na veljavnost že veljavnih delegiranih aktov.

4. Komisija takoj po sprejetju delegiranega akta o njem sočasno uradno obvesti Evropski parlament in Svet.

5. Vsak delegirani akt, sprejet v skladu s členom 4, členom 7(1), členom 11(3), členom 43(5) in (6) ter členom 48(5), začne veljati le, če mu niti Evropski parlament niti Svet ne nasprotuje v roku treh mesecev od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu ali če sta pred iztekom tega roka tako Evropski parlament kot Svet obvestila Komisijo, da mu ne bosta nasprotovala. Ta rok se na pobudo Evropskega parlamenta ali Sveta podaljša za tri mesece.

Člen 74

Postopek v odboru

1. Komisiji pomaga odbor. Ta odbor je odbor v smislu Uredbe (EU) št. 182/2011.

2. Pri sklicevanju na ta odstavek se uporablja člen 5 Uredbe (EU) št. 182/2011.

NASLOV XII

KONČNE DOLOČBE

Člen 75

Spremembe Uredbe (ES) št. 300/2008

V členu 4(3) Uredbe (ES) št. 300/2008 se doda naslednji pododstavek:

„Pri sprejemanju podrobnih ukrepov v zvezi s tehničnimi specifikacijami za varnostno opremo in postopke za njeno odobritev in uporabo v zvezi z umetnointeligenčnimi sistemi v smislu Uredbe (EU) YYY/XX [o umetni inteligenci] Evropskega parlamenta in Sveta* se upoštevajo zahteve iz poglavja 2 naslova III navedene uredbe.

_____

* Uredba (EU) YYY/XX [o umetni inteligenci] (UL …).“

Člen 76

Spremembe Uredbe (EU) št. 167/2013

V členu 17(5) Uredbe (EU) št. 167/2013 se doda naslednji pododstavek:

„Pri sprejemanju delegiranih aktov v skladu s prvim pododstavkom o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) YYY/XX [o umetni inteligenci] Evropskega parlamenta in Sveta*, se upoštevajo zahteve iz poglavja 2 naslova III navedene uredbe.

_____

* Uredba (EU) YYY/XX [o umetni inteligenci] (UL …).“

Člen 77

Spremembe Uredbe (EU) št. 168/2013

V členu 22(5) Uredbe (EU) št. 168/2013 se doda naslednji pododstavek:

„Pri sprejemanju delegiranih aktov v skladu s prvim pododstavkom o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) YYY/XX [o umetni inteligenci] Evropskega parlamenta in Sveta*, se upoštevajo zahteve iz poglavja 2 naslova III navedene uredbe.

_____

* Uredba (EU) YYY/XX [o umetni inteligenci] (UL …).“

Člen 78

Sprememba Direktive 2014/90/EU

V členu 8 Direktive 2014/90/EU se doda naslednji odstavek:

„4. Za umetnointeligenčne sisteme, ki so varnostne komponente v smislu Uredbe (EU) YYY/XX [o umetni inteligenci] Evropskega parlamenta in Sveta*, Komisija pri izvajanju svojih dejavnosti v skladu z odstavkom 1 ter pri sprejemanju tehničnih specifikacij in standardov testiranja v skladu z odstavkoma 2 in 3 upošteva zahteve iz poglavja 2 naslova III navedene uredbe.

_____

* Uredba (EU) YYY/XX [o umetni inteligenci] (UL …).“.

Člen 79

Sprememba Direktive (EU) 2016/797

V členu 5 Direktive (EU) 2016/797 se doda naslednji odstavek:

„12. Pri sprejemanju delegiranih aktov v skladu z odstavkom 1 in izvedbenih aktov v skladu z odstavkom 11 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) YYY/XX [o umetni inteligenci] Evropskega parlamenta in Sveta*, se upoštevajo zahteve iz poglavja 2 naslova III navedene uredbe.

_____

* Uredba (EU) YYY/XX [o umetni inteligenci] (UL …).“.

Člen 80

Sprememba Uredbe (EU) 2018/858

V členu 5 Uredbe (EU) 2018/858 se doda naslednji odstavek:

„4. Pri sprejemanju delegiranih aktov v skladu z odstavkom 3 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) YYY/XX [o umetni inteligenci] Evropskega parlamenta in Sveta*, se upoštevajo zahteve iz poglavja 2 naslova III navedene uredbe.

_____

* Uredba (EU) YYY/XX [o umetni inteligenci] (UL …).“.

Člen 81

Sprememba Uredbe (EU) 2018/1139

Uredba (EU) 2018/1139 se spremeni:

(1) V členu 17 se doda naslednji odstavek:

„3. Brez poseganja v odstavek 2 se pri sprejemanju izvedbenih aktov v skladu z odstavkom 1 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) YYY/XX [o umetni inteligenci] Evropskega parlamenta in Sveta*, upoštevajo zahteve iz poglavja 2 naslova III navedene uredbe.

_____

* Uredba (EU) YYY/XX [o umetni inteligenci] (UL …).“

(2) V členu 19 se doda naslednji odstavek:

„4. Pri sprejemanju delegiranih aktov v skladu z odstavkom 1 in 2 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) YYY/XX [o umetni inteligenci], se upoštevajo zahteve iz poglavja 2 naslova III navedene uredbe.“

(3) V členu 43 se doda naslednji odstavek:

„4. Pri sprejemanju izvedbenih aktov v skladu z odstavkom 1 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) YYY/XX [o umetni inteligenci], se upoštevajo zahteve iz poglavja 2 naslova III navedene uredbe.“

(4) V členu 47 se doda naslednji odstavek:

„3. Pri sprejemanju delegiranih aktov v skladu z odstavkom 1 in 2 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) YYY/XX [o umetni inteligenci], se upoštevajo zahteve iz poglavja 2 naslova III navedene uredbe.“

(5) V členu 57 se doda naslednji odstavek:

„Pri sprejemanju teh izvedbenih aktov o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) YYY/XX [o umetni inteligenci], se upoštevajo zahteve iz poglavja 2 naslova III navedene uredbe.“

(6) V členu 58 se doda naslednji odstavek:

„3. Pri sprejemanju delegiranih aktov v skladu z odstavkom 1 in 2 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) YYY/XX [o umetni inteligenci], se upoštevajo zahteve iz poglavja 2 naslova III navedene uredbe.“

Člen 82

Sprememba Uredbe (EU) 2019/2144

V členu 11 Uredbe (EU) 2019/2144 se doda naslednji odstavek:

„3. Pri sprejemanju izvedbenih aktov v skladu z odstavkom 2 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) YYY/XX [o umetni inteligenci]

Evropskega parlamenta in Sveta*, se upoštevajo zahteve iz poglavja 2 naslova III navedene uredbe.

_____

* Uredba (EU) YYY/XX [o umetni inteligenci] (UL …).“.

Člen 83

Umetnointeligenčni sistemi, ki so že dani na trg ali v uporabo

1. Ta uredba se ne uporablja za umetnointeligenčne sisteme, ki so komponente informacijskih sistemov velikega obsega, vzpostavljenih s pravnimi akti iz Priloge IX, ki so bili dani na trg ali v uporabo prej kot *[12 mesecev po datumu začetka uporabe te uredbe iz člena 85(2)]*, razen če se zaradi nadomestitve ali spremembe navedenih pravnih aktov bistveno spremeni zasnova ali predvideni namen zadevnega umetnointeligenčnega sistema ali umetnointeligenčnih sistemov.

   Zahteve iz te uredbe se po potrebi upoštevajo pri ocenjevanju vsakega obsežnega informacijskega sistema, vzpostavljenega s pravnimi akti iz Priloge IX, ki ga je treba izvesti, kot je določeno v teh zadevnih aktih.

2. Ta uredba se uporablja za umetnointeligenčne sisteme velikega tveganja, razen tistih iz odstavka 1, ki so bili dani na trg ali v uporabo pred [*datumom začetka uporabe te uredbe iz člena 85(2)*], samo če se od navedenega datuma pri teh sistemih bistveno spremeni njihova zasnova ali predvideni namen.

Člen 84

Ocena in pregled

1. Komisija enkrat letno po začetku veljavnosti te uredbe oceni potrebo po spremembi seznama iz Priloge III.

2. Komisija [*v treh letih po začetku uporabe te uredbe iz člena 85(2)*] ter nato vsaka štiri leta Evropskemu parlamentu in Svetu predloži poročilo o oceni in pregledu te uredbe. Poročila se objavijo.

3. V poročilih iz odstavka 2 se posebna pozornost nameni naslednjemu:

   (a) stanje finančnih in človeških virov pristojnih nacionalnih organov za učinkovito izvajanje nalog, dodeljenih s to uredbo;

   (b) stanje kazni, zlasti upravnih glob iz člena 71(1), ki jih države članice uporabljajo za kršitve določb te uredbe.

4. Komisija [*v treh letih po začetku uporabe te uredbe iz člena 85(2)*] ter nato vsaka štiri leta oceni vpliv in učinkovitost kodeksov ravnanja za spodbujanje uporabe zahtev iz poglavja 2 naslova III in morebitnih drugih dodatnih zahtev za umetnointeligenčne sisteme, ki niso umetnointeligenčni sistemi velikega tveganja.

5. Za namene odstavkov 1 do 4 odbor, države članice in pristojni nacionalni organi Komisiji na njeno zahtevo zagotovijo informacije.

6. Komisija pri izvajanju ocenjevanj in pregledov iz odstavkov 1 in 4 upošteva stališča in ugotovitve Odbora, Evropskega parlamenta, Sveta ter drugih ustreznih organov ali virov.

7. Komisija po potrebi predloži ustrezne predloge za spremembo te uredbe, zlasti ob upoštevanju razvoja tehnologije in glede na stanje napredka v informacijski družbi.

Člen 85

Začetek veljavnosti in uporaba

1. Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.
2. Ta uredba se začne uporabljati [24 mesecev po začetku veljavnosti te uredbe].
3. Z odstopanjem od odstavka 2:
   (a) poglavje 4 naslova III in naslov VI se začneta uporabljati [*tri mesece po začetku veljavnosti te uredbe*];
   (b) člen 71 se začne uporabljati [dvanajst mesecev po začetku veljavnosti te uredbe].

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju,

Za Evropski parlament	*Za Svet*
predsednik	*predsednik*

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

1. OKVIR PREDLOGA/POBUDE

1.1 Naslov predloga/pobude

1.2 Zadevna področja

1.3 Ukrep, na katerega se predlog/pobuda nanaša

1.4 Cilji

1.4.1 Splošni cilji

1.4.2 Specifični cilji

1.4.3 Pričakovani rezultati in posledice

1.4.4 Kazalniki smotrnosti

1.5 Utemeljitev predloga/pobude

1.5.1 Potrebe, ki jih je treba zadovoljiti kratkoročno ali dolgoročno, vključno s podrobno časovnico za uvajanje ustreznih ukrepov za izvajanje pobude

1.5.2 Dodana vrednost ukrepanja Unije (ki je lahko posledica različnih dejavnikov, npr. boljšega usklajevanja, pravne varnosti, večje učinkovitosti ali dopolnjevanja). Za namene te točke je „dodana vrednost ukrepanja Unije“ vrednost, ki izhaja iz ukrepanja Unije in predstavlja dodatno vrednost poleg tiste, ki bi jo sicer ustvarile države članice same

1.5.3 Spoznanja iz podobnih izkušenj v preteklosti

1.5.4 Skladnost z večletnim finančnim okvirom in možne sinergije z drugimi ustreznimi instrumenti

1.5.5 Ocena različnih razpoložljivih možnosti financiranja, vključno z možnostmi za prerazporeditev

1.6 Trajanje predloga/pobude in finančnih posledic

1.7 Načrtovani načini upravljanja

2. UKREPI UPRAVLJANJA

2.1 Pravila o spremljanju in poročanju

2.2 Upravljavski in kontrolni sistem

2.2.1 Utemeljitev načinov upravljanja, mehanizmov financiranja, načinov plačevanja in predlagane strategije kontrol

2.2.2 Podatki o ugotovljenih tveganjih in vzpostavljenih sistemih notranjih kontrol za njihovo zmanjševanje

2.2.3 Ocena in utemeljitev stroškovne učinkovitosti kontrol (razmerje „stroški kontrol ÷ vrednost z njimi povezanih upravljanih sredstev“) ter ocena pričakovane stopnje tveganja napake (ob plačilu in ob zaključku)

2.3 Ukrepi za preprečevanje goljufij in nepravilnosti

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1 Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

3.2 Ocenjene finančne posledice predloga za odobritve

3.2.1 Povzetek ocenjenih posledic za odobritve za poslovanje

3.2.2 Ocenjene realizacije, financirane z odobritvami za poslovanje

3.2.3 Povzetek ocenjenih posledic za upravne odobritve

3.2.4 Skladnost z veljavnim večletnim finančnim okvirom

3.2.5 Udeležba tretjih oseb pri financiranju

3.3 Ocenjene posledice za prihodke

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

1. OKVIR PREDLOGA/POBUDE

1.1. Naslov predloga/pobude

Uredba Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci (akt o umetni inteligenci) in spremembi nekaterih zakonodajnih aktov Unije

1.2. Zadevna področja

Komunikacijska omrežja, vsebine in tehnologija;

notranji trg, industrija, podjetništvo ter mala in srednja podjetja;

proračunski učinki se nanašajo na nove naloge, zaupane Komisiji, vključno s podporo odboru EU za umetno inteligenco;

Dejavnost: oblikovanje digitalne prihodnosti Evrope.

1.3. Ukrep, na katerega se predlog/pobuda nanaša

X **Nov ukrep**

☐ **Nov ukrep na podlagi pilotnega projekta / pripravljalnega ukrepa**[64]

☐ **Podaljšanje obstoječega ukrepa**

☐ **Ukrep, preusmerjen na nov ukrep**

1.4. Cilji

1.4.1. Splošni cilji

Splošni cilj intervencije je zagotoviti pravilno delovanje enotnega trga z ustvarjanjem pogojev za razvoj in uporabo zaupanja vredne umetne inteligence v Uniji.

1.4.2. Specifični cilji

Specifični cilj št. 1

Določiti posebne zahteve za umetnointeligenčne sisteme in obveznosti za vse udeležence v vrednostni verigi, da se zagotovi, da so umetnointeligenčni sistemi, ki so dani na trg in se uporabljajo, varni ter spoštujejo obstoječo zakonodajo o temeljnih pravicah in vrednotah Unije.

Specifični cilj št. 2

Zagotoviti pravno varnost za olajšanje naložb in inovacij na področju umetne inteligence, tako da se jasno določi, katere bistvene zahteve, obveznosti ter postopke za skladnost in usklajenost je treba upoštevati za uvedbo ali uporabo umetnointeligenčnega sistema na trgu Unije.

Specifični cilj št. 3

Izboljšati upravljanje in učinkovito izvrševanje obstoječe zakonodaje o temeljnih pravicah in varnostnih zahtevah, ki se uporabljajo za umetnointeligenčne sisteme, z zagotavljanjem novih pooblastil, virov in jasnih pravil za ustrezne organe glede

[64] Kot je navedeno v členu 54(2)(a) ali (b) finančne uredbe

postopkov ugotavljanja skladnosti in naknadnega spremljanja ter delitve nalog upravljanja in nadzora med nacionalno ravnjo in ravnjo EU.

Specifični cilj št. 4

Olajšati razvoj enotnega trga za zakonite, varne in zaupanja vredne uporabe umetne inteligence ter preprečiti razdrobljenost trga s sprejetjem ukrepov EU za določitev minimalnih zahtev za umetnointeligenčne sisteme, ki se dajejo in uporabljajo na trgu Unije v skladu z veljavno zakonodajo o temeljnih pravicah in varnosti.

1.4.3. Pričakovani rezultati in posledice

Navedite, kakšne učinke naj bi imel(-a) predlog/pobuda za upravičence/ciljne skupine.

Dobavitelji umetne inteligence bi morali imeti koristi od minimalnega, vendar jasnega sklopa zahtev, ki ustvarja pravno varnost in zagotavlja dostop do celotnega enotnega trga.

Uporabnikom umetne inteligence bi morala koristiti pravna varnost, da so umetnointeligenčni sistemi velikega tveganja, ki jih kupujejo, skladni z evropskimi zakoni in vrednotami.

Potrošniki bi morali imeti koristi od zmanjšanja tveganja kršitev njihove varnosti ali temeljnih pravic.

1.4.4. Kazalniki smotrnosti

Navedite, s katerimi kazalniki se bo spremljalo izvajanje predloga/pobude.

Kazalnik 1

Število hudih incidentov ali delovanj umetne inteligence, ki pomenijo hud incident ali kršitev obveznosti v zvezi s temeljnimi pravicami (polletno) po področjih uporabe in izračunano (a) v absolutnem smislu, (b) kot delež izdanih namenov uporab in (c) kot delež zadevnih državljanov.

Kazalnik 2

(a) Skupne naložbe v umetno inteligenco v EU (letno)

(b) Skupne naložbe v umetno inteligenco po državah članicah (letno)

(c) Delež podjetij, ki uporabljajo umetno inteligenco (letno)

(d) Delež MSP, ki uporabljajo umetno inteligenco (letno)

(a) in (b) se izračunata na podlagi uradnih virov in primerjata z zasebnimi ocenami

(c) in (d) se zbirata z rednimi raziskavami podjetij

1.5. Utemeljitev predloga/pobude

1.5.1. Potrebe, ki jih je treba zadovoljiti kratkoročno ali dolgoročno, vključno s podrobno časovnico za uvajanje ustreznih ukrepov za izvajanje pobude

Uredba bi se morala v celoti uporabljati eno leto in pol po sprejetju. Vendar bi morali biti elementi strukture upravljanja vzpostavljeni že pred tem. Države članice zlasti že prej imenujejo obstoječe organe in/ali ustanovijo nove organe, ki izvajajo naloge, določene v zakonodaji, Evropski odbor za umetno inteligenco pa mora biti ustanovljen in mora delovati. Do začetka uporabe bi morala evropska podatkovna zbirka umetnointeligenčnih sistemov v celoti delovati. Zato je treba vzporedno s postopkom sprejemanja razviti podatkovno zbirko, tako da se bo njen razvoj končal, ko bo uredba začela veljati.

1.5.2. Dodana vrednost ukrepanja Unije (ki je lahko posledica različnih dejavnikov, npr. boljšega usklajevanja, pravne varnosti, večje učinkovitosti ali dopolnjevanja). Za namene te točke je „dodana vrednost ukrepanja Unije“ vrednost, ki izhaja iz ukrepanja Unije in predstavlja dodatno vrednost poleg tiste, ki bi jo sicer ustvarile države članice same.

Nastajajoči neenotni okvir potencialno različnih nacionalnih pravil bo oviral nemoteno zagotavljanje umetnointeligenčnih sistemov po vsej EU ter je neučinkovit pri zagotavljanju varnosti in zaščite temeljnih pravic in vrednot Unije v različnih državah članicah. Skupni zakonodajni ukrep EU na področju umetne inteligence bi lahko spodbudil notranji trg ter ima velik potencial, da evropski industriji zagotovi konkurenčno prednost na svetovnem prizorišču in ekonomijo obsega, ki je posamezne države članice same ne morejo doseči.

1.5.3. Spoznanja iz podobnih izkušenj v preteklosti

Direktiva o elektronskem poslovanju (Direktiva 2000/31/ES) določa osnovni okvir za delovanje enotnega trga in nadzor digitalnih storitev ter vzpostavlja osnovno strukturo za splošni mehanizem sodelovanja med državami članicami, pri čemer načeloma zajema vse zahteve, ki se uporabljajo za digitalne storitve. Pri oceni Direktive so bile ugotovljene pomanjkljivosti glede več vidikov tega mehanizma sodelovanja, vključno s pomembnimi postopkovnimi vidiki, kot je neobstoj jasnih časovnih okvirov za odziv držav članic skupaj s splošno neodzivnostjo na zahteve njihovih partnerjev. Z leti je to povzročilo nezaupanje med državami članicami pri obravnavanju pomislekov glede ponudnikov čezmejnih digitalnih storitev. Pri vrednotenju Direktive je bila ugotovljena potreba po opredelitvi diferenciranega nabora pravil in zahtev na evropski ravni. Zato bi bil za izvajanje posebnih obveznosti iz te uredbe potreben poseben mehanizem sodelovanja na ravni EU s strukturo upravljanja, ki bi zagotavljala usklajevanje posameznih pristojnih organov na ravni EU.

1.5.4. Skladnost z večletnim finančnim okvirom in možne sinergije z drugimi ustreznimi instrumenti

Uredba o določitvi harmoniziranih pravil o umetni inteligenci in spremembi nekaterih zakonodajnih aktov Unije določa nov skupni okvir zahtev za sisteme umetne inteligence, ki precej presega okvir, ki ga določa obstoječa zakonodaja. Zato je treba s tem predlogom vzpostaviti novo nacionalno in evropsko regulativno in usklajevalno funkcijo.

Kar zadeva možne sinergije z drugimi ustreznimi instrumenti, lahko vlogo priglasitvenih organov na nacionalni ravni opravljajo nacionalni organi, ki opravljajo podobne naloge v skladu z drugimi predpisi EU.

Poleg tega s povečanjem zaupanja v umetno inteligenco in s tem spodbujanjem naložb v razvoj in sprejetje umetne inteligence dopolnjuje program za digitalno Evropo, za katerega je spodbujanje širjenja umetne inteligence ena od petih prednostnih nalog.

1.5.5. Ocena različnih razpoložljivih možnosti financiranja, vključno z možnostmi za prerazporeditev

Osebje bo prerazporejeno. Drugi stroški se bodo krili iz sredstev programa za digitalno Evropo glede na to, da cilj te uredbe – zagotavljanje zaupanja vredne

umetne inteligence – neposredno prispeva k enemu ključnih ciljev programa za digitalno Evrope – pospeševanju razvoja in uvajanja umetne inteligence v Evropi.

1.6. Trajanje predloga/pobude in finančnih posledic

☐ **Časovno omejeno**

– ☐ od [D. MMMM] LLLL do [D. MMMM] LLLL,

– ☐ finančne posledice med letoma LLLL in LLLL za odobritve za prevzem obveznosti ter med letoma LLLL in LLLL za odobritve plačil.

X **Časovno neomejeno**

– Izvajanje z obdobjem uvajanja od enega/dveh (še ni potrjeno) let,

– ki mu sledi izvajanje v celoti.

1.7. Načrtovani načini upravljanja[65]

X **Neposredno upravljanje** s strani Komisije:

– ☐ z lastnimi službami, vključno s svojim osebjem v delegacijah Unije,

– ☐ prek izvajalskih agencij.

☐ **Deljeno upravljanje** z državami članicami.

☐ **Posredno upravljanje**, tako da se naloge izvrševanja proračuna poverijo:

– ☐ tretjim državam ali organom, ki jih te imenujejo,

– ☐ mednarodnim organizacijam in njihovim agencijam (navedite),

– ☐ EIB in Evropskemu investicijskemu skladu,

– ☐ organom iz členov 70 in 71 finančne uredbe,

– ☐ subjektom javnega prava,

– ☐ subjektom zasebnega prava, ki opravljajo javne storitve, kolikor ti subjekti zagotavljajo ustrezna finančna jamstva,

– ☐ subjektom zasebnega prava države članice, ki so pooblaščeni za izvajanje javno-zasebnih partnerstev in ki zagotavljajo ustrezna finančna jamstva,

– ☐ osebam, pooblaščenim za izvajanje določenih ukrepov SZVP na podlagi naslova V PEU in opredeljenim v zadevnem temeljnem aktu.

– *Pri navedbi več kot enega načina upravljanja je treba to natančneje obrazložiti v oddelku „opombe“.*

Opombe

[65] Pojasnila o načinih upravljanja in sklici na finančno uredbo so na voljo na spletišču BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

2. UKREPI UPRAVLJANJA

2.1. Pravila o spremljanju in poročanju

Navedite pogostost in pogoje.

Uredba bo pregledana in ocenjena pet let po začetku veljavnosti te uredbe. Komisija bo o ugotovitvah ocene poročala Evropskemu parlamentu, Svetu in Evropskemu ekonomsko-socialnemu odboru.

2.2. Upravljavski in kontrolni sistemi

2.2.1. Utemeljitev načinov upravljanja, mehanizmov financiranja, načinov plačevanja in predlagane strategije kontrol

Uredba določa novo politiko v zvezi s harmoniziranimi pravili za zagotavljanje umetnointeligenčnih sistemov na notranjem trgu, ob tem pa zagotavlja spoštovanje varnosti in temeljnih pravic. Ta nova pravila zahtevajo mehanizem za usklajenost pri čezmejni uporabi obveznosti iz te uredbe v obliki nove svetovalne skupine, ki usklajuje dejavnosti nacionalnih organov.

Za izpolnjevanje teh novih nalog je treba službam Komisije zagotoviti ustrezna sredstva. Po ocenah je za izvrševanje nove uredbe potrebnih 10 EPDČ (5 EPDČ za podporo dejavnostim odbora in 5 EPDČ za Evropskega nadzornika za varstvo podatkov, ki deluje kot priglasitveni organ za umetnointeligenčne sisteme, ki jih uvede organ Evropske unije).

2.2.2. Podatki o ugotovljenih tveganjih in vzpostavljenih sistemih notranjih kontrol za njihovo zmanjševanje

Poleg tega je predvideno, da bi morala odboru pomagati upravna struktura Komisije, da bi lahko člani odbora sprejemali informirane analize na podlagi dejanskih dokazov, in da bi se ustanovila strokovna skupina, ki bi po potrebi zagotavljala dodatno strokovno znanje.

2.2.3. Ocena in utemeljitev stroškovne učinkovitosti kontrol (razmerje „stroški kontrol ÷ vrednost z njimi povezanih upravljanih sredstev“) ter ocena pričakovane stopnje tveganja napake (ob plačilu in ob zaključku)

Pri odhodkih za sestanke se glede na nizko vrednost posameznih transakcij (npr. povračilo potnih stroškov za delegata na sestanku) zdijo standardni kontrolni postopki zadostni. V zvezi z razvojem podatkovne zbirke ima GD CNECT vzpostavljen močan sistem notranje kontrole s centraliziranimi dejavnostmi javnega naročanja.

2.3. Ukrepi za preprečevanje goljufij in nepravilnosti

Navedite obstoječe ali načrtovane preprečevalne in zaščitne ukrepe, npr. iz strategije za boj proti goljufijam.

Obstoječi ukrepi za preprečevanje goljufij, ki se uporabljajo za Komisijo, bodo zajemali dodatne odobritve, potrebne za to uredbo.

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1. Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

- Obstoječe proračunske vrstice

Po vrstnem redu razdelkov večletnega finančnega okvira in proračunskih vrstic

Razdelek večletnega finančnega okvira	Proračunska vrstica	Type of Vrsta odhodkov	Prispevek			
	številka	Dif./nedif. [66]	držav Efte[67]	držav kandidatk [68]	tretjih držav	po členu 21(2)(b) finančne uredbe
7	20 02 06 Upravni odhodki	Nedif.	NE	NE	NE	NE
1	02 04 03 Umetna inteligenca programa za digitalno Evropo	Dif.	DA	NE	NE	NE
1	02 01 30 01 Odhodki za podporo programu za digitalno Evropo	Nedif.	DA	NE	NE	NE

3.2. Ocenjene finančne posledice predloga za odobritve

3.2.1. Povzetek ocenjenih posledic za odhodke za odobritve za poslovanje

– ☐ Za predlog/pobudo niso potrebne odobritve za poslovanje.

– X Za predlog/pobudo so potrebne odobritve za poslovanje, kot je pojasnjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

66 Dif. = diferencirana sredstva / nedif. = nediferencirana sredstva.

67 Efta: Evropsko združenje za prosto trgovino.

68 Države kandidatke in po potrebi potencialne države kandidatke z Zahodnega Balkana.

Razdelek večletnega finančnega okvira	1	

GD CNECT				Year**2022**	Year**2023**	Year**2024**	Year**2025**	Year**2026**	Year**2027**[69]	**SKUPAJ**	
• Odobritve za poslovanje											
Proračunska vrstica[70] 02 04 03		obveznosti	(1a)		1,000						**1,000**
		plačila	(2a)		0,600	0,100	0,100	0,100	0,100		**1,000**
Proračunska vrstica		obveznosti	(1b)								
		plačila	(2b)								
Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov[71]											
Proračunska vrstica 02 01 30 01			(3)		0,240	0,240	0,240	0,240	0,240		**1,200**
Odobritve za GD CNECT, SKUPAJ		obveznosti	= 1a + 1b + 3		**1,240**		**0,240**	**0,240**	**0,240**		**2,200**
		plačila	= 2a + 2b + 3		**0,840**	**0,340**	**0,340**	**0,340**	**0,340**		**2,200**

• Odobritve za poslovanje SKUPAJ		obveznosti	(4)		1,000						**1,000**

69 Okvirno in odvisno od razpoložljivih proračunskih sredstev.

70 Po uradni proračunski nomenklaturi.

71 Tehnična in/ali upravna pomoč ter odhodki za podporo izvajanja programov in/ali ukrepov EU (prej vrstice BA), posredne raziskave, neposredne raziskave.

	plačila	(5)		0,600	0,100	0,100	0,100	0,100		**1,000**
• Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov, SKUPAJ		(6)		**0,240**	**0,240**	**0,240**	**0,240**	**0,240**		**1,200**
Odobritve iz RAZDELKA 1 večletnega finančnega okvira, SKUPAJ	obveznosti	= 4 + 6		1,240	0,240	0,240	0,240	0,240		**2,200**
	plačila	= 5 + 6		0,840	0,340	0,340	0,340	0,340		**2,200**

Če ima predlog/pobuda posledice za več razdelkov, ponovite zgornji odsek:

• Odobritve za poslovanje SKUPAJ (vsi razdelki za poslovanje)	obveznosti	(4)								
	plačila	(5)								
• Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov, SKUPAJ (vsi razdelki za poslovanje)		(6)								
Odobritve iz RAZDELKOV od 1 do 6, SKUPAJ večletnega finančnega okvira(referenčni znesek)	obveznosti	= 4 + 6								
	plačila	= 5 + 6								

Razdelek večletnega finančnega okvira	7	„Upravni odhodki“

Ta oddelek se izpolni s „proračunskimi podatki upravne narave“, ki jih je treba najprej vnesti v Prilogo k oceni finančnih posledic zakonodajnega predloga (Priloga V k notranjim pravilom), ki se prenese v sistem DECIDE za namene posvetovanj med službami.

v mio. EUR (na tri decimalna mesta natančno)

		Year**2023**	Year**2024**	Year**2025**	Year**2026**	Leto **2027**	**Po letu 2027** [72]	**SKUPAJ**
GD CNECT								
• Človeški viri		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Drugi upravni odhodki		**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,050**
GD CNECT, SKUPAJ	**odobritve**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,850**
Evropski nadzornik za varstvo podatkov								
• Človeški viri		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Drugi upravni odhodki								
ENVP, SKUPAJ	**odobritve**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,800**
Odobritve iz RAZDELKA 7 večletnega finančnega okvira, SKUPAJ	(obveznosti skupaj = plačila skupaj)	1,530	1,530	1,530	1,530	1,530	1,530	**7,650**

v mio. EUR (na tri decimalna mesta natančno)

		Year**2022**	Year**2023**	Year**2024**	Year**2025**	Leto **2026**	Leto **2027**		**SKUPAJ**
Odobritve iz RAZDELKOV	obveznosti		2,770	1,770	1,770	1,770	1,770		**9,850**

[72] Vsi podatki v tem stolpcu so okvirni ter odvisni od nadaljevanja programov in razpoložljivosti odobritev.

od 1 do 7večletnega finančnega okvira, SKUPAJ	plačila		2,370	1,870	1,870	1,870	1,870	**9,850**

3.2.2. Ocenjene realizacije, financirane z odobritvami za poslovanje

odobritve za prevzem obveznosti v mio. EUR (na tri decimalna mesta natančno)

Cilji in realizacije ⇩			Year**2022**		Year**2023**		Year**2024**		Year**2025**		Year**2026**		Year**2027**		After**2027**[73]		**SKUPAJ**	
	REALIZACIJE																	
	vrsta	povprečni stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število realizacij skupaj	stroški realizacij skupaj
SPECIFIČNI CILJ št. 1[74] …																		
Podatkovna zbirka					1	1,000	1		1		1		1		1	0,100	1	1,000
Sestanki – realizacija					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Dejavnosti obveščanja					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Seštevek za specifični cilj št. 1																		
SPECIFIČNI CILJ št. 2 …																		
– realizacija																		
Seštevek za specifični cilj št. 2																		
SKUPAJ					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

[73] Vsi podatki v tem stolpcu so okvirni ter odvisni od nadaljevanja programov in razpoložljivosti odobritev.

[74] Kakor je opisan v točki 1.4.2 „Specifični cilji …“.

3.2.3. Povzetek ocenjenih posledic za upravne odobritve

– ☐ Za predlog/pobudo niso potrebne odobritve za upravne zadeve.

– X Za predlog/pobudo so potrebne odobritve za upravne zadeve, kot je pojasnjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

	Year**2022**	Year**2023**	Year**2024**	Year**2025**	Year**2026**	Year**2027**	**Vsako leto po 2027**[75]	**SKUPAJ**
RAZDELEK 7 večletnega finančnega okvira								
Človeški viri		1,520	1,520	1,520	1,520	1,520	**1,520**	**7,600**
Drugi upravni odhodki		0,010	0,010	0,010	0,010	0,010	**0,010**	**0,050**
Seštevek RAZDELEK 7 večletnega finančnega okvira		1,530	1,530	1,530	1,530	1,530	**1,530**	**7,650**
Odobritve zunaj RAZDELKA 7[76] **večletnega finančnega okvira**								
Človeški viri								
Drugi odhodki za upravne zadeve		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
Seštevek zunaj RAZDELKA 7 večletnega finančnega okvira		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
SKUPAJ		**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**8,850**

Potrebe po odobritvah za človeške vire in druge upravne odhodke se krijejo z odobritvami GD, ki so že dodeljene za upravljanje ukrepa in/ali so bile prerazporejene znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v postopku letne dodelitve virov glede na proračunske omejitve.

75 Vsi podatki v tem stolpcu so okvirni ter odvisni od nadaljevanja programov in razpoložljivosti odobritev.

76 Tehnična in/ali upravna pomoč ter odhodki za podporo izvajanja programov in/ali ukrepov EU (prej vrstice BA), posredne raziskave, neposredne raziskave.

3.2.3.1. Ocenjene potrebe po človeških virih

– ☐ Za predlog/pobudo niso potrebni človeški viri.

– X Za predlog/pobudo so potrebni človeški viri, kot je pojasnjeno v nadaljevanju:

ocena, izražena v ekvivalentu polnega delovnega časa

.		Year**2023**	Leto **2024**	Leto **2025**	**2026**	**2027**	**Po letu 2027**[77]	
• Delovna mesta v skladu s kadrovskim načrtom (uradniki in začasni uslužbenci)								
20 01 02 01 (sedež in predstavništva Komisije)		10	10	10	10	10	10	
20 01 02 03 (delegacije)								
01 01 01 01 (posredne raziskave)								
01 01 01 11 (neposredne raziskave)								
Druge proračunske vrstice (navedite)								
• Zunanji sodelavci (v ekvivalentu polnega delovnega časa: EPDČ)[78]								
20 02 01 (PU, NNS, ZU iz splošnih sredstev)								
20 02 03 (PU, LU, NNS, ZU in MSD na delegacijah)								
XX 01 xx **yy zz** [79]	– na sedežu							
	– na delegacijah							
01 01 01 02 (PU, NNS, ZU za posredne raziskave)								
01 01 01 12 (PU, NNS, ZU za neposredne raziskave)								
Druge proračunske vrstice (navedite)								
SKUPAJ		**10**	**10**	**10**	**10**	**10**	**10**	

XX je zadevno področje ali naslov v proračunu.

Potrebe po človeških virih se krijejo z osebjem GD, ki je že dodeljeno za upravljanje ukrepa in/ali je bilo prerazporejeno znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v postopku letne dodelitve virov glede na proračunske omejitve.

Od ENVP se pričakuje, da bo zagotovil polovico potrebnih sredstev.

Opis nalog:

Uradniki in začasni uslužbenci	Za pripravo skupno 13–16 sestankov, osnutkov poročil, nadaljevanje dela na področju politik, npr. v zvezi s prihodnjimi spremembami seznama namenov uporabe umetnointeligenčnih sistemov velikega tveganja, ter vzdrževanje odnosov z organi držav članic bodo potrebni štirje EPDČ AD in 1 EPDČ AST. Za umetnointeligenčne sisteme, ki jih razvijajo institucije EU, je odgovoren Evropski nadzornik za varstvo podatkov. Na podlagi preteklih izkušenj je mogoče oceniti, da bo za izpolnjevanje nalog ENVP v skladu z osnutkom zakonodaje potrebnih 5 EPDČ AD.
Zunanji sodelavci	

[77] Vsi podatki v tem stolpcu so okvirni ter odvisni od nadaljevanja programov in razpoložljivosti odobritev.

[78] PU = pogodbeni uslužbenec; LU = lokalni uslužbenec; NNS = napoteni nacionalni strokovnjak; ZU = začasni uslužbenec; MSD = mladi strokovnjak na delegaciji.

[79] Dodatna zgornja meja za zunanje sodelavce v okviru odobritev za poslovanje (prej vrstice BA).

3.2.4. Skladnost z veljavnim večletnim finančnim okvirom

Predlog/pobuda:

– X se lahko v celoti financira s prerazporeditvijo znotraj zadevnega razdelka večletnega finančnega okvira;

Ponovno programiranje ni potrebno.

– ☐ zahteva uporabo nedodeljene razlike do zgornje meje v zadevnem razdelku večletnega finančnega okvira in/ali uporabo posebnih instrumentov, kot so opredeljeni v uredbi o večletnem finančnem okviru;

Pojasnite te zahteve ter navedite zadevne razdelke in proračunske vrstice, ustrezne zneske in instrumente, ki naj bi bili uporabljeni.

– ☐ zahteva spremembo večletnega finančnega okvira.

Pojasnite te zahteve ter navedite zadevne razdelke in proračunske vrstice ter ustrezne zneske.

3.2.5. Udeležba tretjih oseb pri financiranju

V predlogu/pobudi:

– X ni načrtovano sofinanciranje tretjih oseb;

– ☐ je načrtovano sofinanciranje, kot je ocenjeno v nadaljevanju:

odobritve v mio. EUR (na tri decimalna mesta natančno)

	Year**N**[80]	Year**N+1**	Year**N+2**	Year**N+3**	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)			Skupaj
Navedite organ, ki bo sofinanciral predlog/pobudo								
Sofinancirane odobritve SKUPAJ								

[80] Leto N je leto začetka izvajanja predloga/pobude. Nadomestite „N“ s pričakovanim prvim letom izvajanja (na primer: 2021). Naredite isto za naslednja leta.

3.3. Ocenjene posledice za prihodke

– ☐ Predlog/pobuda ima finančne posledice, kot je pojasnjeno v nadaljevanju:

– ☐ Predlog/pobuda ima finančne posledice, kot je pojasnjeno v nadaljevanju:

  – ☐ za druge prihodke.

  – ☐ za druge prihodke.

  – Navedite, ali so prihodki dodeljeni za odhodkovne vrstice ☐.

v mio. EUR (na tri decimalna mesta natančno)

Prihodkovna proračunska vrstica	Odobritve na voljo za tekoče proračunsko leto	Posledice predloga/pobude[81]						
		Year**N**	Year**N+1**	Year**N+2**	Year**N+3**	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)		
Člen …….								

Za namenske prejemke navedite zadevne odhodkovne proračunske vrstice.

Druge opombe (npr. metoda/formula za izračun posledic za prihodke ali druge informacije).

[81] Pri tradicionalnih lastnih sredstvih (carine, prelevmani na sladkor) se navedejo neto zneski, tj. bruto zneski po odbitku 20 % stroškov pobiranja.