Svet
Evropske unije

Bruselj, 25. november 2022
(OR. en)

14954/22

Medinstitucionalna zadeva:
2021/0106(COD)

LIMITE

TELECOM 472
JAI 1494
COPEN 396
CYBER 374
DATAPROTECT 320
EJUSTICE 89
COSI 293
IXIM 267
ENFOPOL 569
RELEX 1556
MI 843
COMPET 918
CODEC 1773

DOPIS

Pošiljatelj:	Odbor stalnih predstavnikov (1. del)
Prejemnik:	Svet
Št. predh. dok.:	14336/22
Št. dok. Kom.:	8115/21
Zadeva:	Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach

I. UVOD

1. Komisija je 21. aprila 2021 sprejela Predlog uredbe o določitvi harmoniziranih pravil o umetni inteligenci **(akt o umetni inteligenci)**.

2. Cilji predloga Komisije, so zagotoviti, da so umetnointeligenčni sistemi, ki so dani na trg Unije in se uporabljajo v Uniji, 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 varnosti ter olajšati razvoj enotnega trga za zakonite, varne in zaupanja vredne uporabe umetne inteligence, hkrati pa preprečiti razdrobljenost trga.

II. DELO V DRUGIH INSTITUCIJAH

3. V Evropskem parlamentu razprave vodi Odbor za notranji trg in varstvo potrošnikov (IMCO; poročevalec: Brando Benifei, S&D, Italija) in Odbor za državljanske svoboščine, pravosodje in notranje zadeve (LIBE; poročevalec: Dragos Tudorache, Renew, Romunija) po postopku s skupnimi sejami odborov. Odbor za pravne zadeve (JURI), Odbor za industrijo, raziskave in energetiko (ITRE) ter Odbor za kulturo in izobraževanje (CULT) sodelujejo pri zakonodajnem delu z deljenimi in/ali izključnimi pristojnostmi. Soporočevalca sta osnutek poročila predstavila aprila 2022, glasovanje o skupnem poročilu odborov IMCO in LIBE pa je predvideno v prvem četrtletju leta 2023.

4. Evropski ekonomsko-socialni odbor je mnenje o predlogu dal 22. septembra 2021, nato pa 2. decembra 2021 še Evropski odbor regij.

5. Evropski odbor za varstvo podatkov (EOVP) in Evropski nadzornik za varstvo podatkov (ENVP) sta 18. junija 2021 dala skupno mnenje o predlogu.

6. Evropska centralna banka (ECB) je mnenje dala 29. decembra 2021 in ga 10. februarja 2022 predstavila Delovni skupini za telekomunikacije in informacijsko družbo (v nadaljnjem besedilu: Delovna skupina TELECOM).

III. TRENUTNO STANJE V SVETU

1. V Svetu je predlog preučila Delovna skupina TELECOM, ki je predlog začela obravnavati med portugalskim predsedovanjem na več sestankih in delavnicah, organiziranih med aprilom in junijem 2021. Delo v zvezi s predlogom se je nadaljevalo med slovenskim predsedovanjem, ki je pripravilo prvi delni kompromisni predlog, ki zajema **člene 1–7 in priloge I–III**. Poleg tega je slovensko predsedstvo organiziralo neformalni poldnevni Svet ministrov in ministric za telekomunikacije, posvečen izključno predlogu akta o umetni inteligenci, na katerem so ministri in ministrice potrdili, da podpirajo horizontalen in humanocentričen pristop k urejanju umetne inteligence. Francosko predsedstvo je nadaljevalo postopek obravnave in do konca svojega mandata preoblikovalo preostale dele besedila **(členi 8–85 in prilogi IV–IX)** ter 17. junija 2022 predstavilo celoten prvi konsolidirani kompromisni predlog akta o umetni inteligenci.

2. Češko predsedstvo je 5. julija 2022 v Delovni skupini TELECOM opravilo orientacijsko razpravo na podlagi dokumenta o političnih možnostih, katerega rezultati so bili uporabljeni za pripravo **drugega kompromisnega besedila.** Na podlagi odzivov delegacij na ta kompromisno besedilo je pripravilo **tretje kompromisno besedilo**, ki ga je Delovna skupina TELECOM predstavila in o njem razpravljala 22. in 29. septembra 2022. Po teh razpravah so bile delegacije pozvane, naj predložijo dodatne pisne pripombe, ki jih je češko predsedstvo uporabilo za osnutek **četrtega kompromisnega predloga**. Češko predsedstvo je na podlagi razprav o četrtem kompromisnem predlogu, ki so potekale 25. oktobra 2022 in 8. novembra 2022 v Delovni skupini za telekomunikacije, ter ob upoštevanju končnih pisnih pripomb držav članic pripravilo **končno različico kompromisnega besedila**, ki je v prilogi. Coreper je 18. novembra preučil ta kompromisni predlog in se **soglasno dogovoril, da ga brez sprememb predloži Svetu PTE (telekomunikacije), da bi lahko na seji 6. decembra 2022 sprejel splošni pristop**.

IV. GLAVNI ELEMENTI KOMPROMISNEGA PREDLOGA

1. Opredelitev umetnointeligenčnega sistema, prepovedane prakse umetne inteligence, seznam primerov uporabe umetne inteligence velikega tveganja v Prilogi III in razvrstitev umetnointeligenčnih sistemov med sisteme velikega tveganja

1.1 Da bi zagotovili, da opredelitev umetnointeligenčnega sistema zagotavlja dovolj jasna merila za razlikovanje med umetno inteligenco in bolj klasičnimi sistemi programske opreme, kompromisno besedilo opredelitev iz **člena 3(1)** omejuje na sisteme, razvite s pristopi strojnega učenja ter pristopi, ki temeljijo na logiki in znanju.

1.2 Kar zadeva prenos pooblastil na Komisijo v zvezi s posodobitvami opredelitve umetnointeligenčnega sistema, je bila črtana **Priloga I** in ustrezno pooblastilo Komisije, da jo posodobi z delegiranimi akti. Namesto tega sta bili dodani novi **uvodni izjavi 6a in 6b**, da bi pojasnili, kaj je mišljeno s pristopi strojnega učenja ter pristopi, ki temeljijo na logiki in znanju. Da bi akt o umetni inteligenci ostal prožen in primeren za prihodnost, je bila v **člen 4** dodana možnost sprejetja izvedbenih aktov za podrobnejšo opredelitev in posodobitev tehnik v okviru pristopov strojnega učenja ter pristopov, ki temeljijo na logiki in znanju.

1.3 Kar zadeva prepovedane prakse umetne inteligence, kompromisno besedilo v **členu 5** vsebuje razširitev prepovedi uporabe umetne inteligence za družbeno točkovanje tudi na zasebne akterje. Poleg tega določba o prepovedi uporabe umetnointeligenčnih sistemov, ki izkoriščajo šibke točke določene skupine oseb, zdaj zajema tudi osebe, ki so ranljive zaradi svojega socialnega ali ekonomskega položaja. Kar zadeva prepoved uporabe sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, kompromisno besedilo pojasnjuje cilje, kadar se šteje, da je taka uporaba nujno potrebna za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in za katere bi bilo treba tem organom izjemoma dovoliti uporabo takih sistemov.

1.4 Kar zadeva seznam primerov uporabe umetne inteligence velikega tveganja iz **Priloge III**, so bili trije od njih črtani (odkrivanje globokih ponaredkov s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, analiza kaznivih dejanj, preverjanje pristnosti potnih listin), dva dodana (kritična digitalna infrastruktura ter življenjsko in zdravstveno zavarovanje), drugi pa so bili natančneje opredeljeni. Hkrati je bil **člen 7(1)** spremenjen, da bi se omogočila poleg vključitve primerov uporabe velikega tveganja na seznam, na podlagi delegiranih aktov, tudi črtanje teh primerov. Za zagotovitev ustrezne zaščite temeljnih pravic v primeru takih izbrisov so bile v **člen 7(3)** dodane dodatne določbe, v katerih so navedeni pogoji, ki bi morali biti izpolnjeni, preden se lahko sprejme delegirani akt.

1.5 Kar zadeva razvrstitev umetnointeligenčnih sistemov med sisteme velikega tveganja, kompromisni predlog zdaj poleg razvrstitve velikega tveganja iz **Priloge III** vključuje dodatno horizontalno raven za zagotovitev, da umetnointeligenčni sistemi, za katere ni verjetno, da bi povzročili resne kršitve temeljnih pravic ali druga znatna tveganja, ne bodo uvrščeni med tvegane. Natančneje, **člen 6(3)** vsebuje nove določbe, v skladu s katerimi bi bilo treba pri razvrstitvi umetnointeligenčnih sistemov med sisteme velikega tveganja upoštevati tudi pomen izhodnih podatkov umetnointeligenčnega sistema v zvezi z zadevnim ukrepom ali odločitvijo, ki jo je treba sprejeti. Pomen izhodnih podatkov umetnointeligenčnega sistema bi se ocenil na podlagi tega, ali so v zvezi z zadevnim ukrepom ali odločitvijo, ki jo je treba sprejeti, zgolj pomožni.

2. Zahteve za umetnointeligenčne sisteme velikega tveganja in odgovornosti različnih akterjev v vrednostni verigi umetne inteligence

2.1 Številne zahteve za umetnointeligenčne sisteme velikega tveganja, kot so določene v **poglavju 2 naslova III** predloga, so bile pojasnjene in prilagojene tako, da so tehnično bolj izvedljive in manj obremenjujoče za deležnike, na primer v zvezi s kakovostjo podatkov ali tehnično dokumentacijo, ki bi jo morala pripraviti mala in srednja podjetja, da bi dokazala, da njihovi umetnointeligenčni sistemi velikega tveganja izpolnjujejo zahteve.

2.2 Glede na to, da se umetnointeligenčni sistemi razvijajo in distribuirajo prek zapletenih vrednostnih verig, kompromisno besedilo vključuje spremembe, ki pojasnjujejo razdelitev odgovornosti in vlog. Dodane so bile na primer nekatere dodatne določbe v **členih 13 in 14**, ki omogočajo učinkovitejše sodelovanje med ponudniki in uporabniki. Namen kompromisnega besedila je tudi pojasniti razmerje med odgovornostmi, ki izhajajo iz akta o umetni inteligenci in tistimi, ki že obstajajo na podlagi druge zakonodaje, kot je ustrezna zakonodaja Unije o varstvu podatkov ali sektorska zakonodaja, tudi kar zadeva sektor finančnih storitev. Poleg tega novi **člen 23a** jasneje navaja primere, v katerih morajo drugi akterji v vrednostni verigi prevzeti odgovornosti ponudnika.

3. **Umetnointeligenčni sistemi za splošne namene**

3.1 Dodan je bil nov **naslov IA**, da bi se upoštevali primeri, ko se lahko umetnointeligenčni sistemi uporabljajo za številne različne namene (umetna inteligenca za splošne namene) in v katerih se lahko tehnologija umetne inteligence za splošne namene vključi v drug sistem, ki lahko postane sistem velikega tveganja. Kompromisno besedilo v **členu 4b(1)** določa, da bi se nekatere zahteve za umetnointeligenčne sisteme velikega tveganja uporabljale tudi za umetnointeligenčne sisteme za splošne namene. Vendar bi bilo treba namesto neposredne uporabe teh zahtev z izvedbenim aktom določiti, kako bi jih bilo treba uporabljati v zvezi z umetnointeligenčnimi sistemi za splošne namene, in sicer na podlagi posvetovanja in podrobne ocene učinka ter ob upoštevanju posebnih značilnosti teh sistemov in z njimi povezane vrednostne verige, tehnične izvedljivosti ter tržnega in tehnološkega razvoja. Uporaba izvedbenega akta bo zagotovila, da bodo države članice ustrezno vključene, in da bodo še naprej odločale o tem, kako se bodo v tem okviru uporabljale zahteve.

3.2 Poleg tega kompromisno besedilo **člena 4b(5)** vključuje tudi možnost sprejetja nadaljnjih izvedbenih aktov, ki bi določali načine sodelovanja med ponudniki umetnointeligenčnih sistemov za splošne namene in drugimi ponudniki, ki nameravajo take sisteme dati v obratovanje ali na trg Unije kot umetnointeligenčne sisteme velikega tveganja, predvsem kar zadeva zagotavljanje informacij.

4. **Pojasnitev področja uporabe predlaganega akta o umetni inteligenci in določb v zvezi z organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj**

4.1 V **členu 2** je izrecno navedena izključitev nacionalne varnosti, obrambe in vojaških namenov iz področja uporabe akta o umetni inteligenci. Podobno je bilo pojasnjeno, da se akt o umetni inteligenci ne bi smel uporabljati za umetnointeligenčne sisteme in njihove izhodne podatke, ki se uporabljajo izključno za raziskave in razvoj, ter za obveznosti ljudi, ki umetno inteligenco uporabljajo za nepoklicne namene, ki ne bi spadali na področje uporabe akta o umetni inteligenci, razen obveznosti glede preglednosti.

4.2 Da bi se upoštevale posebnosti organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, so bile določbe v zvezi z uporabo umetnointeligenčnih sistemov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj večkrat spremenjene. Nekatere s tem povezane opredelitve pojmov iz **člena 3**, kot sta „sistem za biometrično identifikacijo na daljavo“ in „sistem za biometrično identifikacijo na daljavo v realnem času“, so bile natančneje določene, da bi se pojasnilo, katere situacije bi spadale v povezan primer prepovedi in uporabe velikega tveganja ter katere situacije ne. Kompromisni predlog vsebuje tudi druge spremembe, ki so ob upoštevanju ustreznih zaščitnih ukrepov namenjene zagotavljanju ustrezne ravni prožnosti pri uporabi umetnointeligenčnih sistemov velikega tveganja s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali razmisleku o tem, ali je treba spoštovati zaupnost občutljivih operativnih podatkov v zvezi z njihovimi dejavnostmi.

5. **Ugotavljanje skladnosti, okvir upravljanja, nadzor trga, izvrševanje in kazni**

5.1 Da bi poenostavili okvir skladnosti za akt o umetni inteligenci, kompromisno besedilo vsebuje več pojasnil in poenostavitev določb o postopkih ugotavljanja skladnosti. Prav tako so bile pojasnjene in poenostavljene določbe v zvezi z nadzorom trga, da bi bile učinkovitejše in bi jih bilo lažje izvajati, pri čemer je bilo upoštevano dejstvo, da je v zvezi s tem potreben sorazmeren pristop. Poleg tega je bil **člen 41** temeljito pregledan, da bi se omejila diskrecijska pravica Komisije v zvezi s sprejetjem izvedbenih aktov o določitvi skupnih tehničnih specifikacij za zahteve za umetnointeligenčne sisteme velikega tveganja in umetnointeligenčne sisteme za splošne namene.

5.2 V kompromisnem besedilu so tudi bistveno spremenjene določbe o odboru za umetno inteligenco (v nadaljnjem besedilu: odbor), da bi se zagotovila njegova večja avtonomija in okrepila njegova vloga v strukturi upravljanja akta o umetni inteligenci. V zvezi s tem sta bila revidirana **člena 56 in 58**, da bi se okrepila vloga odbora, ki bi tako moral biti v boljšem položaju za zagotavljanje podpore državam članicam pri izvajanju in izvrševanju akta o umetni inteligenci. Natančneje, naloge odbora so bile razširjene in določena je bila njegova sestava. Da bi zagotovili sodelovanje deležnikov v zvezi z vsemi vprašanji, povezanimi z izvajanjem akta o umetni inteligenci, vključno s pripravo izvedbenih in delegiranih aktov, je bila dodana nova zahteva, da odbor ustanovi stalno podskupino, ki bo služila kot platforma za širok krog deležnikov. Za okrepitev skladnosti upravljanja in izvrševanja akta o umetni inteligenci po vsej Uniji bi bilo treba ustanoviti tudi dve drugi stalni podskupini za organe za nadzor trga in priglasitvene organe.

5.3 Za nadaljnje izboljšanje okvira upravljanja kompromisno besedilo vključuje nova člena **(68a in 68b)**. **Člen 68a** vključuje zahtevo, da Komisija imenuje eno ali več preizkuševalnih zmogljivosti Unije na področju umetne inteligence, ki bi morale zagotavljati neodvisno tehnično ali znanstveno svetovanje na zahtevo odbora ali organov za nadzor trga, **člen 68b** pa določa, da mora Komisija vzpostaviti centralno skupino neodvisnih strokovnjakov za podporo dejavnostim izvrševanja, ki se zahtevajo v skladu z aktom o umetni inteligenci. Nazadnje obstaja tudi nov **člen 58a**, ki določa obveznost Komisije, da pripravi smernice o uporabi akta o umetni inteligenci.

5.4 Kar zadeva kazni za kršitve določb akta o umetni inteligenci, kompromisno besedilo v **členu 71** določa sorazmernejše zgornje meje zneska upravnih glob za MSP in zagonska podjetja. Poleg tega so bila v **členu 71(6)** dodana še štiri merila za odločanje o višini upravnih glob, da bi se dodatno zaščitila njihova splošna sorazmernost.

6. **Preglednost in druge določbe v korist prizadetih oseb**

6.1 Kompromisni predlog vključuje številne spremembe, ki povečujejo preglednost v zvezi z uporabo umetnointeligenčnih sistemov velikega tveganja. Predvsem je bil posodobljen **člen 51**, ki navaja, da se bodo morali tudi nekateri uporabniki umetnointeligenčnega sistema velikega tveganja, ki so javni organi, agencije ali telesa, registrirati v podatkovni zbirki EU za umetnointeligenčne sisteme velikega tveganja iz Priloge III. Poleg tega novi **člen 52(2a)** poudarja obveznost uporabnikov sistema za prepoznavanje čustev, da obvestijo fizične osebe, kadar so izpostavljene takemu sistemu.

6.2 Kompromisni predlog v novem **členu 63(11)** tudi jasno določa, da se lahko fizična ali pravna oseba, ki utemeljeno meni, da je prišlo do kršitve določb akta o umetni inteligenci, pritoži pri ustreznem organu za nadzor trga in lahko pričakuje, da bo taka pritožba obravnavana v skladu z namenskimi postopki tega organa.

7. **Ukrepi v podporo inovacijam**

7.1 Da bi ustvarili pravni okvir, ki bo bolj naklonjen inovacijam, in da bi spodbudili z dokazi podprto regulativno učenje, so bile določbe o ukrepih v podporo inovacijam iz **člena 53** v kompromisnem besedilu bistveno spremenjene. Predvsem je bilo pojasnjeno, da bi morali regulativni peskovniki za umetno inteligenco, ki naj bi vzpostavili nadzorovano okolje za razvoj, testiranje in potrjevanje inovativnih umetnointeligenčnih sistemov pod neposrednim nadzorom in smernicami nacionalnih pristojnih organov, omogočati tudi testiranje inovativnih umetnointeligenčnih sistemov v dejanskih razmerah. Poleg tega so bile dodane nove določbe v **členih 54a in 54b**, ki omogočajo nenadzorovano testiranje umetnointeligenčnih sistemov v dejanskih razmerah, in sicer pod posebnimi pogoji in zaščitnimi ukrepi. V obeh primerih je v kompromisnem besedilu pojasnjeno, kako je treba ta nova pravila razlagati v povezavi z drugo obstoječo sektorsko zakonodajo o regulativnih peskovnikih.

7.2 Da bi zmanjšali upravno breme za manjša podjetja, kompromisno besedilo v **členu 55** vključuje seznam ukrepov, ki jih mora Komisija sprejeti za podporo takim gospodarskim subjektom, v **členu 55a** pa določa nekatera omejena in jasno opredeljena odstopanja.

V. ZAKLJUČEK

1. Svet naj zato:
   - preuči kompromisno besedilo iz priloge k temu dopisu,
   - na seji Sveta PTE (telekomunikacije) 6. decembra 2022 potrdi splošni pristop glede Predloga uredbe o določitvi harmoniziranih pravil o umetni inteligenci (akt o umetni inteligenci).

_____

PRILOGA

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

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

(Besedilo velja za EGP)

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

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

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora[1],

ob upoštevanju mnenja Odbora regij[2],

ob upoštevanju mnenja Evropske centralne banke[3],

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

[1] UL C […], […], str. […].
[2] UL C […], […], str. […].
[3] Navedba mnenja ECB

(1) Namen te uredbe je izboljšati delovanje notranjega trga z določitvijo enotnega pravnega okvira, predvsem 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, uvažajo 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 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 obratovanje 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 in na podlagi dela strokovne skupine na visoki ravni za umetno inteligenco, kot je navedeno v smernicah za zaupanja vredno umetno inteligenco v EU, ta uredba podpira cilj, da Unija postane vodilna v svetu pri razvoju varne, zaupanja vredne in etične umetne inteligence, kot je navedel Evropski svet[4], ter zagotavlja zaščito etičnih načel, kot je izrecno zahteval Evropski parlament[5].

---

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

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

(5a) Harmonizirana pravila o dajanju umetnointeligenčnih sistemov na trg, v obratovanje in uporabo, določena v tej uredbi, bi se morala uporabljati v vseh sektorjih in v skladu s pristopom novega zakonodajnega okvira ne bi smela posegati v veljavno pravo Unije, predvsem o varstvu podatkov, varstvu potrošnikov, temeljnih pravicah, zaposlovanju in varnosti proizvodov, katerega ta uredba dopolnjuje. Zato vse pravice in pravna sredstva, ki jih takšno pravo Unije zagotavlja potrošnikom in drugim osebam, na katere lahko umetnointeligenčni sistemi negativno vplivajo, tudi v zvezi z nadomestilom morebitne škode v skladu z Direktivo Sveta 85/374/EGS z dne 25. julija 1985 o približevanju zakonov in drugih predpisov držav članic v zvezi z odgovornostjo za proizvode z napako, ostanejo nespremenjeni in se v celoti uporabljajo. Namen te uredbe je tudi okrepiti učinkovitost takih obstoječih pravic in pravnih sredstev z določitvijo posebnih zahtev in obveznosti, tudi glede preglednosti, tehnične dokumentacije in vodenja evidenc umetnointeligenčnih sistemov. Poleg tega bi se morale obveznosti, naložene različnim operaterjem, vključenim v vrednostno verigo umetne inteligence v skladu s to uredbo, uporabljati brez poseganja v nacionalno zakonodajo, ki je v skladu s pravom Unije in katere učinek je omejitev uporabe nekaterih umetnointeligenčnih sistemov, kadar taki zakoni ne spadajo na področje uporabe te uredbe ali so namenjeni uresničevanju drugih legitimnih ciljev javnega interesa, ki niso cilji iz te uredbe. Ta uredba na primer ne bi smela vplivati na nacionalno delovno pravo in pravo o varstvu mladoletnikov (tj. oseb, mlajših od 18 let), ob upoštevanju Splošne pripombe Združenih narodov št. 25 (2021) o otrokovih pravicah, če se to pravo ne nanaša posebej na umetnointeligenčne sisteme in so ti namenjeni uresničevanju drugih legitimnih ciljev javnega interesa.

(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 umetne inteligence, kot so njene zmogljivosti učenja, sklepanja ali modeliranja, pri čemer bi jo bilo treba razlikovati od enostavnejših sistemov programske opreme in programskih pristopov. Konkretno, za namene te uredbe bi morali biti umetnointeligenčni sistemi zmožni, da na podlagi podatkov in vhodnih podatkov, ki so ustvarjeni strojno ali jih ustvari človek, z uporabo strojnega učenja in/ali pristopov, ki temeljijo na logiki in znanju, sklepajo o načinu za dosego sklopa ciljev, ki jih določi človek, ter ustvarjajo izhodne podatke, kot so vsebine za generativne umetnointeligenčne sisteme (na primer besedila, videoposnetki ali slike), napovedi, priporočila ali odločitve, ki vplivajo na okolje, s katerim je sistem v interakciji, bodisi v fizični bodisi digitalni razsežnosti. Sistem, ki za samodejno izvajanje operacij uporablja pravila, ki jih opredelijo izključno fizične osebe, se ne bi smel šteti za umetnointeligenčni sistem. 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). Pojem avtonomije umetnointeligenčnega sistema se nanaša na stopnjo delovanja takega sistema brez človeškega sodelovanja.

(6a) Pristopi strojnega učenja so usmerjeni na razvoj sistemov, ki se lahko učijo in na podlagi sklepanja iz podatkov rešijo aplikacijski problem, ne da bi bili izrecno programirani s sklopom navodil po korakih od vhoda do izhoda. Učenje se nanaša na računalniški proces, pri katerem se na podlagi podatkov optimizirajo parametri modela, ki je matematični konstrukt in ustvarja izhodne podatke na podlagi vhodnih podatkov. Vrsta težav, ki jih obravnava strojno učenje, običajno vključuje naloge, pri katerih drugi pristopi niso uspešni, bodisi ker problem ni ustrezno formaliziran ali ker rešitev problema ni izvedljiva s pristopi, ki ne temeljijo na učenju. Pristopi strojnega učenja vključujejo na primer nadzorovano, nenadzorovano in spodbujevalno učenje, pri katerih se uporabljajo različne metode, vključno z globokim učenjem z nevronskimi mrežami, statističnimi tehnikami za učenje in sklepanje (vključno na primer z logistično regresijo, Bayesovim ocenjevanjem) ter metodami iskanja in optimizacije.

(6b) Logični pristopi in pristopi, ki temeljijo na znanju, so pri reševanju aplikacijskih problemov usmerjeni na razvoj sistemov z zmožnostmi logičnega sklepanja o znanju. Taki sistemi običajno vključujejo bazo znanja in inferenčni sistem, ki s sklepanjem na podlagi znanja ustvarja izhodne podatke. Baza znanja, ki jo običajno kodirajo človeški strokovnjaki, predstavlja entitete in logična razmerja, pomembna za aplikacijski problem, in sicer tako, da se določijo formalizmi, ki temeljijo na pravilih, ontologijah ali diagramih znanja. Inferenčni sistem deluje na podlagi baze znanja in pridobiva nove informacije z operacijami, kot so razvrščanje, iskanje, prileganje ali veriženje. Pristopi, ki temeljijo na logiki in znanju, vključujejo na primer predstavitev znanja, induktivno (logično) programiranje, baze znanja, inferenčne in deduktivne sisteme, (simbolno) sklepanje, strokovne sisteme ter metode iskanja in optimizacije.

(6c) Da se zagotovijo enotni pogoji za izvajanje te uredbe v zvezi s pristopi strojnega učenja ter pristopi, ki temeljijo na logiki in znanju, ter da se upošteva tržni in tehnološki razvoj, bi bilo treba na Komisijo prenesti izvedbena pooblastila.

(6d) Pojem „uporabnik“ iz te uredbe bi bilo treba razlagati kot vsako fizično ali pravno osebo, vključno z javnim organom, agencijo ali drugim telesom, ki uporablja umetnointeligenčni sistem, pod pristojnostjo katerega se sistem uporablja. Glede na vrsto umetnointeligenčnega sistema lahko uporaba sistema vpliva na osebe, ki niso uporabnik.

(7) Pojem biometričnih podatkov, uporabljen v tej uredbi, bi bilo treba razlagati skladno s pojmom biometričnih podatkov, kot je opredeljen v členu 4(14) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta[6], členu 3(18) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta[7] ter členu 3(13) Direktive (EU) 2016/680 Evropskega parlamenta in Sveta[8].

[6] 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).

[7] Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

[8] 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).

(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, običajno na daljavo, brez njihovega dejavnega sodelovanja, s primerjavo biometričnih podatkov osebe z biometričnimi podatki iz odložišča referenčnih podatkov, ne glede na uporabljeno tehnologijo, procese ali vrste biometričnih podatkov. Taki sistemi za biometrično identifikacijo na daljavo se običajno uporabljajo za hkratno zaznavanje (skeniranje) več oseb ali njihovega vedenja, da se znatno olajša identifikacija več oseb brez njihovega dejavnega sodelovanja. Taka opredelitev izključuje sisteme za preverjanje/avtentifikacijo z izključnim namenom potrditve identitete določene fizične osebe, ter sisteme, ki se uporabljajo za potrjevanje identitete fizične osebe izključno z namenom dostopa do storitve, naprave ali prostorov. Ta izključitev je utemeljena z dejstvom, da bodo imeli taki sistemi verjetno manjši vpliv na temeljne pravice fizičnih oseb v primerjavi s sistemi za biometrično identifikacijo na daljavo, ki se lahko uporabljajo za obdelavo biometričnih podatkov velikega števila oseb. 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) Za namene te uredbe bi bilo treba pojem javno dostopnega prostora razumeti kot vsak fizični prostor, ki je dostopen nedoločenemu številu fizičnih oseb, ne glede na to, ali je ta prostor v zasebni ali javni lasti, in ne glede na dejavnost, za katero se ta kraj uporablja, kot je komercialna (na primer trgovine, restavracije, kavarne), storitvena (na primer banke, poklicne dejavnosti, gostinske ali nastanitvene dejavnosti), športna (na primer bazeni, telovadnice, stadioni), prevozna (na primer avtobusne postaje, postaje podzemne železnice in železniške postaje, letališča, prevozna sredstva), razvedrilna (na primer kinematografi, gledališča, muzeji, koncertne in konferenčne dvorane) dejavnost, dejavnosti v prostem času ali druge (na primer javne ceste in trgi, parki, gozdovi, igrišča). Prostor bi bilo treba opredeliti kot javno dostopen tudi, če za dostop ne glede na morebitne omejitve zmogljivosti ali varnostne omejitve veljajo nekateri vnaprej določeni pogoji, ki jih lahko izpolni nedoločeno število oseb, kot je nakup vozovnice, predhodna registracija ali določena starost. Nasprotno pa se prostor ne bi smel šteti za javno dostopnega, če je dostop omejen na določene in opredeljene fizične osebe na podlagi prava Unije ali nacionalnega prava, ki se neposredno nanaša na javno varnost ali varovanje, ali če se oseba, ki ima v tem prostoru ustrezno avtoriteto, glede tega jasno opredeli. Dejanska možnost samega dostopa (na primer odklenjena vrata, odprta vrata v ograji) ne pomeni, da je prostor javno dostopen, če obstajajo znaki ali okoliščine, ki kažejo na nasprotno (na primer znaki, ki prepovedujejo ali omejujejo dostop). Prostori podjetij in tovarn ter pisarne in delovni prostori, do katerih naj bi lahko dostopali samo ustrezni zaposleni in ponudniki storitev, so prostori, ki niso javno dostopni. Javno dostopni prostori ne bi smeli vključevati zaporov ali območij mejne kontrole. Nekatera druga območja lahko zajemajo tako javno dostopne kot javno nedostopne prostore, kot sta hodnik ali avla zasebne stanovanjske zgradbe, prek katere se dostopa do zdravniške pisarne, ali letališče. Spletni prostori prav tako niso zajeti, saj niso fizični prostori. 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 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. 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 prihodnjem 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. Organi držav članic prejemnic ter institucije, uradi in telesa Unije ter telesa, ki uporabljajo take izhodne podatke v Uniji, so še naprej odgovorni za zagotavljanje, da je njihova uporaba skladna s pravom Unije. Ko se ti mednarodni sporazumi revidirajo ali se v prihodnosti sklenejo novi, bi si morale pogodbenice kar najbolj prizadevati za uskladitev teh sporazumov z zahtevami iz te uredbe.

(12) Ta uredba bi se morala uporabljati tudi za institucije, urade, organe in agencije Unije, kadar delujejo kot ponudniki ali uporabniki umetnointeligenčnega sistema.

(-12a) Če in kolikor so umetnointeligenčni sistemi s spremembami ali brez njih dani na trg, v obratovanje ali se uporabljajo za vojaške ali obrambne namene ali namene nacionalne varnostni, bi morali biti izključeni iz področja uporabe te uredbe ne glede na to, katera vrsta subjekta izvaja te dejavnosti, tj. ali je to javni ali zasebni subjekt. Kar zadeva vojaške in obrambne namene, je taka izključitev utemeljena tako s členom 4(2) PEU kot tudi s posebnostmi obrambne politike držav članic in skupne obrambne politike Unije iz poglavja 2 naslova V Pogodbe o Evropski uniji (PEU), za katere velja mednarodno javno pravo, ki je zato ustreznejši pravni okvir za ureditev umetnointeligenčnih sistemov v kontekstu uporabe smrtonosne sile in drugih umetnointeligenčnih sistemov v okviru vojaških in obrambnih dejavnosti. Kar zadeva namene nacionalne varnosti, je izključitev utemeljena tako z dejstvom, da nacionalna varnost ostaja v izključni pristojnosti držav članic v skladu s členom 4(2) PEU, kot tudi s posebno naravo in operativnimi potrebami dejavnosti nacionalne varnosti in posebnimi nacionalnimi pravili, ki se uporabljajo za te dejavnosti. Če pa se umetnointeligenčni sistem, ki je bil razvit, dan na trg, v obratovanje ali se uporablja v vojaške ali obrambne namene ali namene nacionalne varnosti, začasno ali stalno uporablja za druge namene (na primer civilne ali humanitarne namene, namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali namene javne varnosti), bi tak sistem spadal na področje uporabe te uredbe. V tem primeru bi moral subjekt, ki sistem uporablja za namene, ki niso vojaški ali obrambni nameni ali nameni nacionalne varnosti, zagotoviti skladnost sistema s to uredbo, razen če je sistem že skladen s to uredbo. Umetnointeligenčni sistemi, ki so dani na trg ali v obratovanje za izključene namene (tj. vojaške, obrambne namene ali namene nacionalne varnosti) in enega ali več neizključenih namenov (na primer civilne namene, namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj itd.), spadajo na področje uporabe te uredbe, ponudniki teh sistemov pa bi morali zagotoviti skladnost s to uredbo. V teh primerih dejstvo, da umetnointeligenčni sistem lahko spada na področje uporabe te uredbe, ne bi smelo vplivati na možnost subjektov, ki izvajajo nacionalne varnostne, obrambne in vojaške dejavnosti, ne glede na vrsto subjekta, ki izvaja te dejavnosti, da uporabljajo umetnointeligenčne sisteme za namene nacionalne varnosti, vojaške in obrambne namene, katerih uporaba je izključena iz področja uporabe te uredbe. Umetnointeligenčni sistem, dan na trg za civilne namene ali namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ki se uporablja s spremembami ali brez njih za vojaške in obrambne namene ali namene nacionalne varnosti, ne bi smel spadati na področje uporabe te uredbe, ne glede na vrsto subjekta, ki izvaja te dejavnosti.

(12a) 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].

(12b) Uredba ne bi smela ogrožati raziskovalne in razvojne dejavnosti in bi morala spoštovati svobodo znanosti. Zato je treba iz njenega področja uporabe izključiti umetnointeligenčne sisteme, ki so posebej razviti in dani v obratovanje izključno za namene znanstvenih raziskav in razvoja, ter zagotoviti, da Uredba ne bi kako drugače vplivala na dejavnosti znanstvenega raziskovanja in razvojne dejavnosti v zvezi z umetnointeligenčnimi sistemi. Določbe te uredbe se prav tako ne bi smele uporabljati za raziskovalno dejavnost ponudnikov, usmerjeno v proizvode. To ne posega v obveznost skladnosti s to uredbo, kadar je umetnointeligenčni sistem, ki spada na področje uporabe te uredbe, dan na trg ali v obratovanje kot rezultat take raziskovalne in razvojne dejavnosti, ter v uporabo določb o regulativnih peskovnikih in preskušanju v dejanskih razmerah. Poleg tega bi morale brez poseganja v navedeno v zvezi z umetnointeligenčnimi sistemi, ki so posebej razviti in dani v obratovanje izključno za namene znanstvenih raziskav in razvoja, za vse druge umetnointeligenčne sisteme, ki se lahko uporabljajo za izvajanje kakršnih koli raziskovalnih in razvojnih dejavnosti, še naprej veljati določbe te uredbe. V vsakem primeru je treba vsakršno raziskovalno in razvojno dejavnost izvajati v skladu s priznanimi etičnimi in strokovnimi standardi za znanstvene raziskave.

(12c) Glede na naravo in kompleksnost vrednostne verige umetnointeligenčnih sistemov je bistveno pojasniti vlogo akterjev, ki lahko prispevajo k razvoju umetnointeligenčnih sistemov, predvsem umetnointeligenčnih sistemov velikega tveganja. Konkretno, treba je pojasniti, da so umetnointeligenčni sistemi za splošne namene tisti, pri katerih ponudnik namerava z njimi opravljati splošno uporabne funkcije, kot je prepoznavanje slike/govora, in v različnih okoliščinah. Lahko se uporabljajo kot samostojni umetnointeligenčni sistemi velikega tveganja ali pa so sestavni deli drugih umetnointeligenčnih sistemov velikega tveganja. Zato bi morale za take sisteme zaradi njihove posebne narave in za zagotovitev pravične delitve odgovornosti vzdolž vrednostne verige umetne inteligence veljati sorazmerne in bolj specifične zahteve in obveznosti iz te uredbe, pri čemer bi bilo treba zagotoviti visoko raven varstva temeljnih pravic, zdravja in varnosti. Poleg tega bi morali ponudniki umetnointeligenčnih sistemov za splošne namene ne glede na to, ali lahko te sisteme uporabljajo drugi ponudniki kot samostojne umetnointeligenčne sisteme velikega tveganja ali kot komponente umetnointeligenčnih sistemov velikega tveganja, po potrebi sodelovati s ponudniki umetnointeligenčnih sistemov velikega tveganja, da bi se jim omogočila skladnost z ustreznimi obveznostmi iz te uredbe, in s pristojnimi organi, ustanovljenimi na podlagi te uredbe. Da bi se upoštevale posebne značilnosti umetnointeligenčnih sistemov za splošne namene ter hitro razvijajoči se trg in tehnološki razvoj na tem področju, bi bilo treba na Komisijo prenesti izvedbena pooblastila, da določi in prilagodi uporabo zahtev iz te uredbe za umetnointeligenčne sisteme za splošne namene ter določi informacije, ki jih morajo deliti ponudniki umetnointeligenčnih sistemov za splošne namene, da se ponudnikom zadevnega umetnointeligenčnega sistema velikega tveganja omogoči izpolnjevanje obveznosti iz te uredbe.

(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) Manipulativne tehnike, ki temeljijo na umetni inteligenci, se lahko uporabljajo za prepričevanje oseb k neželenemu vedenju ali za zavajanje, pri čemer se te osebe spodbuja k odločitvam na način, ki spodkopava ali ovira njihovo avtonomijo, odločanje ali svobodno izbiro. Dajanje na trg, v obratovanje ali uporabo nekaterih umetnointeligenčnih sistemov, ki bistveno izkrivljajo človekovo vedenje in pri katerih obstaja verjetnost povzročitve fizične ali psihične škode, so še posebej nevarni in bi jih bilo zato treba prepovedati. Taki umetnointeligenčni sistemi uporabljajo subliminalne komponente, kot so zvočni, slikovni ali video dražljaji, ki jih osebe ne morejo zaznati, saj taki dražljaji presegajo človekovo dojemanje, ali druge subliminalne tehnike, ki spodkopavajo ali ovirajo posameznikovo avtonomijo, odločanje ali svobodno izbiro na načine, ki se jih ljudje ne zavedajo, v primeru, da se jih zavedajo, pa jih ne morejo nadzorovati ali se jim upreti, na primer v primeru vmesnikov stroj-možgani ali virtualne resničnosti. Poleg tega lahko umetnointeligenčni sistemi tudi sicer izkoriščajo ranljivosti določene skupine oseb zaradi njihove starosti, invalidnosti v smislu Direktive (EU) 2019/882 ali posebnih socialnih ali gospodarskih razmer, zaradi katerih so te osebe verjetno bolj izpostavljene izkoriščanju, na primer osebe, ki živijo v skrajni revščini, ter etnične ali verske manjšine. Taki umetnointeligenčni sistemi se lahko dajo na trg, v obratovanje ali uporabo z namenom ali učinkom bistvenega izkrivljanja vedenja osebe in na način, ki povzroči ali bo razumno verjetno povzročil fizično ali psihično škodo tej ali drugi osebi ali skupinam oseb, vključno s škodo, ki se lahko sčasoma nakopiči. Namere o izkrivljanju vedenja ni mogoče predvideti, če je izkrivljanje posledica dejavnikov zunaj umetnointeligenčnega sistema, na katere ponudnik ali uporabnik ne more vplivati, torej dejavnikov, ki jih ponudnik ali uporabnik umetnointeligenčnega sistema morda ne more razumno predvideti in ublažiti. V vsakem primeru ni nujno, da ponudnik ali uporabnik namerava povzročiti fizično ali psihično škodo, če je taka škoda posledica manipulativnih ali izkoriščevalskih praks, ki temeljijo na umetni inteligenci. Prepoved takih praks umetne inteligence dopolnjujejo določbe iz Direktive 2005/29/ES, predvsem v smislu, da so nepoštene poslovne prakse, ki potrošnikom povzročajo gospodarsko ali finančno škodo, prepovedane v vseh okoliščinah, ne glede na to, ali se izvajajo prek umetnointeligenčnih sistemov ali kako drugače. Prepoved manipulativnih in izkoriščevalskih praks iz te uredbe ne bi smela vplivati na zakonite prakse v okviru zdravljenja, kot je psihološko zdravljenje duševne bolezni ali telesna rehabilitacija, kadar se te prakse izvajajo v skladu z veljavnimi medicinskimi standardi in zakonodajo. Poleg tega se običajne in zakonite poslovne prakse, ki so skladne z veljavnim pravom, same po sebi ne bi smele šteti za škodljive manipulativne prakse umetne inteligence.

(17) Umetnointeligenčni sistemi, ki zagotavljajo družbeno točkovanje fizičnih oseb s strani javnih organov ali zasebnih akterjev, 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 fizične osebe na podlagi njihovega družbenega vedenja v več kontekstih oziroma na podlagi znanih ali predvidenih osebnih ali osebnostnih lastnosti. 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. Umetnointeligenčni sistemi, ki vključujejo take nesprejemljive prakse točkovanja, bi zato morali biti prepovedani. Ta prepoved ne bi smela vplivati na zakonite prakse ocenjevanja fizičnih oseb za enega ali več posebnih namenov v skladu z zakonodajo.

(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 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[9], 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. Poleg tega bi morala ta uredba organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organom za nadzor meje, organom, pristojnim za priseljevanje, ali azilnim organom še naprej omogočati izvajanje ugotavljanja identitete v prisotnosti zadevne osebe v skladu s pogoji, ki so za tako ugotavljanje določeni v pravu Unije in nacionalnem pravu. Predvsem bi morali imeti organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organi za nadzor meje, organi, pristojni za priseljevanje, ali azilni organi možnost, da za identifikacijo osebe, ki med ugotavljanjem identitete tako ugotavljanje zavrne ali ne more navesti ali dokazati svoje identitete, uporabijo informacijske sisteme v skladu s pravom Unije ali nacionalnim pravom, ne da bi morali v skladu s to uredbo pridobiti predhodno dovoljenje. To je lahko na primer oseba, vpletena v kaznivo dejanje, ki organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ni pripravljena ali ne more razkriti svoje identitete zaradi nesreče ali zdravstvenega stanja.

[9] 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).

(20) Za zagotovitev odgovorne in sorazmerne uporabe teh sistemov je pomembno tudi določiti, da bi bilo treba v vsakem od teh izčrpno naštetih in ozko opredeljenih primerov upoštevati nekatere elemente, predvsem 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, predvsem ob upoštevanju dokazov ali znakov glede groženj, žrtev ali storilca. Referenčna podatkovna zbirka o osebah bi morala biti primerna za vsak primer uporabe v vsakem od 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. Takšno dovoljenje bi bilo treba načeloma pridobiti pred uporabo sistema za identifikacijo osebe ali oseb. Izjeme tega pravila bi morale biti dovoljene v ustrezno utemeljenih nujnih primerih, tj. primerih, ko je uporaba zadevnih sistemov potrebna do te mere, 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.

(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, bi morale biti še naprej izpolnjene vse zahteve, ki izhajajo iz člena 10 Direktive (EU) 2016/680. Za namene, ki niso preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, je v skladu s členom 9(1) Uredbe (EU) 2016/679 in členom 10(1) Uredbe (EU) 2018/1725 prepovedano obdelovati biometrične podatke za namene edinstvene identifikacije posameznika, razen v primerih, navedenih v drugem odstavku vsakega od zgoraj navedenih členov.

(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), (3) in (4) 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), (3) in (4) 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[10], Uredbe (EU) št. 167/2013 Evropskega parlamenta in Sveta[11], Uredbe (EU) št. 168/2013 Evropskega parlamenta in Sveta[12], Direktive 2014/90/EU Evropskega parlamenta in Sveta[13], Direktive (EU) 2016/797 Evropskega parlamenta in Sveta[14], Uredbe (EU) 2018/858 Evropskega parlamenta in Sveta[15], Uredbe (EU) 2018/1139 Evropskega parlamenta in Sveta[16] in Uredbe (EU) 2019/2144 Evropskega parlamenta in Sveta[17], 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.

---

10 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).

11 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).

12 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).

13 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).

14 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).

15 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).

16 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).

17 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).

(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[18] ter Uredbo (EU) 2017/746 Evropskega parlamenta in Sveta[19], kadar je za proizvode srednjega in velikega tveganja predvideno ugotavljanje skladnosti s strani tretjih oseb.

[18] 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).

[19] 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 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. Pomembno je pojasniti tudi, da lahko v primerih z velikim tveganjem, navedenih v Prilogi III, obstajajo sistemi, ki ne povzročijo bistvenega tveganja za pravne interese, zaščitene v teh primerih, ob upoštevanju izhodnih podatkov, ki jih ustvari umetnointeligenčni sistem. Zato bi se moral za umetnointeligenčni sistem velikega tveganja šteti le sistem, katerega izhodni podatki imajo v razmerju do zadevnega ukrepa ali odločitve velik pomen (tj. niso zgolj pomožni) in tako ustvarjajo veliko tveganje za zaščitene pravne interese. Na primer kadar gre pri informacijah, ki jih človeku zagotovijo umetnointeligenčni sistemi, za profiliranje fizičnih oseb v smislu člena 4(4) Uredbe (EU) 2016/679 in člena 3(4) Direktive (EU) 2016/680 in člena 3(5) Uredbe (EU) 2018/1725, se take informacije v okviru umetnointeligenčnih sistemov velikega tveganja iz Priloge III običajno ne bi smele šteti kot zgolj pomožne. Če pa so izhodni podatki umetnointeligenčnega sistema le zanemarljivega ali majhnega pomena za človekove ukrepe ali odločitve, se lahko štejejo za zgolj pomožne, tudi na primer umetnointeligenčni sistemi, ki se uporabljajo za prevajanje v informativne namene ali za upravljanje dokumentov.

(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, raso, 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 kritične digitalne infrastrukture, kot je navedena v Prilogi I, točka 8, Direktive o odpornosti kritičnih subjektov, 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. Varnostne komponente kritične infrastrukture, vključno s kritično digitalno infrastrukturo, so sistemi, ki se uporabljajo neposredno za zaščito fizične celovitosti kritične infrastrukture ali zdravja in varnosti oseb in premoženja, vendar niso potrebne za delovanje sistema. Nedelovanje ali napačno delovanje takih komponent bi lahko ustvarilo neposredno tveganje za fizično celovitost kritične infrastrukture in posledično tveganje za zdravje in varnost oseb in premoženja. Komponente, namenjene izključno za uporabo v namene kibernetske varnosti, se ne bi smele šteti kot varnostne komponente. Primeri varnostnih komponent take kritične infrastrukture lahko vključujejo sisteme za spremljanje vodnega tlaka ali sisteme za upravljanje požarnega alarma v okviru centrov računalništva v oblaku.

(35) Umetnointeligenčne sisteme, ki se uporabljajo v izobraževanju ali poklicnem usposabljanju, zlasti za določanje dostopa, sprejem ali razvrščanje oseb v izobraževalne ustanove in ustanove za poklicno usposabljanje ali programe na vseh ravneh ali za evalvacijo učnih izidov oseb, bi bilo treba obravnavati kot sisteme velikega tveganja, saj lahko določajo izobraževalni in poklicni potek življenja osebe ter tako vplivajo na zmožnost preživljanja teh oseb. 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 na podlagi vedenja posameznika oziroma osebnostnih lastnosti ali značilnosti, 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 mikro ali mala podjetja, opredeljena v Prilogi k Priporočilu Komisije 2003/361/ES za lastno uporabo. Fizične osebe, ki zaprosijo za bistvene 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, vključno s tem, ali so upravičenci legitimno upravičeni do takih ugodnosti ali storitev, lahko ti sistemi 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. Umetnointeligenčni sistemi se vse pogosteje uporabljajo tudi za oceno tveganja v zvezi s fizičnimi osebami in določanjem cen v primeru življenjskega in zdravstvenega zavarovanja, kar lahko, če niso ustrezno zasnovani, razviti in uporabljeni, vodi do resnih posledic za življenje in zdravje ljudi, vključno s finančno izključenostjo in diskriminacijo. Za zagotovitev doslednega pristopa v sektorju finančnih storitev bi se morala uporabljati navedena izjema za mikro ali mala podjetja v primeru lastne uporabe, če ta podjetja sama zagotovijo in dajo v uporabo umetnointeligenčni sistem za namene prodaje svojih zavarovalnih produktov.

(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 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. Umetnointeligenčni sistemi, posebej namenjeni uporabi v upravnih postopkih s strani davčnih in carinskih organov ter finančnoobveščevalnih enot, ki izvajajo upravne naloge analiziranja informacij na podlagi zakonodaje Unije o preprečevanju pranja denarja, 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 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[20], Uredbe (ES) št. 810/2009 Evropskega parlamenta in Sveta[21] in druge ustrezne zakonodaje.

[20] 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).

[21] 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).

(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 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.

(41) Dejstvo, da je umetnointeligenčni sistem v skladu s to uredbo razvrščen kot sistem velikega tveganja, ne bi smelo pomeniti, da je uporaba sistema 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, razen če je v tej uredbi izrecno določeno drugače.

(42) Za zmanjševanje tveganj, ki jih predstavljajo umetnointeligenčni sistemi velikega tveganja, ki so dani na trg ali kako drugače dani v uporabo na trgu Unije, bi morale veljati nekatere obvezne zahteve ob upoštevanju predvidenega namena uporabe sistema in v skladu s sistemom obvladovanja tveganja, ki ga vzpostavi ponudnik. Zlasti bi moral sistem obvladovanja tveganja sestavljati neprekinjen ponavljajoč se proces, ki se načrtuje in izvaja v celotni življenjski dobi umetnointeligenčnega sistema velikega tveganja. Ta proces bi moral zagotoviti, da ponudnik opredeli in analizira tveganja za zdravje, varnost in temeljne pravice oseb, ki bi jih sistem lahko prizadel glede na njegov predvideni namen, vključno z morebitnimi tveganji, ki izhajajo iz interakcije med umetnointeligenčnim sistemom in okoljem, v katerem deluje, ter sprejme ustrezne ukrepe za obvladovanje tveganja v skladu s splošno priznanim stanjem tehnike.

(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 potrjevanje bi morali biti zadostno relevantni in imeti ustrezne statistične lastnosti, tudi v zvezi z osebami ali skupinami oseb, na katerih naj bi se uporabljal umetnointeligenčni sistem velikega tveganja. Ti nabori podatkov ne bi smeli vsebovati napak in bi morali biti čim bolj popolni glede na predvideni namen umetnointeligenčnega sistema, pri tem pa sorazmerno upoštevati tehnično izvedljivost in splošno priznano stanje tehnike, razpoložljivost podatkov in izvajanje ustreznih ukrepov za obvladovanje tveganja, da bi se morebitne pomanjkljivosti naborov podatkov ustrezno obravnavale. Zahteva, da morajo biti nabori podatkov popolni in brez napak, ne bi smela vplivati na uporabo tehnik za ohranjanje zasebnosti v okviru razvoja in testiranja umetnointeligenčnih sistemov. Nabori učnih in testnih podatkov ter podatkov za potrjevanje bi morali v obsegu, ki ga zahteva njihov predvideni namen, upoštevati 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 v smislu člena 9(2)(g) Uredbe (EU) 2016/679 in člena 10(2)g) Uredbe (EU) 2018/1725, da se zagotovijo spremljanje, odkrivanje in odpravljanje pristranskosti v zvezi z umetnointeligenčnimi sistemi velikega tveganja.

(44a) Pri uporabi načel iz člena 5(1)(c) Uredbe 2016/679 in člena 4(1)(c) Uredbe 2018/1725, zlasti načela najmanjšega obsega podatkov, v zvezi z nabori učnih in testnih podatkov ter podatkov za potrjevanje na podlagi te uredbe bi bilo treba upoštevati celoten življenjski cikel umetnointeligenčnega sistema.

(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. Poleg tega bi morali ponudniki ali uporabniki voditi dnevnike, ki jih samodejno ustvari umetnointeligenčni sistem velikega tveganja, tudi na primer izhodne podatke, začetni datum in čas itd., če so tak sistem in z njim povezani dnevniki pod njihovim nadzorom, za ustrezno obdobje, v katerem bodo lahko izpolnili svoje obveznosti.

(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 oseb, ki bi lahko bile prizadete zaradi sistema glede na njegov predvideni namen, kjer je to primerno. Za lažje razumevanje navodil za uporabo s strani uporabnika bi morali po potrebi vsebovati ilustrirane primere.

(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. Glede na pomembne posledice, ki jih napačni zadetki v nekaterih sistemih za biometrično identifikacijo ljudi pomenijo za osebe, je za te sisteme ustrezno določiti okrepljeno zahtevo po človekovem nadzoru, tako da uporabnik ne more sprejeti ukrepa ali odločitve na podlagi identifikacije, ki izhaja iz sistema, če tega nista ločeno preverili in potrdili vsaj dve fizični osebi. Ti osebi sta lahko iz enega ali več subjektov in vključujeta osebo, ki upravlja ali uporablja sistem. Ta zahteva ne bi smela ustvariti nepotrebnega bremena ali zamud in lahko bi zadoščalo, da bi se ločeni preverjanji različnih oseb samodejno zabeležili v dnevnikih, ki jih ustvari sistem.

(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. Morali bi biti odporni na škodljivo ali kako drugače nezaželeno ravnanje, ki je lahko posledica omejitev znotraj sistema ali okolja, v katerem sistem deluje (npr. napake, okvare, nedoslednosti, nepričakovane situacije). Umetnointeligenčni sistemi velikega tveganja bi morali biti zato zasnovani in razviti z ustreznimi tehničnimi rešitvami, da bi se preprečilo ali minimaliziralo škodljivo ali kako drugače nezaželeno ravnanje, kot so na primer mehanizmi, ki omogočajo, da sistem varno prekine delovanje (načrt varne odpovedi) v primeru nekaterih anomalij ali ko delovanje poteka zunaj nekaterih vnaprej določenih omejitev. 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[22] o določitvi zahtev za akreditacijo in nadzor trga proizvodov, Sklepom št. 768/2008/ES Evropskega parlamenta in Sveta[23] o skupnem okviru za trženje proizvodov in Uredbo (EU) 2019/1020 Evropskega parlamenta in Sveta[24] o nadzoru trga in skladnosti proizvodov („novi zakonodajni okvir za trženje proizvodov“).

(52a) V skladu z načeli novega zakonodajnega okvira je treba določiti posebne obveznosti za zadevne operaterje znotraj vrednostne verige umetne inteligence, da se zagotovi pravna varnost in olajša zagotavljanje skladnosti s to uredbo. V nekaterih situacijah bi lahko ti operaterji imeli več kot eno vlogo hkrati in bi morali zato kumulativno izpolnjevati vse zadevne obveznosti, povezane s temi vlogami. Na primer operater bi lahko bil distributer in uvoznik hkrati.

(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.

---

22 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).

23 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).

24 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).

(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.

(54a) Za zagotovitev pravne varnosti je treba pojasniti, da bi bilo treba pod določenimi pogoji vsako fizično ali pravno osebo šteti za ponudnika novega umetnointeligenčnega sistema velikega tveganja in bi zato morala prevzeti vse zadevne obveznosti. To bi na primer veljalo, če ta oseba umetnointeligenčni sistemi velikega tveganja, ki je že dan na trg ali v uporabo, opremi s svojim imenom ali blagovno znamko, ali če spremeni predvideni namen umetnointeligenčnega sistema, ki ni sistem velikega tveganja in je že dan na trg ali v uporabo, na tak način, da spremenjeni sistem postane umetnointeligenčni sistem velikega tveganja. Te določbe bi se morale uporabljati brez poseganja v bolj specifične določbe v okviru nekatere sektorske zakonodaje novega zakonodajnega okvira, ki naj bi se uporabljala skupaj s to uredbo. Na primer člen 16, odstavek 2, Uredbe 745/2017, ki določa, da se nekatere spremembe ne bi smele šteti kot spremembe pripomočka, ki bi lahko vplivale na skladnost z veljavnimi zahtevami, bi se moral še naprej uporabljati za umetnointeligenčne sisteme velikega tveganja, ki so medicinski pripomočki v smislu navedene uredbe.

(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 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.

(56a) Za ponudnike, ki nimajo sedeža v Uniji, ima pooblaščeni zastopnik osrednjo vlogo pri zagotavljanju skladnosti umetnointeligenčnih sistemov velikega tveganja, ki jih ti ponudniki dajejo na trg ali v uporabo v Uniji, in je njihova kontaktna oseba s sedežem v Uniji. Glede na to osrednjo vlogo in za zagotovitev prevzema odgovornosti za namene izvrševanja te uredbe je primerno, da je pooblaščeni zastopnik skupaj s ponudnikom solidarno odgovoren za umetnointeligenčne sisteme velikega tveganja z napako. Odgovornost pooblaščenega zastopnika iz te uredbe ne posega v določbe Direktive 85/374/EGS o odgovornosti za proizvode z napako.

(57) [črtano]

(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. Te obveznosti ne bi smele posegati v druge obveznosti uporabnikov v zvezi z umetnointeligenčnimi sistemi velikega tveganja na podlagi prava Unije ali nacionalnega prava in se ne bi smele uporabljati, kadar se navedeni sistemi uporabljajo v okviru osebne nepoklicne dejavnosti.

(58a) Primerno je pojasniti, da ta uredba ne vpliva na obveznosti ponudnikov in uporabnikov umetnointeligenčnih sistemov v njihovi vlogi upravljavcev ali obdelovalcev podatkov, ki izhajajo iz prava Unije o varstvu osebnih podatkov, kolikor zasnova, razvoj ali uporaba umetnointeligenčnih sistemov vključuje obdelavo osebnih podatkov. Prav tako je primerno pojasniti, da posamezniki, na katere se nanašajo osebni podatki, še naprej uživajo vse pravice in jamstva, ki jim jih podeljuje tovrstno pravo Unije, tudi pravice, povezane izključno z avtomatiziranim sprejemanjem posameznih odločitev, vključno z oblikovanjem profilov. Harmonizirana pravila za dajanje na trg, v uporabo in uporabo umetnointeligenčnih sistemov, določena na podlagi te uredbe, bi morala olajšati učinkovito izvajanje in omogočiti uveljavljanje pravic posameznikov, na katere se nanašajo osebni podatki, in drugih pravnih sredstev, zagotovljenih na podlagi prava Unije o varstvu osebnih podatkov in drugih temeljnih pravic.

(59) [črtano]

(60) [črtano]

(61) Standardizacija bi morala imeti ključno vlogo pri zagotavljanju tehničnih rešitev za ponudnike, da se zagotovi skladnost s to uredbo, v skladu z najsodobnejšo tehnologijo. 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[25] in od katerih se ponavadi pričakuje, da odražajo najsodobnejšo tehnologijo. Ker pa ni ustreznih sklicevanj na harmonizirane standarde, bi morala imeti Komisija možnost, da kot izredno nadomestno rešitev z izvedbenimi akti določi skupne specifikacije za nekatere zahteve na podlagi te uredbe, da se ponudniku olajša obveznost izpolnjevanja zahtev iz te uredbe, kadar je postopek standardizacije blokiran ali kadar pride do zamud pri določitvi ustreznega harmoniziranega standarda. Če do take zamude pride zaradi tehnične zapletenosti zadevnega standarda, bi morala Komisija to upoštevati, preden bi preučila določitev skupnih specifikacij. Ustrezna udeležba malih in srednjih podjetij pri pripravi standardov, ki podpirajo izvajanje te uredbe, je bistvena za spodbujanje inovacij in konkurenčnosti na področju umetne inteligence v Uniji. Takšno udeležbo bi bilo treba ustrezno zagotoviti v skladu s členoma 5 in 6 Uredbe (EU) št. 1025/2012.

[25] 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).

(61a) Primerno je, da brez poseganja v uporabo harmoniziranih standardov in skupnih specifikacij za ponudnike velja domneva o skladnosti z ustrezno zahtevo glede podatkov, kadar je bil njihov umetnointeligenčni sistem velikega tveganja naučen in preskušen na podlagi podatkov, ki odražajo posebno geografsko, vedenjsko ali funkcionalno okolje, v katerem naj bi se umetnointeligenčni sistem uporabljal. Podobno bi bilo treba v skladu s členom 54(3) Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta domnevati, da so umetnointeligenčni sistemi velikega tveganja, ki so bili certificirani ali za katere je bila izdana izjava o skladnosti v okviru sheme za kibernetsko varnost in sklici na katere so bili objavljeni v Uradnem listu Evropske unije, skladni z zahtevo glede kibernetske varnosti iz te uredbe. To ne posega v prostovoljno naravo navedene sheme za kibernetsko varnost.

(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] 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. Kar zadeva umetnointeligenčne sisteme velikega tveganja, povezane z izdelki, zajetimi v uredbah 745/2017 in 746/2017 o medicinskih pripomočkih, uporaba zahtev iz te uredbe ne bi smela posegati v logiko obvladovanja tveganja in oceno razmerja med koristmi in tveganji, ki se izvedeta v okviru medicinskih pripomočkov, in bi ju morala upoštevati.

(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 priglasiti priglašene organe, če izpolnjujejo vrsto zahtev, zlasti glede neodvisnosti, pristojnosti in neobstoja navzkrižja interesov. Pristojni nacionalni organi bi morali priglasitev teh organov poslati Komisiji in drugim državam članicam prek elektronskega orodja za priglasitev, ki ga razvije in upravlja Komisija v skladu s členom R23 Sklepa št. 768/2008/ES.

(66) V skladu s skupno uveljavljenim pojmom bistvene spremembe za proizvode, ki jih ureja harmonizacijska zakonodaja Unije, je primerno, da se ob vsaki spremembi, ki bi lahko vplivala na skladnost umetnointeligenčnega sistema velikega tveganja s to uredbo (npr. spremembi strukture operacijskega sistema ali programske opreme), ali kadar se spremeni predvideni namen sistema, ta umetnointeligenčni sistem šteje za nov umetnointeligenčni sistem, za katerega bi bilo treba opraviti novo ugotavljanje skladnosti. Vendar spremembe algoritma in delovanja umetnointeligenčnih sistemov, ki se po tem, ko so dani na trg ali v uporabo, še naprej „učijo“ (tj. samodejno prilagajajo način izvajanja funkcij), ne bi smele pomeniti bistvene spremembe, če jih je ponudnik določil vnaprej in ocenil v okviru ugotavljanja skladnosti.

(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 se registrirajo v podatkovni zbirki EU, ki jo vzpostavi in upravlja Komisija, in da v tej zbirki registrirajo tudi informacije o svojih umetnointeligenčnih sistemih velikega tveganja. Pred uporabo umetnointeligenčnega sistema velikega tveganja iz Priloge III se uporabniki umetnointeligenčnih sistemov velikega tveganja, ki so javni organi, agencije ali organi, razen organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organov za nadzor meja, organov za priseljevanje ali azil, in organov, ki so uporabniki umetnointeligenčnih sistemov velikega tveganja na področju kritične infrastrukture, prav tako registrirajo v navedeni podatkovni zbirki in izberejo sistem, ki ga nameravajo uporabljati. Komisija bi morala biti upravljavec navedene zbirke podatkov v skladu z Uredbo (EU) 2018/1725 Evropskega parlamenta in Sveta[26]. 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.

[26] 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).

(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 bi bilo treba fizične osebe obvestiti, da so v stiku z umetnointeligenčnim sistemom, razen če je to očitno z vidika fizične osebe, ki je razmeroma dobro obveščena, pozorna in preudarna, ob upoštevanju okoliščin in okvira uporabe. Pri izvajanju take obveznosti bi bilo treba upoštevati značilnosti posameznikov, ki pripadajo ranljivim skupinam zaradi svoje starosti ali invalidnosti, kolikor je namen umetnointeligenčnega sistema tudi interakcija s temi skupinami. Poleg tega bi bilo treba fizične osebe obvestiti, kadar so izpostavljene sistemom, ki lahko z obdelavo njihovih biometričnih podatkov prepoznajo čustva ali namere teh oseb ali sklepajo o njih ali razvrstijo te osebe v posebne kategorije. Tovrstne posebne kategorije se lahko nanašajo na značilnosti, kot so spol, starost, barva las, barva oči, tetovaže, osebne lastnosti, etnično poreklo, osebne želje in interesi, ali na druge vidike, kot sta spolna ali politična usmerjenost. 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. Skladnost z navedenimi obveznostmi obveščanja se ne bi smela razlagati, kot da pomeni, da je uporaba sistema ali njegovih izhodnih podatkov zakonita v skladu s to uredbo ali drugim pravom Unije in pravom držav članic ter ne bi smela posegati v druge obveznosti glede preglednosti za uporabnike umetnointeligenčnih sistemov, določene v pravu Unije ali nacionalnem pravu. Poleg tega se ne bi smela razlagati, kot da pomeni, da uporaba sistema ali njegovih izhodnih podatkov ovira pravico do svobode izražanja in pravico do svobode umetnosti in znanosti, ki ju zagotavlja Listina EU o temeljnih pravicah, zlasti kadar je vsebina del očitno ustvarjalnega, satiričnega, umetniškega ali fiktivnega dela ali programa, ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine tretjih strani.

(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 za umetno inteligenco 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), vključno z zagonskimi podjetji. Sodelovanje pri regulativnem peskovniku za umetno inteligenco bi moralo biti osredotočeno na vprašanja, ki ustvarjajo pravno negotovost za ponudnike in potencialne ponudnike pri inovacijah, eksperimentiranju z umetno inteligenco v Uniji in prispevanju k regulativnemu učenju, ki temelji na dokazih. Nadzor umetnointeligenčnih sistemov pri regulativnem peskovniku za umetno inteligenco bi zato moral zajemati njihov razvoj, usposabljanje, testiranje in potrjevanje, preden so sistemi dani na trg ali v uporabo, ter pojem in pojav bistvenih sprememb, zaradi katerih bi lahko bil potreben nov postopek ugotavljanja skladnosti. Pristojni nacionalni organi, ki vzpostavijo regulativne peskovnike za umetno inteligenco, bi morali po potrebi sodelovati z drugimi ustreznimi organi, vključno s tistimi, ki nadzirajo varstvo temeljnih pravic, in bi lahko omogočili sodelovanje drugih akterjev v umetnointeligenčnem ekosistemu, kot so nacionalne ali evropske organizacije za standardizacijo, priglašeni organi, centri za testiranje in eksperimentiranje, laboratoriji za raziskave in eksperimentiranje, inovacijska vozlišča ter ustrezne organizacije deležnikov in civilne družbe. 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. Regulativni peskovniki za umetno inteligenco, vzpostavljeni na podlagi te uredbe, ne bi smeli posegati v drugo zakonodajo, ki omogoča vzpostavitev drugih peskovnikov, katerih namen je zagotoviti skladnost z drugo zakonodajo, ki ne zajema te uredbe. Ustrezni pristojni organi, odgovorni za te druge regulativne peskovnike, bi morali po potrebi upoštevati koristi uporabe teh peskovnikov tudi za zagotavljanje skladnosti umetnointeligenčnih sistemov s to uredbo. Po dogovoru med pristojnimi nacionalnimi organi in udeleženci v okviru regulativnega peskovnika za umetno inteligenco se lahko testiranje v dejanskih razmerah izvaja in nadzira tudi v okviru regulativnega peskovnika za umetno inteligenco.

(-72a) Ta uredba bi morala zagotoviti pravno podlago za udeležence v okviru regulativnega peskovnika za umetno inteligenco 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) in 9(2)(g) Uredbe (EU) 2016/679 in členom 5 in 10 Uredbe (EU) 2018/1725 ter brez poseganja v člena 4(2) in 10 Direktive (EU) 2016/680. Vse druge obveznosti upravljavcev podatkov in pravice posameznikov, na katere se nanašajo osebni podatki, na podlagi Uredbe (EU) 2016/679, Uredbe (EU) 2018/1725 in Direktive (EU) 2016/680 se še naprej uporabljajo. Zlasti ta uredba ne bi smela zagotavljati pravne podlage v smislu člena 22(2)(b) Uredbe (EU) 2016/679 in člena 24(2)(b) Uredbe (EU) 2018/1725. Udeleženci v peskovniku bi morali zagotoviti ustrezne zaščitne ukrepe in sodelovati s pristojnimi organi, tudi z 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.

(72a) Da bi pospešili proces razvoja umetnointeligenčnih sistemov velikega tveganja iz Priloge III in njihovega dajanja na trg, je pomembno, da imajo tudi ponudniki ali potencialni ponudniki takih sistemov lahko koristi od posebne ureditve za testiranje teh sistemov v dejanskih razmerah, ne da bi sodelovali v okviru regulativnega peskovnika za umetno inteligenco. Vendar bi bilo treba v takih primerih in ob upoštevanju možnih posledic takega testiranja za posameznike zagotoviti, da se z Uredbo za ponudnike ali potencialne ponudnike uvedejo ustrezna in zadostna jamstva in pogoji. Taka jamstva bi morala med drugim vključevati zahtevo po informirani privolitvi fizičnih oseb za sodelovanje pri testiranju v dejanskih razmerah, z izjemo preprečevanja, odkrivanja in preiskovanja kaznivih dejanj v primerih, ko bi pridobitev informirane privolitve preprečila testiranje umetnointeligenčnega sistema. Privolitev posameznikov, da sodelujejo pri takem testiranju v skladu s to uredbo, se razlikuje od privolitve posameznikov, na katere se nanašajo osebni podatki, za obdelavo njihovih osebnih podatkov v skladu z ustrezno zakonodajo o varstvu podatkov in ne posega vanjo.

(73) Za spodbujanje in zaščito inovacij je pomembno, da se upoštevajo zlasti interesi ponudnikov in uporabnikov umetnointeligenčnih sistemov, ki so MSP. 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 ponudnikov, ki so MSP. 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.

(73a) Za spodbujanje in zaščito inovacij bi morali platforma za umetno inteligenco na zahtevo, vsi ustrezni programi in projekti EU za financiranje, kot sta programa Digitalna Evropa in Obzorje Evropa, ki jih izvajajo Komisija in države članice na nacionalni ravni ali ravni EU, prispevati k doseganju ciljev te uredbe.

(74) Zlasti da bi čim bolj zmanjšali tveganja za izvajanje, ki so posledica pomanjkanja znanja in strokovnega znanja na trgu, ter da bi ponudnikom, predvsem MSP, 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.

(74a) Poleg tega je za zagotovitev sorazmernosti glede na zelo majhno velikost nekaterih operaterjev v zvezi s stroški inovacij primerno, da so mikropodjetja izvzeta iz najdražjih obveznosti, kot je vzpostavitev sistema upravljanja kakovosti, kar bi zmanjšalo upravno breme in stroške za ta podjetja, ne da bi vplivalo na raven zaščite in potrebo po skladnosti z zahtevami za umetnointeligenčne sisteme velikega tveganja.

(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 odražati različne interese umetnointeligenčnega ekosistema, sestavljati pa bi ga morali predstavniki držav članic. Za zagotovitev sodelovanja ustreznih deležnikov bi bilo treba ustanoviti stalno podskupino odbora. Odbor bi moral biti odgovoren za številne svetovalne naloge, med drugim za izdajanje mnenj, priporočil, nasvetov, ali prispevati k smernicam o zadevah, povezanih z izvajanjem te uredbe, vključno z zadevami v zvezi z izvrševanjem, tehničnimi specifikacijami ali obstoječimi standardi v zvezi z zahtevami iz te uredbe, ter svetovanje Komisiji ter državam članicam in njihovim pristojnim nacionalnim organom pri posebnih vprašanjih v zvezi z umetno inteligenco. Da bi državam članicam omogočili nekaj prožnosti pri imenovanju njihovih predstavnikov v odboru za umetno inteligenco, so lahko ti predstavniki katere koli osebe, ki pripadajo javnim subjektom in bi morale imeti ustrezne pristojnosti in pooblastila za lažje usklajevanje na nacionalni ravni in prispevanje k izpolnjevanju nalog odbora. Odbor bi moral ustanoviti dve stalni podskupini, da bi zagotovili platformo za sodelovanje in izmenjavo med organi za nadzor trga in priglasitvenimi organi o vprašanjih, povezanih z nadzorom trga oziroma priglašenimi organi. Stalna podskupina za nadzor trga bi morala delovati kot skupina za upravno koordinacijo (ADCO) za to uredbo v smislu člena 30 Uredbe (EU) 2019/1020. V skladu z vlogo in nalogami Komisije v skladu s členom 33 Uredbe (EU) 2019/1020 bi morala Komisija podpirati dejavnosti stalne podskupine za nadzor trga z ocenjevanji ali študijami trga, zlasti z namenom opredelitve vidikov te uredbe, ki zahtevajo posebno in nujno usklajevanje med organi za nadzor trga. Odbor lahko po potrebi ustanovi druge stalne ali začasne podskupine za preučitev posebnih vprašanj. Odbor bi moral po potrebi sodelovati tudi z ustreznimi organi EU, strokovnimi skupinami in mrežami, dejavnimi v okviru ustrezne zakonodaje EU, zlasti tudi s tistimi, ki so dejavni na podlagi ustrezne uredbe EU o podatkih, digitalnih proizvodih in storitvah.

(76a) Komisija bi morala dejavno podpirati države članice in operaterje pri izvajanju in izvrševanju te uredbe. V zvezi s tem bi morala pripraviti smernice o posameznih temah, da bi olajšala uporabo te uredbe, pri čemer bi morala posebno pozornost nameniti potrebam MSP in zagonskih podjetij v sektorjih, za katere je najverjetneje, da bodo prizadeti. Da bi podprli ustrezno izvrševanje in zmogljivosti držav članic, bi bilo treba vzpostaviti seznam centrov Unije za testiranje umetne inteligence in ustreznih strokovnjakov ter jih dati na voljo državam članicam.

(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. Države članice se lahko v skladu s svojimi posebnimi nacionalnimi organizacijskimi značilnostmi in potrebami odločijo za imenovanje katerega koli javnega subjekta za opravljanje nalog pristojnih nacionalnih organov v smislu te uredbe.

(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, 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. Organi za nadzor trga, imenovani v skladu s to uredbo, bi morali imeti vsa izvršilna pooblastila na podlagi te uredbe in Uredbe (EU) 2019/1020 ter bi morali svoja pooblastila in dolžnosti izvajati neodvisno, nepristransko in brez predsodkov. Čeprav za večino umetnointeligenčnih sistemov ne veljajo posebne zahteve in obveznosti iz te uredbe, lahko organi za nadzor trga sprejmejo ukrepe v zvezi z vsemi umetnointeligenčnimi sistemi, če ti predstavljajo tveganje v skladu s to uredbo. Zaradi posebne narave institucij, agencij in organov Unije, ki spadajo v področje uporabe te uredbe, je primerno imenovati Evropskega nadzornika za varstvo podatkov kot pristojnega organa za nadzor trga zanje. To ne bi smelo posegati v imenovanje pristojnih nacionalnih organov s strani držav članic. Dejavnosti nadzora trga ne bi smele vplivati na zmožnost nadzorovanih subjektov, da svoje naloge opravljajo neodvisno, kadar je taka neodvisnost zahtevana na podlagi prava Unije.

(79a) Ta uredba ne posega v pristojnosti, naloge, pooblastila in neodvisnost ustreznih nacionalnih javnih organov ali teles, ki nadzorujejo uporabo prava Unije o varstvu temeljnih pravic, vključno z organi za enakost in organi za varstvo podatkov. Kadar je to potrebno za njihove naloge, bi morali imeti navedeni nacionalni javni organi ali telesa tudi dostop do kakršne koli dokumentacije, pripravljene v skladu s to uredbo. Določiti bi bilo treba poseben zaščitni postopek za zagotavljanje ustreznega in pravočasnega izvrševanja v zvezi z umetnointeligenčnimi sistemi, ki predstavljajo tveganje za zdravje, varnost in temeljne pravice. Postopek za take umetnointeligenčne sisteme, ki predstavljajo tveganje, bi bilo treba uporabljati za umetnointeligenčne sisteme velikega tveganja, ki predstavljajo tveganje, prepovedane sisteme, ki so bili dani na trg, v uporabo ali se uporabljajo v skladu s prepovedanimi praksami iz te uredbe, in umetnointeligenčne sisteme, ki so bili dani na voljo v nasprotju z zahtevami glede preglednosti iz te uredbe in predstavljajo tveganje.

(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, 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, razen če se država članica ne odloči, da bo za opravljanje teh nalog nadzora trga imenovala drug organ. Ti pristojni organi bi morali imeti vsa pooblastila na podlagi te uredbe in Uredbe (EU) 2019/1020 o nadzoru trga, da bi izvrševali zahteve in obveznosti iz te uredbe, vključno s pooblastili za izvajanje naknadnih dejavnosti nadzora trga, ki jih je mogoče po potrebi vključiti v njihove obstoječe nadzorne mehanizme in postopke v skladu z zadevno zakonodajo Unije o finančnih storitvah. Primerno je predvideti, da bi morali nacionalni organi, odgovorni za nadzor kreditnih institucij, ki jih ureja Direktiva 2013/36/EU in sodelujejo v enotnem mehanizmu nadzora (EMN), vzpostavljenem z Uredbo Sveta št. 1024/2013, kadar delujejo kot organi za nadzor trga v skladu s to uredbo, Evropski centralni banki nemudoma sporočiti vse informacije, pridobljene med njihovimi dejavnostmi nadzora trga, ki bi lahko bile zanimive za naloge bonitetnega nadzora Evropske centralne banke, kot so določene v navedeni uredbi. 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[27], je primerno v obstoječe obveznosti in postopke iz Direktive 2013/36/EU vključiti tudi 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. Ista ureditev bi se morala uporabljati za zavarovalnice in pozavarovalnice ter zavarovalne holdinge v skladu z Direktivo 2009/138/EU (Solventnost II) in zavarovalne posrednike v skladu z Direktivo (EU) 2016/97 ter druge vrste finančnih institucij, za katere veljajo zahteve glede notranjega upravljanja,

[27] 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).

ureditev ali postopkov, vzpostavljenih v skladu z ustrezno zakonodajo Unije o finančnih storitvah, da se zagotovita doslednost in enaka obravnava v finančnem sektorju.

(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 zahtev, ki veljajo za umetnointeligenčne sisteme velikega tveganja, prilagojenih glede na predvideni namen sistemov in manjše tveganje v zvezi z njimi. 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.

(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[28] 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, v skladu s pravom Unije ali nacionalnim pravom.

[28] 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).

(84) Države članice bi morale sprejeti vse potrebne ukrepe za zagotovitev izvajanja določb iz te uredbe, tudi tako, da bi določile učinkovite, sorazmerne in odvračilne kazni za kršitve teh določb, ob upoštevanju načela *ne bis in idem*. 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 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[29]. 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. Taka posvetovanja in svetovalna podpora bi se morali izvajati tudi v okviru dejavnosti odbora za umetno inteligenco in njegovih podskupin.

[29] UL L 123, 12.5.2016, str. 1.

(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[30]. Zlasti je pomembno, da Komisija v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje, kadar koli je pri zgodnji pripravi osnutkov izvedbenih aktov potrebno širše strokovno znanje, uporabi strokovne skupine, se posvetuje s ciljnimi deležniki ali po potrebi izvede javna posvetovanja. Taka posvetovanja in svetovalna podpora bi se morali izvajati tudi v okviru dejavnosti odbora za umetno inteligenco in njegovih podskupin, tudi priprave izvedbenih aktov v zvezi s členi 4, 4b in 6.

(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.

(87a) Da se zagotovita pravna varnost in ustrezno prilagoditveno obdobje za operaterje ter preprečijo motnje na trgu, vključno z zagotavljanjem neprekinjene uporabe umetnointeligenčnih sistemov, je primerno, da se ta uredba uporablja za umetnointeligenčne sisteme velikega tveganja, ki so bili dani na trg ali v uporabo pred splošnim datumom začetka njene uporabe, le če se pri navedenih sistemih od navedenega datuma bistveno spremeni njihova zasnova ali predvideni namen. Primerno je pojasniti, da bi bilo treba v zvezi s tem pojem bistvene spremembe razumeti kot vsebinsko enakovreden pojmu bistvene spremembe, ki se uporablja samo za umetnointeligenčne sisteme velikega tveganja, kot so opredeljeni v tej uredbi.

[30] 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).

(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 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 nekatere umetnointeligenčne sisteme;

(d) pravila o spremljanju trga, nadzoru trga in upravljanju;

(e) ukrepe v podporo inovacijam.

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 so ti ponudniki fizično prisotni ali imajo sedež v Uniji ali v tretji državi;

(b) uporabnike umetnointeligenčnih sistemov, ki so fizično prisotni ali imajo sedež v Uniji;

(c) ponudnike in uporabnike umetnointeligenčnih sistemov, ki so fizično prisotni ali imajo sedež v tretji državi, kadar se izhodni podatki, ki jih sistem ustvari, uporabljajo v Uniji;

(d) uvoznike in distributerje umetnointeligenčnih sistemov;

(e) proizvajalce proizvodov, ki dajejo umetnointeligenčni sistem na trg ali v uporabo skupaj s svojim proizvodom in pod svojim imenom ali blagovno znamko;

(f) pooblaščene zastopnike ponudnikov s sedežem v Uniji.

2. Za umetnointeligenčne sisteme, ki so razvrščeni med umetnointeligenčne sisteme velikega tveganja v skladu s členoma 6 (1) in 6(2) v povezavi s proizvodi, zajetimi v harmonizacijsko zakonodajo Unije s seznama v Prilogi II, oddelek B, se uporablja samo člen 84 te uredbe. Člen 53 se uporablja le, če so bile zahteve za umetnointeligenčne sisteme velikega tveganja iz te uredbe vključene v to harmonizacijsko zakonodajo Unije.

3. Ta uredba se ne uporablja za umetnointeligenčne sisteme, če in kolikor so bili dani na trg, dani v uporabo ali se uporabljajo s spremembami ali brez sprememb takih sistemov za namene dejavnosti, ki ne spadajo na področje uporabe prava Unije, in v vsakem primeru za dejavnosti v zvezi z vojaško, obrambno ali nacionalno varnostjo, ne glede na vrsto subjekta, ki izvaja te dejavnosti.

   Poleg tega se ta uredba ne uporablja za umetnointeligenčne sisteme, ki niso dani na trg ali v uporabo v Uniji, kadar se izhodni podatki uporabljajo v Uniji za namene dejavnosti, ki ne spadajo na področje uporabe prava Unije, in v vsakem primeru za dejavnosti v zvezi z vojaško, obrambno ali nacionalno varnostjo, ne glede na vrsto subjekta, ki izvaja te dejavnosti.

4. Ta uredba se ne uporablja za javne organe v tretji državi in 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 poglavja II, oddelek 4, Direktive 2000/31/ES Evropskega parlamenta in Sveta[31] [*ki se nadomestijo z ustreznimi določbami akta o digitalnih storitvah*].

6. Ta uredba se ne uporablja za umetnointeligenčne sisteme, vključno z njihovimi izhodnimi podatki, posebej razvite in dane v uporabo zgolj za namene znanstvenih raziskav in razvoja.

7. Ta uredba se ne uporablja za raziskovalne in razvojne dejavnosti v zvezi z umetnointeligenčnimi sistemi.

8. Ta uredba se ne uporablja za obveznosti uporabnikov, ki so fizične osebe in ki uporabljajo umetnointeligenčne sisteme v okviru popolnoma osebne nepoklicne dejavnosti, razen člena 52.

[31] 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).

Člen 3

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „umetnointeligenčni sistem“ pomeni sistem, ki je zasnovan za delovanje z elementi avtonomije in ki na podlagi podatkov in vhodnih podatkov iz strojnih in/ali človeških virov, sklepa, kako doseči določen sklop ciljev z uporabo strojnega učenja in/ali pristopov, ki temeljijo na logiki in znanju, ter ustvarja sistemske izhodne podatke, kot so vsebine (generativni umetnointeligenčni sistemi), napovedi, priporočila ali odločitve, ki vplivajo na okolja, s katerimi je umetnointeligenčni sistem v stiku;

(1a) „življenjski cikel umetnointeligenčnega sistema“ pomeni trajanje umetnointeligenčnega sistema od zasnove do upokojitve. Brez poseganja v pristojnosti organov za nadzor trga se lahko taka upokojitev zgodi kadar koli v obdobju spremljanja po dajanju na trg na podlagi odločitve ponudnika in pomeni, da se sistema ne sme več uporabljati. Življenjski cikel umetnointeligenčnega sistema se konča tudi z bistveno spremembo tega sistema, ki jo izvede ponudnik ali katera koli druga fizična ali pravna oseba, pri čemer se bistveno spremenjeni umetnointeligenčni sistem šteje za nov umetnointeligenčni sistem;

(1b) „umetnointeligenčni sistem za splošne namene“ pomeni umetnointeligenčni sistem, s katerim namerava ponudnik – ne glede na to, kako je dan na trg ali v uporabo, tudi kot odprtokodna programska oprema – opravljati splošno uporabne funkcije, kot so prepoznavanje podob ali govora, ustvarjanje zvočnih ali videovsebin, odkrivanje vzorcev, odgovarjanje na vprašanja ter prevajanje in drugo; umetnointeligenčni sistem za splošne namene se lahko uporablja v različnih kontekstih in se lahko vključi v različne druge umetnointeligenčne sisteme;

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

(3) [črtano];

(3a) „mikro, mala in srednja podjetja“ (v nadaljnjem besedilu: MSP) pomeni podjetja, kakor so opredeljena v Priporočilu Komisije 2003/361/ES o opredelitvi mikro, malih in srednje velikih podjetij;

(4) „uporabnik“ pomeni vsako fizično ali pravno osebo, tudi javni organ, agencijo ali drug organ, pod čigar pristojnostjo se sistem uporablja;

(5) „pooblaščeni zastopnik“ pomeni vsako fizično ali pravno osebo, ki je fizično prisotna ali ima sedež v Uniji in je od ponudnika umetnointeligenčnega sistema prejela in sprejela pisno pooblastilo, da v njegovem imenu opravlja in izvaja obveznosti in postopke, določene s to uredbo;

(5a) „proizvajalec proizvoda“ pomeni proizvajalca v smislu katerega koli akta s seznama harmonizacijske zakonodaje Unije v Prilogi II;

(6) „uvoznik“ pomeni vsako fizično ali pravno osebo, ki je fizično prisotna ali ima sedež v Uniji, ki da na trg 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;

(8) „operater“ pomeni ponudnika, proizvajalca proizvoda, uporabnika, pooblaščenega zastopnika, uvoznika ali 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 bodisi brezplačno;

(11) „dajanje v uporabo“ pomeni dobavo umetnointeligenčnega sistema za prvo uporabo neposredno uporabniku ali za lastno uporabo v Uniji 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;

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

(17) „umik umetnointeligenčnega sistema“ pomeni vsak ukrep, s katerim se prepreči dostopnost umetnointeligenčnega sistema iz dobavne verige na trgu;

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

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

(20) „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;

(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 spremembo predvidenega namena, za katerega je bil umetnointeligenčni sistem ocenjen; 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.

(24) „oznaka skladnosti CE“ (oznaka CE) pomeni oznako, s katero ponudnik izjavlja, da je umetnointeligenčni sistem skladen z zahtevami iz naslova III, poglavje 2, ali člena 4b te uredbe in drugega veljavnega pravnega akta Unije o harmonizaciji pogojev za trženje proizvodov („harmonizacijska zakonodaja Unije“), ki določa njeno pritrjevanje;

(25) „sistem za spremljanje po dajanju na trg“ pomeni vse dejavnosti, ki jih izvajajo ponudniki umetnointeligenčnih sistemov, da bi 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) „skupna specifikacija“ pomeni sklop tehničnih specifikacij, kot so opredeljene v točki 4 člena 2 Uredbe (EU) št. 1025/2012 in ki zagotavljajo sredstva za izpolnjevanje nekaterih zahtev, določenih s to uredbo;

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

(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, kot so podobe obraza ali daktiloskopski podatki;

(34) „sistem za prepoznavanje čustev“ pomeni umetnointeligenčni sistem za prepoznavanje čustev ali sklepanje o psihološkem stanju, 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 na podlagi njihovih biometričnih podatkov;

(36) „sistem za biometrično identifikacijo na daljavo“ pomeni umetnointeligenčni sistem za identifikacijo fizičnih oseb običajno na daljavo, brez njihovega dejavnega sodelovanja, s primerjavo biometričnih podatkov osebe z biometričnimi podatki iz referenčne podatkovne zbirke;

(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 zgodiho takoj ali skoraj trenutno.

(38) [črtano]

(39) „javno dostopni prostor“ pomeni vsak fizični prostor v javni ali zasebni lasti, ki je dostopen nedoločenemu številu fizičnih oseb, ne glede na to, ali so bili določeni pogoji ali okoliščine za dostop vnaprej določeni, in ne glede na morebitne omejitve zmogljivosti;

(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 organi za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj izvajajo ali se izvajajo v njihovem imenu za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem;

(42) [črtano]

(43) „pristojni nacionalni organ“ pomeni katerikoli naslednji organ: priglasitveni organ in organ za nadzor trga. Pri umetnointeligenčnih sistemih, ki jih dajo v uporabo ali jih uporabljajo institucije, agencije, uradi in organi EU, Evropski nadzornik za varstvo podatkov izpolnjuje obveznosti, ki so v državah članicah zaupane pristojnemu nacionalnemu organu, po potrebi pa se vsako sklicevanje na pristojne nacionalne organe ali organe za nadzor trga v tej uredbi razume kot sklicevanje na Evropskega nadzornika za varstvo podatkov;

(44) „hud incident“ pomeni vsak incident ali okvaro umetnointeligenčnega sistema, ki neposredno ali posredno povzroči:

(a) smrt osebe ali hudo škodo za zdravje osebe;

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

(c) kršitev obveznosti iz prava Unije, namenjenih varstvu temeljnih pravic;

(d) resna škoda za premoženje ali okolje;

(45) „kritična infrastruktura“ pomeni sredstvo, sistem ali njegov del, nujen za izvajanje storitve, ki je bistvena za ohranitev ključnih družbenih funkcij ali gospodarskih dejavnosti v smislu člena 2(4) in (5) Direktive .../... o odpornosti kritičnih subjektov;

(46) „osebni podatki“ pomeni osebne podatke, kakor so opredeljeni v členu 4(1) Uredbe (EU) 2016/679;

(47) „neosebni podatki“ pomeni podatke, ki niso osebni podatki, kakor so opredeljeni v členu 4(1) Uredbe (EU) 2016/679;

(48) „testiranje v dejanskih razmerah“ pomeni začasno testiranje umetnointeligenčnega sistema za predvideni namen v dejanskih razmerah zunaj laboratorija ali drugače simuliranega okolja z namenom zbiranja zanesljivih podatkov ter ugotavljanja in preverjanja skladnosti umetnointeligenčnega sistema z zahtevami iz te uredbe; testiranje v dejanskih razmerah se ne šteje za dajanje umetnointeligenčnega sistema na trg ali v uporabo v smislu te uredbe, če so izpolnjeni vsi pogoji iz člena 53 ali člena 54a;

(49) „načrt testiranja v dejanskih razmerah“ pomeni dokument, ki opisuje cilje, metodologijo, geografsko, populacijsko in časovno področje uporabe, spremljanje, organizacijo in izvajanje testiranja v dejanskih razmerah;

(50) „udeleženec“ za namen testiranje v dejanskih razmerah pomeni fizično osebo, ki sodeluje pri testiranju v dejanskih razmerah;

(51) „privolitev po seznanitvi“ pomeni, da udeleženec svobodno in prostovoljno izrazi pripravljenost sodelovati pri določenem testiranju v dejanskih razmerah, potem ko je bil seznanjen z vsemi vidiki testiranja, ki so pomembni za njegovo odločitev za sodelovanje; v primeru mladoletnikov in udeležencev, ki niso sposobni odločati o sebi, privolitev po seznanitvi da njihov zakonito imenovani zastopnik;

(52) „regulativni peskovnik za umetno inteligenco“ pomeni konkreten okvir, ki ga vzpostavi pristojni nacionalni organ in ki ponudnikom ali potencialnim ponudnikom umetnointeligenčnih sistemov omogoča razvoj, učenje, potrjevanje in testiranje, kadar je to ustrezno v dejanskih razmerah, inovativnega umetnointeligenčnega sistema v skladu s posebnim načrtom za omejen čas pod regulativnim nadzorom.

Člen 4

Izvedbeni akti

Za zagotovitev enotnih pogojev za izvajanje te uredbe v zvezi s pristopi k strojnemu učenju ter pristopi, ki temeljijo na logiki in znanju, iz člena 3(1) lahko Komisija sprejme izvedbene akte, s katerimi določi tehnične elemente teh pristopov, pri čemer upošteva tržni in tehnološki razvoj. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 74(2).

NASLOV IA

UMETNOINTELIGENČNI SISTEMI ZA SPLOŠNE NAMENE

Člen 4a

Skladnost umetnointeligenčnih sistemov za splošne namene s to uredbo

1. Brez poseganja v člene 5, 52, 53 in 69 te uredbe umetnointeligenčni sistemi za splošne namene izpolnjujejo le zahteve in obveznosti iz člena 4b.

2. Take zahteve in obveznosti se uporabljajo ne glede na to, ali je umetnointeligenčni sistem za splošne namene dan na trg ali v uporabo kot prednaučeni model in ali mora uporabnik umetnointeligenčnega sistema za splošno rabo ta model še izpopolniti.

Člen 4b

Zahteve za umetnointeligenčne sisteme za splošne namene in obveznosti za ponudnike takih sistemov

1. Umetnointeligenčni sistemi za splošne namene, ki se lahko uporabljajo kot umetnointeligenčni sistemi velikega tveganja ali kot komponente umetnointeligenčnega sistema velikega tveganja v smislu člena 6, izpolnjujejo zahteve iz naslova III, poglavje 2, te uredbe od datuma začetka uporabe izvedbenih aktov, ki jih Komisija sprejme v skladu s postopkom pregleda iz člena 74(2), najpozneje 18 mesecev po začetku veljavnosti te uredbe. Ti izvedbeni akti določajo in prilagajajo uporabo zahtev iz naslova III, poglavje 2, za umetnointeligenčne sisteme za splošne namene glede na njihove značilnosti, tehnično izvedljivost in posebnosti vrednostne verige umetne inteligence ter tržni in tehnološki razvoj. Pri izpolnjevanju teh zahtev se upošteva splošno priznano stanje tehnike.

2. Ponudniki umetnointeligenčnih sistemov za splošne namene iz odstavka 1 od datuma začetka uporabe izvedbenih aktov iz odstavka 1 izpolnjujejo obveznosti iz členov 16aa, 16e, 16f, 16 g, 16i, 16j, 25, 48 in 61.

3. Za namene izpolnjevanja obveznosti iz člena 16e ponudniki upoštevajo postopek ugotavljanja skladnosti na podlagi notranje kontrole iz Priloge VI, točki 3 in 4.

4. Ponudniki takih sistemov hranijo tudi tehnično dokumentacijo iz člena 11, ki je pristojnim nacionalnim organom na voljo še deset let po tem, ko je bil umetnointeligenčni sistem za splošne namene dan na trg Unije ali v uporabo v Uniji.

5. Ponudniki umetnointeligenčnih sistemov za splošne namene sodelujejo z drugimi ponudniki, ki nameravajo take sisteme dati v uporabo ali na trg Unije kot umetnointeligenčne sisteme velikega tveganja ali kot komponente umetnointeligenčnih sistemov velikega tveganja, in jim zagotavljajo potrebne informacije, da bi jim omogočili izpolnjevanje njihovih obveznosti iz te uredbe. Tako sodelovanje med ponudniki po potrebi varuje pravice intelektualne lastnine in zaupne poslovne informacije ali poslovne skrivnosti v skladu s členom 70. Za zagotovitev enotnih pogojev izvajanja te uredbe v zvezi z informacijami, ki jih morajo izmenjati ponudniki umetnointeligenčnih sistemov za splošne namene, lahko Komisija sprejme izvedbene akte v skladu s postopkom pregleda iz člena 74(2).

6. Pri izpolnjevanju zahtev in obveznosti iz pododstavkov 1, 2 in 3:

– se vsako sklicevanje na predvideni namen razume kot sklicevanje na morebitno uporabo umetnointeligenčnih sistemov za splošne namene kot umetnointeligenčnih sistemov velikega tveganja ali kot komponent umetnointeligenčnih sistemov velikega tveganja v smislu člena 6;

– se vsako sklicevanje na zahteve za umetnointeligenčne sisteme velikega tveganja v naslovu III, poglavje 2 razume kot sklicevanje samo na zahteve iz tega člena.

Člen 4c

Izjeme od člena 4b

1. Člen 4b se ne uporablja, če je ponudnik v navodilih za uporabo ali informacijah, ki spremljajo umetnointeligenčni sistem za splošno rabo, izrecno izključil vse uporabe z visokim tveganjem.

2. Takšna izključitev se izvede v dobri veri in se ne šteje za upravičeno, če ima ponudnik zadostne razloge za domnevo, da bi bil sistem lahko zlorabljen.

3. Kadar ponudnik odkrije tržno zlorabo ali je o njej obveščen, sprejme vse potrebne in sorazmerne ukrepe, da se prepreči takšno nadaljnjo zlorabo, zlasti ob upoštevanju obsega zlorabe in resnosti s tem povezanih tveganj.

NASLOV II

PREPOVEDANE PRAKSE UMETNE INTELIGENCE

Člen 5

1. Prepovedane so naslednje prakse umetne inteligence:

(a) dajanje na trg, dajanje v uporabo ali uporaba umetnointeligenčnega sistema, ki uporablja subliminalne tehnike, ki presegajo zavest osebe, s ciljem, da bi bistveno izkrivil vedenje osebe na način, ki tej ali drugi osebi povzroči ali bi ji verjetno lahko povzročil fizično ali psihično škodo, ali je to njegov učinek;

(b) dajanje na trg, dajanje v uporabo ali uporaba umetnointeligenčnega sistema, ki izkorišča katere koli šibke točke določene skupine oseb zaradi njihove starosti, invalidnosti ali posebnega socialnega ali ekonomskega položaja, s ciljem, da bi bistveno izkrivil vedenje osebe iz te skupine na način, ki tej ali drugi osebi povzroči ali bi ji verjetno lahko povzročil fizično ali psihično škodo, ali je to njegov učinek;

(c) dajanje na trg, dajanje v uporabo ali uporaba umetnointeligenčnih sistemov za ocenjevanje ali razvrščanje fizičnih oseb 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 skupin v družbenih okoliščinah, ki niso povezane s konteksti, v katerih so bili podatki prvotno ustvarjeni ali zbrani;

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

(d) uporaba sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih s strani organov organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali v njihovem imenu 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;

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

(iii) lokalizacijo ali identifikacijo fizične osebe za namene vodenja kazenske preiskave, pregona ali izvršitve kazenske sankcije za kazniva dejanja iz člena 2(2) Okvirnega sklepa Sveta 2002/584/PNZ[32], ki se v zadevni državi članici kaznujejo z zaporno kaznijo ali ukrepom, vezanim na odvzem prostosti najmanj treh let, ali druga določena kazniva dejanja, ki se v zadevni državi članici kaznujejo z zaporno kaznijo ali ukrepom, vezanim na odvzem prostosti najmanj pet let, kot je določeno v pravu 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;

[32] 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).

(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 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, pod pogojem, da se za tako dovoljenje nemudoma zaprosi med uporabo umetnointeligenčnega sistema, če pa je tako dovoljenje zavrnjeno, se uporaba nemudoma ustavi.

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 v svoji nacionalni zakonodaji določi potrebna podrobna pravila za zahtevo, izdajo in izvajanje ter nadzor in poročanje 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 KOT UMETNOINTELIGENČNIH SISTEMOV VELIKEGA TVEGANJA

Člen 6

Pravila razvrstitve za umetnointeligenčne sisteme velikega tveganja

1. Umetnointeligenčni sistem, ki je sam proizvod, ki ga zajema harmonizacijska zakonodaja Unije iz Priloge II, se šteje za sistem velikega tveganja, če je treba zanj opraviti ugotavljanje skladnosti, ki ga izvede tretja stran, zaradi dajanja tega proizvoda na trg ali v uporabo v skladu z zgoraj omenjeno zakonodajo.

2. Umetnointeligenčni sistem, ki je namenjen uporabi kot varnostna komponenta proizvoda, ki ga zajema zakonodaja iz odstavka 1, se šteje za sistem velikega tveganja, če je treba zanj opraviti ugotavljanje skladnosti, ki ga izvede tretja stran, zaradi dajanja tega proizvoda na trg ali v uporabo v skladu z zgoraj omenjeno zakonodajo. Ta določba se uporablja ne glede na to, ali je umetnointeligenčni sistem dan na trg ali v uporabo neodvisno od proizvoda.

3. Umetnointeligenčni sistemi iz Priloge III se štejejo za umetnointeligenčne sisteme velikega tveganja, razen če je rezultat sistema v razmerju do zadevnega ukrepa ali odločitve, ki jo je treba sprejeti, zgolj pomožen, in zato ni verjetnosti, da bi vodil v pomembno tveganje za zdravje, varnost ali temeljne pravice.

Da se zagotovijo enotni pogoji za izvajanje te uredbe, Komisija najpozneje eno leto po začetku veljavnosti te uredbe sprejme izvedbene akte, v katerih določi okoliščine, v katerih bi bili izhodni podatki umetnointeligenčnega sistema iz Priloge III v zvezi z zadevnim ukrepom ali odločitvijo, ki jo je treba sprejeti, zgolj dodatek. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 74(2).

Člen 7

Spremembe Priloge III

1. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 73 za spremembo 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 področju 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 izida, ustvarjenega s sistemom umetne inteligence, ni 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;

(i) razsežnost in verjetnost koristi od uporabe umetne inteligence za posameznike, skupine ali družbo na splošno.

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

(a) zadevni umetnointeligenčni sistem(i) velikega tveganja ob upoštevanju meril iz odstavka 2 ne predstavljajo več večjih tveganj za temeljne pravice, zdravje ali varnost;

(b) črtanje ne zmanjšuje splošne ravni varovanja zdravja, varnosti in temeljnih pravic v skladu s pravom Unije.

POGLAVJE 2

ZAHTEVE ZA UMETNOINTELIGENČNE SISTEME VELIKEGA TVEGANJA

Člen 8

Izpolnjevanje zahtev

1. Umetnointeligenčni sistemi velikega tveganja izpolnjujejo zahteve iz tega poglavja po potrebi ob upoštevanju splošno priznavanega stanja tehnike.

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 tveganj

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

2. Sistem obvladovanja tveganja pomeni neprekinjen ponavljajoč se proces, ki se načrtuje in 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, ki so najbolj verjetna z vidika zdravja, varnosti in temeljnih pravic glede na predvideni namen umetnointeligenčnega sistema velikega tveganja;

   (b) [črtano];

   (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.

   Tveganja iz tega odstavka se nanašajo samo na tista, ki jih je mogoče razumno ublažiti ali odpraviti z razvojem ali zasnovo umetnointeligenčnega sistema velikega tveganja ali zagotovitvijo ustreznih tehničnih informacij.

3. Pri ukrepih za obvladovanje tveganja iz točke (d) odstavka 2 se ustrezno upoštevajo učinki in možen medsebojni vpliv, ki izhajajo iz skupne uporabe zahtev iz tega poglavja 2, da se učinkoviteje čim bolj zmanjšajo tveganja, obenem pa se doseže ustrezno ravnovesje pri izvajanju ukrepov za izpolnjevanje teh zahtev.

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.

Pri določanju najustreznejših ukrepov za obvladovanje tveganja se zagotovi naslednje:

(a) odpraviti ali zmanjšati tveganja, ugotovljena in ocenjena v skladu z odstavkom 2, v največji možni meri z ustrezno zasnovo in razvojem umetnointeligenčnega sistema velikega tveganja;

(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.

V prid 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 so testirani, da se zagotovi, da delujejo na način, ki je združljiv z njihovim predvidenim namenom, in izpolnjujeo zahteve iz tega poglavja.

6. Postopki testiranja lahko vključujejo testiranje v dejanskih okoliščinah v skladu s členom 54a.

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 sistemu obvladovanja tveganja iz odstavkov 1 do 7 se posebej upošteva, ali je verjetno, da bodo do zadevnega umetnointeligenčnega sistema velikega tveganja dostopale osebe, mlajše od 18 let oziroma ali bo sistem vplival nanje.

9. Pri ponudnikih umetnointeligenčnih sistemov velikega tveganja, za katere veljajo zahteve v zvezi z notranjimi procesi za upravljanje tveganj v skladu z ustreznim sektorskim pravom Unije, so vidiki, opisani v odstavkih 1 do 8 lahko del postopkov upravljanja tveganj, vzpostavljenih v skladu s tem pravom.

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) postopke zbiranja 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, za katere je verjetno, da bodo vplivale na zdravje in varnost fizičnih oseb ali povzročile diskriminacijo, prepovedano s pravom Unije;

(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 in v največji možni meri 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, ki ne uporabljajo tehnik, ki vključujejo učenje modelov s podatki, se odstavki 2 do 5 uporabljajo le za testne podatke.

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 jasno in celovito zagotavlja vse potrebne informacije za ugotavljanje skladnosti umetnointeligenčnega sistema z navedenimi zahtevami. Vsebovati mora vsaj elemente iz Priloge IV oziroma v primeru MSP, vključno z zagonskimi podjetji, morebitno enakovredno dokumentacijo, ki služi istim ciljem, razen če pristojni organ šteje to za neprimerno.

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 sistem tehnično omogoča samodejno beleženje dogodkov („dnevniki“) ves življenjski cikel sistema.

2. Da se zagotovi raven sledljivosti delovanja umetnointeligenčnega sistema, ki ustreza predvidenemu namenu sistema, zmogljivosti vodenja dnevnikov omogočajo beleženje dogodkov, pomembnih za:

   (i) prepoznavanje situacij, ki lahko povzročijo, da bi umetnointeligenčni sistem predstavljal tveganje v smislu člena 65(1), ali vodijo v bistvene spremembe;

   (ii) spremljanje po dajanju na trg iz člena 61 in

   (iii) spremljanje delovanja umetnointeligenčnega sistema velikega tveganja iz člena 29(4).

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 se doseže skladnost z ustreznimi obveznostmi uporabnika in ponudnika iz poglavja 3 tega naslova, uporabnikom pa omogoči razumevanje in pravilna uporaba sistema.

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 navajajo:

   (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) predvideni namen, vključno s posebnim geografskim, vedenjskim ali funkcionalnim okoljem, v katerem naj bi se umetnointeligenčni sistem velikega tveganja uporabljal;

      (ii) raven točnosti, vključno s pripadajočimi metrikami, 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, ki lahko privedejo do tveganj za zdravje in varnost ali za temeljne pravice iz člena 9(2);

(iv) kadar je to primerno, njegovo vedenje v zvezi s specifičnimi 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;

(vi) kadar je to primerno, opis pričakovanih rezultatov 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) potrebne računalniške in strojnoopremne vire, življenjsko dobo umetnointeligenčnega sistema velikega tveganja ter vse potrebne vzdrževalne in negovalne ukrepe, vključno z njihovo pogostnostjo, za zagotovitev pravilnega delovanja tega umetnointeligenčnega sistema, tudi v zvezi s posodobitvami programske opreme;

(f) opis mehanizma, vgrajenega v umetnointeligenčni sistem, ki uporabnikom omogoča ustrezno zbiranje, hrambo in razlaganje dnevnikov, kadar je to ustrezno.

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 vrstami ukrepov:

(a) ukrepi, določenimi in vgrajenimi, če je to tehnično izvedljivo, v umetnointeligenčni sistem velikega tveganja s strani ponudnika, preden je sistem dan na trg ali v uporabo;

(b) ukrepi, ki jih ponudnik določi pred dajanjem umetnointeligenčnega sistema velikega tveganja na trg ali v uporabo in so primerni za izvedbo s strani uporabnika.

4. Za namene izvajanja odstavkov 1 do 3 se umetnointeligenčni sistem velikega tveganja uporabniku zagotovi tako, da fizične osebe, ki jim je dodeljen človekov nadzor, kot je ustrezno in sorazmerno z okoliščinami:

(a) razumejo zmogljivosti in omejitve umetnointeligenčnega sistema velikega tveganja ter so sposobne ustrezno spremljati njegovo delovanje;

(b) se zavedajo morebitne težnje po samodejnem zanašanju ali prevelikem zanašanju na izhodne podatke umetnointeligenčnega sistema velikega tveganja („pristranskost zaradi avtomatizacije“);

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

(d) se v specifičnih situacijah odločijo, da umetnointeligenčnega sistema velikega tveganja ne bodo uporabili ali bodo kako drugače zanemarili, presegli ali izničili izhodne podatke umetnointeligenčnega sistema velikega tveganja;

(e) posežejo v delovanje umetnointeligenčnega sistema velikega tveganja ali ga prekinejo 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 ločeno preverita in potrdita vsaj dve fizični osebi. Zahteva o ločeni preverbi s strani vsaj dveh fizičnih oseb se ne uporablja za umetnointeligenčne sisteme velikega tveganja, ki se uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, v primerih, ko je po pravu Unije in nacionalnem pravu uporaba te zahteve nesorazmerna.

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.

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

   Umetnointeligenčne sisteme velikega tveganja, ki se po dajanju na trg ali v uporabo še naprej učijo, je treba razviti tako, da se v največji možni meri odpravi tveganje morebiti pristranskih izhodnih podatkov, ki bi vplivali na vhodne podatke za prihodnje operacije („povratne zanke“), in se to ustrezno obravnava s primernimi blažilnimi ukrepi.

4. 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;

(aa) navedejo svoje ime, registrirano trgovsko ime ali registrirano blagovno znamko, naslov, na katerem so dosegljivi, v umetnointeligenčnem sistemu velikega tveganja ali, kadar to ni mogoče, na embalaži ali spremni dokumentaciji, kot je ustrezno;

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

(c) hranijo tehnično dokumentacijo iz člena 18;

(d) kadar je to pod njihovim nadzorom, hranijo dnevnike, ki jih samodejno ustvarijo njihovi umetnointeligenčni sistemi velikega tveganja iz člena 20;

(e) zagotovijo, da umetnointeligenčni sistem velikega tveganja pred dajanjem na trg ali v uporabo opravi ustrezen postopek ugotavljanja skladnosti iz člena 43;

(f) izpolnjujejo obveznosti registracije iz člena 51(1);

(g) sprejmejo potrebne popravne ukrepe iz člena 21, če umetnointeligenčni sistem velikega tveganja ni skladen z zahtevami iz poglavja 2 tega naslova;

(h) obvestijo ustrezni pristojni nacionalni organ 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 razvoj, nadzor kakovosti in zagotavljanje kakovosti 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 incidentihv 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.

2a. Pri ponudnikih umetnointeligenčnih sistemov velikega tveganja, za katere veljajo obveznosti v zvezi s sistemom upravljanja kakovosti v skladu z ustreznim sektorskim pravom Unije, so vidiki, opisani v odstavku 1 lahko del sistemov upravljanja kakovosti, vzpostavljenih v skladu s tem pravom.

3. Za ponudnike, ki so finančne institucije, za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki v skladu z zakonodajo Unije o finančnih storitvah, se šteje, da je obveznost vzpostavitve sistema vodenja kakovosti z izjemo odstavka 1, točke (g), (h) in (i), izpolnjena z upoštevanjem pravil o ureditvah ali procesih notranjega upravljanja v skladu z ustrezno zakonodajo Unije o finančnih storitvah. V tem okviru se upoštevajo vsi harmonizirani standardi iz člena 40 te uredbe.

Člen 18

Vodenje dokumentacije

1. 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.

1a. Vsaka država članica določi pogoje, pod katerimi je dokumentacija iz odstavka 1 na voljo pristojnim nacionalnim organom za obdobje iz navedenega odstavka v primerih, ko gre ponudnik ali njegov pooblaščeni zastopnik, ki ima sedež na njenem ozemlju, v stečaj ali preneha opravljati svojo dejavnost pred koncem tega obdobja.

2. Ponudniki, ki so finančne institucije, za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki v skladu z zakonodajo Unije o finančnih storitvah, vodijo tehnično dokumentacijo kot del dokumentacije, ki se hrani v skladu z ustrezno zakonodajo Unije o finančnih storitvah.

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. [črtano]

Člen 20

Samodejno ustvarjeni dnevniki

1. Ponudniki umetnointeligenčnih sistemov velikega tveganja vodijo dnevnike iz člena 12(1), 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. Hranijo jih za obdobje vsaj šestih mesecev, razen če je v veljavnem pravu Unije ali nacionalnem pravu, zlasti v pravu Unije o varstvo osebnih podatkov, določeno drugače.

2. Ponudniki, ki so finančne institucije, za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki v skladu z zakonodajo Unije o finančnih storitvah, vodijo dnevnike, ki jih samodejno ustvarijo njihovi umetnointeligenčni sistemi velikega tveganja, kot del dokumentacije, ki se hrani v skladu z ustrezno zakonodajo Unije o finančnih storitvah.

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 – če je ustrezno – preiščejo vzroke v sodelovanju z uporabnikom, ki poroča, in 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, in sicer v jeziku, ki ga organ zadevne države članice zlahka razume. Ponudniki na podlagi obrazložene zahteve pristojnega nacionalnega organa temu organu omogočijo tudi dostop do dnevnikov iz člena 12(1), 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 23a

Pogoji, pod katerimi za druge osebe veljajo enake obveznosti kot za ponudnika

1. Vse fizične ali pravne osebe se za namene te uredbe štejejo za ponudnika umetnointeligenčnega sistema velikega tveganja in zanje veljajo obveznosti ponudnika iz člena 16 v kateri koli od naslednjih okoliščin:

   (a) svoje ime ali blagovno znamko dajo na umetnointeligenčni sistem velikega tveganja, ki je že bil dan na trg ali v uporabo, brez poseganja v pogodbene dogovore, ki določajo, da so obveznosti dodeljene drugače;

(b) [črtano]

(c) znatno spremenijo umetnointeligenčni sistem velikega tveganja, ki je že dan na trg ali v uporabo;

(d) spremenijo predvideni namen umetnointeligenčnega sistema, ki ni sistem velikega tveganja in ki je že dan na trg ali v uporabo, tako da spremenjeni sistem postane umetnointeligenčni sistem velikega tveganja;

(e) umetnointeligenčni sistem za splošne namene dajo na trg ali v uporabo kot umetnointeligenčni sistem velikega tveganja ali kot komponento umetnointeligenčnega sistema velikega tveganja.

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

3. Za umetnointeligenčne sisteme velikega tveganja, ki so varnostne komponente proizvodov, za katere se uporabljajo pravni akti iz oddelka A Priloge II, se proizvajalec teh proizvodov šteje za ponudnika umetnointeligenčnega sistema velikega tveganja in zanj veljajo obveznosti v skladu s členom 16 v skladu z enim od naslednjih scenarijev:

(i) umetnointeligenčni sistem velikega tveganja se da na trg skupaj s proizvodom pod imenom ali blagovno znamko proizvajalca proizvoda;

(ii) umetnointeligenčni sistem velikega tveganja se da v uporabo pod imenom ali blagovno znamko proizvajalca proizvoda, potem ko je bil proizvod dan na trg.

Člen 24

[črtano]

Člen 25

Pooblaščeni zastopniki

1. 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. Za namene te uredbe pooblastilo omogoča pooblaščenemu zastopniku, da opravlja naslednje naloge:

(-a) preveri, da je bila pripravljena izjava EU o skladnosti in tehnična dokumentacija ter da je ponudnik izvedel ustrezen postopek ugotavljanja skladnosti;

(a) hrani kontaktne podatke ponudnika, ki je določil pooblaščenega zastopnika, izvod izjave EU o skladnosti; tehnično dokumentacijo in, če je ustrezno, potrdilo, ki ga je izdal priglašeni organ, kar je pristojnim nacionalnim organom in nacionalnim organom iz člena 63(7) na voljo še deset let po tem, ko je bil umetnointeligenčni sistem velikega tveganja dan na trg ali v uporabo;

(b) pristojnemu nacionalnemu organu na obrazloženo zahtevo zagotovi vse informacije in dokumentacijo, vključno s tisto, ki se hrani v skladu s točko (b), potrebne za dokazovanje skladnosti umetnointeligenčnega sistema velikega tveganja z zahtevami iz poglavja 2 tega naslova, vključno z dostopom do dnevnikov iz člena 12(1), 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 obrazloženo zahtevo sodeluje s pristojnimi nacionalnimi organi pri vseh ukrepih, ki jih slednji sprejmejo v zvezi z umetnointeligenčnim sistemom velikega tveganja;

(d) izpolnjuje obveznosti registracije iz člena 51(1) in, če registracijo sistema izvede ponudnik sam, preveri, ali so informacije iz dela II, 1 do 11, Priloge VIII pravilne.

Pooblaščeni zastopnik odstopi od pooblastila, če ima zadostne razloge za domnevo, da ponudnik ravna v nasprotju s svojimi obveznostmi iz te uredbe. V tem primeru o odstopu od pooblastila in razlogih zanj nemudoma obvesti organ za nadzor trga države članice, v kateri ima sedež, in po potrebi ustrezni priglašeni organ.

Pooblaščeni zastopnik je pravno odgovoren za umetnointeligenčne sisteme z napako na isti podlagi kot ponudnik ter skupaj in solidarno z njim v zvezi z njegovo morebitno odgovornostjo v skladu z Direktivo Sveta 85/374/EGS.

Člen 26

Obveznosti uvoznikov

1. Pred dajanjem umetnointeligenčnega sistema velikega tveganja na trg uvozniki tega sistema zagotovijo, da je skladen s to uredbo, tako da preverijo:

(a) da je ponudnik za ta umetnointeligenčnegi sistemi izvedel ustrezen postopek ugotavljanja skladnosti iz člena 43;

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

(c) da je sistem opremljen z zahtevano oznako skladnosti CE ter so mu priloženi izjava EU o skladnosti in navodila za uporabo;

(d) da je ponudnik določil pooblaščenega zastopnika iz člena 25.

2. Kadar ima uvoznik zadostne razloge za domnevo, da umetnointeligenčni sistem velikega tveganja ni skladen s to uredbo ali je ponarejen ali ga spremlja ponarejena dokumentacija, tega sistema ne da na trg, dokler ni zagotovljena skladnost zadevnega umetnointeligenčnega sistema. Kadar umetnointeligenčni sistem velikega tveganja predstavlja tveganje v smislu člena 65(1), uvoznik o tem obvesti ponudnika umetnointeligenčnega sistema, pooblaščenega zastopnika in organe za nadzor trga.

3. Uvozniki navedejo svoje ime, registrirano trgovsko ime ali registrirano blagovno znamko, 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.

4a. Uvoznik še 10 let po tem, ko je bil umetnointeligenčni sistem dan na trg ali v uporabo, hranijo izvod potrdila, ki ga je izdal priglašeni organ, če je ustrezno, navodil za uporabo in izjave EU o skladnosti.

5. Uvozniki pristojnim nacionalnim organom na utemeljeno zahtevo predložijo vse potrebne informacije in dokumentacijo, vključno s tistimi, ki se hranijo v skladu z odstavkom 5, da dokažejo skladnost umetnointeligenčnega sistema velikega tveganja z zahtevami iz poglavja 2 tega naslova v jeziku, ki ga ta pristojni nacionalni organ zlahka razume. V ta namen zagotovijo tudi, da je tem organom lahko na voljo tehnična dokumentacija.

5a. Uvoznik sodeluje z nacionalnimi pristojnimi organi pri vseh ukrepih, ki jih ti organi sprejmejo v zvezi z umetnointeligenčnim sistemom, katerega uvoznik je.

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 CE, ali mu je priložen izvod izjave EU o skladnosti in navodila za uporabo ter ali sta ponudnik in uvoznik sistema, kot je ustrezno, izpolnila vsak svoje obveznosti iz člena 16, točka (b), oziroma člena 26(3).

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, kot je ustrezno.

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, kot je ustrezno. 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 o dejavnostih, kot je opisano v odstavkih od 1 do 4.

5a. Distributerji sodelujejo s pristojnimi nacionalnimi organi pri vseh ukrepih, ki jih ti organi sprejmejo v zvezi z umetnointeligenčnim sistemom, katerega distributerji so.

Člen 28

[črtano]

Člen 29

Obveznosti uporabnikov umetnointeligenčnih sistemov velikega tveganja

1. Uporabniki umetnointeligenčnih sistemov velikega tveganja uporabljajo take sisteme v skladu s priloženimi navodili za uporabo, na podlagi odstavkov 2 in 5 tega člena.

1a. Uporabniki človekov nadzor dodelijo fizičnim osebam, ki imajo potrebno pristojnost, usposobljenost in pooblastila.

2. Obveznosti iz odstavka 1 in 1a 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 izvajajo človekov nadzor in 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 in prekinejo uporabo umetnointeligenčnega sistema. Če uporabnik ne more priti v stik s ponudnikom, se smiselno uporablja člen 62. Ta obveznost ne zajema občutljivih operativnih podatkov uporabnikov umetnointeligenčnih sistemov, ki so organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj.

Za uporabnike, ki so finančne institucije, za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki v skladu z zakonodajo Unije o finančnih storitvah, se šteje, da je obveznost spremljanja iz prvega pododstavka izpolnjena z upoštevanjem pravil o ureditvah, procesih in mehanizmih notranjega upravljanja na podlagi ustrezne zakonodaje o finančnih storitvah.

5. Uporabniki umetnointeligenčnih sistemov velikega tveganja vodijo dnevnike iz člena 12(1), ki jih samodejno ustvari ta umetnointeligenčni sistem velikega tveganja, če so ti dnevniki pod njihovim nadzorom. Hranijo jih za obdobje vsaj šestih mesecev, razen če je v veljavnem pravu Unije ali nacionalnem pravu, zlasti v pravu Unije o varstvo osebnih podatkov, določeno drugače.

Uporabniki, ki so finančne institucije, za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali procesi v skladu z zakonodajo Unije o finančnih storitvah, vodijo dnevnike kot del dokumentacije, ki se hrani na podlagi ustrezne zakonodaje Unije o finančnih storitvah.

5a. Uporabniki umetnointeligenčnih sistemov velikega tveganja, ki so javni organi, agencije ali organi, razen organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organov za nadzor meja, organov, pristojnih za priseljevanje ali azilnih organov, izpolnjujejo obveznosti registracije iz člena 51. Če ugotovijo, da sistem, ki ga nameravajo uporabljati, ni bil registriran v podatkovni zbirki EU iz člena 60, tega sistema ne uporabljajo in o tem obvestijo ponudnika ali distributerja.

6. 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.

6a. Uporabniki sodelujejo s pristojnimi nacionalnimi organi pri vseh ukrepih, ki jih ti organi sprejmejo v zvezi z umetnointeligenčnim sistemom, katerega uporabniki so.

POGLAVJE 4

PRIGLASITVENI IN PRIGLAŠENI ORGANI

Člen 30

Priglasitveni organi

1. Vsaka država članica imenuje ali vzpostavi najmanj en 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 odločijo, da ocenjevanje in spremljanje iz odstavka 1 izvaja nacionalni akreditacijski organ v smislu Uredbe (ES) št. 765/2008 in v skladu z njo.

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, ki jih pridobijo v skladu s členom 70.

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

8. [črtano]

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 sistemov, 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. Priglašeni organ posodobi dokumentacijo iz odstavka 2 in odstavka 3, kadar pride do pomembnih sprememb, da bi organu, pristojnemu za priglašene organe, omogočil spremljanje in preverjanje, ali se vse zahteve, določene v členu 33, stalno upoštevajo.

Člen 32

Postopek priglasitve

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

2. Priglasitveni organi priglasijo te organe Komisiji in ostalim državam članicam z uporabo elektronskega orodja za priglasitev, ki ga je razvila in ga upravlja Komisija.

3. Priglasitev iz odstavka 2 vključuje vse podrobnosti o dejavnostih ugotavljanja skladnosti, modul ali module za ugotavljanje skladnosti in zadevne umetnointeligenčne sisteme ter ustrezno potrdilo o usposobljenosti. Kadar priglasitev ne temelji na potrdilu o akreditaciji iz člena 31(2), priglasitveni organ Komisiji in drugim državam članicam predloži dokumentarna dokazila, ki potrjujejo usposobljenost organa za ugotavljanje skladnosti in vzpostavljene ureditve, s čimer se zagotovi, da bo organ pod redno spremljan in bo stalno izpolnjeval zahteve iz člena 33.

4. Zadevni organ za ugotavljanje skladnosti lahko izvaja dejavnosti priglašenega organa le, če Komisija ali druge države članice ne vložijo ugovora v dveh tednih od priglasitve s strani priglasitvenega organa, če vključuje potrdilo o akreditaciji iz člena 31(2), ali v dveh mesecih od priglasitve s strani priglasitvenega organa, če vključuje dokumentarna dokazila iz člena 31(3).

5. [črtano]

Člen 33

Zahteve v zvezi s priglašenimi organi

1. Priglašeni organ je ustanovljen v skladu z nacionalnim pravom in je pravna oseba.

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 v skladu s členom 70 spoštujejo 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 ustrezno zavarovanje odgovornosti za svoje dejavnosti ugotavljanja skladnosti, razen če odgovornost prevzame država članica, v kateri se nahajajo, v skladu z nacionalnim pravom ali če je ta država članica sama 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. Priglašeni organ ima stalno na voljo dovolj upravnega, tehničnega, pravnega 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. [črtano]

Člen 33a

Domneva o skladnosti z zahtevami v zvezi s priglašenimi organi

Kadar organ za ugotavljanje skladnosti dokaže svojo skladnost z merili, določenimi v ustreznih harmoniziranih standardih ali njihovih delih, katerih sklici so bili objavljeni v Uradnem listu Evropske unije, se domneva, da izpolnjuje zahteve iz člena 33, kolikor veljavni harmonizirani standardi zajemajo navedene zahteve.

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. Zadevni dokumenti v zvezi z ocenjevanjem usposobljenosti podizvajalca ali hčerinskega podjetja in delom, ki ga izvaja v skladu s to uredbo, so na voljo priglasitvenemu organu pet let od datuma zaključka podizvajanja.

Člen 34a

Operativne obveznosti priglašenih organov

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

2. Priglašeni organi izvajajo svoje dejavnosti, pri čemer se izognejo nepotrebnim bremenom za ponudnike, in ustrezno upoštevajo velikost podjetja, sektor, v katerem deluje, njegovo strukturo in stopnjo zahtevnosti zadevnega umetnointeligenčnega sistema velikega tveganja. Pri tem priglašeni organ vseeno upošteva stopnjo strogosti in zaščite, ki sta potrebni za skladnost umetnointeligenčnega sistema velikega tveganja z zahtevami te uredbe.

3. 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 ter da se olajša ocenjevanje, opisano v tem poglavju.

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. Priglasitveni organ uradno obvesti Komisijo in druge države članice o vseh pomembnih spremembah priglasitve priglašenega organa z uporabo elektronskega orodja za priglasitev iz člena 32(2).

2. Postopki iz členov 31 in 32 se uporabljajo za razširitev področja uporabe priglasitve. Za druge spremembe priglasitve, torej ne za razširitev njenega področja uporabe, se uporabljajo postopki, opisani v naslednjih odstavkih.

Če priglašeni organ sklene, da bo prenehal izvajati dejavnosti za ugotavljanje skladnosti, o tem čim prej obvesti priglasitveni organ in zadevne ponudnike, v primeru načrtovanega prenehanja pa eno leto pred prenehanjem izvajanja svojih dejavnosti. Potrdila lahko ostanejo začasno veljavna devet mesecev po prenehanju dejavnosti priglašenega organa, pod pogojem, da je drug priglašeni organ pisno potrdil, da bo prevzel odgovornost za umetnointeligenčne sisteme, na katere se ta potrdila nanašajo. Novi priglašeni organ opravi celotno oceno zadevnih umetnointeligenčnih sistemov do konca tega obdobja, šele nato izda nova potrdila za te sisteme. Kadar priglašeni organ preneha opravljati svojo dejavnost, priglasitveni organ prekliče imenovanje.

3. Kadar ima priglasitveni organ zadostne razloge za domnevo, da priglašeni organ ne izpolnjuje več zahtev iz člena 33 ali da ne izpolnjuje svojih obveznosti, priglasitveni organ, pod pogojem, da je imel priglašeni organ možnost, da predstavi svoja stališča, omeji, začasno prekliče ali umakne priglasitev, kot je primerno glede na resnost neizpolnjevanja teh zahtev ali neizpolnjevanja teh obveznosti. O tem nemudoma ustrezno obvesti Komisijo in druge države članice.

4. Če se imenovanje priglašenega organa začasno prekliče, omeji oziroma v celoti ali delno prekliče, priglašeni organ o tem obvesti zadevne proizvajalce najpozneje v 10 dneh.

5. V primeru omejitve, začasnega preklica ali umika priglasitve priglasitveni organ izvede ustrezne ukrepe za zagotovitev, da se gradivo zadevnega priglašenega organa ohrani in je na voljo priglasitvenim organom v drugih državah članicah ter organom, pristojnim za nadzor trga, če to zahtevajo.

6. V primeru omejitve, začasnega preklica ali preklica imenovanja priglasitveni organ:

   a) oceni vpliv na potrdila, ki jih je izdal priglašeni organ;

   b) Komisiji in drugim državam članicam v treh mesecih od uradnega obvestila o priglasitvi sprememb predloži poročilo o svojih ugotovitvah;

   c) od priglašenega organa zahteva, da v razumnem časovnem roku, ki ga določi organ, začasno prekliče ali umakne vsa neupravičeno izdana potrdila, da se zagotovi skladnost umetnointeligenčnih sistemov na trgu;

   d) obvesti Komisijo in države članice o potrdilih, za katera je zahteval začasni preklic ali umik;

e) zagotovi pristojnim nacionalnim organom države članice, v kateri ima ponudnik registriran sedež poslovanja, vse ustrezne informacije o potrdilih, za katera je zahteval začasni preklic ali umik. Ta pristojni organ sprejme ustrezne ukrepe za preprečitev morebitnega tveganja za zdravje, varnost ali temeljne pravice, če je to potrebno.

7. Razen neupravičeno izdanih potrdil in kadar je bila priglasitev začasno preklicana ali omejena, ostanejo potrdila veljavna v naslednjih okoliščinah:

a) priglasitveni organ je v enem mesecu od začasnega preklica ali omejitve potrdil, da v zvezi s potrdili, za katere velja začasen preklic ali omejitev, ni nobenega tveganja za zdravje, varnost ali temeljne pravice, in določil časovni potek in ukrepe, ki naj bi bili potrebni za odpravo začasnega preklica ali omejitve, ali

b) priglasitveni organ je potrdil, da v obdobju začasnega preklica ali omejitve ne bo izdano, spremenjeno ali ponovno izdano nobeno potrdilo, povezano z začasnim preklicem, poleg tega pa navede, ali je priglašeni organ med obdobjem začasnega preklica ali omejitve še vedno sposoben spremljati in ostati pristojen za veljavna izdana potrdila. Če organ, pristojen za priglašene organe, ugotovi, da priglašeni organ ni sposoben potrditi obstoječih izdanih potrdil: ponudnik pristojnim nacionalnim organom države članice, v kateri ima ponudnik sistema, na katerega se nanaša potrdilo, registrirani sedež poslovanja, v treh mesecih od začasnega preklica ali omejitve predloži pisno potrdilo, da drug kvalificiran priglašeni organ začasno prevzema naloge priglašenega organa, da bo spremljal in prevzel odgovornost za potrdila v obdobju začasnega preklica ali omejitve.

8. Razen v primeru neupravičeno izdanih potrdil in kadar je bilo imenovanje preklicano, ostanejo potrdila v naslednjih okoliščinah veljavna še devet mesecev:

a) če je pristojni nacionalni organ države članice, v kateri ima ponudnik umetnointeligenčnega sistema, na katerega se nanaša potrdilo, registrirani sedež poslovanja, potrdil, da v povezavi z zadevnimi sistemi ni tveganja za zdravje, varnost in temeljne pravice, ter

b) če je drugi priglašeni organ pisno potrdil, da bo takoj prevzel odgovornost za te sisteme in v dvanajstih mesecih od preklica imenovanja zaključil njihovo ocenjevanje.

V okoliščinah iz prvega pododstavka sme pristojni nacionalni organ države članice, v kateri ima ponudnik sistema, na katerega se nanaša potrdilo, sedež poslovanja, podaljšati začasno veljavnost potrdil še za nadaljnja obdobja treh mesecev, ki pa skupaj ne smejo trajati dlje kot dvanajst mesecev.

Pristojni nacionalni organ ali priglašeni organ, ki prevzame naloge priglašenega organa, na katerega vpliva sprememba priglasitve, o tem takoj obvesti Komisijo, druge države članice in druge priglašene organe.

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 v skladu s členom 70.

4. Kadar Komisija ugotovi, da priglašeni organ ne izpolnjuje ali ne izpolnjuje več zahtev iz člena 33, obvesti priglasitveni organ o razlogih za takšno ugotovitev in od njega zahteva, da sprejme potrebne popravne ukrepe, vključno z začasnim preklicem, omejitvijo ali preklicem imenovanja, če je to potrebno. Če priglasitveni organ ne sprejme potrebnih popravljalnih ukrepov, lahko Komisija z izvedbenimi akti začasno prekliče, omeji ali umakne priglasitev. 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 z umetnointeligenčnimi sistemi velikega tveganja vzpostavi ustrezno usklajevanje in sodelovanje med priglašenimi organi, dejavnimi v postopkih ugotavljanja skladnosti na podlagi te uredbe, in da pravilno delujejo v obliki sektorske skupine priglašenih organov.

2. Priglasitveni organ zagotovi, 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, če izpolnjujejo zahteve iz člena 33.

POGLAVJE 5

STANDARDI, UGOTAVLJANJE SKLADNOSTI, POTRDILA, REGISTRACIJA

Člen 40

Harmonizirani standardi

1. Za umetnointeligenčne sisteme velikega tveganja ali umetnointeligenčne sisteme za splošne namene, ki so skladni 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 ali, kot je ustrezno, z zahtevami iz člena 4a in člena 4b, kolikor ti standardi zajemajo te zahteve.

2. Komisija pri izdaji zahteve za standardizacijo evropskim organizacijam za standardizacijo v skladu s členom 10 Uredbe 1025/2012 določi, da so standardi skladni, jasno navedeni in pripravljeni tako, da so njihovi cilji zlasti:

   a) zagotavljati, da so umetnointeligenčni sistemi, ki so dani na trg ali v uporabo v Uniji, varni in spoštujejo vrednote Unije ter krepijo odprto strateško avtonomijo Unije;

   b) spodbujati naložbe in inovacije na področju umetne inteligence s povečanjem pravne varnosti ter konkurenčnosti in rasti trga Unije;

   c) krepiti večdeležniško upravljanje, kjer bodo zastopani vsi ustrezni evropski deležniki (npr. industrija, MSP, civilna družba, raziskovalci);

   d) prispevati h krepitvi globalnega sodelovanja pri standardizaciji na področju umetne inteligence, ki je v skladu z vrednotami in interesi Unije.

Komisija od evropskih organizacij za standardizacijo zahteva, da zagotovijo dokaze o svojih najboljših prizadevanjih za izpolnitev zgoraj navedenih ciljev.

Člen 41

Skupne specifikacije

1. Na Komisijo se prenese pooblastilo za sprejemanje izvedbenih aktov v skladu s postopkom pregleda iz člena 74(2), ki določa skupne tehnične specifikacije za zahteve iz poglavja 2 tega naslova ali, kot je ustrezno, z zahtevami iz člena 4a in člena 4b, po posvetovanju z odborom za umetno inteligenco iz člena 56, kadar so izpolnjeni naslednji pogoji:

   (a) v Uradnem listu Evropske unije v skladu z Uredbo (EU) št. 1025/2012 ni objavljen noben sklic na harmonizirane standarde, ki zajemajo ustrezne bistvene zdravstvene in varnostne zahteve;

   (b) Komisija je v skladu s členom 10(1) Uredbe 1025/2012 zahtevala, da ena ali več evropskih organizacij za standardizacijo pripravi osnutek harmoniziranega standarda za zahteve iz poglavja 2 tega naslova;

   (c) nobena od evropskih organizacij za standardizacijo ni sprejela zahteve iz točke (b) oziroma harmonizirani standardi, ki obravnavajo to zahtevo, niso bili predloženi v roku, določenem v skladu s členom 10(1) Uredbe 1025/2012, oziroma navedeni standardi niso skladni z zahtevo.

1a. Komisija pred pripravo osnutka izvedbenega akta obvesti odbor iz člena 22 Uredbe (EU) št. 1025/2012, da meni, da so pogoji iz odstavka 1 izpolnjeni.

2. Komisija pri zgodnji pripravi osnutka izvedbenega akta o določitvi skupne specifikacije izpolni cilje iz člena 40(2) in zbere mnenja ustreznih organov ali strokovnih skupin, ustanovljenih v skladu z ustreznim sektorskim pravom Unije. Komisija na podlagi tega posvetovanja pripravi osnutek izvedbenega akta.

3. Za umetnointeligenčne sisteme velikega tveganja ali umetnointeligenčne sisteme za splošne namene, ki so v skladu s skupnimi specifikacijami iz odstavka 1, se domneva, da so skladni z zahtevami iz poglavja 2 tega naslova ali, kot je ustrezno, z zahtevami iz člena 4a in člena 4b, kolikor te skupne specifikacije zajemajo te zahteve.

4. Kadar se sklici na harmonizirani standard objavijo v Uradnem listu Evropske unije, se izvedbeni akti iz odstavka 1, ki zajemajo zahteve iz poglavja 2 tega naslova ali zahteve iz člena 4a in člena 4b, razveljavijo, kot je ustrezno.

5. Kadar država članica meni, da skupna specifikacija ne izpolnjuje v celoti zahtev iz poglavja 2 tega naslova ali zahtev iz člena 4a in člena 4b, kot je ustrezno, o tem s podrobno obrazložitvijo obvesti Komisijo, Komisija pa te informacije oceni in po potrebi spremeni izvedbeni akt, ki določa zadevno skupno specifikacijo.

Člen 42

Domneva o skladnosti z nekaterimi zahtevami

1. Za umetnointeligenčne sisteme velikega tveganja, ki so bili naučeni in testirani na podlagi podatkov, ki odražajo posebno geografsko, vedenjsko ali funkcionalno okolje, v katerem naj bi se uporabljali, se domneva, da izpolnjujejo ustrezne zahteve iz člena 10(4).

2. Za umetnointeligenčne sisteme velikega tveganja in umetnointeligenčne sisteme za splošne namene, 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[33] in na katere sklici so bili objavljeni v Uradnem listu Evropske unije, se domneva, da so 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, izbere enega od naslednjih postopkov:

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

   (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.

[33] 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).

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 in umetnointeligenčne sisteme za splošne namene ponudniki upoštevajo postopek ugotavljanja skladnosti na podlagi notranje kontrole iz Priloge VI, ki ne predvideva sodelovanja priglašenega organa.

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 postopka priglasitve 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. [črtano]

5. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 73 za posodobitev prilog VI in VII 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 jeziku, ki je ustreznim organom v državi članici, v kateri ima priglašeni organ sedež, zlahka razumljiv.

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. Vsako dopolnilo k potrdilu ostane veljavno, dokler je veljavno potrdilo, ki ga to dopolnjuje.

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

Na voljo mora biti pritožbeni postopek proti odločitvam priglašenih organov.

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 sistemi, predloži ustrezne informacije o vprašanjih v zvezi z negativnimi rezultati ugotavljanja skladnosti, na zahtevo pa tudi pozitivnimi rezultati ugotavljanja skladnosti.

4. Obveznosti iz odstavkov 1 do 3 se upoštevajo v skladu s členom 70.

Člen 47

Odstopanje od postopkov ugotavljanja skladnosti

1. Z odstopanjem od člena 43 in na podlagi ustrezno utemeljene zahteve 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, ob upoštevanju izjemnih razlogov, ki upravičujejo odstopanje. Ti postopki se zaključijo brez nepotrebnega odlašanja.

1a. V ustrezno utemeljenih nujnih primerih iz izjemnih razlogov javne varnosti ali v primeru posebne, precejšnje in neposredne grožnje za življenje ali telesno varnost fizičnih oseb lahko organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali organi civilne zaščite dajo v uporabo določen umetnointeligenčni sistem velikega tveganja brez dovoljenja iz odstavka 1, če se se za tako dovoljenje nemudoma zaprosi med uporabo ali po njej, če pa je tako dovoljenje zavrnjeno, se uporaba nemudoma prekine, vsi rezultati in izhodni podatki iz te uporabe pa se takoj zavržejo.

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. Ta obveznost ne zajema občutljivih operativnih podatkov v zvezi z dejavnostmi organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj.

3. [črtano]

4. [črtano]

5. [črtano]

6. Za umetnointeligenčne sisteme velikega tveganja, povezane s proizvodi, zajetimi v harmonizacijski zakonodaji Unije iz Priloge II, oddelek A, se uporabljajo samo postopki za ugotavljanje odstopanja od skladnosti, določeni v navedeni zakonodaji.

Člen 48

Izjava EU o skladnosti

1. Ponudnik za vsak umetnointeligenčni sistem sestavi pisno ali elektronsko podpisano 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 jezik, ki ga pristojni nacionalni organi v državi članici oziroma državah članicah, v katerih je umetnointeligenčni sistem velikega tveganja dostopen, zlahka razumejo.

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 harmonizacijsko 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 CE

1. Za oznako skladnosti CE veljajo splošna načela iz člena 30 Uredbe (ES) št. 765/2008.

2. 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.

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

[črtano]

Člen 51

Registracija zadevnih operaterjev in umetnointeligenčnih sistemov velikega tveganja s seznama v Prilogi III

1. Ponudnik ali, kjer je to ustrezno, pooblaščeni zastopnik pred dajanjem umetnointeligenčnega sistema velikega tveganja, razen umetnointeligenčnih sistemov velikega tveganja s seznama v Prilogi III, točke 1, 6 in 7, v uporabo na področjih preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, upravljanja migracij, azila in nadzora meja ter umetnointeligenčnih sistemov velikega tveganja iz Priloge III, točka 2, se ponudnik in, kadar je to primerno, pooblaščeni predstavnik registrirata v podatkovni zbirki EU iz člena 60. Ponudnik ali, kadar je to primerno, pooblaščeni zastopnik v navedeni podatkovni zbirki registrira tudi svoje sisteme.

2. Pred uporabo umetnointeligenčnega sistema velikega tveganja s seznama v Prilogi III se uporabniki umetnointeligenčnih sistemov velikega tveganja, ki so javni organi, agencije, organi ali subjekti, ki delujejo v njihovem imenu, registrirajo v podatkovni zbirki EU iz člena 60 in izberejo sistem, ki ga nameravajo uporabljati.

   Obveznosti iz prejšnjega pododstavka se ne uporabljajo za organe ali agencije za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organe za nadzor meja, organe, pristojne za priseljevanje, ali azilne organe ter organe ali agencije, ki uporabljajo umetnointeligenčne sisteme velikega tveganja iz Priloge III, točka 2, pa tudi za subjekte, ki delujejo v njihovem imenu.

NASLOV IV

OBVEZNOSTI GLEDE PREGLEDNOSTI ZA PONUDNIKE IN UPORABNIKE NEKATERIH UMETNOINTELIGENČNIH SISTEMOV

Člen 52

Obveznosti glede preglednosti za ponudnike in uporabnike nekaterih umetnointeligenčnih sistemov

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 očitno z vidika fizične osebe, ki je razmeroma dobro obveščena, pozorna in preudarna, ob upoštevanju okoliščin in okvira uporabe. Ta obveznost se ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine tretjih strani ne uporablja za umetnointeligenčne sisteme, ki so z zakonom odobreni za odkrivanje, preprečevanje, preiskovanje in pregon kaznivih dejanj, razen če so ti sistemi na voljo javnosti za prijavo kaznivega dejanja.

2. Uporabniki sistema za biometrično kategorizacijo o delovanju sistema obvestijo fizične osebe, ki so mu izpostavljene. Ta obveznost se ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine tretjih strani ne uporablja za umetnointeligenčne sisteme, ki se uporabljajo za biometrično kategorizacijo ter so z zakonom dovoljeni za odkrivanje, preprečevanje in preiskovanje kaznivih dejanj.

2a. Uporabniki sistema za prepoznavanje čustev o delovanju sistema obvestijo fizične osebe, ki so mu izpostavljene. Ta obveznost se ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine tretjih strani ne uporablja za umetnointeligenčne sisteme, ki se uporabljajo za prepoznavanje čustev 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 ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine tretjih osebne uporablja, kadar je uporaba z zakonom dovoljena za odkrivanje, preprečevanje, preiskovanje in pregon kaznivih dejanj ali kadar je vsebina del očitno ustvarjalnega, satiričnega, umetniškega ali fiktivnega dela ali programa.

3a. Informacije iz odstavkov 1 do 3 se dajo na voljo fizičnim osebam na jasen in razločljiv način ter najpozneje ob prvem stiku ali izpostavljenosti.

4. Odstavki 1, 2, 2a ter 3 in 3a ne vplivajo na zahteve in obveznosti iz naslova III te uredbe in ne posegajo v druge obveznosti glede preglednosti za uporabnike umetnointeligenčnih sistemov, določene v pravu Unije ali nacionalnem pravu.

NASLOV V

UKREPI V PODPORO INOVACIJAM

Člen 53

Regulativni peskovniki za umetno inteligenco

-1a. Pristojni nacionalni organi lahko vzpostavijo regulativne peskovnike za umetno inteligenco za razvoj, učenje, testiranje in potrjevanje inovativnih umetnointeligenčnih sistemov pod neposrednim nadzorom, v skladu s smernicami in ob podpori pristojnega nacionalnega organa, preden so ti sistemi dani na trg ali v uporabo. Takšni regulativni peskovniki lahko vključujejo testiranje v dejanskih razmerah, ki ga nadzorujejo pristojni nacionalni organi.

-1b. [črtano]

-1c. Pristojni nacionalni organi po potrebi sodelujejo z drugimi ustreznimi organi in lahko omogočijo sodelovanje drugih akterjev v umetnointeligenčnem ekosistemu.

-1d. Ta člen ne vpliva na druge regulativne peskovnike, vzpostavljene v skladu z nacionalnim pravom ali pravom Unije, tudi v primerih, ko so proizvodi ali storitve, ki se v njih testirajo, povezani z uporabo inovativnih umetnointeligenčnih sistemov. Države članice zagotovijo ustrezno raven sodelovanja med organi, ki nadzorujejo te druge peskovnike, in pristojnimi nacionalnimi organi.

1. [črtano]

1a. [črtano]

1b. Namen vzpostavitve regulativnih peskovnikov za umetno inteligenco na podlagi te uredbe je prispevati k enemu ali več od naslednjih ciljev:

a) spodbujati inovacije in konkurenčnost ter olajšati razvoj umetnointeligenčnega ekosistema;
b) olajšati in pospešiti dostop umetnointeligenčnih sistemov do trga Unije, zlasti če so njihovi ponudniki mala in srednja podjetja (MSP), vključno z zagonskimi podjetji;
c) izboljšati pravno varnost in prispevati k izmenjavi dobrih praks s sodelovanjem z organi, vključenimi v regulativni peskovnik za umetno inteligenco, da se zagotovi prihodnja skladnost s to uredbo ter po potrebi z drugo zakonodajo Unije in držav članic;
d) prispevati k regulativnemu učenju, ki temelji na dokazih.

2. [črtano]

2a. Dostop do regulativnih peskovnikov za umetno inteligenco ima vsak ponudnik ali potencialni ponudnik umetnointeligenčnega sistema, ki izpolnjuje merila za upravičenost in izbor iz odstavka 6(a) in ki so ga izbrali pristojni nacionalni organi po izbirnem postopku iz odstavka 6(b). Ponudniki ali potencialni ponudniki lahko vloge predložijo tudi v partnerstvu z uporabniki ali drugimi ustreznimi tretjimi osebami.

Sodelovanje v regulativnem peskovniku za umetno inteligenco je omejeno na obdobje, ki je primerno glede na kompleksnost in obseg projekta. Pristojni nacionalni organ lahko to obdobje podaljša.

Sodelovanje v regulativnem peskovniku za umetno inteligenco temelji na posebnem načrtu iz odstavka 6 tega člena, o katerem se dogovorijo udeleženci in pristojni nacionalni organi, kot je ustrezno.

3. Sodelovanje v regulativnih peskovnikih za umetno inteligenco ne vpliva na nadzorna in popravljalna pooblastila pristojnih organov, ki nadzorujejo peskovnik. Ti organi svoja nadzorna pooblastila izvajajo prožno in v mejah zadevne zakonodaje ter uporabijo svoja diskrecijska pooblastila pri izvajanju pravnih določb za določen projekt peskovnika za umetno inteligenco, da bi podprli inovacije na področju umetne inteligence v Uniji.

Če udeleženci spoštujejo načrt peskovnika in pogoje za sodelovanje iz odstavka 6(c) ter v dobri veri upoštevajo smernice organov, organi ne naložijo upravnih glob za kršitev veljavne zakonodaje Unije ali države članice v zvezi z umetnointeligenčnim sistemom, ki se nadzoruje v peskovniku, vključno z določbami te uredbe.

4. Udeleženci so v skladu z veljavno zakonodajo Unije in držav članic o odgovornosti še naprej odgovorni za škodo, povzročeno med njihovim sodelovanjem v regulativnem peskovniku za umetno inteligenco.

4a. Pristojni nacionalni organ na zahtevo ponudnika ali potencialnega ponudnika umetnointeligenčnega sistema po potrebi predloži pisno dokazilo o dejavnostih, ki so bile uspešno izvedene v peskovniku. Pristojni nacionalni organ zagotovi tudi poročilo o izstopu, v katerem podrobno opiše dejavnosti, izvedene v peskovniku, ter povezane rezultate in učne izide. Tako pisno dokazilo in poročilo o izstopu bi lahko organi za nadzor trga ali priglašeni organi, kot je ustrezno, upoštevali v okviru postopkov ugotavljanja skladnosti ali preverjanj za nadzor trga.

Evropska komisija in Odbor za umetno inteligenco sta ob upoštevanju določb o zaupnosti iz člena 70 in s soglasjem udeležencev v peskovniku pooblaščena za dostop do poročil o izstopu in jih po potrebi upoštevata pri izvajanju svojih nalog iz te uredbe. Če se udeleženec in pristojni nacionalni organ s tem izrecno strinjata, se lahko poročilo o izstopu objavi na enotni informacijski platformi iz člena 55(3)(b).

4b. Regulativni peskovniki za umetno inteligenco so zasnovani in se izvajajo tako, da po potrebi olajšujejo čezmejno sodelovanje med pristojnimi nacionalnimi organi.

5. Pristojni nacionalni organi objavijo letna poročila o izvajanju regulativnih peskovnikov za umetno inteligenco, 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. Ta letna poročila se predložijo Odboru za umetno inteligenco, ki objavi povzetek vseh dobrih praks, pridobljenih izkušenj in priporočil. Ta obveznost objave letnih poročil ne zajema občutljivih operativnih podatkov v zvezi z dejavnostmi organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organov za nadzor meje in organov, pristojnih za priseljevanje, ali azilnih organov. Komisija in Odbor za umetno inteligenco pri izvajanju svojih nalog na podlagi te uredbe po potrebi upoštevata letna poročila.

5b. Komisija zagotovi, da so informacije o regulativnih peskovnikih za umetno inteligenco, tudi tistih, vzpostavljenih na podlagi tega člena, na voljo na enotni informacijski platformi iz člena 55(3)(b).

6. Načini in pogoji za vzpostavitev in delovanje regulativnih peskovnikov za umetno inteligenco na podlagi te uredbe se sprejmejo z izvedbenimi akti v skladu s postopkom pregleda iz člena 74(2).

Načini in pogoji v največji možni meri podpirajo prožnost pristojnih nacionalnih organov, da vzpostavijo in upravljajo svoje regulativne peskovnike za umetno inteligenco, spodbujajo inovacije in regulativno učenje ter zlasti upoštevajo posebne okoliščine in zmogljivosti sodelujočih MSP, vključno z zagonskimi podjetji.

Navedeni izvedbeni akti vključujejo skupna glavna načela o naslednjih vprašanjih:

a) upravičenosti in izboru za sodelovanje v regulativnem peskovniku za umetno inteligenco;
b) postopku za prijavo, sodelovanje, spremljanje, izstop iz regulativnega peskovnika za umetno inteligenco in njegovo prenehanje, vključno z načrtom peskovnika in poročilom o izstopu;
c) pogojih, ki veljajo za udeležence.

7. Kadar pristojni nacionalni organi presojajo o odobritvi testiranja v dejanskih razmerah, ki se nadzoruje v okviru regulativnega peskovnika za umetno inteligenco, vzpostavljenega na podlagi tega člena, se z udeleženci izrecno dogovorijo o pogojih takega testiranja in zlasti o ustreznih zaščitnih ukrepih za zaščito temeljnih pravic, zdravja in varnosti. Po potrebi sodelujejo z drugimi pristojnimi nacionalnimi organi, da bi zagotovili dosledne prakse po vsej Uniji.

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, lahko obdelujejo za namene razvoja, testiranja in učenja inovativnih umetnointeligenčnih sistemov v peskovniku pod naslednjimi kumulativnimi pogoji:

   (a) javni organ ali druga fizična ali pravna oseba javnega ali zasebnega prava razvije inovativne umetnointeligenčne sisteme za zaščito bistvenega javnega interesa na enem ali več naslednjih področjih:

      (i) [črtano]

      (ii) javna varnost in zdravje, vključno s preprečevanjem, nadzorom in zdravljenjem bolezni ter izboljšanjem sistemov zdravstvenega varstva;

      (iii) varstvo in izboljšanje kakovosti okolja, vključno z zelenim prehodom, blaženjem podnebnih sprememb in prilagajanjem nanje;

      (iv) energetska trajnostnost, promet in mobilnost;

      (v) učinkovitost in kakovost javne uprave in javnih storitev;

      (vi) kibernetska varnost in odpornost kritične infrastrukture;

   (b) obdelani podatki so potrebni za izpolnjevanje ene ali več zahtev iz naslova III, poglavje 2, 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 pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, kot je navedeno v členu 35 Uredbe (EU) 2016/679 in členu 39 Uredbe (EU) 2018/1725, ter 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, ki niso udeleženci peskovnika, razen če do takega razkritja pride v skladu z Uredbo (EU) 2016/679 ali, kjer je ustrezno, Uredbo (EU) 2018/725 in so se vsi udeleženci s tem strinjali;

(f) nobena obdelava osebnih podatkov v okviru peskovnika ne vpliva na uveljavljanje pravic posameznikov, na katere se nanašajo osebni podatki, kot so določene v pravu Unije o varstvu osebnih podatkov, zlasti členu 22 Uredbe (EU) 2016/679 in členu 24 Uredbe (EU) 2018/1725;

(g) vsi osebni podatki, obdelani v okviru peskovnika, so zaščiteni z ustreznimi tehničnimi in organizacijskimi ukrepi in 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, razen če je v pravu Unije ali nacionalnem pravu določeno drugače;

(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 iz Priloge IV;

(j) kratek povzetek projekta umetne inteligence, razvitega v peskovniku, njegovi cilji in pričakovani rezultati so objavljeni na spletišču pristojnih organov. Ta obveznost ne zajema občutljivih operativnih podatkov v zvezi z dejavnostmi organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organov za nadzor meje in organov, pristojnih za priseljevanje, ali azilnih organov.

1a. Za namene 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 organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj obdelava osebnih podatkov v regulativnih peskovnikih za umetno inteligenco temelji na posebnem pravu države članice ali Unije in zanjo veljajo enaki kumulativni pogoji, kot so navedeni v odstavku 1.

2. Odstavek 1 ne posega v pravo Unije ali držav članic, ki določa podlago za obdelavo osebnih podatkov, potrebno za namene razvoja, testiranja in učenja inovativnih umetnointeligenčnih sistemov, ali katero koli drugo pravno podlago v skladu s pravom Unije o varstvu osebnih podatkov.

Člen 54a

Testiranje umetnointeligenčnih sistemov velikega tveganja v dejanskih razmerah zunaj regulativnih peskovnikov za umetno inteligenco

1. Testiranje umetnointeligenčnih sistemov v dejanskih razmerah zunaj regulativnih peskovnikov za umetno inteligenco lahko izvajajo ponudniki ali potencialni ponudniki umetnointeligenčnih sistemov velikega tveganja s seznama v Prilogi III v skladu z določbami tega člena in načrtom testiranja v dejanskih razmerah iz tega člena.

Podrobni elementi načrta testiranja v dejanskih razmerah se določijo v izvedbenih aktih, ki jih Komisija sprejme v skladu s postopkom pregleda iz člena 74(2).

Ta določba ne posega v zakonodajo Unije ali držav članic za testiranje umetnointeligenčnih sistemov velikega tveganja, povezanih s proizvodi, zajetimi v zakonodaji iz Priloge II, v dejanskih razmerah.

2. Ponudniki ali potencialni ponudniki lahko testiranje umetnointeligenčnih sistemov velikega tveganja s seznama v Prilogi III v dejanskih razmerah izvedejo kadar koli, preden dajo umetnointeligenčni sistem na trg ali v uporabo, bodisi sami bodisi v partnerstvu z enim ali več potencialnimi uporabniki.

3. Testiranje umetnointeligenčnih sistemov velikega tveganja v dejanskih razmerah na podlagi tega člena ne posega v etično presojo, ki se lahko zahteva v skladu z nacionalnim pravom ali pravom Unije.

4. Ponudniki ali potencialni ponudniki lahko testiranje v dejanskih razmerah izvajajo le, če so izpolnjeni vsi naslednji pogoji:

(a) ponudnik ali potencialni ponudnik je pripravil načrt testiranja v dejanskih razmerah in ga predložil organu za nadzor trga v državi članici oziroma državah članicah, v katerih se bo izvajalo testiranje v dejanskih razmerah;

(b) organ za nadzor trga v državi članici oziroma državah članicah, v katerih se bo izvajalo testiranje v dejanskih razmerah, testiranju ni nasprotoval v 30 dneh po njegovi predložitvi;

(c) ponudnik ali potencialni ponudnik, z izjemo umetnointeligenčnih sistemov velikega tveganja iz Priloge III, točke 1, 6 in 7, na področjih preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, upravljanja migracij, azila in nadzora meja ter umetnointeligenčnih sistemov velikega tveganja iz Priloge III, točka 2, je registriral testiranje v dejanskih razmerah v podatkovni zbirki EU iz člena 60(5a) z vseevropsko enotno identifikacijsko številko in informacijami, določenimi v Prilogi VIIIa;

(d) ponudnik ali potencialni ponudnik, ki izvaja testiranje v dejanskih razmerah, ima sedež v Uniji ali je imenoval pravnega zastopnika za namene testiranja v dejanskih razmerah, ki ima sedež v Uniji;

(e) podatki, zbrani in obdelani za namene testiranja v dejanskih razmerah, se ne prenesejo v države zunaj Unije, razen če so pri prenosu in obdelavi zagotovljeni zaščitni ukrepi, enakovredni tistim, ki jih določa pravo Unije;

(f) testiranje v dejanskih razmerah ne traja dlje, kot je potrebno za dosego njegovih ciljev, v nobenem primeru pa ne dlje kot 12 mesecev;

(g) osebe, ki pripadajo ranljivim skupinam zaradi svoje starosti ali telesne ali duševne invalidnosti, so ustrezno zaščitene;

(h) [črtano]

(i) kadar ponudnik ali potencialni ponudnik testiranje v dejanskih razmerah organizira v sodelovanju z enim ali več potencialnimi uporabniki, so bili slednji obveščeni o vseh vidikih testiranja, ki so pomembni za njihovo odločitev za sodelovanje, in so prejeli ustrezna navodila za uporabo umetnointeligenčnega sistema iz člena 13; ponudnik ali potencialni ponudnik in uporabniki sklenejo sporazum, ki določa njihove vloge in odgovornosti, da se zagotovi skladnost z določbami za testiranje v dejanskih razmerah na podlagi te uredbe ter druge veljavne zakonodaje Unije in držav članic;

(j) udeleženci testiranja v dejanskih razmerah so dali privolitev po seznanitvi v skladu s členom 54b, v primeru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ko bi pridobitev privolitve po seznanitvi preprečila testiranje umetnointeligenčnega sistema, pa samo testiranje in rezultati testiranja v dejanskih razmerah ne smejo negativno vplivati na udeleženca;

(k) testiranje v dejanskih razmerah učinkovito nadzorujejo ponudnik ali potencialni ponudnik in uporabniki z osebami, ki so ustrezno kvalificirane na zadevnem področju in imajo potrebne zmogljivosti, usposobljenost in pooblastila za opravljanje svojih nalog;

(l) napovedi, priporočila ali odločitve umetnointeligenčnega sistema je mogoče učinkovito izničiti ali zanemariti.

5. Vsak udeleženec testiranja v dejanskih razmerah oziroma njegov zakonito imenovani zastopnik se lahko brez kakršne koli škode in brez obrazložitve kadar koli umakne iz testiranja, tako da prekliče svojo privolitev po seznanitvi. Preklic privolitve po seznanitvi ne vpliva na dejavnosti, ki se že izvajajo, in uporabo podatkov, pridobljenih na podlagi privolitve po seznanitvi pred njenim preklicem.

6. Vsak hud incident, ugotovljen med testiranjem v dejanskih razmerah, se sporoči nacionalnemu organu za nadzor trga v skladu s členom 62 te uredbe. Ponudnik ali potencialni ponudnik sprejme takojšnje blažilne ukrepe ali, če to ni mogoče, testiranje v dejanskih razmerah začasno prekine, dokler ne pride do tovrstne ublažitve, v nasprotnem primeru pa ga dokončno prekine. Ponudnik ali potencialni ponudnik po taki dokončni prekinitvi testiranja v dejanskih razmerah vzpostavi postopek za takojšnji preklic umetnointeligenčnega sistema.

7. Ponudniki ali potencialni ponudniki obvestijo nacionalni organ za nadzor trga v državi članici oziroma državah članicah, v katerih se izvaja testiranje v dejanskih razmerah, o začasni ali dokončni prekinitvi testiranja v dejanskih razmerah in o končnih rezultatih.

8. Ponudnik ali potencialni ponudnik je v skladu z veljavno zakonodajo Unije in držav članic o odgovornosti odgovoren za škodo, povzročeno med njegovim sodelovanjem pri testiranju v dejanskih razmerah.

Člen 54b

Privolitev po seznanitvi za sodelovanje pri testiranju v dejanskih razmerah zunaj regulativnih peskovnikov za umetno inteligenco

1. Za namene testiranja v dejanskih razmerah na podlagi člena 54a udeleženec testiranja da prostovoljno privolitev po seznanitvi, preden začne sodelovati pri takem testiranju in po tem, ko je bil z jedrnatimi, jasnimi, ustreznimi in razumljivimi informacijami ustrezno obveščen o:

(i) naravi in ciljih testiranja v dejanskih razmerah ter morebitnih nevšečnostih, ki so lahko povezane z njegovim sodelovanjem;

(ii) pogojih, pod katerimi se bo izvajalo testiranje v dejanskih razmerah, vključno s pričakovanim trajanjem sodelovanja udeleženca;

(iii) udeležencevih pravicah in zagotovilih v zvezi s sodelovanjem, zlasti o svoji pravici, da zavrne sodelovanje in da se lahko brez kakršne koli škode in brez obrazložitve kadar koli umakne iz testiranja v dejanskih razmerah;

(iv) načinih za vložitev zahteve, da se napovedi, priporočila ali odločitve umetnointeligenčnega sistema izničijo ali zanemarijo;

(v) vseevropski enotni identifikacijski številki testiranja v dejanskih razmerah v skladu s členom 54a(4c) in kontaktnih podatkih ponudnika ali njegovega zakonitega zastopnika, od katerega je mogoče dobiti dodatne informacije.

2. Privolitev po seznanitvi se datira in dokumentira, udeleženec ali njegov zakoniti zastopnik pa prejme kopijo.

Člen 55

Podporni ukrepi za operaterje, zlasti MSP, vključno z zagonskimi podjetji

1. Države članice sprejmejo naslednje ukrepe:

(a) MSP, vključno z zagonskimi podjetji, zagotovijo prednostni dostop do regulativnih peskovnikov za umetno inteligenco, če izpolnjujejo merila za upravičenost in izbor;

(b) organizirajo posebne dejavnosti ozaveščanja in usposabljanja o uporabi te uredbe, prilagojene potrebam MSP, vključno z zagonskimi podjetji, in po potrebi lokalnih javnih organov;

(c) po potrebi vzpostavijo poseben kanal za komunikacijo z MSP, vključno z zagonskimi podjetji, in po potrebi lokalnimi javnimi organi, da jim svetujejo in odgovarjajo na vprašanja o izvajanju te uredbe, tudi v zvezi s sodelovanjem v regulativnih peskovnikih za umetno inteligenco.

2. Pri določanju pristojbin za ugotavljanje skladnosti na podlagi člena 43 se upoštevajo posebni interesi in potrebe ponudnikov, ki so MSP, vključno z zagonskimi podjetji, pri čemer se te pristojbine znižajo sorazmerno z njihovo velikostjo, velikostjo trga in drugimi ustreznimi kazalniki.

3. Komisija sprejme naslednje ukrepe:

(a) na zahtevo Odbora za umetno inteligenco zagotovi standardizirane predloge za področja, ki jih zajema ta uredba;

(b) razvija in vzdržuje enotno informacijsko platformo, na kateri so vsem operaterjem po vsej Uniji na voljo informacije v zvezi s to uredbo, ki so enostavne za uporabo;

(c) organizira ustrezne komunikacijske kampanje za ozaveščanje o obveznostih, ki izhajajo iz te uredbe;

(d) ocenjuje in spodbuja zbliževanja dobrih praks v postopkih javnega naročanja v zvezi z umetnointeligenčnimi sistemi.

Člen 55a

Odstopanja za določene operaterje

1. Obveznosti iz člena 17 te uredbe se ne uporabljajo za mikropodjetja, kot so opredeljena v členu 2(3) Priloge k Priporočilu Komisije 2003/361/ES o opredelitvi mikro, malih in srednjih podjetij, če ta podjetja nimajo partnerskih podjetij ali povezanih podjetij, kot so opredeljena v členu 3 iste priloge.

2. Odstavek 1 se ne razlaga tako, da bi bili ti operaterji oproščeni izpolnjevanja katerih koli drugih zahtev in obveznosti iz te uredbe, vključno s tistimi iz členov 9, 61 in 62.

3. Zahteve in obveznosti za umetnointeligenčne sisteme za splošne namene iz člena 4b se ne uporabljajo za mikro, mala in srednja podjetja, če ta podjetja nimajo partnerskih podjetij ali povezanih podjetij, kot so opredeljena v členu 3 Priloge k Priporočilu Komisije 2003/361/ES o opredelitvi mikro, malih in srednjih podjetij.

NASLOV VI

UPRAVLJANJE

POGLAVJE 1

EVROPSKI ODBOR ZA UMETNO INTELIGENCO

Člen 56

Ustanovitev in struktura Evropskega odbora za umetno inteligenco

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

2. Odbor sestavlja po en predstavnik vsake države članice. Evropski nadzornik za varstvo podatkov sodeluje kot opazovalec. Sestankov Odbora se udeležuje tudi Komisija brez udeležbe pri glasovanju.

   Odbor se lahko vsakič posebej odloči, da na sestanek povabi druge nacionalne organe, telesa ali strokovnjake in organe, telesa ali strokovnjake Unije, kadar so obravnavana vprašanja zanje pomembna.

2a. Države članice imenujejo svojega predstavnika za obdobje treh let z možnostjo enkratnega podaljšanja.

2aa. Države članice zagotovijo, da njihovi predstavniki v Odboru:

   (i) imajo v svoji državi članici ustrezne pristojnosti in pooblastila, da dejavno prispevajo k izpolnjevanju nalog Odbora iz člena 58;

   (ii) so določeni kot enotna kontaktna točka v odnosu do Odbora in, kjer je to ustrezno, ob upoštevanju potreb držav članic kot enotna kontaktna točka za deležnike;

(iii) so pooblaščeni za spodbujanje doslednosti in usklajevanja med pristojnimi nacionalnimi organi v svoji državi članici v zvezi z izvajanjem te uredbe, vključno z zbiranjem ustreznih podatkov in informacij za namene opravljanja njihovih nalog v Odboru.

3. Imenovani predstavniki držav članic z dvotretjinsko večino sprejmejo poslovnik Odbora.

V poslovniku so določeni zlasti potek izbirnega postopka, trajanje mandata in specifikacije nalog predsednika, načini glasovanja ter organizacija dejavnosti Odbora in njegovih podskupin.

Odbor ustanovi stalno podskupino, ki deluje kot platforma, prek katere lahko deležniki Odboru svetujejo o vseh vprašanjih, povezanih z izvajanjem te uredbe, vključno s pripravo izvedbenih in delegiranih aktov. V ta namen se k sodelovanju v tej podskupini povabijo organizacije, ki zastopajo interese ponudnikov in uporabnikov umetnointeligenčnih sistemov, vključno z MSP in zagonskimi podjetji, ter organizacije civilne družbe, predstavniki prizadetih oseb, raziskovalci, organizacije za standardizacijo, priglašeni organi, laboratoriji ter obrati za preskušanje in poskuse. Odbor ustanovi dve stalni podskupini, da bi zagotovili platformo za sodelovanje in izmenjavo med organi za nadzor trga in priglasitvenimi organi o vprašanjih, povezanih z nadzorom trga oziroma priglašenimi organi.

Odbor lahko po potrebi ustanovi druge stalne ali začasne podskupine za preučitev posebnih vprašanj. Kjer je to ustrezno, so lahko deležniki iz prejšnjega pododstavka povabljeni v take podskupine ali na posamezne sestanke navedenih podskupin v vlogi opazovalcev.

3a. Odbor je organiziran in se upravlja tako, da zagotavlja objektivnost in nepristranskost svojih dejavnosti.

4. Odboru predseduje eden od predstavnikov držav članic. Komisija na zahtevo predsednika skliče sestanke in pripravi dnevni red v skladu z nalogami Odbora na podlagi te uredbe in njegovega poslovnika. Komisija zagotavlja upravno in analitično podporo dejavnostim Odbora v skladu s to uredbo.

Člen 57

[črtano]

Člen 58

Naloge Odbora

Odbor svetuje in pomaga Komisiji in državam članicam, da se olajša dosledna in učinkovita uporaba te uredbe. V ta namen lahko Odbor zlasti:

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

(b) prispeva k harmonizaciji upravnih praks v državah članicah, tudi v zvezi z odstopanjem od postopkov ugotavljanja skladnosti iz člena 47, delovanjem regulativnih peskovnikov ter testiranjem v dejanskih razmerah iz členov 53, 54 in 54a;

(c) na zahtevo Komisije ali na lastno pobudo izda priporočila in pisna mnenja o vseh pomembnih zadevah v zvezi z izvajanjem te uredbe ter njeno dosledno in učinkovito uporabo, vključno:

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

(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;

(d) svetuje Komisiji o morebitni potrebi po spremembi Priloge III v skladu s členoma 4 in 7, pri čemer upošteva ustrezne razpoložljive dokaze in najnovejši tehnološki razvoj;

(e) svetuje Komisiji med pripravo delegiranega ali izvedbenega akta na podlagi te uredbe;

(f) po potrebi sodeluje z ustreznimi organi, strokovnimi skupinami in mrežami EU, zlasti na področju varnosti proizvodov, kibernetske varnosti, konkurence, digitalnih in medijskih storitev, finančnih storitev, kriptovalut, varstva potrošnikov ter varstva podatkov in temeljnih pravic;

(g) prispeva in zagotavlja ustrezno svetovanje Komisiji pri pripravi smernic iz člena 58a ali zahteva razvoj takih smernic;

(h) pomaga pri delu organov za nadzor trga ter v sodelovanju in po dogovoru z zadevnimi organi za nadzor trga spodbuja in podpira čezmejne preiskave nadzora trga, tudi v zvezi s pojavom sistemskih tveganj, ki lahko izhajajo iz umetnointeligenčnih sistemov;

(i) prispeva k oceni potreb po usposabljanju osebja držav članic, ki sodeluje pri izvajanju te uredbe;

(j) svetuje Komisiji v zvezi z mednarodnimi zadevami na področju umetne inteligence.

POGLAVJE 1A

SMERNICE KOMISIJE

Člen 58a

Smernice Komisije glede izvajanja te uredbe

1. Komisija na zahtevo držav članic ali Odbora ali na lastno pobudo izda smernice glede praktičnega izvajanja te uredbe, zlasti glede:

   (i) uporabe zahtev iz členov 8 do 15;

   (ii) prepovedanih praks iz člena 5;

   (iii) praktičnega izvajanja določb v zvezi z vsebinskimi spremembami;

   (iv) praktičnega izvajanja enotnih pogojev iz člena 6, odstavek 3, vključno s primeri v zvezi z umetnointeligenčnimi sistemi velikega tveganja iz Priloge III;

   (v) praktičnega izvajanja obveznosti glede preglednosti iz člena 52;

   (vi) razmerja med to uredbo in drugo ustrezno zakonodajo Unije, tudi kar zadeva skladnost njunega izvrševanja.

Komisija pri izdaji takih smernic posebno pozornost nameni potrebam MSP, vključno z zagonskimi podjetji, lokalnih javnih organov in sektorjev, ki jih bo ta uredba najverjetneje prizadela.

POGLAVJE 2

PRISTOJNI NACIONALNI ORGANI

Člen 59

Imenovanje pristojnih nacionalnih organov

1. [črtano]

2. Vsaka država članica ustanovi ali imenuje vsaj en priglasitveni organ in vsaj en organ za nadzor trga za namene te uredbe kot pristojne nacionalne organe. Ti pristojni nacionalni organi so organizirani tako, da zagotavljajo objektivnost in nepristranskost svojih dejavnosti in nalog. Če se ta načela spoštujejo, lahko take dejavnosti in naloge izvaja eden ali več imenovanih organov v skladu z organizacijskimi potrebami države članice.

3. Države članice obvestijo Komisijo o svojem imenovanju ali imenovanjih.

4. Države članice zagotovijo, da imajo pristojni nacionalni organi na voljo ustrezne finančne vire, tehnično opremo in dobro usposobljene človeške vire za učinkovito izpolnjevanje svojih nalog v skladu s to uredbo.

5. Države članice do *[eno leto po začetku veljavnosti te uredbe]* in nato šest mesecev pred rokom iz člena 84(2) Komisijo obvestijo o stanju finančnih virov, tehnične opreme in človeških virov pristojnih nacionalnih organov skupaj z oceno njihove ustreznosti. Komisija navedene informacije posreduje Odboru v razpravo in morebitna priporočila.

6. Komisija olajša izmenjavo izkušenj med pristojnimi nacionalnimi organi.

7. Pristojni nacionalni organi lahko svetujejo glede izvajanja te uredbe, tudi po meri za ponudnike, ki so MSP, vključno z zagonskimi podjetji. 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 na podlagi navedene zakonodaje 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 UMETNOINTELIGENČNE SISTEME VELIKEGA TVEGANJA S SEZNAMA V PRILOGI III

Člen 60

Podatkovna zbirka EU za umetnointeligenčne sisteme velikega tveganja s seznama v Prilogi III

1. Komisija v sodelovanju z državami članicami vzpostavi in vzdržuje podatkovno zbirko EU, ki vsebuje informacije iz odstavka 2 o zadevnih operaterjih in umetnointeligenčnih sistemih velikega tveganja s seznama v Prilogi III, registriranih v skladu s členoma 51 in 54a. Komisija se pri določanju funkcionalnih specifikacij take podatkovne zbirke posvetuje z Evropskim odborom za umetno inteligenco.

2. Podatke iz Priloge VIII, del I, v podatkovno zbirko EU, kakor je ustrezno, vnesejo ponudniki, pooblaščeni zastopniki in ustrezni uporabniki ob njihovi registraciji. Podatke iz Priloge VIII, del II, točke 1 do 11, v podatkovno zbirko EU vnesejo ponudniki ali, kjer je to ustrezno, pooblaščeni zastopnik v skladu s členom 51. Podatkovna zbirka samodejno ustvari podatke iz Priloge VIII, del II, točka 12, na podlagi informacij, ki jih zadevni uporabniki zagotovijo v skladu s členom 51(2). Podatke iz Priloge VIIIa v podatkovno zbirko vnesejo potencialni ponudniki ali ponudniki v skladu s členom 54a.

3. [črtano]

4. Podatkovna zbirka EU ne vsebuje osebnih podatkov, razen informacij iz Priloge VIII, in ne posega v člen 70.

5. Komisija je upravljavec podatkovne zbirke EU. Ponudnikom, potencialnim ponudnikom in uporabnikom zagotavlja ustrezno tehnično in upravno podporo.

5a. Informacije v podatkovni zbirki EU, registrirane v skladu s členom 51, so dostopne javnosti. Informacije, registrirane v skladu s členom 54a, so dostopne samo organom za nadzor trga in Komisiji, razen če je potencialni ponudnik ali ponudnik dal soglasje, da so te informacije dostopne tudi javnosti.

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 s tveganji umetnointeligenčnega sistema velikega tveganja.

2. Da se ponudniku omogoči, da oceni skladnost umetnointeligenčnih sistemov z zahtevami iz naslova III, poglavje 2, v njihovem celotnem življenjskem ciklu, se v sistemu spremljanja po dajanju na trg zbirajo, dokumentirajo in analizirajo ustrezni podatki o delovanju umetnointeligenčnih sistemov velikega tveganja, ki jih lahko zagotovijo uporabniki ali se lahko zbirajo iz drugih virov. Ta obveznost ne zajema občutljivih operativnih podatkov uporabnikov umetnointeligenčnih sistemov, ki so organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj.

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 predlogi za načrt spremljanja po dajanju na trg in seznam elementov, ki jih je treba vključiti v načrt.

4. Kadar sta sistem in načrt spremljanja po dajanju na trg že vzpostavljena na podlagi navedene zakonodaje, se za umetnointeligenčne sisteme velikega tveganja, ki jih zajemajo pravni akti iz Priloge II, oddelek A, dokumentacija za spremljanje po dajanju na trg, kot je pripravljena na podlagi navedene zakonodaje, šteje za zadostno, pod pogojem, da se uporabi predloga iz odstavka 3.

Prvi pododstavek se uporablja tudi za umetnointeligenčne sisteme velikega tveganja iz točke 5 Priloge III, ki jih dajo na trg ali v uporabo finančne institucije, za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki na podlagi zakonodaje Unije o finančnih storitvah.

POGLAVJE 2

IZMENJAVA INFORMACIJ O HUDIH INCIDENTIH

Člen 62

Poročanje o hudih incidentih

1. Ponudniki umetnointeligenčnih sistemov velikega tveganja, ki so dani na trg Unije, sporočijo vsak hud incident organom za nadzor trga držav članic, v katerih je prišlo do navedenega incidenta.

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

2. Zadevni organ za nadzor trga po prejemu uradnega obvestila o hudem incidentu iz člena 3(44)(c) obvesti nacionalne javne organe ali telesa iz člena 64(3). Komisija pripravi posebne smernice za lažje izpolnjevanje obveznosti iz odstavka 1. Navedene smernice se izdajo najpozneje 12 mesecev po začetku veljavnosti te uredbe.

3. Za umetnointeligenčne sisteme velikega tveganja iz točke 5 Priloge III, ki jih dajo na trg ali v uporabo ponudniki, ki so finančne institucije, za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki na podlagi zakonodaje Unije o finančnih storitvah, je priglasitev resnih incidentov omejena na tiste iz člena 3(44)(c).

4. 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 priglasitev hudih incidentov omejena na tiste iz člena 3(44)(c) in se pošlje pristojnemu nacionalnemu organu, ki ga v ta namen izberejo države članice, v katerih se je navedeni incident zgodil.

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 na podlagi Uredbe (EU) 2019/1020 se razume kot sklicevanje na vse operaterje, opredeljene v členu 2 te uredbe;

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

2. Organi za nadzor trga v okviru svojih obveznosti poročanja iz člena 34(4) Uredbe (EU) 2019/1020 Komisiji poročajo o rezultatih zadevnih dejavnosti nadzora trga na podlagi te uredbe.

3. Za umetnointeligenčne sisteme velikega tveganja, povezane s proizvodi, za katere se uporabljajo pravni akti iz Priloge II, oddelek A, je organ za nadzor trga za namene te uredbe organ, odgovoren za dejavnosti nadzora trga, določene v navedenih pravnih aktih, ali, v utemeljenih okoliščinah in pod pogojem, da je zagotovljeno usklajevanje, drug zadevni organ, ki ga opredeli država članica.

   Postopki iz členov 65, 66, 67 in 68 te uredbe se ne uporabljajo za umetnointeligenčne sisteme, povezane s proizvodi, za katere se uporabljajo pravni akti iz Priloge II, oddelek A, če taki pravni akti že določajo postopke z istim ciljem. V takem primeru se namesto tega uporabijo ti sektorski postopki.

4. Za umetnointeligenčne sisteme velikega tveganja, ki so dani na trg ali v uporabo ali jih uporabljajo finančne institucije, ki jih ureja zakonodaja Unije o finančnih storitvah, je organ za nadzor trga za namene te uredbe zadevni nacionalni organ, odgovoren za finančni nadzor navedenih institucij v skladu z navedeno zakonodajo, če je dajanje umetnointeligenčnega sistema na trg ali v uporabo ali uporaba umetnointeligenčnega sistema neposredno povezana z zagotavljanjem navedenih finančnih storitev.

   Z odstopanjem od prejšnjega pododstavka lahko država članica v utemeljenih okoliščinah in pod pogojem, da je zagotovljeno usklajevanje, za organ za nadzor trga za namene te uredbe določi drug zadevni organ.

   Nacionalni organi za nadzor trga, ki nadzorujejo regulirane kreditne institucije, regulirane v skladu z Direktivo 2013/36/EU, ki sodelujejo v enotnem mehanizmu nadzora (EMN), vzpostavljenem z Uredbo Sveta št. 1204/2013, bi morali Evropski centralni banki brez odlašanja sporočiti vse informacije, ugotovljene pri njihovih dejavnostih nadzora trga, ki bi lahko bile zanimive za naloge bonitetnega nadzora Evropske centralne banke, kot so določene v navedeni uredbi.

5. Za umetnointeligenčne sisteme velikega tveganja iz točke 1(a), če se sistemi uporabljajo za namene kazenskega pregona, točke 6, 7 in 8 Priloge III, države članice kot organe za nadzor trga za namene te uredbe imenujejo bodisi nacionalne organe, ki nadzirajo dejavnosti organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organov za nadzor meje, organov, pristojnih za priseljevanje, azilnih ali pravosodnih organov, bodisi pristojne nadzorne organe za varstvo podatkov na podlagi Direktive (EU) 2016/680 ali Uredbe (EU) 2016/679. Dejavnosti nadzora trga nikakor ne vplivajo na neodvisnost pravosodnih organov ali kako drugače posegajo v njihove dejavnosti, kadar delujejo v okviru svoje sodne pristojnosti.

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.

8. Brez poseganja v pooblastila na podlagi Uredbe (EU) 2019/1020 ter kadar je to ustrezno in omejeno na to, kar je potrebno za izpolnjevanje njihovih nalog, ponudnik organom za nadzor trga omogoči polni dostop do dokumentacije ter naborov podatkov za usposabljanje, potrjevanje in testiranje, ki se uporabljajo za razvoj umetnointeligenčnega sistema velikega tveganja, vključno z vmesniki za aplikacijsko programiranje (API) ali drugimi ustreznimi tehničnimi sredstvi in orodji, ki omogočajo oddaljeni dostop, kjer je to ustrezno in ob upoštevanju varnostnih zaščitnih ukrepov.

9. Organom za nadzor trga se dostop do izvorne kode umetnointeligenčnega sistema velikega tveganja odobri na podlagi utemeljene zahteve in samo, če sta izpolnjena naslednja kumulativna pogoja:

(a) dostop do izvorne kode je potreben za oceno skladnosti umetnointeligenčnega sistema velikega tveganja z zahtevami iz naslova III, poglavje 2, ter

(b) postopki preskušanja/revizije in preverjanja na podlagi podatkov in dokumentacije, ki jih je zagotovil ponudnik, so bili izčrpani ali so se izkazali za nezadostne.

10. Vse informacije in dokumentacija, ki jih pridobijo organi za nadzor trga, se obravnavajo v skladu z obveznostmi glede zaupnosti iz člena 70.

11. Pritožbe pri ustreznem organu za nadzor trga lahko vloži vsaka fizična ali pravna oseba, ki utemeljeno meni, da je prišlo do kršitve določb te uredbe.

V skladu s členom 11(3)(e) in (7)(a) Uredbe (EU) 2019/1020 se pritožbe upoštevajo za namene izvajanja dejavnosti nadzora trga in se obravnavajo v skladu z namenskimi postopki, ki jih zato vzpostavijo organi za nadzor trga.

Člen 63a

Nadzor testiranja v dejanskih razmerah s strani organov za nadzor trga

1. Organi za nadzor trga so pristojni in pooblaščeni za zagotavljanje, da je testiranje v dejanskih razmerah skladno s to uredbo.

2. Kadar se testiranje v dejanskih razmerah izvaja za umetnointeligenčne sisteme, ki se nadzorujejo v regulativnem peskovniku za umetno inteligenco v skladu s členom 54, organi za nadzor trga preverijo skladnost z določbami člena 54a v okviru svoje nadzorne vloge za regulativni peskovnik za umetno inteligenco. Navedeni organi lahko po potrebi dovolijo, da ponudnik ali potencialni ponudnik opravi testiranje v dejanskih razmerah z odstopanjem od pogojev iz člena 54a(4)(f) in (g).

3. Kadar potencialni ponudnik, ponudnik ali katera koli tretja oseba obvesti organ za nadzor trga o hudem incidentu ali ima druge razloge za domnevo, da pogoji iz členov 54a in 54b niso izpolnjeni, lahko na svojem ozemlju po potrebi sprejme katero koli od naslednjih odločitev:

(a) začasno prekine ali konča testiranje v dejanskih razmerah;

(b) od ponudnika ali potencialnega ponudnika in uporabnika ali uporabnikov zahteva, da spremenijo kateri koli vidik testiranja v dejanskih razmerah.

4. Kadar organ za nadzor trga sprejme odločitev iz odstavka 3 tega člena ali izda ugovor v smislu člena 54a(4)(b), se v odločitvi ali ugovoru navedejo razlogi zanj ali zanjo ter načini in pogoji, pod katerimi lahko ponudnik ali potencialni ponudnik izpodbija odločitev ali ugovor.

5. Kjer je to ustrezno, kadar organ za nadzor trga sprejme odločitev iz odstavka 3 tega člena, razloge za to sporoči organom za nadzor trga drugih držav članic, v katerih je bil umetnointeligenčni sistem testiran v skladu z načrtom testiranja.

Člen 64

Pooblastila organov, ki varujejo temeljne pravice

1. [črtano]

2. [črtano]

3. Nacionalni javni organi ali telesa, ki nadzorujejo ali uveljavljajo spoštovanje obveznosti na podlagi prava Unije o varstvu temeljnih pravic, vključno s pravico do nediskriminacije, v zvezi z uporabo umetnointeligenčnih sistemov velikega tveganja iz Priloge III, so pooblaščeni, da zahtevajo kakršno koli dokumentacijo, ustvarjeno ali hranjeno na podlagi te uredbe, in dostopajo do nje, kadar je dostop do navedene dokumentacije potreben za izvrševanje pristojnosti v okviru njihovih pooblastil v mejah njihove pristojnosti. Zadevni javni organ ali telo 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 ali telesa iz odstavka 3 in objavi seznam. 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 na podlagi prava Unije, namenjene zaščiti temeljnih pravic, lahko javni organ ali telo 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 ali telesa, 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 členu 3, točka 19, Uredbe (EU) 2019/1020, kar zadeva tveganja za zdravje ali varnost ali temeljne pravice 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. Če so opredeljena tveganja za temeljne pravice, 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 nepotrebnega odlašanja zahteva, da sprejme vse ustrezne popravne ukrepe, da zagotovi skladnost umetnointeligenčnega sistema, ga umakne s trga ali prekliče v roku, ki ga lahko določi.

   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 brez nepotrebnega odlašanja 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 nepotrebnega odlašanja uradno obvesti Komisijo in druge države članice.

6. Uradne informacije iz odstavka 5 vsebujejo vse razpoložljive podrobnosti, zlasti informacije, 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) neskladnosti s prepovedjo praks umetne inteligence iz člena 5;

(a) neizpolnjevanja zahtev iz naslova III, poglavje 2, s strani umetnointeligenčnega sistema velikega tveganja;

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

(c) neskladnosti z določbami iz člena 52;

(d) neskladnosti umetnointeligenčnih sistemov za splošne namene z zahtevami in obveznostmi iz člena 4a.

7. Organi za nadzor trga držav članic, ki niso organi za nadzor trga države članice, ki je začela postopek, brez nepotrebnega 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 uradnega obvestila iz odstavka 5 ne poda ugovora glede začasnega ukrepa, ki ga je sprejela država članica, se šteje, da je navedeni ukrep upravičen. To ne posega v postopkovne pravice zadevnega operaterja v skladu s členom 18 Uredbe (EU) 2019/1020. Obdobje iz prvega stavka tega odstavka se skrajša na 30 dni v primeru neskladnosti s prepovedjo praks umetne inteligence iz člena 5.

9. Organi za nadzor trga vseh držav članic nato zagotovijo sprejetje ustreznih omejevalnih ukrepov v zvezi z zadevnim umetnointeligenčnim sistemom, kot je umik proizvoda s trga, brez nepotrebnega odlašanja.

Člen 66

Zaščitni postopek Unije

1. Kadar država članica v treh mesecih od prejema priglasitve iz člena 65(5) ali v 30 dneh v primeru neskladnosti s prepovedjo praks umetne inteligence iz člena 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 nepotrebnega odlašanja posvetuje z organom za nadzor trga zadevne države članice in operaterjem ali operaterji ter oceni nacionalni ukrep. Komisija na podlagi rezultatov navedene ocene odloči, ali je nacionalni ukrep upravičen ali ne, v devetih mesecih, ali v 60 dneh v primeru neskladnosti s prepovedjo praks umetne inteligence iz člena 5, od uradnega obvestila iz člena 65(5). O tej odločitvi uradno obvesti zadevno državo članico. Komisija o taki odločitvi obvesti tudi druge države članice.

2. Če Komisija meni, da je ukrep, ki ga je sprejel organ za nadzor trga zadevne države članice, upravičen, organi za nadzor trga vseh držav članic zagotovijo, da se v zvezi z zadevnim umetnointeligenčnim sistemom sprejmejo ustrezni omejevalni ukrepi, kot je umik umetnointeligenčnega sistema z njihovega trga brez nepotrebnega odlašanja, in o tem ustrezno obvestijo Komisijo. Če Komisija meni, da nacionalni ukrep ni upravičen, organ za nadzor trga zadevne države članice ukrep prekliče in o tem obvesti Komisijo.

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 velikega tveganja ali za splošne namene, ki predstavljajo tveganje

1. Kadar organ za nadzor trga države članice po opravljeni oceni iz člena 65 ugotovi, da je umetnointeligenčni sistem velikega tveganja ali za splošne namene sicer v skladu s to direktivo, vendar predstavlja tveganje za zdravje ali varnost oseb ali za temeljne pravice, 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 brez nepotrebnega odlašanja v roku, ki ga lahko predpiše.

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. Navedene informacije vključujejo vse razpoložljive podrobnosti, zlasti podatke, potrebne za identifikacijo zadevnega umetnointeligenčnega sistema, poreklo in dobavno verigo umetnointeligenčnega sistema, naravo zadevnega tveganja ter naravo in trajanje sprejetih nacionalnih ukrepov.

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

5. Komisija svojo odločitev naslovi na zadevno državo članico in obvesti vse druge 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 v roku, ki ga lahko predpiše:

   (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 priglašenega organa, ki je vključen v postopek ugotavljanja skladnosti, kjer je to ustrezno, 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.

Člen 68a

Preizkuševalne zmogljivosti Unije na področju umetne inteligence

1. Komisija imenuje eno ali več preizkuševalnih zmogljivosti Unije v skladu s členom 21 Uredbe (EU) 2019/1020 na področju umetne inteligence.

2. Brez poseganja v dejavnosti preizkuševalnih zmogljivosti Unije iz člena 21(6) Uredbe (EU) 2019/1020 preizkuševalne zmogljivosti Unije iz odstavka 1 na zahtevo odbora ali organov za nadzor trga zagotavljajo tudi neodvisno tehnično ali znanstveno svetovanje.

Člen 68b

Osrednja skupina neodvisnih strokovnjakov

1. Komisija na zahtevo Odbora za umetno inteligenco z izvedbenim aktom sprejme določbe o vzpostavitvi, vzdrževanju in financiranju osrednje skupine neodvisnih strokovnjakov za podporo dejavnostim izvrševanja na podlagi te uredbe.

2. Strokovnjake izbere Komisija in jih vključi v osrednjo skupino na podlagi najnovejšega znanstvenega ali tehničnega strokovnega znanja na področju umetne inteligence, pri čemer ustrezno upošteva tehnična področja, ki jih zajemajo zahteve in obveznosti iz te uredbe, ter dejavnosti organov za nadzor trga v skladu s členom 11 Uredbe (EU) 2019/1020. Komisija opredeli število strokovnjakov v skupini v skladu s potrebami.

3. Strokovnjaki imajo lahko naslednje naloge:

(a) svetujejo in podpirajo delo organov za nadzor trga na njihovo zahtevo;

(b) podpirajo čezmejne preiskave nadzora trga iz člena 58(h), brez poseganja v pooblastila organov za nadzor trga;

(c) svetujejo Komisiji in jo podpirajo pri opravljanju njenih nalog v okviru zaščitne klavzule v skladu s členom 66.

4. Strokovnjaki svoje naloge opravljajo nepristransko in objektivno ter zagotavljajo zaupnost informacij in podatkov, pridobljenih pri izvajanju njihovih nalog in dejavnosti. Vsak strokovnjak predloži izjavo o interesih, ki je javno dostopna. Komisija vzpostavi sisteme in postopke za aktivno obvladovanje in preprečevanje morebitnih nasprotij interesov.

5. Od držav članic se lahko zahteva, da plačajo pristojbine za svetovanje in podporo strokovnjakov. Strukturo in višino pristojbin ter višino in strukturo povračljivih stroškov sprejme Komisija z izvedbenim aktom iz odstavka 1, pri čemer upošteva cilje ustreznega izvajanja te uredbe, stroškovno učinkovitost in potrebo, da se vsem državam članicam zagotovi učinkovit dostop do strokovnjakov.

6. Komisija državam članicam po potrebi omogoči pravočasen dostop do strokovnjakov in zagotovi, da je kombinacija podpornih dejavnosti, ki jih izvajajo preizkuševalne zmogljivosti Unije v skladu s členom 68a, in strokovnjakov v skladu s tem členom, učinkovito organizirana in zagotavlja največjo možno dodano vrednost.

NASLOV IX

KODEKSI RAVNANJA

Člen 69

Kodeksi ravnanja za prostovoljno uporabo posebnih zahtev

1. Komisija in države članice v največji možni meri olajšujejo pripravo kodeksov ravnanja, namenjenih spodbujanju prostovoljne uporabe ene ali več zahtev iz naslova III, poglavje 2, te uredbe za umetnointeligenčne sisteme, ki niso umetnointeligenčni sistemi velikega tveganja, ob tem pa upoštevajo razpoložljive, tehnične rešitve, ki omogočajo uporabo takšnih zahtev.

2. Komisija in države članice olajšujejo pripravo kodeksov ravnanja, namenjenih spodbujanju prostovoljne uporabe posebnih zahtev za vse umetnointeligenčne sisteme, povezanih na primer z okoljsko trajnostjo, tudi glede načrtovanja energetske učinkovitosti, z dostopnostjo za invalide, sodelovanjem deležnikov pri zasnovi in razvoju umetnointeligenčnih sistemov ter z raznolikostjo razvojnih skupin na podlagi jasnih ciljev in ključnih kazalnikov uspešnosti za merjenje doseganja teh ciljev. Komisija in države članice po potrebi olajšujejo tudi pripravo prostovoljnih kodeksov ravnanja glede obveznosti uporabnikov v zvezi z umetnointeligenčnimi sistemi.

3. Kodekse ravnanja, ki se uporabljajo prostovoljno, lahko pripravijo posamezni ponudniki umetnointeligenčnih sistemov ali organizacije, ki jih zastopajo, ali oboji, tudi z vključevanjem uporabnikov in vseh deležnikov ter njihovih predstavniških organizacij, ali po potrebi uporabniki v zvezi s svojimi obveznostmi. Kodeksi ravnanja lahko zajemajo enega ali več umetnointeligenčnih sistemov ob upoštevanju podobnosti predvidenega namena zadevnih sistemov.

4. Komisija in države članice pri spodbujanju in olajševanju priprave kodeksov ravnanja iz tega člena upoštevajo posebne interese in potrebe ponudnikov, ki so MSP, vključno z zagonskimi podjetji.

NASLOV X

ZAUPNOST IN KAZNI

Člen 70

Zaupnost

1. Pristojni nacionalni organi, priglašeni organi, Komisija, odbor in druge fizične ali pravne osebe, vključene v uporabo te uredbe, v skladu s pravom Unije ali nacionalnim pravom vzpostavijo ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovijo 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) javni interes in interes nacionalne varnosti;

(d) celovitost kazenskih ali upravnih postopkov;

(e) celovitost informacij, ki veljajo za tajne v skladu s pravom Unije ali nacionalnim pravom.

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 za nadzor meje, organi, pristojni za priseljevanje, ali organi za presojo prošenj za azil, kadar bi tako razkritje ogrozilo javne in nacionalne varnostne interese. Ta obveznost izmenjave informacij ne zajema občutljivih operativnih podatkov v zvezi z dejavnostmi organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organov za nadzor meje in organov, pristojnih za priseljevanje, ali organov za azil.

Kadar so organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organi, pristojni za priseljevanje, ali organi 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 na pravice in obveznosti Komisije, držav članic, zadevnih organov in priglašenih organov v zvezi z izmenjavo informacij in razširjanjem opozoril, tudi v okviru čezmejnega sodelovanja, niti na obveznosti zadevnih strani, da zagotovijo informacije na podlagi kazenskega prava držav članic.

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 velikost in interese ponudnikov, ki so MSP, vključno z zagonskimi podjetji, ter njihovo ekonomsko sposobnost. Upoštevajo tudi, ali se umetnointeligenčni sistem uporablja v okviru osebne nepoklicne dejavnosti.

2. Države članice Komisijo nemudoma uradno obvestijo o navedenih pravilih in ukrepih ter o morebitnih poznejših spremembah, ki vplivajo nanje.

3. Neupoštevanje katere od prepovedi praks umetne inteligence iz člena 5 se kaznuje z upravnimi globami 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. V primeru MSP, vključno z zagonskimi podjetji, te globe znašajo do 3 % njihovega svetovnega letnega prometa za preteklo proračunsko leto.

4. Kršitve naslednjih določb, ki se nanašajo na operaterje in priglašene organe, se kaznujejo 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:

(–a) obveznosti ponudnikov na podlagi členov 4b in 4c;

(a) obveznosti ponudnikov na podlagi člena 16;

(b) obveznosti za nekatere druge osebe na podlagi člena 23a;

(c) obveznosti pooblaščenih zastopnikov na podlagi člena 25;

(d) obveznosti uvoznikov na podlagi člena 26;

(e) obveznosti distributerjev na podlagi člena 27;

(f) obveznosti uporabnikov na podlagi člena 29, odstavki 1 do 6a;

(g) zahteve in obveznosti priglašenih organov na podlagi člena 33, člena 34(1), 34(3) in 34(4) ter člena 34a;

(h) obveznosti ponudnikov in uporabnikov glede preglednosti na podlagi člena 52.

V primeru MSP, vključno z zagonskimi podjetji, te globe znašajo do 2 % njihovega svetovnega letnega prometa za preteklo proračunsko leto.

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. V primeru MSP, vključno z zagonskimi podjetji, te globe znašajo do 1 % njihovega svetovnega letnega prometa za preteklo proračunsko leto.

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;

(aa) ali je kršitev naklepna ali posledica malomarnosti;

(ab) vsak ukrep operaterja za odpravo kršitve in blažitev morebitnih škodljivih učinkov kršitve;

(b) ali so drugi organi za nadzor trga v ostalih državah članicah že naložili upravne globe istemu operaterju za isto kršitev;

(ba) ali so drugi organi istemu operaterju že naložili upravne globe za kršitve ostale zakonodaje Unije ali nacionalne zakonodaje, kadar so take kršitve posledica iste dejavnosti ali opustitve dejanja, ki pomeni zadevno kršitev tega akta;

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

(d) morebitni drugi oteževalni ali olajševalni dejavniki v zvezi z okoliščinami primera, kot so pridobljene finančne koristi ali preprečene izgube, ki neposredno ali posredno izhajajo iz kršitve.

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.

9. Organ za nadzor trga izvaja pooblastila iz tega člena na podlagi ustreznih postopkovnih zaščitnih ukrepov v skladu s pravom Unije in pravom države članice, vključno z učinkovitim pravnim sredstvom in ustreznim pravnim postopkom.

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. Neupoštevanje katere od prepovedi praks umetne inteligence iz člena 5 se kaznuje z upravnimi globami v višini do 500 000 EUR.

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 je preneseno na Komisijo pod pogoji, določenimi v tem členu.

2. Pooblastilo iz členov 7(1), 7(3), 11(3), 43(5) in (6) ter 48(5) se prenese na Komisijo za obdobje pet let od [*datuma začetka veljavnosti te uredbe*].

   Komisija pripravi poročilo o prenosu pooblastila najpozneje devet mesecev pred koncem petletnega obdobja. Prenos pooblastila se samodejno podaljšuje za enako dolga obdobja, razen če Evropski parlament ali Svet nasprotuje temu podaljšanju najpozneje tri mesece pred koncem vsakega obdobja.

3. Pooblastilo iz členov 7(1), 7(3), 11(3), 43(5) in (6) ter 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. Sklep 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. Delegirani akt, sprejet na podlagi členov 7(1), 7(3), 11(3), 43(5) in (6) ter 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 pred iztekom tega roka tako Evropski parlament kot Svet obvestita 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

Spremembe Uredbe (EU) št. 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

Spremembe Uredbe (EU) št. 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

Spremembe Uredbe (EU) št. 2019/2144

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

„3. Pri sprejemanju delegiranih 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. [črtano]

1b. Komisija vsakih 24 mesecev po začetku veljavnosti te uredbe in do konca trajanja prenosa pooblastila oceni potrebo po spremembi seznama iz Priloge III. Ugotovitve te ocene se predstavijo Evropskemu parlamentu in Svetu.

2. Komisija [*v treh letih po datumu začetka 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 sredstev, tehnične opreme 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 datumu začetka uporabe te uredbe iz člena 85(2)*] ter nato po potrebi vsaka štiri leta oceni vpliv in učinkovitost prostovoljnih kodeksov ravnanja za spodbujanje uporabe zahtev iz naslova III, poglavje 2, za umetnointeligenčne sisteme, ki niso umetnointeligenčni sistemi velikega tveganja, in morebitnih drugih dodatnih zahtev za umetnointeligenčne sisteme, tudi glede okoljske trajnostnosti.

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

6. Komisija pri izvajanju ocenjevanj in pregledov iz odstavkov 1a do 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 [36 mesecev po začetku veljavnosti te uredbe].

3. Z odstopanjem od odstavka 2:

   (a) naslov III, poglavje 4, in naslov VI se začneta uporabljati [12 mesecev 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*
predsednica	*predsednik/predsednica*

PRILOGA I

(črtano)

PRILOGA II

SEZNAM HARMONIZACIJSKE ZAKONODAJE UNIJE

Oddelek A – Seznam harmonizacijske zakonodaje Unije na podlagi novega zakonodajnega okvira

1. Direktiva 2006/42/ES Evropskega parlamenta in Sveta z dne 17. maja 2006 o strojih in spremembah Direktive 95/16/ES (UL L 157, 9.6.2006, str. 24) [kakor je bila razveljavljena z uredbo o strojih];

2. Direktiva 2009/48/ES Evropskega parlamenta in Sveta z dne 18. junija 2009 o varnosti igrač (UL L 170, 30.6.2009, str. 1);

3. Direktiva 2013/53/EU Evropskega parlamenta in Sveta z dne 20. novembra 2013 o plovilih za rekreacijo in osebnih plovilih ter razveljavitvi Direktive 94/25/ES (UL L 354, 28.12.2013, str. 90);

4. Direktiva 2014/33/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o harmonizaciji zakonodaje držav članic v zvezi z dvigali in varnostnimi komponentami za dvigala (UL L 96, 29.3.2014, str. 251);

5. Direktiva 2014/34/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o harmonizaciji zakonodaj držav članic v zvezi z opremo in zaščitnimi sistemi, namenjenimi za uporabo v potencialno eksplozivnih atmosferah (UL L 96, 29.3.2014, str. 309);

6. Direktiva 2014/53/EU Evropskega parlamenta in Sveta z dne 16. aprila 2014 o harmonizaciji zakonodaj držav članic v zvezi z dostopnostjo radijske opreme na trgu in razveljavitvi Direktive 1999/5/ES (UL L 153, 22.5.2014, str. 62);

7. Direktiva 2014/68/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o harmonizaciji zakonodaje držav članic v zvezi z omogočanjem dostopnosti tlačne opreme na trgu (UL L 189, 27.6.2014, str. 164);

8. Uredba (EU) 2016/424 Evropskega parlamenta in Sveta z dne 9. marca 2016 o žičniških napravah in razveljavitvi Direktive 2000/9/ES (UL L 81, 31.3.2016, str. 1);

9. Uredba (EU) 2016/425 Evropskega parlamenta in Sveta z dne 9. marca 2016 o osebni varovalni opremi in razveljavitvi Direktive Sveta 89/686/EGS (UL L 81, 31.3.2016, str. 51);

10. Uredba (EU) 2016/426 Evropskega parlamenta in Sveta z dne 9. marca 2016 o napravah, v katerih zgoreva plinasto gorivo, in razveljavitvi Direktive 2009/142/ES (UL L 81, 31.3.2016, str. 99);

11. 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);

12. 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).

Oddelek B. Seznam druge harmonizacijske zakonodaje Unije

1. 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);

2. 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);

3. 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);

4. 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);

5. 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).

6. 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);

7. 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);

8. 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), kolikor gre za oblikovanje, proizvodnjo in dajanje na trg zrakoplovov iz točk (a) in (b) člena 2(1) navedene uredbe v zvezi z brezpilotnimi zrakoplovi in njihovimi motorji, propelerji, deli in opremo za njihovo daljinsko upravljanje.

PRILOGA III

UMETNOINTELIGENČNI SISTEMI VELIKEGA TVEGANJA IZ ČLENA 6(3)

Na vsakem področju iz točk 1–8 se umetnointeligenčni sistemi, izrecno navedeni pod vsako črko, štejejo za umetnointeligenčne sisteme velikega tveganja na podlagi člena 6(3):

1. biometrija:

   (a) sistemi za biometrično identifikacijo na daljavo;

2. kritična infrastruktura:

   (a) umetnointeligenčni sistemi, namenjeni za uporabo kot varnostne komponente pri upravljanju in delovanju kritične digitalne infrastrukture, cestnega prometa ter oskrbe z vodo, plinom, ogrevanjem in električno energijo;

3. izobraževanje in poklicno usposabljanje:

   (b) umetnointeligenčni sistemi, namenjeni določanju dostopa do zavodov ali programov za izobraževanje in poklicno usposabljanje na vseh ravneh, sprejema fizičnih oseb v te zavode ali programe oziroma dodeljevanja fizičnih oseb tem zavodom ali programom;

   (c) umetnointeligenčni sistemi, namenjeni evalvaciji učnih izidov, tudi kadar se ti izidi uporabljajo za usmerjanje učnega procesa fizičnih oseb v zavodih ali programih za izobraževanje in poklicno usposabljanje na vseh ravneh;

4. zaposlovanje, upravljanje delavcev in dostop do samozaposlitve:

   (d) umetnointeligenčni sistemi, namenjeni zaposlovanju ali izbiri fizičnih oseb, zlasti za ciljno oglaševanje delovnih mest, analizo in filtriranje prijav za zaposlitev ter ocenjevanje kandidatov;

(e) umetnointeligenčni sistemi, namenjeni odločanju o napredovanju in prenehanju z delom povezanih pogodbenih razmerij, dodeljevanju nalog na podlagi vedenja posameznika oziroma osebnostnih lastnosti ali značilnosti ter spremljanju in ocenjevanju uspešnosti in vedenja oseb v takih razmerjih;

5. uživanje bistvenih zasebnih in javnih storitev in ugodnosti ter dostop do njih:

(f) umetnointeligenčni sistemi, ki naj bi jih uporabljali javni organi ali naj bi se uporabljali v njihovem imenu za ocenjevanje upravičenosti fizičnih oseb do bistvenih ugodnosti in storitev javne pomoči ter za dodelitev, zmanjšanje, preklic ali povračilo takih ugodnosti in storitev;

(g) umetnointeligenčni sistemi, namenjeni ocenjevanju kreditne sposobnosti fizičnih oseb ali določanju njihove kreditne ocene, razen umetnointeligenčnih sistemov, ki jih za lastne potrebe uporabljajo ponudniki, ki so mikro ali malo podjetje, kakor je opredeljeno v Prilogi k Priporočilu Komisije 2003/361/ES;

(h) umetnointeligenčni sistemi, namenjeni uporabi za napotitev služb za ukrepanje ob nesrečah, vključno z gasilci in medicinsko pomočjo, ali določanje prednosti pri njihovi napotitvi;

(i) umetnointeligenčni sistemi, namenjeni za oceno tveganja in določanje cen v zvezi s fizičnimi osebami v primeru življenjskega in zdravstvenega zavarovanja, razen umetnointeligenčnih sistemov, ki jih za lastne potrebe uporabljajo ponudniki, ki so mikro ali malo podjetje, kakor je opredeljeno v Prilogi k Priporočilu Komisije 2003/361/ES;

6. preprečevanje, odkrivanje in preiskovanje kaznivih dejanj:

(j) umetnointeligenčni sistemi, ki naj bi jih organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali kdo drug v njihovem imenu uporabljal za oceno tveganja, ali bi fizična oseba storila ali ponovila kaznivo dejanje, ali tveganja, ali bi bila fizična oseba potencialna žrtev kaznivih dejanj;

(k) umetnointeligenčni sistemi, ki naj bi jih organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali kdo drug v njihovem imenu uporabljal kot poligrafe in podobna orodja ali za ugotavljanje čustvenega stanja fizične osebe;

(l) [črtano]

(m) umetnointeligenčni sistemi, ki naj bi jih organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali kdo drug v njihovem imenu uporabljal za oceno zanesljivosti dokazov med preiskavo ali pregonom kaznivih dejanj;

(n) umetnointeligenčni sistemi, ki naj bi jih organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali kdo drug v njihovem imenu uporabljal za napovedovanje storitve ali ponovitve dejanskega ali potencialnega kaznivega dejanja na podlagi oblikovanja profilov fizičnih oseb iz člena 3(4) Direktive (EU) 2016/680 ali oceno osebnostnih lastnosti in značilnosti ali preteklega kaznivega ravnanja fizičnih oseb ali skupin;

(o) umetnointeligenčni sistemi, ki naj bi jih organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali kdo drug v njihovem imenu med odkrivanjem, preiskovanjem ali pregonom kaznivih dejanj uporabljal za oblikovanje profilov fizičnih oseb iz člena 3(4) Direktive (EU) 2016/680;

(p) [črtano]

7. upravljanje migracij, azila in nadzora meje:

(q) umetnointeligenčni sistemi, ki naj bi jih pristojni javni organi ali kdo drug v njihovem imenu uporabljal kot poligrafe in podobna orodja ali za ugotavljanje čustvenega stanja fizične osebe;

(r) umetnointeligenčni sistemi, ki naj bi jih pristojni javni organi ali kdo drug v njihovem imenu uporabljal za oceno tveganja, vključno z varnostnim tveganjem, tveganjem nedovoljenih migracij ali zdravstvenim tveganjem, ki ga predstavlja fizična oseba, ki namerava vstopiti ali je vstopila na ozemlje države članice;

(s) [črtano]

(t) umetnointeligenčni sistemi, ki naj bi jih pristojni javni organi ali kdo drug v njihovem imenu uporabljal za preučevanje prošenj za azil, vizume in dovoljenja za prebivanje ter s tem povezanih pritožb glede upravičenosti fizičnih oseb, ki zaprosijo za status;

8. pravosodje in demokratični procesi:

(u) umetnointeligenčni sistemi, ki naj bi jih pravosodni organ ali kdo drug v njihovem imenu uporabljal za razlago dejstev ali prava ter za apliciranje prava na konkreten sklop dejstev.

PRILOGA IV

TEHNIČNA DOKUMENTACIJA iz člena 11(1)

Tehnična dokumentacija iz člena 11(1) vsebuje vsaj naslednje informacije, kot velja za zadevni umetnointeligenčni sistem:

1. splošen opis umetnointeligenčnega sistema, vključno z:

   (v) njegovim predvidenim namenom, osebami, ki razvijajo sistem, ter datumom in različico sistema;

   (w) opisom, kako umetnointeligenčni sistem deluje vzajemno s strojno ali programsko opremo, ki ni del samega umetnointeligenčnega sistema, ali se lahko uporablja za vzajemno delovanje z njo, če je ustrezno;

   (x) različicami ustrezne programske opreme ali strojne programske opreme in morebitnimi zahtevami v zvezi s posodobitvijo različice;

   (y) opisom vseh oblik, v katerih je umetnointeligenčni sistem dan na trg ali v uporabo (npr. programski paket, vgrajen v strojno opremo, ki ga je mogoče prenesti, vmesnik za aplikacijsko programiranje itd.);

   (z) opisom strojne opreme, na kateri naj bi deloval umetnointeligenčni sistem;

   (aa) če je umetnointeligenčni sistem sestavni del izdelkov, fotografijami ali ilustracijami, ki prikazujejo zunanje značilnosti, oznake in notranjo razporeditev teh izdelkov;

   (bb) navodili za uporabo za uporabnika in po potrebi navodili za namestitev;

2. podroben opis elementov umetnointeligenčnega sistema in postopka za njegov razvoj, vključno z:

   (cc) metodami in ukrepi, izvedenimi za razvoj umetnointeligenčnega sistema, po potrebi vključno z uporabo prednaučenih sistemov ali orodij, ki so jih zagotovile tretje osebe, in načinom, kako jih je ponudnik uporabil, integriral ali spremenil;

(dd) specifikacijami zasnove sistema, in sicer splošno logiko umetnointeligenčnega sistema in algoritmov; ključnimi odločitvami glede zasnove sistema, vključno z utemeljitvijo in predpostavkami, tudi glede oseb ali skupin oseb, za katere naj bi se sistem uporabljal; glavnimi izbirami klasifikacije; informacijami o tem, kaj naj bi sistem optimiziral in kako pomembni so različni parametri; opis pričakovanih rezultatov sistema; odločitvami o morebitnih kompromisih glede tehničnih rešitev, sprejetih za izpolnitev zahtev iz poglavja 2 naslova III;

(ee) opisom arhitekture sistema, ki pojasnjuje, kako se sestavni deli programske opreme medsebojno nadgrajujejo ali vzajemno učinkujejo in so vključeni v celotno obdelavo; računalniškimi viri, uporabljenimi za razvoj, učenje, testiranje in potrjevanje umetnointeligenčnega sistema;

(ff) po potrebi zahtevami glede podatkov v zvezi s podatkovnimi listi, ki opisujejo metodologije in tehnike učenja ter uporabljene nabore učnih podatkov, vključno s splošnim opisom teh naborov podatkov, informacijami o njihovem izvoru, obsegu in glavnih značilnostih; načinom, kako so bili podatki pridobljeni in izbrani; postopki označevanja (npr. za nadzorovano učenje), metodologijami čiščenja podatkov (npr. odkrivanje osamelcev);

(gg) oceno potrebnih ukrepov človekovega nadzora v skladu s členom 14, vključno z oceno potrebnih tehničnih ukrepov, ki uporabnikom olajšajo razlago rezultatov umetnointeligenčnih sistemov, v skladu s členom 13(3)(d);

(hh) če je primerno, podrobnim opisom vnaprej določenih sprememb umetnointeligenčnega sistema in njegovih zmogljivosti skupaj z vsemi ustreznimi informacijami v zvezi s tehničnimi rešitvami, sprejetimi za zagotovitev stalne skladnosti umetnointeligenčnega sistema z ustreznimi zahtevami iz poglavja 2 naslova III;

(ii) uporabljenimi postopki potrjevanja in testiranja, vključno z informacijami o uporabljenih podatkih za potrditev in testnih podatkih ter njihovih glavnih značilnostih; metrikami, uporabljenimi za merjenje točnosti, robustnosti, kibernetske varnosti in skladnosti z drugimi ustreznimi zahtevami iz poglavja 2 naslova III, pa tudi za merjenje potencialno diskriminatornih učinkov; dnevniki testiranj in vsemi poročili o testiranjih z datumi in podpisi odgovornih oseb, tudi v zvezi z vnaprej določenimi spremembami iz točke (f);

3. podrobne informacije o spremljanju, delovanju in nadzoru umetnointeligenčnega sistema, zlasti glede: njegovih zmogljivosti in omejitev delovanja, vključno s stopnjami točnosti za določene osebe ali skupine oseb, za katere naj bi se sistem uporabljal, in splošno pričakovano stopnjo točnosti glede na predvideni namen; predvidljivih nenamernih rezultatov in virov tveganj za zdravje in varnost, temeljne pravice in diskriminacijo glede na predvideni namen umetnointeligenčnega sistema; potrebnih ukrepov človekovega nadzora v skladu s členom 14, vključno z vzpostavljenimi tehničnimi ukrepi, ki uporabnikom olajšajo razlago rezultatov umetnointeligenčnih sistemov; specifikacij o vhodnih podatkih, kot je ustrezno;

4. podroben opis sistema obvladovanja tveganja v skladu s členom 9;

5. opis pomembnih sprememb, ki jih je v življenjskem ciklu sistema naredil ponudnik;

6. seznam harmoniziranih standardov, ki so bili delno ali v celoti uporabljeni in katerih sklici so bili objavljeni v Uradnem listu Evropske unije; če taki harmonizirani standardi niso bili uporabljeni, podroben opis rešitev, sprejetih za izpolnitev zahtev iz poglavja 2 naslova III, vključno s seznamom drugih uporabljenih ustreznih standardov in tehničnih specifikacij;

7. izvod izjave EU o skladnosti;

8. podroben opis vzpostavljenega sistema za ocenjevanje zmogljivosti umetnointeligenčnega sistema v obdobju po dajanju na trg v skladu s členom 61, vključno z načrtom spremljanja po dajanju na trg iz člena 61(3).

PRILOGA V

IZJAVA EU O SKLADNOSTI

Izjava EU o skladnosti iz člena 48 vsebuje vse naslednje podatke:

1. ime in vrsto umetnointeligenčnega sistema ter morebitne dodatne nedvoumne navedbe, ki omogočajo identifikacijo in sledljivost umetnointeligenčnega sistema;

2. ime in naslov ponudnika ali, če je ustrezno, njegovega pooblaščenega zastopnika;

3. izjavo, da je za izdajo izjave EU o skladnosti odgovoren izključno ponudnik;

4. izjavo, da je zadevni umetnointeligenčni sistem v skladu s to uredbo in po potrebi z drugimi določbami ustrezne zakonodaje Unije, ki določa izdajanje izjave EU o skladnosti;

5. sklice na morebitne uporabljene ustrezne harmonizirane standarde ali druge skupne specifikacije, v zvezi s katerimi je navedena skladnost;

6. če je ustrezno, ime in identifikacijsko številko priglašenega organa, opis postopka ugotavljanja skladnosti in identifikacijo izdanega potrdila;

7. kraj in datum izdaje izjave, ime in funkcijo podpisnika ter navedbo, za koga in v imenu koga ta oseba podpisuje izjavo, in podpis.

PRILOGA VI

POSTOPEK UGOTAVLJANJA SKLADNOSTI NA PODLAGI NOTRANJEGA NADZORA

1. Postopek ugotavljanja skladnosti na podlagi notranjega nadzora je postopek ugotavljanja skladnosti, ki temelji na točkah 2 do 4.

2. Ponudnik preveri, ali vzpostavljeni sistem upravljanja kakovosti izpolnjuje zahteve iz člena 17.

3. Ponudnik preuči informacije iz tehnične dokumentacije, da bi ocenil skladnost umetnointeligenčnega sistema z ustreznimi bistvenimi zahtevami iz poglavja 2 naslova III.

4. Ponudnik tudi preveri, ali sta postopek načrtovanja in razvoja umetnointeligenčnega sistema ter njegovo spremljanje po dajanju na trg iz člena 61 skladna s tehnično dokumentacijo.

PRILOGA VII

SKLADNOST NA PODLAGI OCENE SISTEMA UPRAVLJANJA KAKOVOSTI IN OCENE TEHNIČNE DOKUMENTACIJE

1. Uvod

Skladnost na podlagi ocene sistema upravljanja kakovosti in ocene tehnične dokumentacije se ugotovi s postopkom ugotavljanja skladnosti, ki temelji na točkah 2–5.

2. Pregled

Odobreni sistem upravljanja kakovosti za načrtovanje, razvoj in testiranje umetnointeligenčnih sistemov v skladu s členom 17 se preuči v skladu s točko 3 in je predmet nadzora, kot je določeno v točki 5. Tehnična dokumentacija umetnointeligenčnega sistema se preuči v skladu s točko 4.

3. Sistem upravljanja kakovosti

3.1. Zahtevek ponudnika vključuje:

(jj) ime in naslov ponudnika in, če je zahtevek vložil pooblaščeni zastopnik, tudi njegovo ime in naslov;

(kk) seznam umetnointeligenčnih sistemov, zajetih v istem sistemu upravljanja kakovosti;

(ll) tehnično dokumentacijo za vse umetnointeligenčne sisteme, zajete v istem sistemu upravljanja kakovosti;

(mm) dokumentacijo v zvezi s sistemom upravljanja kakovosti, ki zajema vse vidike iz člena 17;

(nn) opis postopkov, ki so vzpostavljeni za ohranjanje ustreznosti in učinkovitosti sistema upravljanja kakovosti;

(oo) pisno izjavo, da isti zahtevek ni bil vložen pri nobenem drugem priglašenem organu.

3.2. Priglašeni organ oceni sistem upravljanja kakovosti, da ugotovi, ali izpolnjuje zahteve iz člena 17.

Odločitev se uradno sporoči ponudniku ali njegovemu pooblaščenemu zastopniku.

Obvestilo vsebuje ugotovitve ocenjevanja sistema upravljanja kakovosti in obrazloženo odločitev o oceni.

3.3. Ponudnik še naprej izvaja in vzdržuje odobreni sistem upravljanja kakovosti, da ostane ustrezen in učinkovit.

3.4. Ponudnik priglašeni organ obvesti o vseh načrtovanih spremembah odobrenega sistema upravljanja kakovosti ali seznama umetnointeligenčnih sistemov, zajetih v njem.

Priglašeni organ pregleda predlagane spremembe in presodi, ali spremenjeni sistem upravljanja kakovosti še naprej izpolnjuje zahteve iz točke 3.2 oziroma ali je potrebna ponovna ocena.

Priglašeni organ ponudnika uradno obvesti o svoji odločitvi. Obvestilo vsebuje ugotovitve pregleda sprememb in utemeljeno odločitev o oceni.

4. Pregled tehnične dokumentacije

4.1. Ponudnik poleg zahtevka iz točke 3 pri priglašenem organu, ki ga izbere sam, vloži vlogo za oceno tehnične dokumentacije v zvezi z umetnointeligenčnim sistemom, ki ga namerava dati na trg ali v uporabo in za katerega se uporablja sistem upravljanja kakovosti iz točke 3.

4.2. Zahtevek vključuje:

(pp) ime in naslov ponudnika;

(qq) pisno izjavo, da enak zahtevek ni bil predložen nobenemu drugemu priglašenemu organu;

(rr) tehnično dokumentacijo iz Priloge IV.

4.3. Priglašeni organ pregleda tehnično dokumentacijo. Kadar je to ustrezno in omejeno na to, kar je potrebno za izpolnjevanje njegovih nalog, se priglašenemu organu omogoči neomejen dostop do uporabljenih naborov učnih in testnih podatkov ter podatkov za potrditev, po potrebi in ob uporabi ustreznih varoval prek vmesnikov za aplikacijsko programiranje (API) ali z drugimi ustreznimi sredstvi in orodji, ki omogočajo dostop na daljavo.

4.4. Pri pregledu tehnične dokumentacije lahko priglašeni organ zahteva, da ponudnik predloži dodatna dokazila ali izvede dodatne teste, da se omogoči ustrezna ocena skladnosti umetnointeligenčnega sistema z zahtevami iz poglavja 2 naslova III. Kadar priglašeni organ ni zadovoljen s testi, ki jih je opravil ponudnik, po potrebi neposredno opravi ustrezne teste.

4.5. Priglašenim organom se na utemeljeno zahtevo odobri dostop do izvorne kode umetnointeligenčnega sistema le, če so izpolnjeni naslednji kumulativni pogoji:

(a) dostop do izvorne kode je potreben za ugotavljanje skladnosti umetnointeligenčnega sistema velikega tveganja z zahtevami iz naslova III, poglavje 2, in

(b) postopki preskušanja/revizije in preverjanja na podlagi podatkov in dokumentacije, ki jih je predložil ponudnik, so bili izčrpani ali so se izkazali za nezadostne.

4.6. Odločitev se uradno sporoči ponudniku ali njegovemu pooblaščenemu zastopniku. Obvestilo vsebuje ugotovitve ocenjevanja tehnične dokumentacije in obrazloženo odločitev o oceni.

Če je umetnointeligenčni sistem v skladu z zahtevami iz poglavja 2 naslova III, priglašeni organ izda potrdilo EU o oceni tehnične dokumentacije. Potrdilo vsebuje ime in naslov ponudnika, ugotovitve pregleda, morebitne pogoje za njegovo veljavnost in podatke, potrebne za identifikacijo umetnointeligenčnega sistema.

Potrdilo in njegove priloge vsebujejo vse potrebne informacije, da se lahko oceni skladnost umetnointeligenčnega sistema in omogoči nadzor umetnointeligenčnega sistema med uporabo, če je ustrezno.

Če umetnointeligenčni sistem ne izpolnjuje zahtev iz poglavja 2 naslova III, priglašeni organ zavrne izdajo potrdila EU o oceni tehnične dokumentacije in o tem ustrezno obvesti vlagatelja s podrobno obrazložitvijo zavrnitve.

Če umetnointeligenčni sistem ne izpolnjuje zahtev glede podatkov, uporabljenih za njegovo učenje, bo pred zahtevkom za novo ugotavljanje skladnosti potrebno ponovno učenje umetnointeligenčnega sistema. V tem primeru utemeljena odločitev o oceni priglašenega organa glede zavrnitve izdaje potrdila EU o oceni tehnične dokumentacije vsebuje posebne premisleke glede kakovosti podatkov, uporabljenih za učenje umetnointeligenčnega sistema, zlasti razloge za neskladnost.

4.7. Vsako spremembo umetnointeligenčnega sistema, ki bi lahko vplivala na njegovo skladnost z zahtevami ali predvidenim namenom, odobri priglašeni organ, ki je izdal potrdilo EU o oceni tehnične dokumentacije. Ponudnik ta priglašeni organ obvesti o svoji nameri, da bo uvedel katero koli od navedenih sprememb, poleg tega ga obvesti tudi, če drugače izve za uvedbo takih sprememb. Priglašeni organ oceni načrtovane spremembe in odloči, ali je zaradi njih potrebno novo ugotavljanje skladnosti v skladu s členom 43(4) oziroma ali bi zadostovala dopolnitev potrdila EU o oceni tehnične dokumentacije. V zadnjenavedenem primeru priglašeni organ oceni spremembe, uradno obvesti ponudnika o svoji odločitvi in mu, če so spremembe odobrene, izda dopolnilo potrdila EU o oceni tehnične dokumentacije.

5. Nadzor odobrenega sistema upravljanja kakovosti

5.1. Namen nadzora, ki ga izvaja priglašeni organ iz točke 3, je zagotoviti, da ponudnik ustrezno izpolnjuje pogoje odobrenega sistema upravljanja kakovosti.

5.2. Za namene ocenjevanja ponudnik priglašenemu organu omogoči dostop do prostorov, v katerih potekajo načrtovanje, razvoj in testiranje umetnointeligenčnih sistemov. Poleg tega bo ponudnik priglašenemu organu posredoval vse potrebne informacije.

5.3. Priglašeni organ opravlja redne presoje, s čimer zagotovi, da ponudnik vzdržuje in izvaja sistem upravljanja kakovosti, poročila o teh presojah pa predloži ponudniku. V okviru teh presoj lahko priglašeni organ izvede dodatne teste umetnointeligenčnih sistemov, za katere je bilo izdano potrdilo EU o oceni tehnične dokumentacije.

PRILOGA VIII

INFORMACIJE, KI JIH JE TREBA PREDLOŽITI OB REGISTRACIJI UMETNOINTELIGENČNIH SISTEMOV VELIKEGA TVEGANJA V SKLADU S ČLENOM 51

Ponudniki, pooblaščeni zastopniki in uporabniki, ki so javni organi, agencije ali organi, predložijo informacije iz dela I. Ponudniki ali po potrebi pooblaščeni predstavniki zagotovijo, da so informacije o njihovih umetnointeligenčnih sistemih velikega tveganja iz dela II, točke 1 do 11, popolne, pravilne in posodobljene. Informacije iz dela II., točka 12, se samodejno generirajo iz baze podatkov.

Del I. Informacije o operaterjih (ob njihovi registraciji)

–1. vrsta operaterja (ponudnik, pooblaščeni zastopnik ali uporabnik);

1. ime, naslov in kontaktni podatki ponudnika;

2. kadar informacije predloži druga oseba v imenu operaterja, ime, naslov in kontaktni podatki te osebe.

Del II. Informacije o umetnointeligenčnem sistemu velikega tveganja

1. ime, naslov in kontaktni podatki ponudnika;

2. ime, naslov in kontaktni podatki pooblaščenega zastopnika, če obstaja;

3. trgovsko ime umetnointeligenčnega sistema ter morebitne dodatne nedvoumne navedbe, ki omogočajo identifikacijo in sledljivost umetnointeligenčnega sistema;

4. opis predvidenega namena umetnointeligenčnega sistema;

5. status umetnointeligenčnega sistema (na trgu ali v uporabi; ni več na trgu/v uporabi, preklican);

6. vrsta, številka in datum izteka veljavnosti potrdila, ki ga je izdal priglašeni organ, ter ime ali identifikacijska številka tega priglašenega organa, če je ustrezno;

7. skeniran izvod potrdila iz točke 6, če je ustrezno;

8. države članice, v katerih se umetnointeligenčni sistem daje ali je bil dan na trg ali v uporabo ali je bil dan na voljo v Uniji;

9. izvod izjave EU o skladnosti iz člena 48;

10. elektronska navodila za uporabo;

11. URL za dodatne informacije (neobvezno).

12. ime, naslov in kontaktni podatki uporabnikov.

PRILOGA VIIIa

INFORMACIJE, KI JIH JE TREBA PREDLOŽITI OB REGISTRACIJI UMETNOINTELIGENČNIH SISTEMOV VELIKEGA TVEGANJA V ZVEZI S TESTIRANJEM V DEJANSKIH RAZMERAH V SKLADU S ČLENOM 54a

V zvezi s testiranjem v dejanskih razmerah, ki ga je treba registrirati v skladu s členom 54a, se predložijo in nato posodabljajo naslednje informacije:

1. vseevropska enotna identifikacijska številka testiranja v dejanskih razmerah;

2. ime in kontaktni podatki ponudnika ali potencialnega ponudnika in uporabnikov, vključenih v testiranje v dejanskih razmerah;

3. kratek opis umetnointeligenčnega sistema, njegov predviden namen in druge informacije, potrebne za identifikacijo sistema;

4. povzetek glavnih značilnosti načrta za preskušanje v dejanskih razmerah;

5. informacije o začasni ali dokončni prekinitvi preskušanja v dejanskih razmerah.

PRILOGA IX

Zakonodaja Unije o obsežnih informacijskih sistemih s področja svobode, varnosti in pravice

1. Schengenski informacijski sistem

(ss) Uredba (EU) 2018/1860 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o uporabi schengenskega informacijskega sistema za vračanje nezakonito prebivajočih državljanov tretjih držav (UL L 312, 7.12.2018, str. 1).

(tt) Uredba (EU) 2018/1861 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o vzpostavitvi, delovanju in uporabi schengenskega informacijskega sistema (SIS) na področju mejnih kontrol, o spremembi Konvencije o izvajanju Schengenskega sporazuma ter o spremembi in razveljavitvi Uredbe (ES) št. 1987/2006 (UL L 312, 7.12.2018, str. 14).

(uu) Uredba (EU) 2018/1862 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o vzpostavitvi, delovanju in uporabi schengenskega informacijskega sistema (SIS) na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah, o spremembi in razveljavitvi Sklepa Sveta 2007/533/PNZ ter o razveljavitvi Uredbe (ES) št. 1986/2006 Evropskega parlamenta in Sveta in Sklepa Komisije 2010/261/EU (UL L 312, 7.12.2018, str. 56).

2. Vizumski informacijski sistem

(vv) Predlog UREDBE EVROPSKEGA PARLAMENTA IN SVETA o spremembi Uredbe (ES) št. 767/2008, Uredbe (ES) št. 810/2009, Uredbe (EU) 2017/2226, Uredbe (EU) 2016/399, Uredbe XX/2018 [uredba o interoperabilnosti] in Odločbe Sveta 2004/512/ES ter o razveljavitvi Sklepa Sveta 2008/633/PNZ (COM(2018) 302 final). Bo posodobljeno, ko sozakonodajalca sprejmeta uredbo (aprila/maja 2021).

3. Eurodac

(ww) Spremenjeni predlog UREDBE EVROPSKEGA PARLAMENTA IN SVETA o vzpostavitvi sistema Eurodac za primerjavo biometričnih podatkov zaradi učinkovite uporabe Uredbe (EU) XXX/XXX [uredba o upravljanju azila in migracij] in Uredbe (EU) XXX/XXX [uredba o preselitvi] za ugotavljanje istovetnosti nezakonito prebivajočih državljanov tretjih držav ali oseb brez državljanstva ter o zahtevah za primerjavo s podatki iz sistema Eurodac, ki jih vložijo organi kazenskega pregona držav članic in Europol za namene kazenskega pregona, ter o spremembi uredb (EU) 2018/1240 in (EU) 2019/818 (COM(2020) 614 final).

4. Sistem vstopa/izstopa

(xx) Uredba (EU) 2017/2226 Evropskega parlamenta in Sveta z dne 30. novembra 2017 o vzpostavitvi sistema vstopa/izstopa (SVI) za evidentiranje podatkov o vstopu in izstopu ter podatkov o zavrnitvi vstopa državljanov tretjih držav pri prehajanju zunanjih meja držav članic in določitvi pogojev za dostop do SVI zaradi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter o spremembi Konvencije o izvajanju Schengenskega sporazuma in uredb (ES) št. 767/2008 ter (EU) št. 1077/2011 (UL L 327, 9.12.2017, str. 20).

5. Evropski sistem za potovalne informacije in odobritve

(yy) Uredba (EU) 2018/1240 Evropskega parlamenta in Sveta z dne 12. septembra 2018 o vzpostavitvi Evropskega sistema za potovalne informacije in odobritve (ETIAS) ter spremembi uredb (EU) št. 1077/2011, (EU) št. 515/2014, (EU) 2016/399, (EU) 2016/1624 in (EU) 2017/2226 (UL L 236, 19.9.2018, str. 1).

(zz) Uredba (EU) 2018/1241 Evropskega parlamenta in Sveta z dne 12. septembra 2018 o spremembi Uredbe (EU) 2016/794 za namene vzpostavitve Evropskega sistema za potovalne informacije in odobritve (ETIAS) (UL L 236, 19.9.2018, str. 72).

6. Evropski informacijski sistem kazenskih evidenc za državljane tretjih držav in osebe brez državljanstva

(aaa) Uredba (EU) 2019/816 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o vzpostavitvi centraliziranega sistema za določitev držav članic, ki imajo informacije o obsodbah državljanov tretjih držav in oseb brez državljanstva (sistem ECRIS-TCN), z namenom dopolnitve evropskega informacijskega sistema kazenskih evidenc ter o spremembi Uredbe (EU) 2018/1726 (UL L 135, 22.5.2019, str. 1).

7. Interoperabilnost

(bbb) Uredba (EU) 2019/817 Evropskega parlamenta in Sveta z dne 20. maja 2019 o vzpostavitvi okvira za interoperabilnost informacijskih sistemov EU na področju meja in vizumov (UL L 135, 22.5.2019, str. 27).

(ccc) Uredba (EU) 2019/818 Evropskega parlamenta in Sveta z dne 20. maja 2019 o vzpostavitvi okvira za interoperabilnost informacijskih sistemov EU na področju policijskega in pravosodnega sodelovanja, azila ter migracij (UL L 135, 22.5.2019, str. 85).