



2024/1689

12.7.2024

UREDBA (EU) 2024/1689 EVROPSKEGA PARLAMENTA IN SVETA

z dne 13. junija 2024

o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci)

(Besedilo velja za EGP)

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

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

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora ⁽¹⁾,

ob upoštevanju mnenja Evropske centralne banke ⁽²⁾,

ob upoštevanju mnenja Odbora regij ⁽³⁾,

v skladu z rednim zakonodajnim postopkom ⁽⁴⁾,

ob upoštevanju naslednjega:

- (1) Namen te uredbe je izboljšati delovanje notranjega trga z določitvijo enotnega pravnega okvira, predvsem za razvoj, dajanje na trg, dajanje v uporabo ter za uporabo umetno-inteligenčnih sistemov (v nadaljnjem besedilu: sistemi UI) v Uniji, v skladu z vrednotami Unije, da bi spodbujali uvajanje na človeka osredotočene in zaupanja vredne umetne inteligence (UI) in hkrati zagotovili visoko raven varovanja zdravja, varnosti in temeljnih pravic, kot so določene v Listini Evropske unije o temeljnih pravicah (v nadaljnjem besedilu: Listina), vključno z demokracijo, pravno državo in varstvom okolja, za zaščito pred škodljivimi učinki sistemov UI v Uniji ter da bi podpirali inovacije. S to uredbo se zagotavlja prosti čezmejni pretok blaga in storitev, ki temeljijo na umetni inteligenci, s čimer se državam članicam preprečuje, da bi uvedle omejitve za razvoj, trženje in uporabo sistemov UI, razen če je to izrecno dovoljeno s to uredbo.
- (2) To uredbo bi bilo treba uporabljati v skladu z vrednotami Unije, zapisanimi v Listini, kar bi olajšalo varstvo fizičnih oseb, podjetij, demokracije, pravne države in varstva okolja, hkrati pa spodbujalo inovacije in zaposlovanje ter Uniji zagotovilo vodilno vlogo pri uvajanju zaupanja vredne UI.
- (3) Sisteme UI je mogoče zlahka uporabljati v številnih različnih gospodarskih in družbenih sektorjih, tudi čezmejno, in lahko enostavno krožijo po vsej Uniji. Nekatere države članice so že preučile možnost sprejetja nacionalnih predpisov, s katerimi bi zagotovile, da je UI zaupanja vredna in 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 sisteme UI. Zato bi bilo treba zagotoviti dosledno in visoko raven varstva po vsej Uniji, da bi dosegli zaupanja vredno UI in hkrati preprečili razlike, ki ovirajo prosti pretok, inovacije, uvajanje in uporabo sistemov UI ter z njimi povezanih proizvodov in

⁽¹⁾ UL C 517, 22.12.2021, str. 56.

⁽²⁾ UL C 115, 11.3.2022, str. 5.

⁽³⁾ UL C 97, 28.2.2022, str. 60.

⁽⁴⁾ Stališče Evropskega parlamenta z dne 13. marca 2024 (še ni objavljeno v Uradnem listu) in odločitev Sveta z dne 21. maja 2024.

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 (PDEU). Kolikor ta uredba vključuje posebna pravila o varstvu posameznikov pri obdelavi osebnih podatkov v zvezi z omejitvami uporabe sistemov UI za biometrično identifikacijo na daljavo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, uporabe sistemov UI za ocene tveganja fizičnih oseb za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter uporabe sistemov UI za biometrično kategorizacijo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, je primerno, da ta uredba, kar zadeva ta posebna pravila, temelji na členu 16 PDEU. Glede na ta posebna pravila in sklicevanje na člen 16 PDEU se je primerno posvetovati z Evropskim odborom za varstvo podatkov.

- (4) UI je hitro razvijajoča se skupina tehnologij, ki prispeva k številnim gospodarskim, okoljskim in družbenim koristim v celotnem spektru panog in družbenih dejavnosti. Uporaba UI lahko z izboljšanjem napovedi, optimizacijo delovanja in dodeljevanja virov ter po meri prilagojenimi digitalnimi rešitvami, ki so na voljo posameznikom in organizacijam, zagotavlja ključne konkurenčne prednosti za podjetja ter podpira družbeno in okoljsko koristne rezultate, na primer na področju zdravstvenega varstva, kmetijstva, varnosti hrane, izobraževanja in usposabljanja, medijev, športa, kulture, upravljanja infrastrukture, energije, prometa in logistike, javnih storitev, varnosti, pravosodja, učinkovite rabe virov in energije, okoljskega spremljanja, ohranjanja in obnovitve biotske raznovrstnosti in ekosistemov ter blažitve podnebnih sprememb in prilagajanja nanje.
- (5) Hkrati lahko UI – odvisno od okoliščin v zvezi z njenim posebnim namenom, uporabo in ravno tehnološkega razvoja – povzroča tveganja ter škodi javnim interesom in temeljnim pravicam, ki jih varuje pravo Unije. Ta škoda je lahko premoženjska ali nepremoženjska, vključno s fizično, psihično, družbeno ali ekonomsko škodo.
- (6) Glede na velik vpliv, ki ga lahko ima UI na družbo, in potrebo po vzpostavitvi zaupanja je bistveno, da se UI in njen regulativni okvir razvijata v skladu z vrednotami Unije iz člena 2 Pogodbe o Evropski uniji (PEU), temeljnimi pravicami in svoboščinami, ki so zapisane v Pogodbah, in, na podlagi člena 6 PEU, v Listini. Osnovni pogoj za UI bi moral biti, da je to tehnologija, osredotočena na človeka. Morala bi biti orodje za ljudi, končni cilj pa bi moral biti povečanje njihove blaginje.
- (7) Da bi zagotovili dosledno in visoko raven zaščite javnih interesov v zvezi z zdravjem, varnostjo in temeljnimi pravicami, bi bilo treba določiti skupna pravila za visokotvegane sisteme UI. Ta pravila bi morala biti skladna z Listino, nediskriminatorna in v skladu z mednarodnimi trgovinskimi zavezami Unije. Treba bi bilo upoštevati tudi Evropsko deklaracijo o digitalnih pravicah in načelih za digitalno desetletje ter Etične smernice za zaupanja vredno umetno inteligenco strokovne skupine na visoki ravni za umetno inteligenco (AI HLEG).
- (8) Da bi spodbujali razvoj, uporabo in uvajanje UI na notranjem trgu, je torej potreben pravni okvir Unije, v katerem bodo določena harmonizirana pravila o umetni inteligenci in bo hkrati zagotovljena visoka raven zaščite javnih interesov, kot so zdravje in varnost ter varstvo temeljnih pravic, vključno z demokracijo, pravno državo in varstvom okolja, kot je priznано in zaščiteno s pravom Unije. Za doseg tega cilja bi bilo treba določiti pravila, s katerimi bo urejeno dajanje nekaterih sistemov UI na trg in v uporabo ter njihova uporaba, s čimer bo zagotovljeno nemoteno delovanje notranjega trga in bo omogočeno, da se v okviru teh sistemov izkoristi načelo prostega pretoka blaga in storitev. Ta pravila bi morala biti jasna in robustna glede varstva temeljnih pravic, morala bi podpirati nove inovativne rešitve in omogočati delovanje evropskega ekosistema javnih in zasebnih akterjev, ki ustvarjajo sisteme UI v skladu z vrednotami Unije, ter uresničevati potencial digitalne preobrazbe v vseh regijah Unije. Z določitvijo teh pravil in ukrepov v podporo inovacijam s posebnim poudarkom na malih in srednjih podjetjih (MSP), vključno s zagonskimi podjetji, ta uredba podpira cilj spodbujanja evropskega na človeka osredotočenega pristopa k umetni inteligenci in vodilnega položaja v svetu pri razvoju varne, zaupanja vredne in etične UI, kot je navedeno v sklepih Evropskega sveta ⁽⁵⁾, in zagotavlja zaščito etičnih načel v skladu z izrecno zahtevo Evropskega parlamenta ⁽⁶⁾.

⁽⁵⁾ Evropski svet, izredno zasedanje Evropskega sveta (1. in 2. oktobra 2020) – sklepi, EUCO 13/20, 2020, str. 6.

⁽⁶⁾ Resolucija Evropskega parlamenta z dne 20. oktobra 2020 s priporočili Komisiji o okviru etičnih vidikov umetne inteligence, robotike in sorodnih tehnologij (dok. 2020/2012(INL)).

- (9) Harmonizirana pravila, ki se uporabljajo za dajanje visokotveganih sistemov UI na trg ali v uporabo ter za njihovo uporabo, bi bilo treba določiti skladno z Uredbo (ES) št. 765/2008 Evropskega parlamenta in Sveta ⁽⁷⁾, Sklepom št. 768/2008/ES Evropskega parlamenta in Sveta ⁽⁸⁾ ter Uredbo (EU) 2019/1020 Evropskega parlamenta in Sveta ⁽⁹⁾ (v nadaljnjem besedilu: novi zakonodajni okvir). Harmonizirana pravila, določena v tej uredbi, bi bilo treba uporabljati v vseh sektorjih, hkrati pa v skladu z novim zakonodajnim okvirom ne bi smela posegati v veljavno pravo Unije, zlasti pravo o varstvu podatkov, varstvu potrošnikov, temeljnih pravicah, zaposlovanju in varstvu delavcev ter varnosti proizvodov, ki ga ta uredba dopolnjuje. Posledično ostanejo nespremenjeni in se v celoti uporabljajo vse pravice in pravna sredstva, ki jih takšno pravo Unije zagotavlja potrošnikom in drugim osebam, na katere bi lahko sistemi UI negativno vplivali, tudi v zvezi z nadomestilom morebitne škode na podlagi Direktive Sveta 85/374/EGS ⁽¹⁰⁾. Poleg tega ta uredba v okviru zaposlovanja in zaščite delavcev ne bi smela vplivati na pravo Unije o socialni politiki in nacionalno delovno pravo, ki je skladno s pravom Unije, v zvezi z zaposlovanjem in delovnimi pogoji, vključno z zdravjem in varnostjo pri delu ter razmerjem med delodajalci in delavci. Tudi ne bi smela vplivati na uveljavljanje temeljnih pravic, ki so priznane v državah članicah in na ravni Unije, vključno s pravico do stavke ali drugih ukrepov, zajetih v specifičnih sistemih odnosov med delodajalci in delojemalci v posameznih državah članicah, ter na pravico do pogajanj, sklepanja in izvrševanja kolektivnih pogodb ali do kolektivnih ukrepov v skladu z nacionalnim pravom. Ta uredba ne bi smela vplivati na določbe za izboljšanje delovnih pogojev pri platformnem delu iz direktive Evropskega parlamenta in Sveta o izboljšanju delovnih pogojev pri platformnem delu. 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 sistemov UI. Poleg tega bi bilo treba obveznosti, naložene različnim operaterjem, vključenim v verigo vrednosti UI na podlagi te uredbe, uporabljati brez poseganja v nacionalno pravo, ki je skladno s pravom Unije in katerega učinek je omejitev uporabe nekaterih sistemov UI, kadar tako pravo ne spada na področje uporabe te uredbe ali je namenjeno uresničevanju legitimnih ciljev v javnem interesu, 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 št. 25 KZNOP (2021) o otrokovih pravicah v zvezi z digitalnim okoljem, če se to pravo ne nanaša posebej na sisteme UI in je namenjeno uresničevanju drugih legitimnih ciljev v javnem interesu.
- (10) Temeljna pravica do varstva osebnih podatkov je zajamčena zlasti z uredbama (EU) 2016/679 ⁽¹¹⁾ in (EU) 2018/1725 ⁽¹²⁾ Evropskega parlamenta in Sveta ter Direktivo (EU) 2016/680 Evropskega parlamenta in Sveta ⁽¹³⁾. Direktiva 2002/58/ES Evropskega parlamenta in Sveta ⁽¹⁴⁾ poleg tega varuje zasebno življenje in zaupnost komunikacij, vključno z zagotavljanjem pogojev za shranjevanje osebnih in neosebnih podatkov na terminalske opreme in za dostop do teh podatkov z nje. Navedeni pravni akti Unije so podlaga za vzdržno in odgovorno obdelavo podatkov, tudi kadar nabori podatkov vključujejo kombinacijo osebnih in neosebnih podatkov. Namen te uredbe ni vplivati na uporabo veljavnega prava Unije, ki ureja obdelavo osebnih podatkov, med drugim tudi ne na naloge in pooblastila neodvisnih nadzornih organov, pristojnih za spremljanje skladnosti s temi instrumenti. Uredba tudi ne vpliva na obveznosti ponudnikov in uvajalcev sistemov UI v njihovi vlogi upravljavcev ali obdelovalcev podatkov, ki izhaja iz prava Unije ali nacionalnega prava o varstvu osebnih podatkov, če zasnova, razvoj ali uporaba sistemov UI vključuje obdelavo osebnih podatkov. Prav tako je treba pojasniti, da posamezniki, na katere se nanašajo
-
- ⁽⁷⁾ Uredba (ES) št. 765/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o določitvi zahtev za akreditacijo in razveljavitvi Uredbe (EGS) št. 339/93 (UL L 218, 13.8.2008, str. 30).
- ⁽⁸⁾ 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).
- ⁽⁹⁾ 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 (UL L 169, 25.6.2019, str. 1).
- ⁽¹⁰⁾ Direktiva 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 (UL L 210, 7.8.1985, str. 29).
- ⁽¹¹⁾ 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).
- ⁽¹²⁾ Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).
- ⁽¹³⁾ Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89).
- ⁽¹⁴⁾ Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (UL L 201, 31.7.2002, str. 37).

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 sistemov UI na trg ali v uporabo ter za njihovo uporabo, ki so 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.

- (11) Ta uredba ne bi smela posegati v določbe o odgovornosti ponudnikov posredniških storitev iz Uredbe (EU) 2022/2065 Evropskega parlamenta in Sveta⁽¹⁵⁾.
- (12) Pojem „sistem UI“ v tej uredbi bi moral biti jasno opredeljen in tesno usklajen z delom mednarodnih organizacij, ki se ukvarjajo z UI, da bi zagotovili pravno varnost, olajšali mednarodno zblíževanje in široko sprejemanje ter hkrati zagotovili prožnost, ki bo omogočala prilagajanje hitremu tehnološkemu razvoju na tem področju. Poleg tega bi morala opredelitev temeljiti na ključnih značilnostih sistemov UI, po katerih se razlikuje od enostavnejših tradicionalnih sistemov programske opreme ali programskih pristopov, in ne bi smela vključevati sistemov, ki temeljijo na pravilih, ki jih za samodejno izvajanje operacij opredelijo izključno fizične osebe. Ključna značilnost sistemov UI je njihova sposobnost sklepanja. Ta sposobnost sklepanja se nanaša na proces pridobivanja izhodnih podatkov, kot so napovedi, vsebina, priporočila ali odločitve, ki lahko vplivajo na fizično in virtualno okolje, ter na sposobnost sistemov UI, da izpeljejo modele ali algoritme ali oboje iz vhodnih vrednosti ali podatkov. Tehnike, ki omogočajo sklepanje pri vzpostavljanju sistema UI, vključujejo pristope strojnega učenja, ki se tega, kako doseči določene cilje, učijo iz podatkov, ter pristope, ki temeljijo na logiki in znanju ter izhajajo iz kodiranega znanja ali simbolične predstavitve naloge, ki jo je treba rešiti. Zmogljivost sistema UI za sklepanje presega osnovno obdelavo podatkov z omogočanjem učenja, prihajanja do zaključkov ali modeliranja. Izraz „temelječ na napravah“ se nanaša na dejstvo, da sisteme UI poganjajo stroji. Sklicevanje na eksplicitne ali implicitne cilje poudarja, da lahko sistemi UI delujejo v skladu z eksplicitnimi ali implicitnimi cilji. Cilji sistema UI se lahko v posebnih okoliščinah razlikujejo od predvidenega namena sistema UI. Za namene te uredbe bi bilo treba okolja razumeti kot kontekste, v katerih delujejo sistemi UI, medtem ko izhodni podatki, ki jih ustvari sistem UI, odražajo različne funkcije, ki jih opravljajo sistemi UI, in vključujejo napovedi, vsebine, priporočila ali odločitve. Sistemi UI so zasnovani tako, da delujejo z različnimi stopnjami avtonomije, kar pomeni, da so do neke mere neodvisni od človeškega sodelovanja in zmožni delovati brez človeškega posredovanja. Prilagodljivost, ki bi jo sistem UI lahko pokazal po uvedbi, se nanaša na sposobnosti samoučenja, ki omogočajo, da se sistem med uporabo spremeni. Sistemi UI se lahko uporabljajo samostojno ali kot komponenta določenega proizvoda, ne glede na to, ali je sistem fizično integriran v proizvod (vgrajen) ali služi funkcionalnosti proizvoda, ne da bi bil vanj integriran (nevgrajen).
- (13) Pojem „uvajalec“ iz te uredbe bi bilo treba razlagati kot vsako fizično ali pravno osebo, vključno z javnim organom, agencijo ali drugim telesom, ki uporablja sistem UI pod svojo pristojnostjo, razen kadar se sistem UI uporablja v okviru osebne nepoklicne dejavnosti. Glede na vrsto sistema UI lahko uporaba sistema vpliva na osebe, ki niso uvajalec.
- (14) Pojem „biometrični podatki“, ki se uporablja v tej uredbi, bi bilo treba razlagati glede na pojem biometričnih podatkov, kot je opredeljen v členu 4, točka 14, Uredbe (EU) 2016/679, členu 3, točka 18, Uredbe (EU) 2018/1725 in členu 3, točka 13, Direktive (EU) 2016/680. Biometrični podatki lahko omogočijo avtentikacijo, identifikacijo ali kategorizacijo fizičnih oseb in prepoznavanje njihovih čustev.
- (15) Pojem „biometrična identifikacija“ iz te uredbe bi bilo treba opredeliti kot avtomatizirano prepoznavanje fizičnih, fizioloških in vedenjskih človeških značilnosti, kot so obraz, gibanje oči, izrazi obraza, oblika telesa, glas, govor, hoja, drža, srčni utrip, krvni tlak, vonj in značilnosti tipkanja, za namene preverjanja identitete posameznika s primerjavo biometričnih podatkov tega posameznika s shranjenimi biometričnimi podatki posameznikov v referenčni podatkovni zbirki ne glede na to, ali je posameznik v to privolil ali ne. To izključuje sisteme UI za biometrično preverjanje, tudi avtentikacijo, katerih edini namen je potrditi, da je določena fizična oseba res ta, za katero se predstavlja, in potrditi identiteto fizične osebe izključno z namenom dostopa do storitve, odklepanja naprave ali varnostnega dostopa do prostorov.

⁽¹⁵⁾ Uredba (EU) 2022/2065 Evropskega parlamenta in Sveta z dne 19. oktobra 2022 o enotnem trgu digitalnih storitev in spremembi Direktive 2000/31/ES (Akt o digitalnih storitvah) (UL L 277, 27.10.2022, str. 1).

- (16) Pojem „biometrična kategorizacija“ iz te uredbe bi bilo treba opredeliti kot razvrstitev fizičnih oseb v posebne kategorije na podlagi njihovih biometričnih podatkov. Takšne posebne kategorije se lahko nanašajo na vidike, kot so spol, starost, barva las, barva oči, tetovaže, vedenjske ali osebnostne lastnosti, jezik, vera, pripadnost narodnostni manjšini, spolna ali politična usmerjenost. To ne vključuje sistemov za biometrično kategorizacijo, ki so izključno pomožni element, neločljivo povezan z drugo komercialno storitvijo, kar pomeni, da tega elementa iz objektivnih tehničnih razlogov ni mogoče uporabiti brez glavne storitve, njegova vključitev ali funkcionalnost pa ni sredstvo za izogibanje uporabi pravil iz te uredbe. Na primer, filtri za kategorizacijo obraznih ali telesnih značilnosti, ki se uporabljajo na spletnih tržnicah, bi lahko bili takšen pomožni element, saj se lahko uporabljajo le v zvezi z glavno storitvijo, ki je prodaja izdelka na način, da se potrošniku omogoči, da si ogleda prikaz izdelka sam, in se mu pomaga pri sprejemanju odločitve o nakupu. Filtre, ki se uporabljajo na spletnih storitvah družbenih omrežij in s katerimi se kategorizirajo obrazne funkcije ali funkcije telesa, da lahko uporabniki dodajajo ali spreminjajo slike ali videoposnetke, bi prav tako lahko šteli za pomožno funkcijo, saj takega filtra ni mogoče uporabljati brez glavne storitve, tj. storitev družbenih omrežij, ki vključuje izmenjavo vsebin na spletu.
- (17) Pojem „sistem za biometrično identifikacijo na daljavo“ iz te uredbe bi bilo treba opredeliti funkcionalno kot sistem UI, namenjen identifikaciji fizičnih oseb brez njihovega dejavnega sodelovanja, običajno na daljavo, s primerjavo biometričnih podatkov osebe z biometričnimi podatki iz referenčne podatkovne zbirke, ne glede na uporabljeno tehnologijo, procese ali vrste biometričnih podatkov. Takšni sistemi za biometrično identifikacijo na daljavo se običajno uporabljajo za hkratno zaznavanje več oseb ali njihovega vedenja, da se bistveno olajša identifikacija fizičnih oseb brez njihovega dejavnega sodelovanja. To izključuje sisteme UI za biometrično preverjanje, tudi avtentikacijo, katerih edini namen je potrditi, da je določena fizična oseba res ta, za katero se predstavlja, in potrditi identiteto fizične osebe izključno z namenom dostopa do storitve, odklepanja naprave ali varnostnega dostopa do 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 brez njihovega dejavnega sodelovanja. Pri sistemih „v realnem času“ se zajemanje biometričnih podatkov, primerjava in identifikacija izvedejo takoj ali skoraj takoj, v vsakem primeru pa brez večje zamude. V zvezi s tem ne bi smelo biti prostora za izogibanje pravilom te uredbe o uporabi zadevnih sistemov UI „v realnem času“, saj je predvidena možnost manjših zamud. 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 CCTV ali zasebne naprave, ki je bilo ustvarjeno pred uporabo sistema v zvezi z zadevnimi fizičnimi osebami.
- (18) Pojem „sistem za prepoznavanje čustev“ iz te uredbe bi bilo treba opredeliti kot sistem UI za prepoznavanje čustev ali namer ali za sklepanje o čustvih ali namerah fizičnih oseb na podlagi njihovih biometričnih podatkov. Pojem se nanaša na čustva ali namere, kot so sreča, žalost, jeza, presenečenje, ogorčenje, zadrega, navdušenje, osramočenost, zaničevanje, zadovoljstvo in zabavanje. Ne vključuje fizičnih stanj, kot sta bolečina ali utrujenost, na primer vključno s sistemi, ki se uporabljajo za odkrivanje stanja utrujenosti poklicnih pilotov ali voznikov za namene preprečevanja nesreč. To tudi ne vključuje zgolj odkrivanja lahko vidnih izrazov, gest ali gibov, razen če se uporabljajo za prepoznavanje čustev ali sklepanje o njih. Ti izrazi so lahko osnovni obrazni izrazi, kot je namrščenost ali nasmeh, ali geste, kot je premikanje dlani, rok ali glave, ali značilnosti glasu osebe, kot je povzdignjen glas ali šepetanje.
- (19) 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 prostor uporablja, denimo za komercialno, na primer trgovine, restavracije, kavarne; storitveno, na primer banke, poklicne dejavnosti, gostinske ali nastanitvene dejavnosti; športno, na primer bazeni, telovadnice, stadioni; prevozno, na primer avtobusne postaje, postaje podzemne železnice in železniške postaje, letališča, prevozna sredstva; razvedrilno, na primer kinematografi, gledališča, muzeji, koncertne in konferenčne dvorane; prostocasno ali drugo dejavnost, na primer javne ceste in trgi, parki, gozdovi, igrišča. Prostor bi bilo treba tudi razvrstiti kot javno dostopen, 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 vstopnice ali 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 bodisi na podlagi prava Unije bodisi na podlagi nacionalnega prava, ki se neposredno nanaša na javno varnost ali varovanje, ali če se oseba, ki ima za ta prostor

ustrezna pooblastila, glede tega jasno opredeli. Dejanska možnost samega dostopa, kot so odklenjena vrata, odprta vrata v ograji, ne pomeni, da je prostor javno dostopen, če obstajajo znaki ali okoliščine, ki kažejo na nasprotno, kot so znaki, ki prepovedujejo ali omejujejo dostop. Prostor podjetij in tovarn ter pisarne in delovni prostori, do katerih naj bi 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. Nekateri drugi prostori lahko zajemajo tako javno dostopne kot javno nedostopne prostore, kot je hodnik ali veža zasebne stanovanjske zgradbe, prek katere se dostopa do zdravniške pisarne, ali letališče. Spletni prostori niso zajeti, saj niso fizični prostori. Ali je določen prostor dostopen javnosti ali ne, pa je treba ugotoviti za vsak primer posebej, ob upoštevanju posebnosti posamezne dane situacije.

- (20) Da bi dosegli največje koristi sistemov UI in hkrati zaščitili temeljne pravice, zdravje in varnost ter omogočili demokratični nadzor, bi morala pismenost na področju UI ponudnikom, uvajalcem in osebam, na katere vpliva sistem UI, omogočiti razumevanje potrebnih pojmov za sprejemanje informiranih odločitev v zvezi s sistemi UI. Ti pojmi se lahko razlikujejo glede na zadevni kontekst in lahko vključujejo razumevanje pravilne uporabe tehničnih elementov v razvojni fazi sistema UI, ukrepe, ki jih je treba uporabiti med njegovo uporabo, ustrezne načine za razlago izhodnih podatkov sistema UI in, v primeru oseb, na katere vpliva sistem UI, znanje, potrebno za razumevanje, kako bodo odločitve, sprejete s pomočjo UI vplivale nanje. V okviru uporabe te uredbe bi morala pismenost na področju UI vsem zadevnim akterjem v verigi vrednosti UI zagotoviti vpogled, potrebne za zagotovitev ustrezne skladnosti s to uredbo in njenega pravilnega izvrševanja. Poleg tega bi lahko široko izvajanje ukrepov za pismenost na področju UI in uvedba ustreznih nadaljnjih ukrepov prispevala k izboljšanju delovnih pogojev ter nazadnje podprla konsolidacijo in inovacijsko pot zaupanja vredne UI v Uniji. Evropski odbor za umetno inteligenco (v nadaljnjem besedilu: Odbor) bi moral podpirati Komisijo pri spodbujanju orodij za pismenost na področju UI, ozaveščenosti javnosti in razumevanja koristi, tveganj, zaščitnih ukrepov, pravic in obveznosti v zvezi z uporabo sistemov UI. Komisija in države članice bi morale v sodelovanju z ustreznimi deležniki olajšati pripravo prostovoljnih kodeksov ravnanja za izboljšanje pismenosti na področju UI med osebami, ki se ukvarjajo z razvojem, delovanjem in uporabo UI.
- (21) Za zagotovitev enakih konkurenčnih pogojev ter učinkovitega varstva pravic in svoboščin posameznikov po vsej Uniji bi se morala pravila iz te uredbe nediskriminatorno uporabljati za ponudnike sistemov UI, ne glede na to, ali imajo sedež v Uniji ali v tretji državi, in za uvajalce sistemov UI s sedežem v Uniji.
- (22) Zaradi svoje digitalne narave bi morali nekateri sistemi UI spadati na področje uporabe te uredbe, tudi če niso dani na trg ali v uporabo oziroma se ne uporabljajo v Uniji. To velja na primer za operaterja s sedežem v Uniji, ki določene storitve naroča pri operaterju s sedežem v tretji državi v zvezi z dejavnostjo, ki jo bo izvajal sistem UI, ki bi bil opredeljen kot visokotvegani sistem. V teh okoliščinah bi lahko sistem UI, ki ga operater uporablja v tretji državi, obdeloval podatke, ki se zakonito zbirajo v Uniji in prenašajo iz nje, ter naročniku v Uniji zagotovil izhodne podatke navedenega sistema UI, ki izhajajo iz te obdelave, ne da bi bil ta sistem UI dan na trg ali v uporabo oziroma bi se uporabljal 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 uvajalce sistemov UI s sedežem v tretji državi, če so izhodni podatki, ki jih ti sistemi ustvarijo, namenjeni uporabi v Uniji. Kljub temu pa 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 sodelovanja ali mednarodnih sporazumov, sklenjenih na ravni Unije ali nacionalni ravni za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter pravosodnega sodelovanja z Unijo ali državami članicami, pod pogojem, da zadevna tretja država ali mednarodne organizacije zagotovijo ustrezne zaščitne ukrepe v zvezi z varstvom temeljnih pravic in svoboščin posameznikov. To lahko po potrebi zajema dejavnosti subjektov, ki so jim tretje države zaupale izvajanje posebnih nalog v podporo takemu sodelovanju na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter pri pravosodnem sodelovanju. Takšni okviri za sodelovanje ali sporazumi so bili vzpostavljeni dvostransko med državami članicami in tretjimi državami ali med Evropsko unijo, Europolom in drugimi agencijami Unije ter tretjimi državami in mednarodnimi organizacijami. Organi, pristojni za nadzor organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter pravosodnih organov v skladu s to uredbo, bi morali oceniti, ali navedeni okviri za sodelovanje ali mednarodni sporazumi vključujejo ustrezne zaščitne ukrepe v zvezi z varstvom temeljnih pravic in svoboščin posameznikov. Nacionalni organi prejemniki ter institucije, organi, uradi in agencije Unije, 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 njihovo usklajevanje z zahtevami iz te uredbe.

- (23) To uredbo bilo treba uporabljati tudi za institucije, organe, urade in agencije Unije, kadar delujejo kot ponudniki ali uvajalci sistema UI.
- (24) Če in kolikor so sistemi UI s spremembami ali brez njih dani na trg ali v uporabo oziroma se uporabljajo za vojaške ali obrambne namene ali namene nacionalne varnosti, bi morali biti izključeni iz področja uporabe te uredbe ne glede na to, katera vrsta subjekta izvaja te dejavnosti, tj. ali gre za 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 naslova V, poglavje 2, PEU, za katere velja mednarodno javno pravo, ki je zato ustrežnejši pravni okvir za ureditev sistemov UI v kontekstu uporabe smrtonosne sile in drugih sistemov UI v kontekstu vojaških in obrambnih dejavnosti. Kar zadeva namene nacionalne varnosti, izključitev upravičuje tako dejstvo, da nacionalna varnost ostaja v izključni pristojnosti držav članic v skladu s členom 4(2) PEU, kot tudi posebna narava in operativne potrebe dejavnosti nacionalne varnosti ter posebna nacionalna pravila, ki se za te dejavnosti uporabljajo. Če pa se sistem UI, ki je bil razvit, dan na trg ali v uporabo oziroma 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 UI uporablja za namene, ki niso vojaški ali obrambni nameni ali nameni nacionalne varnosti, zagotoviti skladnost sistema UI s to uredbo, razen če je sistem že skladen s to uredbo. Sistemi UI, ki so dani na trg ali v uporabo za izključene namene, tj. vojaške, obrambne namene ali namene nacionalne varnosti, in enega ali več neizključenih namenov, kot so civilni nameni ali nameni preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, spadajo na področje uporabe te uredbe, njihovi ponudniki pa bi morali zagotoviti skladnost s to uredbo. V teh primerih dejstvo, da sistem UI 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 teh subjektov), da uporabljajo sisteme UI za namene nacionalne varnosti, vojaške in obrambne namene, katerih uporaba je izključena iz področja uporabe te uredbe. Sistem UI, 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.
- (25) S to uredbo bi bilo treba podpirati inovacije in spoštovati svobodo znanosti ter z njo ne bi smeli ogroziti raziskovalnih in razvojnih dejavnosti. Zato je treba iz njenega področja uporabe izključiti sisteme in modele UI, ki so bili posebej razviti in dani v uporabo izključno za znanstvene raziskave in razvoj. Poleg tega je treba zagotoviti, da ta uredba ne vpliva kako drugače na znanstvene raziskave in razvoj sistemov ali modelov UI, preden se dajo na trg ali v uporabo. Tudi kar zadeva v proizvodni usmerjene raziskave, testiranje in razvoj sistemov ali modelov UI, se določbe te uredbe ne bi smele uporabljati pred dajanjem teh sistemov in modelov v uporabo ali na trg. Ta izključitev pa ne posega v obveznost skladnosti s to uredbo, če je sistem UI, ki spada na področje uporabe te uredbe, dan na trg ali v uporabo kot rezultat take raziskovalne in razvojne dejavnosti, ter v uporabo določb o regulativnih peskovnikih za UI in testiranju v realnih razmerah. Poleg tega bi morale brez poseganja v izključitev sistemov UI, ki so posebej razviti in dani v uporabo izključno za namene znanstvenih raziskav in razvoja, za vse druge sisteme UI, ki se lahko uporabljajo za izvajanje kakršnih koli raziskovalnih in razvojnih dejavnosti, še naprej veljati določbe te uredbe. V vsakem primeru bi bilo treba vsakršno raziskovalno in razvojno dejavnost izvajati v skladu s priznanimi etičnimi in strokovnimi standardi za znanstvene raziskave ter v skladu z veljavnim pravom Unije.
- (26) Za uvedbo sorazmernega in učinkovitega sklopa zavezujočih pravil za sisteme UI bi bilo treba upoštevati 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 sistemi UI. Zato je treba prepovedati nekatere nesprejemljive prakse UI, določiti zahteve za visokotvegane sisteme UI in obveznosti za zadevne operaterje ter določiti obveznosti glede preglednosti za nekatere sisteme UI.

- (27) Čeprav je pristop, ki temelji na tveganju, podlaga za sorazmeren in učinkovit sklop zavezujočih pravil, je pomembno opozoriti na Etične smernice za zaupanja vredno umetno inteligenco iz leta 2019, ki jih je razvila neodvisna strokovna skupina na visoki ravni za umetno inteligenco (AI HLEG), ki jo je imenovala Komisija. V teh smernicah je AI HLEG razvila sedem nezavezujočih etičnih načel za UI, ki naj bi pomagala zagotoviti, da je UI zaupanja vredna in etično zanesljiva. Teh sedem načel vključuje človeško delovanje in nadzor, tehnično robustnost in varnost, zasebnost in upravljanje podatkov, preglednost, raznolikost, nediskriminacijo in pravičnost ter družbeno in okoljsko blaginjo in odgovornost. Brez poseganja v pravno zavezujoče zahteve te uredbe in katerega koli drugega veljavnega prava Unije te smernice prispevajo k oblikovanju skladne, zaupanja vredne in na človeka osredotočene UI v skladu z Listino in vrednotami, na katerih temelji Unija. V skladu s smernicami AI HLEG človeško delovanje in nadzor pomeni, da se sistemi UI razvijajo in uporabljajo kot orodje, ki služi ljudem, spoštuje človeško dostojanstvo in osebno avtonomijo ter deluje tako, da ga ljudje lahko ustrezno upravljajo in nadzorujejo. Tehnična robustnost in varnost pomeni, da se sistemi UI razvijajo in uporabljajo na način, ki omogoča robustnost v primeru težav in odpornost proti poskusom spremembe uporabe ali učinkovitosti sistema UI, ki bi lahko tretjim osebam omogočila nezakonito uporabo, in čim bolj zmanjša nenamerno škodo. Zasebnost in upravljanje podatkov pomeni, da se sistemi UI razvijajo in uporabljajo v skladu s pravili o zasebnosti in varstvu podatkov, hkrati pa obdelujejo podatke, ki izpolnjujejo visoke standarde v smislu kakovosti in celovitosti. Preglednost pomeni, da se sistemi UI razvijajo in uporabljajo na način, ki omogoča ustrezno sledljivost in razločljivost, obenem pa so ljudje seznanjeni s tem, da komunicirajo ali da so v stiku s sistemom UI, uvajalci so ustrezno obveščeni o zmogljivostih in omejitvah zadevnega sistema UI, osebe, na katere vpliva sistem UI, pa o svojih pravicah. Raznolikost, nediskriminacija in pravičnost pomeni, da se sistemi UI razvijajo in uporabljajo na način, ki vključuje različne akterje in spodbuja enakopraven dostop, enakost spolov in kulturno raznolikost, hkrati pa se preprečujejo diskriminatorni učinki in nepravilni predsodki, ki jih pravo Unije ali držav članic prepoveduje. Družbena in okoljska blaginja pomeni, da se sistemi UI razvijajo in uporabljajo na trajnosten in okolju prijazen način ter v korist vseh ljudi, hkrati pa se spremljajo in ocenjujejo dolgoročni vplivi na posameznika, družbo in demokracijo. Ta načela bi bilo treba uporabljati tudi pri zasnovi in uporabi modelov UI, kadar je mogoče. V vsakem primeru bi morala biti podlaga za pripravo kodeksov ravnanja na podlagi te uredbe. Vsi deležniki, vključno z industrijo, akademskimi krogi, civilno družbo in organizacijami za standardizacijo, naj ustrezno upoštevajo etična načela za razvoj prostovoljnih najboljših praks in standardov.
- (28) Poleg številnih koristnih uporab UI jo je mogoče tudi zlorabiti, tako da bi nastala nova in močna orodja za prakse manipulacije, izkoriščanja in družbenega nadzora. Take prakse so še posebej škodljive in zlonamerne 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, določenimi v Listini, vključno s pravico do nediskriminacije, varstva podatkov in zasebnosti ter pravicami otroka.
- (29) Z UI omogočene manipulativne tehnike se lahko uporabljajo za napeljevanje oseb k neželenemu vedenju ali za njihovo zavajanje, tako da se jih spodbuja k odločitvam na način, ki spodkopava in ovira njihovo avtonomijo, odločanje in svobodno izbiro. Dajanje na trg, dajanje v uporabo ali uporaba nekaterih sistemov UI s ciljem ali učinkom bistvenega izkrivljanja človeškega vedenja, pri čemer je verjetno, da bo nastala znatna škoda, zlasti z dovolj pomembnimi škodljivimi učinki na telesno ali duševno zdravje ali finančne interese, je še posebej nevarno oziroma nevarna in bi ga oziroma jo bilo zato treba prepovedati. Takšni sistemi UI uporabljajo subliminalne komponente, kot so zvočni, slikovni ali video dražljaji, ki jih osebe ne morejo zaznati, ker ti dražljaji presegajo človekovo dožemanje, ali druge manipulativne ali zavajajoče tehnike, ki spodkopavajo ali ovirajo posameznikovo avtonomijo, odločanje ali svobodno izbiro na načine, da se ljudje ne zavedajo teh tehnik ali pa, kadar se jih zavedajo, so kljub temu lahko zavedeni ali jih ne morejo nadzorovati ali se jim upreti. To bi bilo na primer mogoče olajšati z vmesniki stroj-možgani ali virtualno resničnostjo, saj omogočajo višjo stopnjo nadzora nad tem, kateri dražljaji so predstavljeni osebam, če lahko bistveno izkrivljajo njihovo vedenje na znatno škodljiv način. Sistemi UI lahko tudi sicer izkoriščajo šibke točke določene osebe ali skupine oseb zaradi njihove starosti, invalidnosti v smislu Direktive (EU) 2019/882 Evropskega parlamenta in Sveta ⁽¹⁶⁾ 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. Takšni sistemi UI se lahko dajo na trg ali v uporabo oziroma se uporabljajo s ciljem ali učinkom bistvenega izkrivljanja vedenja osebe, in sicer na način, ki tej ali drugi osebi ali skupinam oseb povzroči znatno škodo, vključno s škodo, ki se lahko sčasoma nakopiči, ali za katerega obstaja razumna verjetnost, da jo bo povzročil, zato bi morali

⁽¹⁶⁾ Direktiva (EU) 2019/882 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o zahtevah glede dostopnosti za proizvode in storitve (UL L 151, 7.6.2019, str. 70).

biti prepovedani. Morda ni mogoče domnevati, da obstaja namen izkrivljanja vedenja, kadar je izkrivljanje posledica dejavnikov zunaj sistema UI, na katere ponudnik ali uvajalec ne more vplivati, in sicer dejavnikov, ki jih ni mogoče razumno predvideti in jih zato ponudnik ali uvajalec sistema UI ne more zmanjšati. V vsakem primeru ni potrebno, da ima ponudnik ali uvajalec namen povzročiti znatno škodo, če takšna škoda izhaja iz manipulativnih ali izkoriščevalskih praks, ki jih omogoča UI. Prepovedi takih praks UI dopolnjujejo določbe Direktive 2005/29/ES Evropskega parlamenta in Sveta ⁽¹⁷⁾, zlasti v smislu, da so nepoštenne poslovne prakse, ki potrošnikom povzročajo gospodarsko ali finančno škodo, prepovedane v vseh okoliščinah, ne glede na to, ali se izvajajo prek sistemov UI 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 pravnimi medicinskimi standardi in zakonodajo, kot na primer izrecna privolitev posameznikov ali njihovih zakonitih zastopnikov. Poleg tega se običajne in zakonite poslovne prakse, na primer na področju oglaševanja, ki so v skladu z veljavnim pravom, same po sebi ne bi smele šteti za škodljive manipulativne z UI omogočene prakse.

- (30) Prepovedati bi bilo treba sisteme za biometrično kategorizacijo, ki temeljijo na biometričnih podatkih fizičnih oseb, kot so obraz ali prstni odtisi posameznika, za sklepanje ali ugotavljanje o političnem prepričanju posameznika, članstvu v sindikatu, verskem ali filozofskem prepričanju, rasi, spolnem življenju ali spolni usmerjenosti. Ta prepoved ne bi smela zajemati zakonitega označevanja, filtriranja ali kategorizacije naborov biometričnih podatkov, pridobljenih v skladu s pravom Unije ali nacionalnim pravom na podlagi biometričnih podatkov, kot je razvrščanje slik glede na barvo las ali oči, ki se lahko na primer uporabljajo na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.
- (31) Sistemi UI, ki zagotavljajo družbeno točkovanje fizičnih oseb s strani javnih ali zasebnih akterjev, lahko vodijo do diskriminatornih rezultatov in izključitve nekaterih skupin. Lahko kršijo pravico do dostojanstva in nediskriminacije ter vrednote enakosti in pravičnosti. Takšni sistemi UI ocenjujejo ali razvrščajo fizične osebe ali skupine fizičnih oseb na podlagi več podatkovnih točk, povezanih z njihovim družbenim vedenjem v več kontekstih ali znanih, predpostavljanih ali predvidenih osebnih ali osebnostnih značilnostih v določenih časovnih obdobjih. Število družbenih točk, dodeljenih s strani takih sistemov UI, lahko vodi do škodljivega ali neugodnega obravnavanja fizičnih oseb ali celotnih skupin le-teh 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. Sisteme UI, ki vključujejo take nesprejemljive prakse točkovanja in povzročajo takšne škodljive ali neugodne rezultate, bi bilo zato treba prepovedati. Ta prepoved ne bi smela vplivati na zakonite prakse ocenjevanja fizičnih oseb, ki se izvajajo za poseben namen v skladu s pravom Unije in nacionalnim pravom.
- (32) Uporaba sistemov UI za biometrično identifikacijo fizičnih oseb na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj je posebej hudo poseganje v pravice in svoboščine zadevnih oseb, kolikor lahko vpliva na zasebno življenje velikega dela prebivalstva, vzbuja občutek stalnega nadzora ter posredno odvraca od uresničevanja svobode zbiranja in drugih temeljnih pravic. Tehnične netočnosti sistemov UI, namenjenih za biometrično identifikacijo fizičnih oseb na daljavo, lahko vodijo do pristranskih rezultatov in diskriminatornih učinkov. Takšni možni pristranski rezultati in diskriminatorni učinki so zlasti pomembni glede na starost, etnično pripadnost, raso, spol ali invalidnost. 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 zadevnih oseb v okviru dejavnosti preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali zaradi vpliva teh dejavnosti nanje.
- (33) Zato bi bilo treba prepovedati uporabo teh sistemov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, razen v izrecno naštetih in ozko opredeljenih primerih, ko je uporaba nujno potrebna za doseg pomembnega javnega interesa, katerega pomen prevlada nad tveganji. Gre na primer za iskanje nekaterih žrtev kaznivih dejanj, vključno s pogrešanimi osebami, nekatere nevarnosti za življenje ali fizično varnost oseb ali varnost pred terorističnim napadom ter lokalizacijo ali identifikacijo storilcev ali osumljencev kaznivih dejanj, navedenih v prilogi k tej uredbi, kadar je za ta kazniva dejanja v zadevni državi članici predpisana zgornja meja zaporne kazni

⁽¹⁷⁾ Direktiva Evropskega parlamenta in Sveta 2005/29/ES z dne 11. maja 2005 o nepoštenih poslovnih praksah podjetij v razmerju do potrošnikov na notranjem trgu ter o spremembi Direktive Sveta 84/450/EGS, direktiv Evropskega parlamenta in Sveta 97/7/ES, 98/27/ES in 2002/65/ES ter Uredbe (ES) št. 2006/2004 Evropskega parlamenta in Sveta (Direktiva o nepoštenih poslovnih praksah) (UL L 149, 11.6.2005, str. 22).

ali ukrepa, vezanega na odvzem prostosti, najmanj štiri leta in so v pravu te države članice opredeljena. 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 seznam kaznivih dejanj iz priloge k tej uredbi temelji na 32 kaznivih dejanjih, naštetih v Okvirnem sklepu Sveta 2002/584/PNZ⁽¹⁸⁾, ob upoštevanju, da so nekatera od teh kaznivih dejanj v praksi verjetno pomembnejša od drugih, saj bi bila lahko uporaba biometrične identifikacije na daljavo v realnem času predvidoma potrebna in sorazmerna v zelo različnem obsegu za praktično izvajanje lokalizacije ali identifikacije storilca ali osumljenca različnih navedenih kaznivih dejanj ter ob upoštevanju verjetnih razlik v resnosti, verjetnosti in obsegu škode ali morebitnih negativnih posledic. Neposredna grožnja za življenje ali fizično varnost fizičnih oseb bi tudi lahko bila posledica resne motnje v kritični infrastrukturi, kot je opredeljena v členu 2, točka 4, Direktive (EU) 2022/2557 Evropskega parlamenta in Sveta⁽¹⁹⁾, kadar bi okvara ali uničenje take kritične infrastrukture povzročilo neposredno grožnjo za življenje ali fizično varnost osebe, med drugim tako, da bi močno škodilo zagotavljanju osnovne oskrbe prebivalstvu ali izvajanju temeljne funkcije države. Poleg tega bi morala ta uredba organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organom mejne kontrole, 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 mejne kontrole, organi, pristojni za priseljevanje, ali azilni organi možnost, da za identifikacijo oseb, ki med ugotavljanjem identitete tako ugotavljanje zavrnejo ali ne morejo 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 bi bila lahko na primer oseba, vpletena v kaznivo dejanje, ki organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ni pripravljena ali zaradi nesreče ali zdravstvenega stanja ne more razkriti svoje identitete.

- (34) Za zagotovitev odgovorne in sorazmerne uporabe teh sistemov je pomembno tudi določiti, da bi bilo treba v vsakem od teh izrecno 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 uporabo sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj uporabljati le za potrditev identitete specifično ciljnega posameznika in bi morala biti omejena na to, kar je nujno potrebno za časovno obdobje ter geografsko in osebno področje uporabe, pri čemer je treba upoštevati zlasti dokaze ali znake v zvezi z grožnjami, žrtvami ali storilcem. Uporaba sistema za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih se dovoli le, če je ustrezní organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj opravil oceno učinkov na temeljne pravice in, če v tej uredbi ni določeno drugače, sistem registriral v podatkovni zbirki, kot je določeno v tej uredbi. Referenčna podatkovna zbirka o osebah bi morala biti primerna za vsak primer uporabe v vsakem od navedenih primerov.

- (35) 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 sodnega organa ali neodvisnega upravnega organa države članice, katerega odločitev je zavezujoča. Tako dovoljenje bi bilo treba načeloma pridobiti pred uporabo sistema UI za identifikacijo osebe ali oseb. Izjeme od tega pravila bi morale biti dovoljene v ustrezno utemeljenih nujnih primerih iz nujnih razlogov, tj. v primerih, ko je uporaba zadevnih sistemov potrebna do te mere, da je dejansko in objektivno nemogoče pridobiti dovoljenje pred začetkom uporabe sistema UI. V takih nujnih primerih bi bilo treba uporabo sistema UI omejiti na absolutni minimum, zanj 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 moral organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v takšnih primerih zaprositi za tako dovoljenje, hkrati pa navesti razloge, zakaj ga ni mogel zahtevati prej, brez nepotrebnega odlašanja in najpozneje v 24 urah. Če se tako dovoljenje zavrne, bi bilo treba takoj prenehati uporabljati sisteme za biometrično identifikacijo v realnem času, povezane s tem dovoljenjem, vse podatke, povezane s tako uporabo, pa bi bilo treba zavreči in izbrisati. Takšni podatki vključujejo vhodne podatke, ki jih sistem UI pridobi neposredno med

⁽¹⁸⁾ 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).

⁽¹⁹⁾ Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114/ES (UL L 333, 27.12.2022, str. 164).

uporabo takega sistema, ter rezultate in izhodne podatke uporabe, povezane s tem dovoljenjem. Ne bi smeli vključevati vhodnih podatkov, ki so zakonito pridobljeni v skladu z drugim pravom Unije ali nacionalnim pravom. V nobenem primeru odločitve, ki bi imela škodljiv pravni učinek na osebo, ne bi smeli sprejeti izključno na podlagi izhodnih podatkov sistema za biometrično identifikacijo na daljavo.

- (36) Da bi lahko ustrezeni organ za nadzor trga in nacionalni organ za varstvo podatkov izvajala svoje naloge v skladu z zahtevami iz te uredbe in nacionalnih pravil, bi ju bilo treba obvestiti o vsaki uporabi sistema za biometrično identifikacijo v realnem času. Organi za nadzor trga in nacionalni organi za varstvo podatkov, ki so bili obveščeni, bi morali Komisiji predložiti letno poročilo o uporabi sistemov za biometrično identifikacijo v realnem času.
- (37) 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 kolikor se je zadevna država članica odločila izrecno predvideti možnost odobritve take uporabe v svojih podrobnih pravilih nacionalnega prava. Zato imajo države članice na podlagi te uredbe še naprej pravico, da take možnosti sploh ne predvidijo ali da jo predvidijo le za nekatere cilje, ki lahko upravičijo dovoljeno uporabo, opredeljeno v tej uredbi. O takih nacionalnih predpisih bi bilo treba uradno obvestiti Komisijo v 30 dneh po njihovem sprejetju.
- (38) Uporaba sistemov UI 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 na podlagi člena 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 na podlagi te uredbe in veljavnimi podrobnimi pravili nacionalnega prava, na podlagi katerih se lahko to dovoljenje uveljavi.
- (39) Pri vsaki obdelavi biometričnih podatkov in drugih osebnih podatkov, vključenih v uporabo sistemov UI 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, člen 9(1) Uredbe (EU) 2016/679 in člen 10(1) Uredbe (EU) 2018/1725 prepovedujeta obdelavo biometričnih podatkov, za katere veljajo omejene izjeme, kot so določene v navedenih členih. Pri uporabi člena 9(1) Uredbe (EU) 2016/679 za uporabo biometrične identifikacije na daljavo za namene, ki niso preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, že veljajo odločitve o prepovedi s strani nacionalnih organov za varstvo podatkov.
- (40) 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 PEU in PDEU, pravila iz člena 5(1), prvi pododstavek, točka (g), kolikor se uporabljajo za uporabo sistemov biometrične kategorizacije za dejavnosti na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah, iz člena 5(1), prvi pododstavek, točka (d), v obsegu, v katerem se uporablja za uporabo sistemov UI, zajetih v navedeni določbi, iz člena 5(1), prvi pododstavek, točka (h), 5(2) do (6) in iz člena 26(10) 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.
- (41) V skladu s členoma 2 in 2a Protokola št. 22 o stališču Danske, ki je priložen PEU in PDEU, Danske ne zavezujejo in se zanj ne uporabljajo pravila iz člena 5(1), prvi pododstavek, točka (g), kolikor se uporabljajo za uporabo sistemov biometrične kategorizacije za dejavnosti na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah, iz člena 5(1), prvi pododstavek, točka (d), v obsegu, v katerem se uporabljata za uporabo sistemov UI, zajetih

v navedeni določbi, iz člena 5(1), prvi pododstavek, točka (h), člena 5(2) do (6) in iz člena 26(10) 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.

- (42) V skladu z domnevo nedolžnosti bi bilo treba fizične osebe v Uniji zmeraj presoјati glede na njihovo dejansko ravnanje. Nikoli jih ne bi smeli presoјati na podlagi ravnanja, ki ga predvideva UI zgolj na podlagi njihovega oblikovanja profilov, osebnostnih lastnosti ali značilnosti, kot so državljanstvo, kraj rojstva, kraj prebivališča, število otrok, stopnja zadolženosti ali vrsta avtomobila, brez utemeljenih razlogov za sum, da je bila ta oseba vpletena v kriminalno dejavnost na podlagi objektivnih preverljivih dejstev in brez človeške ocene. Zato bi bilo treba prepovedati ocene tveganja, ki se izvajajo v zvezi s fizičnimi osebami, da se oceni verjetnost, da bodo te osebe storile kaznivo dejanje, ali da se predvidi dejansko ali potencialno kaznivo dejanje samo na podlagi oblikovanja profilov teh fizičnih oseb ali ocene njihovih osebnostnih lastnosti in značilnosti. V nobenem primeru ta prepoved ne vključuje ali se ne nanaša na analizo tveganja, ki ne temelji na oblikovanju profilov oseb ali na osebnostnih lastnostih in značilnostih posameznikov, kot so sistemi UI, ki uporabljajo analizo tveganja za oceno verjetnosti finančnih goljufij s strani podjetij na podlagi sumljivih transakcij ali orodij za analizo tveganja, ki omogočajo napovedovanje verjetnosti lokalizacije prepovedanih drog ali nezakonitega blaga s strani carinskih organov, na primer na podlagi znanih trgovskih poti.
- (43) Treba bi bilo prepovedati dajanje na trg, dajanje v uporabo za ta posebni namen ali uporabo sistemov UI, ki ustvarjajo ali širijo podatkovne zbirke za prepoznavanje obrazov z neciljnim odvzemom podob obraza z interneta ali posnetkov sistema CCTV, saj ta praksa prispeva k občutku množičnega nadzora in lahko povzroči hude kršitve temeljnih pravic, vključno s pravico do zasebnosti.
- (44) Obstajajo resni pomisleki glede znanstvene podlage sistemov UI, katerih namen je prepoznavanje čustev ali sklepanje o njih, zlasti zato, ker se izražanje čustev med kulturami in okoliščinami ter celo pri enem samem posamezniku zelo razlikuje. Med ključnimi pomanjkljivostmi takšnih sistemov so omejena zanesljivost, premajhna specifičnost in omejena možnost posplošitve. Zato lahko sistemi UI, ki prepoznavajo čustva ali namere fizičnih oseb na podlagi svojih biometričnih podatkov ali ki iz njih sklepajo, vodijo do diskriminatornih rezultatov ter posegajo v pravice in svobode zadevnih oseb. Glede na neravnovesje moči v kontekstu dela ali izobraževanja ter intruzivne narave teh sistemov bi lahko takšni sistemi povzročili škodljivo ali neugodno obravnavo nekaterih fizičnih oseb ali celotnih skupin fizičnih oseb. Zato bi bilo treba prepovedati dajanje na trg, dajanje v uporabo ali uporabo sistemov UI, namenjenih odkrivanju čustvenega stanja posameznikov v situacijah, povezanih z delovnim mestom in izobraževanjem. Ta prepoved ne bi smela zajemati sistemov UI, danih na trg izključno iz zdravstvenih ali varnostnih razlogov, kot so sistemi za terapevtsko uporabo.
- (45) Ta uredba ne bi smela vplivati na prakse, ki jih prepoveduje pravo Unije, vključno s pravom o varstvu podatkov, pravom o nediskriminaciji, pravom o varstvu potrošnikov in konkurenčnim pravom.
- (46) Visokotvegane sisteme UI bi bilo treba dati na trg Unije ali v uporabo ali jih uporabiti le, če izpolnjujejo nekatere obvezne zahteve. Navedene zahteve bi morale zagotoviti, da visokotvegani sistemi UI, 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. Kot je pojasnjeno v obvestilu Komisije „Modri vodnik“ o izvajanju pravil EU o proizvodih iz leta 2022 ⁽²⁰⁾, je na podlagi novega zakonodajnega okvira splošno pravilo, da se več kot en pravni akt harmonizacijske zakonodaje Unije, kot sta uredbi (EU) 2017/745 ⁽²¹⁾ in (EU) 2017/746 ⁽²²⁾ Evropskega parlamenta in Sveta ter Direktiva 2006/42/ES Evropskega parlamenta in Sveta ⁽²³⁾, lahko uporablja za en proizvod, saj se lahko omogočanje dostopnosti ali dajanje v uporabo izvede le, če je proizvod skladen z vso veljavno harmonizacijsko zakonodajo Unije. Da bi zagotovili doslednost in preprečili nepotrebna upravna bremena ali

⁽²⁰⁾ UL C 247, 29.6.2022, str. 1.

⁽²¹⁾ 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).

⁽²²⁾ 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).

⁽²³⁾ 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).

stroške, bi morali ponudnikom proizvoda, ki vsebuje enega ali več visokotveganih sistemov UI, za katere se uporabljajo zahteve iz te uredbe in harmonizacijske zakonodaje Unije iz priloge k tej uredbi, omogočiti prožnost glede operativnih odločitev o tem, kako na optimalen način zagotoviti skladnost proizvoda, ki vsebuje enega ali več sistemov UI, z vsemi veljavnimi zahtevami harmonizacijske zakonodaje Unije. Sistemi UI, opredeljeni kot visokotvegani, 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.

- (47) Sistemi UI bi lahko imeli škodljiv učinek na zdravje in varnost ljudi, zlasti kadar taki sistemi delujejo kot varnostne 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 s sistemi UI. Vse bolj avtonomni roboti, ki se uporabljajo v proizvodnji ali za osebno pomoč in oskrbo, bi morali biti na primer sposobni varno delovati in opravljati svoje funkcije v kompleksnih 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.
- (48) Pri razvrstitvi sistema UI med sisteme visokega tveganja je zlasti pomemben obseg škodljivega vpliva sistema UI na temeljne pravice, varovane z Listino. Te pravice vključujejo pravico do človekovega dostojanstva, spoštovanja zasebnega in družinskega življenja, varstvo osebnih podatkov, svobodo izražanja in obveščanja, svobodo zbiranja in združevanja, pravico do nediskriminacije, pravico do izobraževanja, varstvo potrošnikov, pravice delavcev, pravice invalidov, enakost spolov, pravice intelektualne lastnine, pravico do učinkovitega pravnega sredstva in nepristranskega sodišča, pravico do obrambe in domneve nedolžnosti ter pravico do dobrega upravljanja. Poleg teh pravic je treba poudariti tudi dejstvo, da imajo otroci posebne pravice, zapisane v členu 24 Listine in v Konvenciji Združenih narodov o otrokovih pravicah (v zvezi z digitalnim okoljem ter podrobneje opredeljene v splošni pripombi št. 25 KZNOP), 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 sistem UI, 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.
- (49) Kar zadeva visokotvegane sisteme UI, ki so varnostne komponente proizvodov ali sistemov ali so sami proizvodi ali sistemi, ki spadajo na področje uporabe Uredbe (ES) št. 300/2008 Evropskega parlamenta in Sveta ⁽²⁴⁾, Uredbe (EU) št. 167/2013 Evropskega parlamenta in Sveta ⁽²⁵⁾, Uredbe (EU) št. 168/2013 Evropskega parlamenta in Sveta ⁽²⁶⁾, Direktive 2014/90/EU Evropskega parlamenta in Sveta ⁽²⁷⁾, Direktive (EU) 2016/797 Evropskega parlamenta in Sveta ⁽²⁸⁾, Uredbe (EU) 2018/858 Evropskega parlamenta in Sveta ⁽²⁹⁾, Uredbe (EU) 2018/1139 Evropskega

⁽²⁴⁾ 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);

⁽²⁵⁾ 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).

⁽²⁶⁾ 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).

⁽²⁷⁾ 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).

⁽²⁸⁾ 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).

⁽²⁹⁾ 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).

parlamenta in Sveta ⁽³⁰⁾ ter Uredbe (EU) 2019/2144 Evropskega parlamenta in Sveta ⁽³¹⁾, je primerno spremeniti navedene akte, da bi zagotovili, da Komisija na podlagi tehničnih in regulativnih posebnosti vsakega sektorja ter brez poseganja v obstoječe mehanizme upravljanja, ugotavljanja skladnosti in izvrševanja ter delo organov, določenih v njih, pri sprejemanju ustreznih delegiranih ali izvedbenih aktov v skladu z navedenimi akti upošteva obvezne zahteve za visokotvegane sisteme UI iz te uredbe.

- (50) Kar zadeva sisteme UI, ki so varnostne komponente proizvodov ali so sami proizvodi s področja uporabe določene harmonizacijske zakonodaje Unije, navedene v prilogi k tej uredbi, jih je primerno na podlagi te uredbe razvrstiti med sisteme visokega tveganja, če je zadevni proizvod v postopku ugotavljanja skladnosti pri organu, ki izvaja ugotavljanje skladnosti s strani tretjih oseb na podlagi ustrezne harmonizacijske zakonodaje 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 in vitro diagnostični medicinski pripomočki, avtomobili in letala.
- (51) Razvrstitev sistema UI kot visokotveganega na podlagi te uredbe ne bi smela nujno pomeniti, da se proizvod, katerega varnostna komponenta je sistem UI, ali sam sistem UI kot proizvod šteje za visokotvegan na podlagi meril iz ustrezne harmonizacijske zakonodaje Unije, ki se uporablja za proizvod. To zlasti velja za uredbi (EU) 2017/745 in (EU) 2017/746, pri katerih je ugotavljanje skladnosti, ki ga opravi tretja oseba, zagotovljeno za izdelke srednjega in visokega tveganja.
- (52) Kar zadeva samostojne sisteme UI in zlasti visokotvegane sisteme UI, razen tistih, ki so varnostne komponente proizvodov ali ki so sami proizvodi, jih je primerno razvrstiti kot sisteme visokega tveganja, če glede na svoj predvideni namen predstavljajo visoko 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. Opredelitev teh sistemov temelji na isti metodologiji in merilih, kot so predvideni tudi za morebitne prihodnje spremembe seznama visokotveganih sistemov UI, za katere bi bilo treba Komisijo pooblastiti, da jih sprejme z delegiranimi akti, da bi upoštevali hiter tehnološki razvoj in morebitne spremembe v uporabi sistemov UI.
- (53) Treba je tudi pojasniti, da lahko obstajajo posebni primeri, v katerih sistemi UI, ki se nanašajo na vnaprej določena področja, navedena v tej uredbi, ne povzročajo znatnega tveganja škode za pravne interese, zaščitene na teh področjih, ker ne vplivajo bistveno na odločanje ali ne škodujejo bistveno tem interesom. Za namene te uredbe bi bilo treba sistem UI, ki ne vpliva bistveno na izid odločanja, razumeti kot sistem UI, ki ne vpliva na vsebino in s tem na rezultat odločanja, bodisi človeškega ali avtomatiziranega. Sistem UI, ki ne vpliva bistveno na izid odločanja, bi lahko vključeval primere, v katerih je izpolnjen eden ali več naslednjih pogojev. Prvi tak pogoj bi moral biti, da je sistem UI namenjen opravljanju ozke postopkovne naloge, kot je sistem UI, ki nestrukturirane podatke pretvori v strukturirane podatke, sistem UI, ki prejete dokumente razvršča v kategorije, ali sistem UI, ki se uporablja za odkrivanje duplikatov v številnih aplikacijah. Te naloge so tako ozke in omejene, da predstavljajo le omejena tveganja, ki se z uporabo sistema UI v okviru, ki je v prilogi k tej uredbi naveden kot uporaba, povezana z visokim tveganjem, ne povečajo. Drugi pogoj bi moral biti, da je namen naloge, ki jo opravlja sistem UI, izboljšati rezultat

⁽³⁰⁾ 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).

⁽³¹⁾ 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).

predhodno zaključene človeške dejavnosti, ki bi lahko bila pomembna za namene visokotvegane uporabe, navedene v prilogi k tej uredbi. Glede na te značilnosti sistem UI zagotavlja le dodatno plast človeške dejavnosti s posledično manjšim tveganjem. Ta pogoj bi se na primer uporabljal za sisteme UI, katerih namen je izboljšati jezik, ki se uporablja v predhodno pripravljenih dokumentih, na primer v zvezi s poklicnim tonom, akademskim slogom jezika ali uskladitvijo besedila s sporočili določene blagovne znamke. Tretji pogoj bi moral biti, da je sistem UI namenjen odkrivanju vzorcev odločanja ali odstopanj od vzorcev predhodnega odločanja. Tveganje bi se zmanjšalo, ker uporaba sistema UI sledi predhodno opravljeni človeški oceni in ni namenjena temu, da bi jo nadomestila ali nanjo vplivala brez ustreznega človeškega pregleda. Takšni sistemi UI vključujejo na primer sisteme, ki se lahko glede na določen vzorec, po katerem neki učitelj ocenjuje, uporabijo za naknadno preverjanje, ali je učitelj morda odstopal od tega vzorca, da bi opozorili na morebitne nedoslednosti ali nepravilnosti. Četrty pogoj bi moral biti, da je sistem UI namenjen opravljanju naloge, ki je le pripravljalna za oceno, relevantno za namene sistemov UI, navedenih v prilogi k tej uredbi, s čimer bi bil morebitni učinek izhodnih podatkov sistema zelo majhen v smislu tveganja, ki ga je treba upoštevati pri oceni. Ta pogoj med drugim zajema pametne rešitve za ravnanje z datotekami, ki vključujejo različne funkcije, kot so indeksiranje, iskanje, obdelava besedil in govora ali povezovanje podatkov z drugimi viri podatkov, ali sisteme UI, ki se uporabljajo za prevajanje prvotnih dokumentov. V vsakem primeru bi bilo treba šteti, da sistemi UI, ki se uporabljajo v primerih uporabe visokega tveganja, navedeni v prilogi k tej uredbi, predstavljajo znatno tveganje škode za zdravje, varnost ali temeljne pravice, če sistem UI vključuje oblikovanje profilov v smislu člena 4, točka 4, Uredbe (EU) 2016/679 ali člena 3, točka 4, Direktive (EU) 2016/680 ali člena 3, točka 5, Uredbe (EU) 2018/1725. Da bi zagotovili sledljivosti in preglednost, bi moral ponudnik, ki meni, da sistem UI na podlagi zgoraj navedenih pogojev ne predstavlja visokega tveganja, pripraviti dokumentacijo o oceni, preden se ta sistem da na trg ali v uporabo, in bi moral to dokumentacijo na zahtevo predložiti pristojnim nacionalnim organom. Takšen ponudnik bi moral sistem UI registrirati v podatkovni zbirki EU, vzpostavljeni s to uredbo. Da bi zagotovili dodatne smernice za praktično izvajanje pogojev, pod katerimi sistemi UI navedeni v prilogi k tej uredbi, izjemoma ne predstavljajo visokega tveganja, bi morala Komisija po posvetovanju z Odborom zagotoviti smernice, v katerih bi bilo določeno, da se praktično izvajanje dopolni s celovitim seznamom praktičnih primerov uporabe visoko tveganih sistemov UI in sistemov UI, ki to niso.

- (54) Ker so biometrični podatki posebna kategorija osebnih podatkov, je primerno, da se več kritičnih primerov uporabe biometričnih sistemov razvrsti kot visokotvegane, če je njihova uporaba dovoljena na podlagi ustreznega prava Unije in nacionalnega prava. Tehnične netočnosti sistemov UI, namenjenih za biometrično identifikacijo fizičnih oseb na daljavo, lahko vodijo do pristranskih rezultatov in diskriminatornih učinkov. Tveganje takšnih pristranskih rezultatov in diskriminatornih učinkov je zlasti pomembno v zvezi s starostjo, etnično pripadnostjo, raso, spolom ali invalidnostjo. Glede na tveganja, ki jih predstavljajo sistemi za biometrično identifikacijo na daljavo, bi jih bilo treba razvrstiti kot sisteme visokega tveganja. Takšna razvrstitev izključuje sisteme UI za biometrično preverjanje, tudi avtentikacijo, katerih edini namen je potrditi, da je določena fizična oseba res ta, za katero se predstavlja, in potrditi identiteto fizične osebe izključno zaradi dostopa do storitve, odklepanja naprave ali varnega dostopa do prostorov. Poleg tega bi bilo kot sisteme visokega tveganja treba razvrstiti sisteme UI, namenjene uporabi za biometrično kategorizacijo v skladu z občutljivimi lastnostmi ali značilnostmi, zaščitnimi na podlagi člena 9(1) Uredbe (EU) 2016/679 na podlagi biometričnih podatkov, če ti niso prepovedani s to uredbo, in sisteme za prepoznavanje čustev, ki niso prepovedani s to uredbo. Biometrični sistemi, ki naj bi se uporabljali izključno za omogočanje ukrepov za kibernetko varnost in varstvo osebnih podatkov, ne bi smeli šteti za visokotvegane sisteme UI.
- (55) V zvezi z upravljanjem in delovanjem kritične infrastrukture je primerno, da se sistemi UI, namenjeni uporabi kot varnostne komponente pri upravljanju in delovanju kritične digitalne infrastrukture, navedene v točki 8 iz Priloge k Direktivi (EU) 2022/2557, cestnega prometa ter oskrbi z vodo, plinom, ogrevanjem in električno energijo, razvrstijo kot sistemi visokega tveganja, saj lahko njihovo nedelovanje ali okvara delovanja ogrožajo 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 za neposredno zaščito fizične celovitosti kritične infrastrukture ali zdravja in varnosti oseb in premoženja, vendar niso potrebne za delovanje sistema. Nedelovanje ali okvara takih komponent bi lahko

povzročila neposredno tveganje za fizično celovitost kritične infrastrukture ter posledično tveganje za zdravje in varnost oseb in premoženja. Komponente, namenjene izključno za uporabo v namene kibernetske varnosti, ne bi smele šteti za varnostne komponente. Primeri varnostnih komponent takšne kritične infrastrukture lahko vključujejo sisteme za spremljanje vodnega tlaka ali sisteme za upravljanje požarnega alarma v okviru centrov računalništva v oblaku.

- (56) Uvajanje sistemov UI v izobraževanju je pomembno za spodbujanje visokokakovostnega digitalnega izobraževanja in usposabljanja, da bi vsem učencem in učiteljem omogočili pridobivanje in deljenje potrebnih digitalnih spretnosti in kompetenc, vključno z medijsko pismenostjo in kritičnim razmišljanjem ter s tem dejavno sodelovanje v gospodarstvu, družbi in demokratičnih procesih. Vendar bi bilo treba sisteme UI, ki se uporabljajo v izobraževanju ali poklicnem usposabljanju, zlasti za določanje dostopa ali sprejema ali za razvrščanje fizičnih oseb v izobraževalne ustanove ali programe in ustanove ali programe za poklicno usposabljanje na vseh ravneh za ocenjevanje učnih izidov oseb, ustrezne ravni izobrazbe posameznika in materialno vplivanje na raven izobraževanja in usposabljanja, ki jo bodo posamezniki prejeli ali bodo lahko dostopali do nje ali za spremljanje in odkrivanje prepovedanega vedenja študentov med testi, razvrstiti kot visokotvegane sisteme UI, saj lahko določajo izobraževalni in poklicni potek življenja osebe in lahko zato vplivajo na zmožnost te osebe, da si zagotovi preživetje. Če so takšni sistemi neustrezno zasnovani in uporabljeni, lahko zlasti hudo posegajo v pravico do izobraževanja in usposabljanja ter pravico do nediskriminacije in ju lahko kršijo ter ohranjajo vzorce diskriminacije iz preteklosti, na primer žensk, nekaterih starostnih skupin, invalidov ali oseb določenega rasnega ali etničnega porekla ali spolne usmerjenosti.
- (57) Sisteme UI, ki se uporabljajo pri zaposlovanju, upravljanju delavcev in dostopu do samozaposlitve, zlasti za zaposlovanje in izbor oseb, za sprejemanje odločitev, ki vplivajo na delovne pogoje, napredovanje ali prenehanje pogodbenih delovnih razmerij, za dodeljevanje nalog na podlagi individualnega vedenja, osebnih lastnosti ali značilnosti ter za spremljanje ali ocenjevanje oseb v z delom povezanih pogodbenih razmerjih, bi bilo treba prav tako razvrstiti med sisteme visokega tveganja, saj lahko ti sistemi občutno vplivajo na prihodnje poklicne možnosti, možnosti preživetja teh oseb in pravice delavcev. Ustrezna pogodbeno delovna razmerja bi morala smiselno vključevati zaposlene in osebe, ki zagotavljajo storitve preko platform, ki so navedene v delovnem programu Komisije za leto 2021. 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 sistemi UI, ki se uporabljajo za spremljanje učinkovitost in vedenja teh oseb, lahko ogrožajo njihove temeljne pravice do varstva podatkov in zasebnosti.
- (58) Drugo področje, na katerem je treba posebno pozornost nameniti uporabi sistemov UI, 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 fizične osebe, ki zaprosijo za ali od javnih organov prejemajo bistvene ugodnosti in storitve javne pomoči, in sicer zdravstvene storitve, dajatve socialne varnosti, socialne storitve, ki zagotavljajo zaščito v primerih, kot so materinstvo, bolezni, nesreče pri delu, odvisnost ali starost ter izguba zaposlitve ter socialna in stanovanjska pomoč, so običajno odvisne od teh ugodnosti in storitev ter so v ranljivem položaju v odnosu do odgovornih organov. Če se sistemi UI uporabljajo za določanje, ali naj organi take ugodnosti in storitve odobrijo, zavrnejo, zmanjšajo, preklicajo ali zahtevajo povračilo, vključno s tem, ali so upravičenci legitimno upravičeni do takih ugodnosti ali storitev, lahko ti sistemi pomembno vplivajo na preživetje oseb in kršijo njihove temeljne pravice, kot so pravica do socialne zaščite, nediskriminacije, človekovega dostojanstva ali učinkovitega pravnega sredstva, in bi zato morali biti opredeljeni kot visokotvegani sistemi UI. 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 sistemov UI, če ti sistemi ne pomenijo visokega tveganja za pravne in fizične osebe. Poleg tega bi bilo treba sisteme UI, ki se uporabljajo za ocenjevanje kreditne ocene ali kreditne sposobnosti fizičnih oseb, razvrstiti kot visokotvegane sisteme UI, saj določajo dostop teh oseb do finančnih sredstev ali bistvenih storitev, kot so stanovanja, električna energija in telekomunikacijske storitve. Sistemi UI, ki se uporabljajo v te namene, lahko povzročijo diskriminacijo oseb ali skupin in ohranijo vzorce diskriminacije iz preteklosti, na primer na podlagi rasnega ali etničnega porekla, spola, invalidnosti, starosti ali spolne usmerjenosti, ali ustvarijo nove oblike diskriminatornih vplivov. Vendar sistemi UI, ki so v pravi Unije določeni za namene odkrivanja goljufij pri ponujanju finančnih storitev ter za bonitetne namene za izračun kapitalskih zahtev kreditnih institucij in zavarovalnic, na podlagi te uredbe ne bi smeli šteti za sisteme visokega tveganja. Poleg tega lahko sistemi UI, namenjeni za oceno tveganja in

oblikovanje cen v zvezi s fizičnimi osebami za zdravstveno in življenjsko zavarovanje, tudi pomembno vplivajo na preživetje oseb in lahko, če niso ustrezno zasnovani, razviti in uporabljeni, kršijo njihove temeljne pravice in povzročijo resne posledice za življenje in zdravje ljudi, vključno s finančno izključenostjo in diskriminacijo. Poleg tega bi bilo treba sisteme UI, ki se uporabljajo za ocenjevanje in razvrščanje klincev v sili fizičnih oseb ali za pošiljanje ali določanje prednosti pri napotitvi služb za ukrepanje ob nesrečah, vključno s policijo, gasilci in medicinsko pomočjo, ter sistemih triaže pacientov v nujnem zdravstvenem varstvu, razvrstiti med sisteme visokega tveganja, saj sprejemajo odločitve v zelo kritičnih razmerah za življenje in zdravje oseb ter njihovo premoženje.

- (59) Glede na vlogo in odgovornost organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, je za njihove ukrepe, ki vključujejo nekatere uporabe sistemov UI, značilna precejšnja stopnja neravnovesja moči, kar lahko vodi do nadzora, prijetja ali odvzema prostosti fizične osebe ter drugih škodljivih vplivov na temeljne pravice, ki jih zagotavlja Listina. Zlasti če se sistem UI ne uči z visokokakovostnimi podatki, ne izpolnjuje ustreznih zahtev glede zmogljivosti, točnosti ali robustnosti ali ni ustrezno zasnovan in testiran, preden je dan na trg ali na kakšen drug način v uporabo, lahko ljudi izpostavi na diskriminatoren ali kako drugače napačen ali nepravilen 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 sistemi UI niso dovolj pregledni, obrazložljivi in dokumentirani. Zato je primerno, da se številni sistemi UI, kolikor je njihova uporaba dovoljena na podlagi zadevnega prava Unije in nacionalnega prava, namenjeni uporabi v okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, razvrstijo med sisteme visokega tveganja, kjer so točnost, zanesljivost in preglednost še posebej pomembni, da se preprečijo škodljivi vplivi, ohrani zaupanje javnosti ter zagotovita odgovornost in učinkovito sodno varstvo. Glede na naravo dejavnosti in s tem povezana tveganja bi morali ti visokotvegani sistemi UI vključevati zlasti sisteme UI, ki so namenjeni uporabi s strani ali v imenu organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali institucij, organov, uradov ali agencij Unije v podporo tem organom pri ocenjevanju tveganja, da fizična oseba postane žrtev kaznivih dejanj, kot so poligrafi in podobna orodja, za ocenjevanje zanesljivosti dokazov med preiskovanjem ali pregonom kaznivih dejanj in, če to ni prepovedano na podlagi te uredbe, za ocenjevanje tveganja, da fizična oseba stori ali ponovi kaznivo dejanje, ne izključno na podlagi oblikovanja profilov fizičnih oseb ali ocene osebnostnih lastnosti in značilnosti ali preteklega kaznivega ravnanja fizičnih oseb ali skupin, za oblikovanje profilov med odkrivanjem, preiskovanjem ali pregonom kaznivih dejanj. Sistemi UI, posebej namenjeni uporabi v upravnih postopkih s strani davčnih in carinskih organov ter finančnoobveščevalnih enot, ki izvajajo upravne naloge analiziranja informacij na podlagi prava Unije o preprečevanju pranja denarja, ne bi smeli biti opredeljeni kot visokotvegani sistemi UI, ki jih uporabljajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj za namen preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj. Organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in drugi ustrezní organi orodij UI ne bi smeli uporabljati tako, da bi postala dejavnik pri neenakosti ali izključenosti. Ne bi smeli zanemariti vpliva uporabe orodij UI na pravice osumljencev do obrambe, zlasti težav pri pridobivanju smiselnih informacij o delovanju teh sistemov in posledičnih težav pri izpodbijanju njihovih rezultatov na sodišču, zlasti s strani fizičnih oseb, ki so predmet preiskave.

- (60) Sistemi UI, ki se uporabljajo pri upravljanju migracij, azila in nadzora meja, vplivajo na osebe, ki so pogosto v posebej ranljivem položaju ter so odvisne od izida ukrepov pristojnih javnih organov. Točnost, nediskriminatornost in preglednost sistemov UI, ki se uporabljajo v teh kontekstih, so zato zlasti pomembni za zagotavljanje spoštovanja temeljnih pravic zadevnih oseb, zlasti njihovih pravic do prostega gibanja, nediskriminacije, varstva zasebnega življenja in osebnih podatkov, mednarodnega varstva in dobrega upravljanja. Zato je primerno, da se med sisteme visokega tveganja razvrstijo sistemi UI, ki so na podlagi ustreznega prava Unije in nacionalnega prava dovoljeni za uporabo s strani ali v imenu pristojnih javnih organov ali institucij, organov, uradov ali agencij Unije, zadolženih za naloge na področju migracij, azila in upravljanja nadzora meja, kot so poligrafi in podobna orodja, 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, vključno s povezano oceno zanesljivosti dokazov, prošelj za azil, vizumov in dovoljenj za prebivanje ter s tem povezanih pritožb zaradi ugotavljanja upravičenosti fizičnih oseb, ki zaprosijo za status, za namene odkrivanja, priznavanja ali identifikacije fizičnih oseb v okviru upravljanja migracij, azila in nadzora meja, z izjemo preverjanja potnih listin. Sistemi UI na področju migracij, azila in upravljanja nadzora meja, ki jih zajema ta uredba, bi morali biti skladni z ustreznimi postopkovnimi zahtevami iz Uredbe (ES) št. 810/2009 Evropskega parlamenta in Sveta⁽³²⁾, Direktive 2013/32/EU

⁽³²⁾ 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).

Evropskega parlamenta in Sveta ⁽³³⁾ ter drugega ustreznega prava Unije. Države članice ali institucije, organi, uradi ali agencije Unije v nobenem primeru ne bi smeli uporabljati sistemov UI na področju migracij, azila in upravljanja nadzora meja kot sredstvo za izogibanje svojim mednarodnim obveznostim iz Konvencije ZN o statusu beguncev, podpisane v Ženevi 28. julija 1951, kakor je bila spremenjena s Protokolom z dne 31. januarja 1967. Prav tako se ne smejo uporabljati za kakršno koli kršitev načela nevrčanja ali za odrekanje varnih in učinkovitih zakonitih poti na ozemlje Unije, vključno s pravico do mednarodne zaščite.

- (61) Nekatere sisteme UI, namenjene razsojanju in demokratičnim procesom, bi bilo treba razvrstiti med sisteme visokega tveganja zaradi njihovega potencialno pomembnega vpliva na demokracijo, pravno državo, osebne svoboščine ter pravico do učinkovitega pravnega sredstva in nepristranskega sodišča. Zlasti zato, da bi zmanjšali tveganja morebitnih pristranskosti, napak in nepreglednosti, je primerno, da se visokotvegani sistemi UI, namenjeni uporabi s strani sodnega organa ali v njegovem imenu za pomoč sodnim organom pri raziskovanju in razlagi dejstev in prava ter pri uporabi prava za konkreten sklop dejstev, opredelijo kot sistemi visokega tveganja. Tudi sisteme UI, ki naj bi jih za te namene uporabljali organi za alternativno reševanje sporov, bi bilo treba šteti za sisteme visokega tveganja, če imajo rezultati postopkov alternativnega reševanja sporov pravne učinke za stranke. Orodja UI se lahko uporabljajo kot pomoč sodnikom pri odločanju ali podpora neodvisnosti sodstva, vendar jih ne bi smela nadomeščati: končno odločanje mora ostati dejavnost, ki jo vodi človek. Razvrščanje sistemov UI kot sistemov visokega tveganja pa se ne bi smelo uporabljati tudi za sisteme UI, namenjene izključno pomožnim upravnim dejavnostim, ki ne vplivajo na dejansko razsojanje v posameznih primerih, kot so anonimizacija ali psevdonimizacija sodnih odločb, dokumentov ali podatkov, komunikacije med osebjem ali upravnih nalog.
- (62) Brez poseganja v pravila iz Uredbe (EU) 2024/900 Evropskega parlamenta in Sveta ⁽³⁴⁾ ter za obravnavanje tveganj neupravičenega zunanjega poseganja v volilno pravico iz člena 39 Listine in nesorazmernih učinkov na demokracijo in pravno državo bi bilo treba sisteme UI, namenjene vplivanju na izid volitev ali referendumov ali na volilno vedenje fizičnih oseb pri glasovanju na volitvah ali referendumih, razvrstiti kot visokotvegane sisteme UI, razen kadar gre za sisteme UI, pri katerih fizične osebe niso neposredno izpostavljene njihovim izhodnim podatkom, kot so orodja, ki se uporabljajo za organizacijo, optimizacijo in strukturiranje političnih kampanj z upravnega in logističnega vidika.
- (63) Dejstva, da je sistem UI na podlagi te uredbe razvrščen kot visokotvegani sistem UI, se ne bi smelo razlagati tako, da pomeni, da je njegova uporaba zakonita na podlagi drugih aktov prava Unije ali na podlagi nacionalnega prava, 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 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.
- (64) Da bi zmanjšali tveganja iz visokotveganih sistemov UI, ki so dani na trg ali v uporabo, in zagotovili visoko raven zanesljivosti, bi bilo treba za visokotvegane sisteme UI uporabljati nekatere obvezne zahteve in pri tem upoštevati predvideni namen in kontekst uporabe sistema UI ter sistem obvladovanja tveganja, ki ga vzpostavi ponudnik. Ponudniki bi pri ukrepih, ki jih sprejmejo za izpolnjevanje obveznih zahtev iz te uredbe, morali upoštevati splošno priznane najsodobnejše tehnološke dosežke na področju UI; ti ukrepi bi morali biti sorazmerni in učinkoviti za doseganje ciljev te uredbe. Kot je pojasnjeno v obvestilu Komisije „Modri vodnik“ o izvajanju pravil EU o proizvodih iz leta 2022, je na podlagi novega zakonodajnega okvira splošno pravilo, da se več kot en pravni akt harmonizacijske zakonodaje Unije lahko uporablja za en proizvod, saj se lahko dostopnost ali dajanje v uporabo izvede le, če je proizvod skladen z vso veljavno harmonizacijsko zakonodajo Unije. Nevarnosti sistemov UI, za katere veljajo zahteve iz te uredbe, se nanašajo na vidike, ki se razlikujejo od obstoječe harmonizacijske zakonodaje Unije, zato naj bi zahteve iz te uredbe dopolnjevale obstoječi del harmonizacijske zakonodaje Unije. Na primer stroji ali medicinski pripomočki, ki vključujejo sistem UI, lahko pomenijo tveganja, ki v bistvenih zdravstvenih in varnostnih zahtevah iz

⁽³³⁾ 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).

⁽³⁴⁾ Uredba (EU) 2024/900 Evropskega parlamenta in Sveta z dne 13. marca 2024 o preglednosti in ciljanem političnem oglaševanju (UL L, 2024/900, 20.3.2024, ELI: <http://data.europa.eu/eli/reg/2024/900/oj>).

ustrezne harmonizirane zakonodaje Unije niso zajeta, saj navedeno sektorsko pravo ne obravnava tveganj, značilnih za sisteme UI. To zahteva hkratno in dopolnjevalno uporabo različnih zakonodajnih aktov. Da bi zagotovili doslednost in preprečili nepotrebno upravno breme ali nepotrebne stroške, bi morali ponudnikom proizvoda, ki vsebuje enega ali več visokotveganih sistemov UI, za katere se uporabljajo zahteve iz te uredbe in harmonizacijske zakonodaje Unije, ki temelji na novem zakonodajnem okviru in je navedena v prilogi k tej uredbi, omogočiti prožnost glede operativnih odločitev o tem, kako na optimalen način zagotoviti skladnost proizvoda, ki vsebuje enega ali več sistemov UI, z vsemi veljavnimi zahtevami harmonizirane zakonodaje Unije. Ta prožnost bi lahko na primer pomenila odločitev ponudnika, da del potrebnih postopkov testiranja in poročanja, informacij in dokumentacije, ki se zahtevajo na podlagi te uredbe, vključi v dokumentacijo in postopke, ki že obstajajo in se zahtevajo na podlagi harmonizacijske zakonodaje Unije, ki temelji na novem zakonodajnem okviru in je navedena v prilogi k tej uredbi. To nikakor ne bi smelo ogroziti obveznosti ponudnika, da izpolnjuje vse veljavne zahteve.

- (65) Sestavni del sistema obvladovanja tveganja bi moral biti neprekinjen ponavljajoč se proces, ki se načrtuje in izvaja v celotnem življenjskem ciklu visokotvegane sistema UI. Ta proces bi moral biti usmerjen v prepoznavanje in zmanjšanje relevantnih tveganj sistemov UI za zdravje, varnost in temeljne pravice. Sistem obvladovanja tveganj bi bilo treba redno pregledovati in posodabljati, da bi zagotovili njegovo stalno učinkovitost ter utemeljitev in dokumentiranje vseh pomembnih odločitev in ukrepov, sprejetih v skladu s to uredbo. S tem postopkom bi bilo treba zagotoviti, da ponudnik opredeli tveganja ali škodljive vplive ter izvaja ukrepe za zmanjšanje znanih in razumno predvidljivih tveganj sistemov UI za zdravje, varnost in temeljne pravice glede na njihov predvideni namen in razumno predvidljivo napačno uporabo, vključno z morebitnimi tveganji, ki izhajajo iz interakcije med sistemom UI in okoljem, v katerem deluje. V okviru sistema obvladovanja tveganj bi bilo treba sprejeti najprimernejše ukrepe za obvladovanje tveganja glede na najsodobnejše tehnološke dosežke na področju UI. Ponudnik bi moral pri opredeljevanju najustreznejših ukrepov za obvladovanje tveganja dokumentirati in pojasniti sprejete odločitve ter po potrebi vključiti strokovnjake in zunanje deležnike. Pri identifikaciji razumno predvidljive napačne uporabe visoko tveganih sistemov UI bi moral ponudnik zajeti uporabe sistemov UI, za katere se kljub temu, da niso neposredno zajete s predvidenim namenom in določene v navodilih za uporabo, lahko razumno pričakuje, da bodo posledica enostavno predvidljivega človeškega vedenja v okviru posebnih značilnosti in uporabe določenega sistema UI. Vse znane ali predvidljive okoliščine, povezane z uporabo visokotvegane sistema UI v skladu s predvidenim namenom ali v razmerah razumno predvidljive napačne uporabe, ki lahko povzročijo tveganja za zdravje in varnost ali temeljne pravice, bi morale biti vključene v navodila za uporabo, ki jih zagotovi ponudnik. S tem se zagotovi, da je uvajalec seznanjen z njimi in jih upošteva pri uporabi visokotvegane sistema UI. Pri opredeljevanju in izvajanju ukrepov za zmanjšanje tveganja za predvidljivo napačno uporabo na podlagi te uredbe ponudnik v okviru obravnavanja predvidljive napačne uporabe ne bi smel zahtevati posebnega dodatnega učenja za visokotvegani sistem UI. Vendar se ponudnike spodbuja, naj po potrebi in če je to ustrezno razmislijo o takih dodatnih ukrepih za učenje, da bi ublažili razumno predvidljive napačne uporabe.
- (66) Za visokotvegane sisteme UI bi morale veljati zahteve glede obvladovanja tveganja, kakovosti in relevantnosti uporabljenih naborov podatkov, tehnične dokumentacije in vodenja evidenc, preglednosti in zagotavljanja informacij uvajalcem, človekovega nadzora ter robustnosti, točnosti in varnosti. Te zahteve so potrebne za učinkovito zmanjšanje tveganj za zdravje, varnost in temeljne pravice. Ker ni v razumni meri na voljo drugih manj omejevalnih ukrepov za trgovino, te zahteve ne predstavljajo neupravičene omejitve trgovine.
- (67) Visokokakovostni podatki in dostop do njih imajo ključno vlogo pri zagotavljanju strukture in zmogljivosti številnih sistemov UI, zlasti kadar se uporabljajo tehnike, ki vključujejo učenje modelov, s katerim bi zagotovili, da bo visokotvegani sistem UI deloval, kot je predvideno, in varno ter da ne bo postal vir diskriminacije, ki je prepovedana s pravom Unije. Visokokakovostni nabori učnih, testnih in validacijskih podatkov zahtevajo izvajanje ustreznih prakse vodenja in upravljanja podatkov. Nabori učnih, testnih in validacijskih podatkov, vključno z oznakami, bi morali biti ustrezni, dovolj reprezentativni in v največji možni meri brez napak in popolni glede na predvideni namen. Da bi olajšali skladnost s pravom Unije o varstvu podatkov, kot je Uredba (EU) 2016/679, bi morale prakse vodenja in upravljanja podatkov v primeru osebnih podatkov vključevati preglednost prvotnega namena zbiranja podatkov. Nabori podatkov bi morali imeti tudi ustrezne statistične lastnosti, tudi kar zadeva osebe ali skupine oseb, v zvezi s katerimi naj bi se uporabljal visokotvegani sistem UI, s posebnim poudarkom na zmanjševanju morebitnih pristranskosti v naborih podatkov, ki bi lahko vplivale na zdravje in varnost oseb, negativno vplivale na temeljne pravice ali povzročile diskriminacijo, prepovedano na podlagi prava Unije, zlasti kadar izhodni podatki vplivajo na

vhodne podatke za prihodnje operacije (povratne zanke). Na primer, pristranskost je lahko inherentno prisotna v osnovnih naborih podatkov, zlasti kadar se uporabljajo pretekli podatki, ali se ustvari, ko se sistemi izvajajo v realnih razmerah. Takšna inherentna pristranskost bi lahko vplivala na rezultate sistemov UI in se tudi običajno postopoma povečuje, zaradi česar se ohranja in povečuje tudi obstoječa diskriminacija, zlasti za osebe, ki pripadajo določenim ranljivim skupinam, vključno z rasnimi ali etničnimi skupinami. Zahteva, da morajo biti nabori podatkov čim bolj popolni in brez napak, ne bi smela vplivati na uporabo tehnik za ohranjanje zasebnosti v okviru razvoja in testiranja sistemov UI. Nabori podatkov morali zlasti v obsegu, ki ga zahteva njihov predvideni namen, upoštevati lastnosti, značilnosti ali elemente, ki so značilni za določeno geografsko, kontekstualno, vedenjsko ali funkcionalno okolje, v katerem naj bi se uporabljal sistem UI. Zahteve v zvezi z upravljanjem podatkov se lahko izpolnijo s pomočjo tretjih oseb, ki ponujajo certificirane storitve zagotavljanja skladnosti s predpisi, vključno s preverjanjem upravljanja podatkov, celovitosti nabora podatkov, praks učenja, validacije in testiranja podatkov, če je zagotovljena skladnost z zahtevami glede podatkov iz te uredbe.

- (68) Za razvoj in ocenjevanje visokotveganih sistemov UI bi morali imeti nekateri akterji, kot so ponudniki, priglasi organi in drugi ustrezni subjekti, kot evropska vozlišča za digitalne inovacije, centri za testiranje in eksperimentiranje ter 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 sistemov UI. Evropski zdravstveni podatkovni prostor bo na področju zdravja na primer olajšal nediskriminatoren dostop do zdravstvenih podatkov in učenje algoritmov UI 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, validacijo in testiranje sistemov UI.
- (69) Pravica do zasebnosti in varstva osebnih podatkov mora biti zagotovljena v celotni življenjski dobi sistema UI. V zvezi s tem se pri obdelavi osebnih podatkov uporabljata načeli najmanjšega obsega podatkov ter vgrajenega in privzetega varstva podatkov, kot sta določeni v pravu Unije o varstvu podatkov. Ukrepi, ki jih ponudniki sprejmejo za zagotovitev skladnosti s temi načeli, lahko vključujejo ne le anonimizacijo in šifriranje, temveč tudi uporabo tehnologije, ki omogoča vnos algoritmov v podatke in učenje sistemov UI brez prenosa med stranmi ali kopiranja samih neobdelanih ali strukturiranih podatkov in brez poseganja v zahteve glede upravljanja podatkov iz te uredbe.
- (70) Da bi zaščitili pravico drugih pred diskriminacijo, ki bi lahko nastala zaradi pristranskosti v sistemih UI, bi morali imeti ponudniki možnost, da izjemoma, če je to nujno potrebno za zagotavljanje odkrivanja in popravljanja pristranskosti v zvezi z visokotveganimi sistemi UI, ob upoštevanju ustreznih zaščitnih ukrepov za temeljne pravice in svoboščine fizičnih oseb ter ob uporabi vseh veljavnih pogojev iz te uredbe ter pogojev iz uredb (EU) 2016/679 in (EU) 2018/1725 ter Direktive (EU) 2016/680, obdelujejo tudi posebne kategorije osebnih podatkov kot zadevo bistvenega javnega interesa v smislu člena 9(2), točka (g), Uredbe (EU) 2016/679 in člena 10(2), točka (g), Uredbe (EU) 2018/1725.
- (71) Razumljive informacije o tem, kako so bili visokotvegani sistemi UI razviti in kako delujejo skozi celotno življenjsko dobo, so bistvene za omogočanje sledljivosti teh sistemov, preverjanje skladnosti z zahtevami iz te uredbe ter spremljanje njihovega delovanja in spremljanje po dajanju na trg. To zahteva vodenje evidenc in razpoložljivost tehnične dokumentacije, ki vsebuje informacije, potrebne za oceno skladnosti sistema UI z ustreznimi zahtevami in olajšanje spremljanja po dajanju na trg. Takšne 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 in biti pripravljene v jasni in celoviti obliki. Tehnično dokumentacijo bi bilo treba ustrezno posodabljati v celotni življenjski dobi sistema UI. Poleg tega bi morali visokotvegani sistemi UI tehnično omogočati samodejno beleženje dogodkov z dnevniki v celotni življenjski dobi sistema.

- (72) Pri reševanju problemov v zvezi z nepreglednostjo in kompleksnostjo nekaterih sistemov UI ter za pomoč uvajalcem pri izpolnjevanju njihovih obveznosti iz te uredbe bi bilo treba za visokotvegane sisteme UI zahtevati preglednost, preden se dajo na trg ali v uporabo. Visokotvegani sistemi UI bi morali biti zasnovani tako, da bi uvajalci lahko razumeli, kako sistem UI deluje, ocenili njegovo funkcionalnost ter razumeli njegove prednosti in omejitve. Visokotveganim sistemom UI bi morale biti priložene ustrezne informacije v obliki navodil za uporabo. Takšne informacije bi morale vključevati značilnosti, zmogljivosti in omejitve zmogljivosti sistema UI. Ti naj bi zajemali informacije o morebitnih znanih in predvidljivih okoliščinah, povezanih z uporabo visokotveganega sistema UI, vključno z ukrepi uvajalcev, ki lahko vplivajo na vedenje in zmogljivost sistema, v katerih lahko sistem UI povzroči tveganja za zdravje, varnost in temeljne pravice, o spremembah, ki jih je ponudnik vnaprej določil in ocenil glede skladnosti, ter o ustreznih ukrepih za človeški nadzor, vključno z ukrepi za lažjo razlago izhodnih podatkov sistema UI s strani uvajalcev. Preglednost, vključno s priloženimi navodili za uporabo, bi morala pomagati uvajalcem pri uporabi sistema in sprejemanju informiranih odločitev. Uvajalci bi morali biti med drugim v boljšem položaju za pravilno izbiro sistema, ki ga nameravajo uporabljati glede na obveznosti, ki veljajo zanje, biti poučeni o nameravani in izključeni uporabi ter pravilno in ustrezno uporabljati sistem UI. Da bi izboljšali čitljivost in dostopnost informacij, vključenih v navodila za uporabo, bi bilo treba, kadar je ustrezno vključiti ponazoritvene primere, na primer glede omejitev ter predvidene in izključene uporabe sistema UI. Ponudniki bi morali zagotoviti, da vsa dokumentacija, vključno z navodili za uporabo, vsebuje smiselne, celovite, dostopne in razumljive informacije, ob upoštevanju potreb in predvidljivega znanja ciljnih uvajalcev. Navodila za uporabo bi morala biti na voljo v jeziku, ki ga določi zadevna država članica in ga ciljni uvajalci brez težav razumejo.
- (73) Visokotvegani sistemi UI bi morali biti zasnovani in razviti tako, da lahko fizične osebe nadzorujejo njihovo delovanje, zagotavljajo, da se uporabljajo, kot je bilo predvideno, in da se njihovi vplivi obravnavajo v celotnem življenjskem ciklu sistema. V ta namen bi moral ponudnik sistema pred dajanjem sistema na trg ali v uporabo določiti ustrezne ukrepe za človeški nadzor. Zlasti bi morali taki ukrepi, kadar je primerno, zagotavljati, da za sistem veljajo vgrajene operativne omejitve, ki jih sistem sam ne more razveljaviti, da se sistem odziva na človeškega operaterja ter da imajo fizične osebe, ki jim je bil dodeljen človekov nadzor, potrebne kompetence, usposobljenost in pooblastila za opravljanje te vloge. Prav tako je bistveno po potrebi zagotoviti, da visokotvegani sistemi UI vključujejo mehanizme za usmerjanje in obveščanje fizične osebe, ki ji je bil dodeljen človeški nadzor, za sprejemanje informiranih odločitev o tem, ali, kdaj in kako posredovati, da bi se izognili negativnim posledicam ali tveganjem, ali ustaviti sistem, če ne deluje, kot je bilo predvideno. Glede na pomembne posledice, ki jih napaka ujemanje v nekaterih sistemih za biometrično identifikacijo ljudi pomeni za osebe, je za te sisteme ustrezno določiti okrepljeno zahtevo po človekovem nadzoru, tako da uvajalec 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 ločena preverjanja različnih oseb samodejno zabeležila v dnevnikih, ki jih ustvari sistem. Glede na posebnosti področij preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, migracij, nadzora meje in azila se ta zahteva ne bi smela uporabljati, kadar je v skladu s pravom Unije ali nacionalnim pravom uporaba te zahteve nesorazmerna.
- (74) Visokotvegani sistemi UI bi morali v celotni življenjski dobi delovati dosledno ter izpolnjevati ustrezno raven točnosti, robustnosti in kibernetске varnosti glede na njihov predvideni namen in v skladu s splošno priznanimi najodobnejšimi tehnološkimi dosežki. Komisijo ter ustrezne organizacije in deležnike se spodbuja, naj ustrezno upoštevajo zmanjšanje tveganj in negativne učinke sistema UI. Pričakovano raven metrik zmogljivosti bi bilo treba navesti v priloženih navodilih za uporabo. Ponudniki so pozvani, naj te informacije sporočijo uvajalcem na jasn in lahko razumljiv način, brez nesporazumov ali zavajajočih izjav. Namen prava Unije o zakonskem meroslovju, vključno z direktivama 2014/31/EU ⁽³⁵⁾ in 2014/32/EU ⁽³⁶⁾ Evropskega parlamenta in Sveta, je zagotoviti točnost meritev ter prispevati k preglednosti in poštenosti trgovinskih poslov. V zvezi s tem bi morala Komisija v sodelovanju z ustreznimi deležniki in organizacijami, kot so organi za meroslovje in primerjalno analizo, po potrebi spodbujati razvoj referenčnih vrednosti in metodologij merjenja za sisteme UI. Pri tem bi se morala Komisija seznaniti z mednarodnimi partnerji, ki se ukvarjajo z meroslovjem in ustreznimi kazalniki merjenja v zvezi z UI, ter z njimi sodelovati.

⁽³⁵⁾ Direktiva 2014/31/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o harmonizaciji zakonodaj držav članic v zvezi z omogočanjem dostopnosti neavtomatskih tehtnic na trgu (UL L 96, 29.3.2014, str. 107).

⁽³⁶⁾ Direktiva 2014/32/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o harmonizaciji zakonodaj držav članic v zvezi z omogočanjem dostopnosti neavtomatskih tehtnic na trgu (UL L 96, 29.3.2014, str. 149).

- (75) Tehnična robustnost je ključna zahteva za visokotvegane sisteme UI. 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). Zato bi bilo treba sprejeti tehnične in organizacijske ukrepe za zagotovitev odpornosti visokotveganih sistemov UI, na primer z zasnovo in razvojem ustreznih tehničnih rešitev za preprečevanje ali zmanjšanje škodljivega ali drugače nezaželenega vedenja. Takšne tehnične rešitve lahko na primer vključujejo mehanizme, ki sistemu omogočajo varno prekinitev delovanja (načrti varne odpovedi), če so prisotne določene nepravilnosti ali delovanje poteka zunaj določenih vnaprej določenih meja. 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 sistem UI.
- (76) Kibernetška varnost ima ključno vlogo pri zagotavljanju odpornosti sistemov UI proti poskusom spreminjanja njihove uporabe, vedenja, zmogljivosti ali ogrožanja njihovih varnostnih lastnosti s strani zlonamernih tretjih oseb, ki izkoriščajo šibke točke sistema. Kibernetški napadi na sisteme UI lahko izkoristijo posebna sredstva UI, kot so nabori učnih podatkov (npr. zastrupitev podatkov) ali naučeni modeli (npr. nasprotovvalni napadi ali sklepanje o članstvu), ali pa šibke točke digitalnih sredstev sistema UI ali osnovne infrastrukture IKT. Da bi zagotovili raven kibernetške varnosti, ki ustreza tveganjem, bi morali ponudniki visokotveganih sistemov UI sprejeti ustrezne ukrepe, kot je varnostni nadzor, in pri tem po potrebi tudi upoštevati osnovne infrastrukture IKT.
- (77) Brez poseganja v zahteve v zvezi z robustnostjo in natančnostjo iz te uredbe se lahko skladnost visokotveganih sistemov UI, ki spadajo na področje uporabe uredbe Evropskega parlamenta in Sveta o horizontalnih zahtevah glede kibernetške varnosti za izdelke z digitalnimi elementi, v skladu z navedeno uredbo, z zahtevami glede kibernetške varnosti iz te uredbe dokaže z izpolnjevanjem bistvenih zahtev glede kibernetške varnosti iz navedene uredbe. Če visokotvegani sistemi UI izpolnjujejo bistvene zahteve iz uredbe o horizontalnih zahtevah glede kibernetške varnosti za izdelke z digitalnimi elementi, štejejo za skladne z zahtevami glede kibernetške varnosti iz te uredbe, če je izpolnjevanje navedenih zahtev dokazano v EU izjavi o skladnosti ali delih izjave, izdane na podlagi navedene uredbe. V ta namen bi bilo treba pri oceni tveganj za kibernetško varnost, povezanih s proizvodom z digitalnimi elementi, razvrščenimi kot visokotvegani sistem UI v skladu s to uredbo, ki se izvede na podlagi uredbe o horizontalnih zahtevah glede kibernetške varnosti za izdelke z digitalnimi elementi, upoštevati tveganja za kibernetško odpornost sistema UI na poskuse nepooblaščenih tretjih oseb, da z izkoriščanjem šibkih točk sistema spremenijo njegovo uporabo, vedenje ali zmogljivost, vključno s šibkimi točkami, ki so specifične za UI, kot so zastrupitev podatkov ali nasprotovvalni napadi, ter v zvezi s tveganji za temeljne pravice, kot je zahtevano v tej uredbi.
- (78) Postopek ugotavljanja skladnosti iz te uredbe bi bilo treba uporabljati v zvezi z bistvenimi zahtevami glede kibernetške varnosti proizvoda z digitalnimi elementi, ki jih zajema uredba o horizontalnih zahtevah glede kibernetške varnosti za izdelke z digitalnimi elementi in je razvrščen kot visokotvegani sistem UI na podlagi te uredbe. Vendar to pravilo ne bi smelo povzročiti znižanja potrebne ravni zanesljivosti za kritične proizvode z digitalnimi elementi, ki jih zajema uredba o horizontalnih zahtevah glede kibernetške varnosti za izdelke z digitalnimi elementi. Zato z odstopanjem od tega pravila za visokotvegane sisteme UI, ki spadajo na področje uporabe te uredbe in so opredeljeni tudi kot pomembni in kritični proizvodi z digitalnimi elementi na podlagi uredbe o horizontalnih zahtevah glede kibernetške varnosti za izdelke z digitalnimi elementi ter se zanje uporablja postopek ugotavljanja skladnosti na podlagi notranjega nadzora iz ene od prilog k tej uredbi, veljajo določbe o ugotavljanju skladnosti iz uredbe o horizontalnih zahtevah glede kibernetške varnosti za izdelke z digitalnimi elementi, kar zadeva bistvene zahteve glede kibernetške varnosti iz navedene uredbe. V tem primeru bi bilo treba za vse druge vidike, ki jih zajema ta uredba, uporabljati ustrezne določbe o ugotavljanju skladnosti na podlagi notranjega nadzora iz ene od prilog k tej uredbi. Komisija bi morala na podlagi poznavanja področja in strokovnega znanja agencije ENISA o politiki kibernetške varnosti in nalogah, dodeljenih agenciji ENISA na podlagi Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta ⁽³⁷⁾, sodelovati z agencijo ENISA pri vprašanjih, povezanih s kibernetško varnostjo sistemov UI.

⁽³⁷⁾ Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetško varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetške varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetški varnosti) (UL L 151, 7.6.2019, str. 15).

- (79) Primerno je, da določena fizična ali pravna oseba, opredeljena kot ponudnik, prevzame odgovornost za dajanje visokotveganega sistema UI na trg ali v uporabo, ne glede na to, ali je ta oseba tista, ki je zasnovala ali razvila sistem.
- (80) Kot podpisnice Konvencije Organizacije združenih narodov o pravicah invalidov so Unija in države članice pravno zavezane, da ščitijo invalide pred diskriminacijo in spodbujajo njihovo enakost, jim zagotovijo, da imajo enako kot drugi dostop do informacijskih in komunikacijskih tehnologij in sistemov, ter da se spoštuje njihova zasebnost. Ob vse večjem pomenu in uporabi sistemov UI bi morala uporaba načel univerzalnega oblikovanja pri vseh novih tehnologijah in storitvah zagotoviti popoln in enakopraven dostop vsem, ki so lahko izpostavljeni tehnologijam UI ali te tehnologije uporabljajo, tudi invalidom, na način, ki v celoti upošteva njihovo prirojeno dostojanstvo in raznolikost. Zato je bistvenega pomena, da ponudniki zagotavljajo popolno skladnost z zahtevami glede dostopnosti, tudi z Direktivo (EU) 2016/2102 Evropskega parlamenta in Sveta⁽³⁸⁾ in Direktivo (EU) 2019/882. Ponudniki bi morali zagotoviti skladnost s temi zahtevami že pri zasnovi. Zato bi bilo treba potrebne ukrepe v čim večji meri vključiti v zasnovo visokotveganega sistema UI.
- (81) 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. Ponudniki visokotveganega sistema UI, za katere veljajo obveznosti v zvezi s sistemi upravljanja kakovosti na podlagi ustreznega sektorskega prava Unije, bi morali imeti možnost, da elemente sistema upravljanja kakovosti iz te uredbe vključijo v obstoječi sistem upravljanja kakovosti, določen v navedenem drugem sektorskem pravu Unije. Pri prihodnjih dejavnostih standardizacije ali smernicah, ki jih sprejme Komisija, bi bilo treba upoštevati tudi dopolnjevanje med to uredbo in obstoječim sektorskim pravom Unije. Javni organi, ki visokotvegane sisteme UI dajo v uporabo za lastno uporabo, lahko sprejmejo in izvajajo pravila za sistem upravljanja kakovosti kot del sistema upravljanja kakovosti, sprejetega bodisi na nacionalni ali na regionalni ravni, ob upoštevanju posebnosti sektorja ter pristojnosti in organizacije zadevnega javnega organa.
- (82) Da se omogoči izvajanje te uredbe in ustvarijo enaki konkurenčni pogoji za operaterje ter ob upoštevanju različnih oblik omogočanja dostopnosti digitalnih proizvodov, je pomembno zagotoviti, da lahko oseba s sedežem v Uniji v vseh okoliščinah organom zagotovi vse potrebne informacije o skladnosti sistema UI. Zato bi morali ponudniki s sedežem v tretjih državah pred dajanjem svojih sistemov UI na voljo v Uniji, s pisnim pooblastilom imenovati pooblaščenega zastopnika s sedežem v Uniji. Ta pooblaščen zastopnik ima ključno vlogo pri zagotavljanju skladnosti visokotveganega sistema UI, ki jih ti ponudniki, ki nimajo sedeža v Uniji, dajejo na trg ali v uporabo v Uniji, in je njihova kontaktna oseba s sedežem v Uniji.
- (83) Glede na naravo in kompleksnost verige vrednosti za sisteme UI ter v skladu z novim zakonodajnim okvirom je bistveno zagotoviti pravno varnost in olajšati skladnost s to uredbo. Zato je treba pojasniti vlogo in posebne obveznosti zadevnih operaterjev v tej verigi vrednosti, kot so uvozniki in distributerji, ki lahko prispevajo k razvoju sistemov UI. 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. Tako bi na primer operater lahko hkrati bil distributer in uvoznik.
- (84) Za zagotovitev pravne varnosti je treba pojasniti, da bi bilo treba pod določenimi pogoji vsakega distributerja, uvoznika, uvajalca ali druge tretje osebe šteti za ponudnika visokotveganega sistema UI in bi zato moral prevzeti vse zadevne obveznosti. To bi veljalo, če ta stranka svoje ime ali znamko vnese v visokotvegani sistem UI, ki je že dan na trg ali v uporabo, brez poseganja v pogodbeno dogovore, ki določajo, da se obveznosti dodelijo drugače. To bi veljalo tudi, če ta stranka bistveno spremeni visokotvegani sistem UI, ki je že bil dan na trg ali v uporabo, na način, da ostane visokotvegani sistem UI v skladu s to uredbo, ali če spremeni predvideni namen sistema UI, vključno z sistemom UI za splošne namene, ki ni bil razvrščen kot sistem visokega tveganja in je že bil dan na trg ali v uporabo, na način, da sistem UI postane sistem visokega tveganja v skladu s to uredbo. Te določbe bi bilo treba uporabljati brez poseganja v bolj specifične določbe v okviru določene harmonizacijske zakonodaje, temelječe na novem zakonodajnem okviru, ki naj bi se uporabljala skupaj s to uredbo. Na primer člen 16(2) Uredbe (EU)

⁽³⁸⁾ Direktiva (EU) 2016/2102 Evropskega parlamenta in Sveta z dne 26. oktobra 2016 o dostopnosti spletišč in mobilnih aplikacij organov javnega sektorja (UL L 327, 2.12.2016, str. 1).

2017/745, v katerem je določeno, da nekatere spremembe ne bi smele šteti kot spremembe pripomočka, ki bi lahko vplivale na skladnost z veljavnimi zahtevami, bi bilo treba še naprej uporabljati za visokotvegane sisteme UI, ki so medicinski pripomočki v smislu navedene uredbe.

- (85) Sistemi UI za splošne namene se lahko uporabljajo kot samostojni visokotvegani sistemi UI ali pa so komponente drugih visokotveganih sistemov UI. Zato bi morali ponudniki takih sistemov zaradi njihove posebne narave in za zagotovitev pravične delitve odgovornosti v verigi vrednosti UI ne glede na to, ali lahko drugi ponudniki te sisteme uporabljajo kot samostojne visokotvegane sisteme UI ali kot komponente visokotveganih sistemov UI in če v tej uredbi ni določeno drugače, tesno sodelovati s ponudniki zadevnih visokotveganih sistemov UI, da bi jim omogočili izpolnjevanje obveznosti iz te uredbe, in s pristojnimi organi, ustanovljenimi na podlagi te uredbe.
- (86) Kadar na podlagi pogojev iz te uredbe ponudnik, ki je sistem UI prvotno dal na trg ali v uporabo, za namene te uredbe ne bi smel več šteti za ponudnika in če ta ponudnik ni izrecno izključil spremembe sistema UI v visokotvegani sistem UI, bi moral nekdani ponudnik kljub temu tesno sodelovati in dati na voljo potrebne informacije ter zagotoviti razumno pričakovani tehnični dostop in drugo pomoč, ki so potrebni za izpolnjevanje obveznosti iz te uredbe, zlasti v zvezi s skladnostjo visokotveganih sistemov UI z ugotavljanjem skladnosti.
- (87) Poleg tega, kadar visokotvegani sistem UI, ki je varnostna komponenta proizvoda, ki spada na področje uporabe harmonizacijske zakonodaje Unije na podlagi novega zakonodajnega okvira, ni dan na trg ali v uporabo neodvisno od proizvoda, bi moral proizvajalec proizvoda, opredeljen v navedeni zakonodaji, izpolnjevati obveznosti ponudnika iz te uredbe in zlasti zagotoviti, da sistem UI, vgrajen v končni proizvod, izpolnjuje zahteve iz te uredbe.
- (88) V verigi vrednosti UI sisteme UI, orodja in storitve, pa tudi komponente ali procese, ki jih ponudnik vključi v sistem UI z različnimi cilji, vključno z učenjem modelov, ponovnim učenjem modelov, testiranjem in ocenjevanjem modelov, vključevanjem v programsko opremo ali drugimi vidiki razvoja modela, pogosto dobavlja več strani. Te strani imajo pomembno vlogo v verigi vrednosti v odnosu do ponudnika visokotvegane sistema UI, v katerega so vključeni njihovi sistemi UI, orodja, storitve, komponente ali procesi, in bi morale temu ponudniku v pisni obliki zagotoviti potrebne informacije, zmožljivosti, tehnični dostop in drugo pomoč na podlagi splošno priznanih najsodobnejših tehnoloških dosežkov, da bi lahko ponudnik v celoti izpolnjeval obveznosti iz te uredbe, ne da bi bile pri tem ogrožene njegove pravice intelektualne lastnine ali poslovne skrivnosti.
- (89) Za tretje osebe, ki javnosti omogočajo dostop do orodij, storitev, postopkov ali komponent UI, ki niso modeli UI za splošne namene, ne bi smela veljati obveznost glede izpolnjevanja zahtev, ki se nanašajo na odgovornosti v verigi vrednosti UI, zlasti do ponudnika, ki jih je uporabil ali vključil, če so ta orodja, storitve, postopki ali komponente UI dostopni na podlagi proste in odprtokodne licence. Razvijalce brezplačnih in odprtokodnih orodij, storitev, postopkov ali komponent UI, ki niso modeli UI za splošne namene, pa bi bilo treba spodbujati k izvajanju splošno sprejetih dokumentacijskih praks, kot so vzorčne kartice in podatkovni listi, da bi pospešili izmenjavo informacij v verigi vrednosti UI, kar bi omogočilo spodbujanje zaupanja vrednih sistemov UI v Uniji.
- (90) Komisija bi lahko razvila in priporočila prostovoljne vzorčne pogodbene pogoje med ponudniki visokotveganih sistemov UI in tretjimi osebami, ki zagotavljajo orodja, storitve, komponente ali procese, ki se uporabljajo ali vključujejo v visokotvegane sisteme UI, da bi olajšali sodelovanje v verigi vrednosti. Komisija bi morala pri oblikovanju prostovoljnih vzorčnih pogodbenih pogojev upoštevati morebitne pogodbene zahteve, ki se uporabljajo v posameznih sektorjih ali poslovnih primerih.
- (91) Glede na naravo sistemov UI ter tveganja za varnost in temeljne pravice, ki so morda povezana z njihovo uporabo, tudi kar zadeva potrebo po zagotovitvi ustreznega spremljanja zmožljivosti sistema UI v realnem življenju, je primerno določiti posebne odgovornosti za uvaljalce. Uvajalci bi morali zlasti sprejeti ustrezne tehnične in organizacijske ukrepe za zagotovitev, da uporabljajo visokotvegane sisteme UI v skladu z navodili za uporabo, pri čemer bi bilo treba določiti nekatere druge obveznosti v zvezi s spremljanjem delovanja sistemov UI in v zvezi z vodenjem evidenc, če je to primerno. Poleg tega bi morali uvaljalci zagotoviti, da imajo osebe, dodeljene za izvajanje navodil za uporabo in človeški nadzor, kot je določeno v tej uredbi, potrebne kompetence, zlasti ustrezno

raven pismenosti, usposobljenosti in pooblastil na področju UI za pravilno izpolnjevanje teh nalog. Te obveznosti ne bi smele posegati v druge obveznosti uvajalcev v zvezi z visokotveganimi sistemi UI na podlagi prava Unije ali nacionalnega prava.

- (92) Ta uredba ne posega v obveznosti delodajalcev, da delavce ali njihove predstavnike obveščajo ali se z njimi posvetujejo na podlagi prava Unije ali nacionalnega prava in prakse, vključno z Direktivo 2002/14/ES Evropskega parlamenta in Sveta ⁽³⁹⁾ o odločitvah o dajanju v uporabo ali uporabi sistemov UI. Še naprej je treba zagotavljati informacije delavcem in njihovim predstavnikom o načrtovani uvedbi visokotveganih sistemov UI na delovnem mestu, kadar niso izpolnjeni pogoji za te obveznosti glede obveščanja ali obveščanja in posvetovanja iz drugih pravnih instrumentov. Poleg tega je taka pravica do obveščenosti pomožna in potrebna za cilj varstva temeljnih pravic, na katerem temelji ta uredba. Zato bi bilo treba v tej uredbi določiti zahtevo po informacijah v ta namen, ne da bi to vplivalo na obstoječe pravice delavcev.
- (93) Poleg tega, da lahko tveganja, povezana s sistemi UI, nastanejo zaradi načina zasnove takih sistemov, lahko tveganja izvirajo tudi iz tega, kako se taki sistemi uporabljajo. Uvajalci visokotvegane sistema UI imajo zato ključno vlogo pri skrbi za zaščito temeljnih pravic, kar dopolnjuje obveznosti ponudnika pri razvoju sistema UI. Uvajalci najbolje razumejo, kako se bo visokotvegani sistem UI dejansko uporabljal, in lahko tako opredelijo potencialna velika tveganja, ki niso bila predvidena v fazi razvoja, saj natančneje poznajo okoliščine uporabe, osebe ali skupine oseb, ki bodo verjetno izpostavljene, vključno z ranljivimi skupinami. Uvajalci visokotveganih sistemov UI, navedeni v eni od prilog k tej uredbi, imajo tudi ključno vlogo pri obveščanju fizičnih oseb in bi morali pri sprejemanju odločitev ali pomoči pri sprejemanju odločitev v zvezi s fizičnimi osebami po potrebi obvestiti fizične osebe, da se zanje uporablja visokotvegani sistem UI. Te informacije bi morale vključevati njegov predvideni namen in vrsto odločitev, ki jih sprejema. Uvajalec bi moral fizične osebe obvestiti tudi o njihovi pravici do obrazložitve iz te uredbe. Kar zadeva visokotvegane sisteme UI, ki se uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, bi bilo treba to obveznost izvajati v skladu s členom 13 Direktive (EU) 2016/680.
- (94) Vsaka obdelava biometričnih podatkov, vključena v uporabo sistemov UI za biometrično identifikacijo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, mora biti skladna s členom 10 Direktive (EU) 2016/680, ki omogoča tako obdelavo le, kadar je to nujno potrebno, ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, in kadar je to dovoljeno v skladu s pravom Unije ali pravom države članice. Kadar je taka uporaba odobrena, je treba spoštovati tudi načela iz člena 4(1) Direktive (EU) 2016/680, vključno z zakonitostjo, pravičnostjo in preglednostjo, omejitvijo namena, točnostjo in omejitvijo shranjevanja.
- (95) Brez poseganja v veljavno pravo Unije, zlasti v Uredbo (EU) 2016/679 in Direktivo (EU) 2016/680, in ob upoštevanju intruzivne narave sistemov za naknadno biometrično identifikacijo na daljavo, bi bilo treba za uporabo sistemov za naknadno biometrično identifikacijo na daljavo uporabljati zaščitne ukrepe. Sisteme za naknadno biometrično identifikacijo na daljavo bi bilo treba vedno uporabljati na način, ki je sorazmeren, zakonit in nujno potreben ter tako ciljno usmerjen v smislu posameznikov, ki jih je treba identificirati, lokacije, časovnega obsega in na podlagi zaprtega nabora podatkov iz zakonito pridobljenih videoposnetkov. V nobenem primeru sistemov za naknadno biometrično identifikacijo na daljavo ne bi smeli uporabljati v okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, da ne bi povzročili neselektivnega nadzora. Pogoji za naknadno biometrično identifikacijo na daljavo v nobenem primeru ne bi smeli biti podlaga za izogibanje pogojem prepovedi in strogim izjemam za biometrično identifikacijo na daljavo v realnem času.
- (96) Da bi učinkovito zagotovili varstvo temeljnih pravic, bi morali uvajalci visokotveganih sistemov UI, ki so osebe javnega prava, ali zasebni subjekti, ki zagotavljajo javne storitve, in uvajalci, ki uporabljajo nekatere visokotvegane sisteme UI, navedene v eni od prilog k tej uredbi, kot so bančni ali zavarovalniški subjekti, pred začetkom uporabe izvesti oceno učinka na temeljne pravice. Storitve, pomembne za posameznike, ki so javne narave, lahko zagotavljajo tudi zasebni subjekti. Zasebni subjekti, ki zagotavljajo takšne javne storitve, so povezani z nalogami v javnem interesu, na primer na področjih izobraževanja, zdravstvenega varstva, socialnih storitev, stanovanj in razsojanja. Cilj ocene učinka na temeljne pravice je, da uvajalec opredeli posebna tveganja za pravice posameznikov ali skupin posameznikov, ki bodo verjetno izpostavljene, in ukrepe, ki jih je treba sprejeti v primeru uresničitve teh tveganj.

⁽³⁹⁾ Direktiva 2002/14/ES Evropskega parlamenta in Sveta z dne 11. marca 2002 o določitvi splošnega okvira za obveščanje in posvetovanje z delavci v Evropski skupnosti (UL L 80, 23.3.2002, str. 29).

Oceno učinka bi bilo treba opraviti pred uvedbo visokotveganega sistema UI in bi jo bilo treba posodobiti, kadar uvajalec meni, da se je spremenil kateri od pomembnih dejavnikov. V oceni učinka bi bilo treba opredeliti ustrezne procese uvajalca, v katerih se bo visokotvegani sistem UI uporabljal v skladu s predvidenim namenom, ter opis obdobja in pogostosti uporabe sistema ter posebnih kategorij fizičnih oseb in skupin, ki bodo verjetno izpostavljene v posebnih okoliščinah uporabe. Ocena bi morala vključevati tudi opredelitev posebnih tveganj škode, ki bi lahko vplivala na temeljne pravice teh oseb ali skupin. Da bi zagotovili pravilno izvedbo te ocene učinka, bi moral uvajalec pri njenem izvajanju upoštevati ustrezne informacije, med drugim tudi tiste, ki jih ponudnik visokotveganega sistema UI navede v navodilih za uporabo. Glede na ugotovljena tveganja bi morali uvajalci določiti ukrepe, ki jih je treba sprejeti v primeru uresničitve teh tveganj, vključno na primer z ureditvami upravljanja v tem posebnem okviru uporabe, kot so ureditve za človeški nadzor v skladu z navodili za uporabo ali obravnavanje pritožb in postopki pravnega varstva, saj bi lahko bili ključni za zmanjšanje tveganj za temeljne pravice v konkretnih primerih uporabe. Po izvedbi te ocene učinka bi moral uvajalec o tem obvestiti ustrezní organ za nadzor trga. Za zbiranje ustreznih informacij, potrebnih za izvedbo ocene učinka, bi lahko uvajalci visokotveganega sistema UI, zlasti kadar se sistemi UI uporabljajo v javnem sektorju, v izvajanje takih ocen učinka in oblikovanje ukrepov, ki jih je treba sprejeti v primeru uresničitve tveganj, po potrebi vključili ustrezne deležnike, vključno s predstavniki skupin oseb, na katere bo sistem UI verjetno vplival, neodvisne strokovnjake in organizacije civilne družbe. Evropski urad za umetno inteligenco (v nadaljnjem besedilu: Urad za UI) bi moral pripraviti predlogo vprašalnika, da bi olajšali skladnost in zmanjšali upravno breme za uvajalce.

- (97) Da bi omogočili pravno varnost, bi moral biti pojem modelov UI za splošne namene jasno opredeljen in ločen od pojma sistemov UI. Opredelitev bi morala temeljiti na ključnih funkcionalnih značilnostih modela UI za splošne namene, zlasti na splošnosti in sposobnosti opravljanja širokega nabora različnih nalog. Ti modeli se običajno učijo s pomočjo velikih količin podatkov z različnimi metodami, kot so samonadzorovano, nenadzorovano ali okrepljeno učenje. Modeli UI za splošne namene se lahko dajo na trg na različne načine, tudi prek knjižnic, vmesnikov za aplikacijsko programiranje (API), kot neposredni prenos ali kot fizična kopija. Ti modeli se lahko dodatno spremenijo ali prilagodijo novim modelom. Čeprav so modeli UI bistvene komponente sistemov UI, sami po sebi niso sistemi UI. Da bi modeli UI postali sistemi UI, jim je treba dodati dodatne komponente, kot je na primer uporabniški vmesnik. Modeli UI so običajno vključeni v sisteme UI in so njihov sestavni del. V tej uredbi so določena posebna pravila za modele UI za splošne namene in modele UI za splošne namene, ki predstavljajo sistemska tveganja, ki bi jih bilo treba uporabljati tudi, kadar so ti modeli vključeni v sistem UI ali tvorijo del sistema UI. Razumeti bi bilo treba, da bi bilo treba obveznosti ponudnikov modelov UI za splošne namene uporabljati, ko bodo ti modeli dani na trg. Če ponudnik modela UI za splošne namene vključi lastni model v svoj sistem UI, ki je dostopen na trgu ali je v uporabi, bi bilo treba šteti, da je ta model dan na trg, zato bi bilo treba še naprej uporabljati obveznosti iz te uredbe za modele, poleg tistih za sisteme UI. Obveznosti, ki so določene za modele, se v nobenem primeru ne bi smeli uporabljati, če se lastni model uporablja za izključno notranje postopke, ki niso bistveni za zagotavljanje proizvoda ali storitve tretjim osebam, in to ne vpliva na pravice fizičnih oseb. Glede na njihove morebitne znatne negativne učinke bi morale za modele UI za splošne namene s sistemskim tveganjem vedno veljati ustrezne obveznosti iz te uredbe. Opredelitev ne bi smela zajemati modelov UI, ki se uporabljajo pred dajanjem na trg izključno za namene raziskav, razvoja in izdelave prototipov. To ne posega v obveznost skladnosti s to uredbo, kadar se po takšnih dejavnostih model da na trg.
- (98) Medtem ko bi bilo mogoče splošnost modela med drugim določiti tudi s številnimi parametri, bi bilo treba šteti, da modeli z vsaj milijardo parametrov in naučeni z veliko količino podatkov, ki uporabljajo samonadzor v velikem obsegu, kažejo znatno splošnost in so sposobni kompetentno opravljati širok nabor različnih nalog.
- (99) Veliki generativni modeli UI so tipičen primer modela UI za splošne namene, saj omogočajo prilagodljivo ustvarjanje vsebin, kot so besedilo, zvočni zapisi, slike ali videoposnetki, ki se lahko zlahka prilagodijo širokemu spektru različnih nalog.
- (100) Kadar je model UI za splošne namene vključen v sistem UI ali je del sistema UI, bi bilo treba ta sistem šteti za sistem UI za splošne namene, če se lahko zaradi te vključitve ta sistem uporablja za različne namene. Sistem UI za splošne namene se lahko uporablja neposredno ali pa se lahko vključi v druge sisteme UI.

- (101) Ponudniki modelov UI za splošne namene imajo posebno vlogo in odgovornost vzdolž verige vrednosti UI, saj so lahko modeli, ki jih zagotavljajo, podlaga za vrsto sistemov nižje v verigi, ki jih pogosto zagotavljajo ponudniki nižje v verigi, ki potrebujejo dobro razumevanje modelov in njihovih zmogljivosti, da bi omogočili vključitev takih modelov v njihove proizvode in izpolnili svoje obveznosti iz te uredbe ali drugih predpisov. Zato bi bilo treba določiti sorazmerne ukrepe za preglednost, vključno s pripravo in posodabljanjem dokumentacije ter zagotavljanjem informacij o modelu UI za splošne namene, ki ga lahko uporabljajo ponudniki nižje v verigi. Ponudnik modela UI za splošne namene bi moral pripraviti in posodabljati tehnično dokumentacijo, da bi jo na zahtevo dal na voljo Uradu za UI in pristojnim nacionalnim organom. Minimalni sklop elementov, ki jih je treba vključiti v tako dokumentacijo, bi bilo treba določiti v posebnih prilogah k tej uredbi. Na Komisijo bi bilo treba prenesti pooblastilo za spreminjanje navedenih prilog z delegiranimi akti glede na hiter tehnološki razvoj.
- (102) Programska oprema in podatki, vključno z modeli, objavljenimi na podlagi proste in odprtokodne licence, ki omogoča njihovo prosto izmenjavo in če uporabniki lahko prosto dostopajo do njih ali njihovih spremenjenih različic, jih uporabljajo, spreminjajo in ponovno distribuira, lahko prispevajo k raziskavam in inovacijam na trgu ter gospodarstvu Unije zagotovijo znatne priložnosti za rast. Razmisliti bi bilo treba o modelih UI za splošne namene, objavljenih na podlagi prostih in odprtokodnih licenc, da bi zagotovili visoko raven preglednosti in odprtosti, če so njihovi parametri, vključno z utežmi, informacijami o arhitekturi modela in informacijami o uporabi modela, javno dostopni. Licenca bi morala šteti za prosto in odprtokodno, tudi kadar uporabnikom omogoča uporabo, kopiranje, distribucijo, preučevanje, spreminjanje in izboljševanje programske opreme in podatkov, vključno z modeli, pod pogojem, da se navede originalni ponudnik modela in da se upoštevajo enaki ali primerljivi pogoji distribucije.
- (103) Brezplačne in odprtokodne komponente UI zajemajo programsko opremo in podatke, vključno z modeli in modeli UI za splošne namene, orodji, storitvami ali procesi sistema UI. Brezplačne in odprtokodne komponente UI se lahko zagotovijo prek različnih kanalov, vključno z njihovim razvojem v odprtih odložiščih. Za namene te uredbe komponente UI, ki se zagotavljajo proti plačilu ali so kako drugače monetizirane, med drugim z zagotavljanjem tehnične podpore ali drugih storitev, tudi prek platforme programske opreme, povezane s komponento UI, ali z uporabo osebnih podatkov iz razlogov, ki niso izključno namenjeni izboljšanju varnosti, združljivosti ali interoperabilnosti programske opreme, z izjemo transakcij med mikropodjetji, ne bi smele biti upravičene do izjem, določenih za brezplačne in odprtokodne komponente UI. Dejstvo, da so komponente UI na voljo prek odprtih odložišč, samo po sebi ne bi smelo pomeniti monetizacije.
- (104) Za ponudnike modelov UI za splošne namene, ki se objavijo na podlagi proste in odprtokodne licence ter katerih parametri, vključno z utežmi, informacijami o arhitekturi modela in informacijami o uporabi modela, so javno dostopni, bi morale veljati izjeme v zvezi z zahtevami glede preglednosti, ki veljajo za modele UI za splošne namene, razen če lahko šteje, da predstavljajo sistemsko tveganje; v tem primeru okoliščina, da je model pregleden in ga spremlja odprtokodna licenca, ne bi smela šteti za zadosten razlog za izključitev izpolnjevanja obveznosti iz te uredbe. V vsakem primeru pa glede na to, da objava modelov UI za splošne namene v okviru proste in odprtokodne licence ne razkrije nujno bistvenih informacij o naboru podatkov, ki se uporablja za učenje ali izpopolnjevanje modela, in o tem, kako je bila s tem zagotovljena skladnost z avtorskim pravom, se izjema, določena za modele UI za splošne namene, od skladnosti z zahtevami, povezanimi s preglednostjo, ne bi smela nanašati na obveznost priprave povzetka vsebine, ki se uporablja za učenje modelov, in obveznost vzpostavitve politike za skladnost z avtorskim pravom Unije, zlasti za opredelitev in skladnost s pridržkom pravic na podlagi člena 4(3) Direktive (EU) 2019/790 Evropskega parlamenta in Sveta ⁽⁴⁰⁾.
- (105) Modeli UI za splošne namene, zlasti veliki generativni modeli UI, ki lahko ustvarijo besedilo, slike in druge vsebine, predstavljajo edinstvene priložnosti za inovacije, pa tudi izzive za umetnike, avtorje in druge ustvarjalce ter njihov način ustvarjanja, razširjanja, uporabe in koriščenja njihovih ustvarjalnih vsebin. Za razvoj in učenje takih modelov je potreben dostop do velikih količin besedil, slik, videoposnetkov in drugih podatkov. Za pridobivanje in analizo takih vsebin, ki so lahko zaščitene z avtorskimi in sorodnimi pravicami, se lahko v tem kontekstu obsežno uporabljajo tehnike besedilnega in podatkovnega rudarjenja. Za vsako uporabo avtorsko zaščitene vsebine je potrebno dovoljenje zadevnega imetnika pravic, razen če se uporabljajo ustrezne izjeme in omejitve avtorskih pravic. Z Direktivo (EU) 2019/790 so bile uvedene izjeme in omejitve, ki pod določenimi pogoji omogočajo reprodukcije in izvlečke del ali drugih zaščitene predmetov za namene besedilnega in podatkovnega rudarjenja. Na podlagi teh

⁽⁴⁰⁾ Direktiva (EU) 2019/790 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o avtorski in sorodnih pravicah na enotnem digitalnem trgu in spremembi direktiv 96/9/ES in 2001/29/ES (UL L 130, 17.5.2019, str. 92).

pravil se lahko imetniki pravic odločijo, da bodo svoje pravice pridržali za svoja dela ali druge zaščitene predmete, da bi preprečili besedilno in podatkovno rudarjenje, razen če se to izvaja za namene znanstvenega raziskovanja. Kadar so pravice do izvetja izrecno in na ustrezen način pridržane, morajo ponudniki modelov UI za splošne namene pridobiti dovoljenje imetnikov pravic, če želijo v zvezi s takimi deli izvajati besedilno in podatkovno rudarjenje.

- (106) Ponudniki, ki dajejo modele UI za splošne namene na trg Unije, bi morali zagotoviti skladnost z ustreznimi obveznostmi iz te uredbe. V ta namen bi morali ponudniki modelov UI za splošne namene vzpostaviti politiko za skladnost s pravom Unije o avtorskih in sorodnih pravicah, zlasti za opredelitev pridržka pravic, ki jih izrazijo imetniki pravic na podlagi člena 4(3) Direktive (EU) 2019/790, in skladnost z njim. Vsak ponudnik, ki daje model UI za splošne namene na trg Unije, bi moral to obveznost izpolnjevati ne glede na jurisdikcijo, v kateri se izvajajo dejanja, povezana z avtorskimi pravicami, na katerih temelji učenje teh modelov UI za splošno rabo. To je potrebno za zagotovitev enakih konkurenčnih pogojev med ponudniki modelov UI za splošne namene, pri čemer noben ponudnik ne bi smel imeti konkurenčne prednosti na trgu Unije z uporabo standardov avtorskih pravic, ki so nižji od standardov, določenih v Uniji.
- (107) Da bi izboljšali preglednost podatkov, ki se uporabljajo pri predhodnem učenju in učenju modelov UI za splošne namene, vključno z besedilom in podatki, zaščitene s pravom, je ustrezno, da ponudniki takih modelov pripravijo in objavijo dovolj podroben povzetek vsebine, ki se uporablja za učenje modela UI za splošne namene. Upoštevajoč potrebo po varovanju poslovnih skrivnosti in zaupnih poslovnih informacij bi moral biti ta povzetek v svojem področju uporabe na splošno izčrpen in ne tehnično podroben, da bi strankam z zakonitimi interesi, vključno z imetniki avtorskih pravic, olajšali uveljavljanje in izvajanje njihovih pravic na podlagi prava Unije, na primer z navedbo glavnih zbirk podatkov ali naborov podatkov, ki so bili uporabljeni pri učenju, kot so velike zasebne ali javne podatkovne zbirke ali podatkovni arhivi, ter z opisno razlago drugih uporabljenih virov podatkov. Primerno je, da Urad za UI zagotovi predlogo za povzetek, ki bi moral biti preprost in učinkovit ter ponudniku omogočiti, da zagotovi zahtevani povzetek v opisni obliki.
- (108) Kar zadeva obveznosti ponudnikov modelov UI za splošne namene, da vzpostavijo politiko za skladnost z avtorskim pravom Unije in javno objavijo povzetek vsebine, uporabljene za učenje, bi moral Urad za UI spremljati, ali je ponudnik izpolnil te obveznosti brez preverjanja ali ocene učnih podatkov za vsak posamezen primer posebej z vidika njihove skladnosti z avtorskimi pravicami. Ta uredba ne vpliva na izvrševanje pravil o avtorskih pravicah, kot je določeno na podlagi prava Unije.
- (109) Izpolnjevanje obveznosti, ki veljajo za ponudnike modelov UI za splošne namene, bi moralo biti sorazmerno in primerno vrsti ponudnika modela, pri čemer bi bilo treba izključiti potrebo glede izpolnjevanja teh obveznosti za osebe, ki razvijajo ali uporabljajo modele za nepoklicne ali znanstvenoraziskovalne namene, vendar bi jih bilo treba kljub temu spodbujati k prostovoljnemu izpolnjevanju teh obveznosti. Brez poseganja v avtorsko pravo Unije bi bilo treba pri izpolnjevanju teh obveznosti ustrezno upoštevati velikost ponudnika in omogočiti poenostavljene načine izpolnjevanja obveznosti za MSP, vključno z zagonskimi podjetji, ki ne bi smeli predstavljati pretiranih stroškov in ne bi smeli odvracati od uporabe takih modelov. V primeru spremembe ali izpopolnjevanja modela bi morale biti obveznosti ponudnikov modelov UI za splošne namene omejene na to spremembo ali izpopolnitev, na primer z dopolnitvijo že obstoječe tehnične dokumentacije z informacijami o spremembah, vključno z novimi viri učnih podatkov, da bi izpolnili obveznosti glede verige vrednosti iz te uredbe.
- (110) Modeli UI za splošne namene bi lahko predstavljali sistemska tveganja, ki med drugim vključujejo vse dejanske ali razumno predvidljive negativne učinke v zvezi z večjimi nesrečami, motnjami v kritičnih sektorjih ter resnimi posledicami za javno zdravje in varnost, vse dejanske ali razumno predvidljive negativne učinke na demokratične procese ter javno in gospodarsko varnost ter razširjanje nezakonitih, lažnih ali diskriminatornih vsebin. Sistemska tveganja bi bilo treba razumeti tako, da se povečujejo z zmogljivostmi in dosegom modela, da se lahko pojavijo v celotnem življenjskem ciklu modela in da nanje vplivajo pogoji napačne uporabe, zanesljivost modela, pravičnost modela in varnost modela, stopnja avtonomije modela, njegov dostop do orodij, novi ali kombinirani načini, strategije objave in distribucije, možnost odstranitve varovalnih mehanizmov in drugi dejavniki. V mednarodnih pristopih je bilo do zdaj zlasti ugotovljeno, da je treba pozornost nameniti tveganjem, ki izhajajo iz morebitne namerne napačne uporabe ali nenamernih problemov pri nadzoru v zvezi z usklajevanjem s človeškim namenom; kemičnim, biološkim, radiološkim in jedrskim tveganjem, kot so načini, kako zmanjšati vstopne ovire, vključno

z razvojem orožja, nabavo njegove zasnove ali njegove uporabo; ofenzivnim kibernetiskim zmogljivostim, kot so načini, ki omogočajo odkrivanje, izkoriščanje ali operativno uporabo šibkih točk; učinkom interakcije in uporabe orodij, vključno na primer z zmogljivostjo za nadzor fizičnih sistemov in motenj v kritični infrastrukturi; tveganjem, povezanimi z modeli, ki izdelujejo kopije ali se „samoreplicirajo“ ali učijo druge modele; načinom, kako lahko modeli povzročijo škodljivo pristranskost in diskriminacijo, ker ustvarjajo tveganja za posameznike, skupnosti ali družbe; omogočanju dezinformacij ali ogrožanju zasebnosti z grožnjami demokratičnim vrednotam in človekovim pravicam; tveganju, da bi določen dogodek lahko povzročil verižno reakcijo z znatnimi negativnimi učinki, ki bi lahko vplivali na celo mesto, celotno domeno dejavnosti ali celotno skupnost.

- (111) Treba bi bilo določiti metodologijo za razvrstitev modelov UI za splošne namene kot modelov UI za splošne namene s sistemskimi tveganji. Ker sistemska tveganja izhajajo iz posebno visokih zmogljivosti, bi bilo treba za model UI za splošne namene šteti, da predstavlja sistemska tveganja, če ima zmogljivosti z visoko učinkovitostjo, ocenjene na podlagi ustreznih tehničnih orodij in metodologij, ali znaten vpliv na notranji trg zaradi svojega dosega. Zmogljivosti z visoko učinkovitostjo v modelih UI za splošne namene pomenijo zmogljivosti, ki so enake zmogljivostim, zabeleženim v najbolj naprednih modelih UI za splošne namene, ali jih presegajo. Celoten nabor zmogljivosti modela bi bilo mogoče bolje razumeti po tem, ko se da na trg ali ko so uvajalci v interakciji z modelom. V skladu z najspodobnejšimi tehnološkimi dosežki v času začetka veljavnosti te uredbe je kumulativni znesek izračuna, ki se uporablja za učenje modela UI za splošne namene, merjen z operacijami s plavajočo vejico, eden od ustreznih približkov za zmogljivosti modela. Kumulativni znesek izračuna, ki se uporablja za učenje, vključuje izračun, ki se uporablja za dejavnosti in metode, namenjene povečanju zmogljivosti modela pred uvedbo, kot so predhodno učenje, sintetično ustvarjanje podatkov in izpopolnjevanje. Zato bi bilo treba določiti začetni prag operacij s plavajočo vejico, ki, če ga doseže model UI za splošne namene, privede do domneve, da model šteje za model UI za splošne namene s sistemskimi tveganji. Ta prag bi bilo treba sčasoma prilagoditi, da bi odražal tehnološke in industrijske spremembe, kot so algoritemske izboljšave ali večja učinkovitost strojne opreme, dopolniti pa bi ga bilo treba z referenčnimi vrednostmi in kazalniki za zmogljivost modela. Za to bi moral Urad za UI sodelovati z znanstveno skupnostjo, industrijo, civilno družbo in drugimi strokovnjaki. Pragovi ter orodja in merila za ocenjevanje zmogljivosti z visoko učinkovitostjo bi morali v veliki meri predvideti splošno naravo, zmogljivosti in povezano sistemska tveganje modelov UI za splošne namene ter bi lahko upoštevali način dajanja modela na trg ali število uporabnikov, na katere bi lahko vplival. Za dopolnitev tega sistema bi morala Komisija imeti možnost, da sprejme posamezne odločitve, s katerimi model UI za splošne namene določi kot model UI za splošne namene s sistemskim tveganjem, če se ugotovi, da ima tak model zmogljivosti ali učinek, enakovreden tistim, zajetim z določenim pragom. To odločitev bi bilo treba sprejeti na podlagi splošne ocene meril za določitev modela UI za splošne namene s sistemskim tveganjem iz ene od prilog k tej uredbi, kot so kakovost ali velikost nabora učnih podatkov, število poslovnih in končnih uporabnikov, načini njihovega vnosa in izhoda, stopnja avtonomije in nadgradljivosti ali orodja, do katerih ima dostop. Komisija bi morala na obrazloženo zahtevo ponudnika, katerega model je bil označen za model UI za splošne namene s sistemskim tveganjem, upoštevati zahtevo in se lahko odloči, da ponovno oceni, ali lahko za model UI za splošne namene še vedno šteje, da predstavlja sistemska tveganja.
- (112) Pojasniti je treba tudi postopek za razvrstitev modela UI za splošne namene s sistemskimi tveganji. Za model UI za splošne namene, ki izpolnjuje veljavni prag za zmogljivosti z visoko učinkovitostjo, bi bilo treba domnevati, da je splošni model UI s sistemskim tveganjem. Ponudnik bi moral Urad za UI obvestiti najpozneje dva tedna po tem, ko so zahteve izpolnjene ali ko je znano, da bo model UI za splošne namene izpolnjeval zahteve, ki vodijo do te domneve. To je zlasti pomembno v zvezi s pragom operacij s plavajočo vejico, saj je pri učenju modelov UI za splošne namene potrebno precejšnje načrtovanje, ki vključuje vnaprejšnjo dodelitev računalniških virov, zato lahko ponudniki modelov UI za splošne namene vedo, ali bi njihov model dosegel prag pred zaključkom učenja. V okviru tega obvestila bi moral biti ponudnik sposoben dokazati, da model UI za splošne namene zaradi svojih posebnih značilnosti izjemoma ne predstavlja sistemskih tveganj in ga zato ne bi smeli razvrstiti kot model UI za splošne

namene s sistemskimi tveganji. Te informacije so dragocene za Urad za UI pri predvidevanju dajanja modelov UI za splošne namene s sistemskimi tveganji na trg, ponudniki pa lahko začnejo zgodaj sodelovati z Uradom za UI. Te informacije so zlasti pomembne v zvezi z modeli UI za splošne namene, za katere se načrtuje, da bodo objavljeni kot odprtokodni, saj bo po objavi odprtokodnega modela morda težje izvajati potrebne ukrepe za zagotovitev skladnosti z obveznostmi iz te uredbe.

- (113) Če Komisija ugotovi, da model UI za splošne namene izpolnjuje zahteve za razvrstitev kot model UI za splošne namene s sistemskim tveganjem, ki pred tem ni bil znan ali o njem zadevni ponudnik ni obvestil Komisije, bi morala biti Komisija pooblaščenca, da ga tako označi. Sistem kvalificiranih opozoril bi moral zagotavljati, da znanstveni odbor obvešča Urad za UI o modelih UI za splošne namene, ki bi jih morebiti bilo treba razvrstiti kot modele UI za splošne namene s sistemskim tveganjem, ter da ima Urad pregled nad lastnimi dejavnostmi spremljanja.
- (114) Za ponudnike modelov UI za splošne namene s sistemskimi tveganji bi morale poleg obveznosti, ki veljajo za ponudnike modelov UI za splošne namene, veljati tudi obveznosti, namenjene prepoznavanju in zmanjšanju teh tveganj ter zagotavljanju ustrezne ravni kibernetske varnosti, ne glede na to, ali se zagotavljajo kot samostojni modeli ali so vgrajeni v sistem UI ali proizvod. Za doseganje teh ciljev bi morala ta uredba od ponudnikov zahtevati, da izvedejo potrebne ocene modelov, zlasti pred prvim dajanjem na trg, vključno z izvajanjem in dokumentiranjem testiranja modelov po načelu kontradiktornosti, po potrebi tudi z notranjim ali neodvisnim zunanjim testiranjem. Poleg tega bi morali ponudniki modelov UI za splošne namene s sistemskimi tveganji redno ocenjevati in zmanjševati sistemska tveganja, med drugim na primer z uvedbo politik za obvladovanje tveganj, kot so postopki za zagotavljanje odgovornosti in upravljanja, spremljanjem po dajanju na trg, sprejetjem ustreznih ukrepov v celotnem življenjskem ciklu modela in sodelovanjem z ustreznimi akterji v celotni verigi vrednosti UI.
- (115) Ponudniki modelov UI za splošne namene s sistemskimi tveganji bi morali oceniti in zmanjšati morebitna sistemska tveganja. Če razvoj ali uporaba modela kljub prizadevanjem za prepoznavanje in preprečevanje tveganj, povezanih z modelom UI za splošne namene, ki lahko predstavlja sistemska tveganja, povzroči resen incident, bi ga moral ponudnik modela UI za splošne namene brez nepotrebnega odlašanja spremljati ter Komisiji in pristojnim nacionalnim organom poročati o vseh ustreznih informacijah in možnih popravnih ukrepih. Poleg tega bi morali ponudniki po potrebi zagotoviti ustrezno raven kibernetske varnosti modela in njegove fizične infrastrukture v celotnem življenjskem ciklu modela. Pri kibernetski varnosti zaradi sistemskih tveganj, povezanih z zlonamerno uporabo ali napadi, bi bilo treba ustrezno upoštevati naključno uhajanje iz modelov, nedovoljene različice, izogibanje varnostnim ukrepom in obrambo pred kibernetskimi napadi, nepooblaščenim dostopom ali krajo modela. Tovrstno varnost bi bilo mogoče olajšati z zaščito uteži modelov, algoritmov, strežnikov in naborov podatkov, na primer z operativnimi varnostnimi ukrepi za informacijsko varnost, posebnimi politikami na področju kibernetske varnosti, ustreznimi tehničnimi in uveljavljenimi rešitvami ter kibernetskim in fizičnim nadzorom dostopa, ki bi bili prilagojeni zadevnim okoliščinam in povezanim tveganjem.
- (116) Urad za UI bi moral spodbujati in olajšati pripravo, pregled in prilagoditev kodeksov prakse in pri tem upoštevati mednarodne pristope. K sodelovanju bi lahko bili povabljeni vsi ponudniki modelov UI za splošne namene. Za zagotovitev, da se v kodeksih prakse odrazijo najsodobnejši tehnološki dosežki in ustrezno upoštevajo različni vidiki, bi moral Urad za UI pri pripravi teh kodeksov sodelovati z ustreznimi pristojnimi nacionalnimi organi, po potrebi pa bi se lahko posvetoval z organizacijami civilne družbe ter drugimi ustreznimi deležniki in strokovnjaki, vključno z znanstvenim odborom. V teh kodeksih prakse bi morale biti določene obveznosti za ponudnike modelov UI za splošne namene in modelov UI za splošne namene s sistemskimi tveganji. Kar zadeva sistemska tveganja, bi morali kodeksi prakse poleg tega prispevati k vzpostavitvi taksonomije tveganja za vrsto in naravo sistemskih tveganj na ravni Unije, vključno z njihovimi viri. Kodeksi prakse bi morali biti osredotočeni tudi na specifične ocene tveganja in ukrepe za zmanjšanje tveganj.
- (117) Kodeksi prakse bi morali biti osrednje orodje za pravilno izpolnjevanje obveznosti za ponudnike modelov UI za splošne namene, ki so določene v tej uredbi. Ponudniki bi morali imeti možnost, da se pri dokazovanju izpolnjevanja obveznosti oprejo na kodekse prakse. Komisija se lahko odloči, da z izvedbenimi akti odobri kodeks prakse in mu podeli splošno veljavnost v Uniji oziroma, kot nadomestno možnost, določi skupna pravila za izvajanje ustreznih obveznosti, če kodeksa prakse do začetka uporabe te uredbe ni mogoče dokončati ali če ga Urad za UI ne šteje za ustreznega. Ko je harmonizirani standard objavljen in ko ga Urad za UI oceni kot primernega za izpolnjevanje

ustreznih obveznosti, bi morala za ponudnike veljati domneva o skladnosti, kadar ti izpolnjujejo evropski harmonizirani standard. Ponudniki modelov UI za splošne namene bi morali biti poleg tega sposobni z nadomestnimi ustreznimi sredstvi dokazati skladnost, če kodeksi prakse ali harmonizirani standardi niso na voljo ali če se odločijo, da se nanje ne bodo zanašali.

- (118) Ta uredba ureja sisteme UI in modele UI, saj za zadevne udeležence na trgu, ki te sisteme in modele dajejo na trg, v uporabo ali jih uporabljajo v Uniji, določa nekatere zahteve in obveznosti, s tem pa dopolnjuje obveznosti za ponudnike posredniških storitev, ki take sisteme ali modele vgrajujejo v svoje storitve, ki jih ureja Uredba (EU) 2022/2065. Kolikor so taki sistemi ali modeli vgrajeni v zelo velike spletne platforme ali zelo velike spletne iskalnike, zanje velja okvir za obvladovanje tveganj iz Uredbe (EU) 2022/2065. Zato bi bilo treba domnevati, da so ustrezne obveznosti iz te uredbe izpolnjene, razen če se v takih modelih pojavijo in prepoznajo pomembna sistemska tveganja, ki niso zajeta v Uredbi (EU) 2022/2065. V tem okviru morajo ponudniki zelo velikih spletnih platform in zelo velikih spletnih iskalnikov oceniti morebitna sistemska tveganja, ki izhajajo iz zasnove, delovanja in uporabe njihovih storitev, vključno s tem, kako zasnova algoritemskih sistemov, ki se uporabljajo v storitvi, lahko prispeva k takim tveganjem, pa tudi sistemska tveganja, ki izhajajo iz morebitne napačne uporabe. Ti ponudniki morajo ob spoštovanju temeljnih pravic sprejeti tudi ustrezne ukrepe za zmanjšanje tveganj.
- (119) Glede na hiter tempo inovacij in tehnološkega razvoja digitalnih storitev, ki spadajo na področje uporabe različnih instrumentov prava Unije, zlasti glede na uporabo in doseganje oseb, ki so jim namenjeni, se lahko sistemi UI, za katere se uporablja ta uredba, zagotavljajo kot posredniške storitve ali kot deli posredniških storitev v smislu Uredbe (EU) 2022/2065, ki bi jo bilo treba razlagati na tehnološko nevtralen način. Sistemi UI se lahko na primer uporabljajo za zagotavljanje spletnih iskalnikov, zlasti če sistem UI, kot je spletni klepetalni robot, načeloma izvaja poizvedbe na vseh spletiščih, nato pa rezultate vključi v svoje obstoječe znanje in posodobljeno znanje uporabi za ustvarjanje enega samega izhodnega podatka, v katerem so združeni različni viri informacij.
- (120) Poleg tega so obveznosti za ponudnike in uvajalce nekaterih sistemov UI iz te uredbe, ki omogočajo odkrivanje in razkrivanje dejstva, da so izhodni podatki teh sistemov umetno ustvarjeni ali prirejeni, še zlasti pomembne zato, da se olajša učinkovito izvajanje Uredbe (EU) 2022/2065. To velja zlasti za obveznosti za ponudnike zelo velikih spletnih platform ali zelo velikih spletnih iskalnikov, da prepoznajo in zmanjšajo sistemska tveganja, ki lahko izhajajo iz razširjanja umetno ustvarjenih ali prirejenih vsebin, zlasti tveganje dejanskih ali predvidljivih negativnih učinkov na demokratične procese, državljansko razpravo in volilne procese, tudi z dezinformacijami.
- (121) Standardizacija bi morala imeti ključno vlogo pri zagotavljanju tehničnih rešitev ponudnikom, da se zagotovi skladnost s to uredbo, ob upoštevanju najsodobnejših tehnoloških dosežkov, ter pri spodbujanju inovacij, konkurenčnosti in rasti na enotnem trgu. Skladnost s harmoniziranimi standardi, kot so opredeljeni v členu 2, točka 1(c), Uredbe (EU) št. 1025/2012 Evropskega parlamenta in Sveta ⁽⁴¹⁾ in od katerih se običajno pričakuje, da odražajo najsodobnejše tehnološke dosežke, bi morala predstavljati sredstvo, s katerim ponudniki dokažejo skladnost z zahtevami iz te uredbe. Zato bi bilo treba spodbujati uravnoteženo zastopanost interesov z vključitvijo vseh ustreznih deležnikov v razvoj standardov, zlasti MSP, potrošniških organizacij ter okoljskih in socialnih deležnikov v skladu s členoma 5 in 6 Uredbe (EU) št. 1025/2012. Da bi lažje dosegli skladnost, bi morala Komisija brez nepotrebnega odlašanja izdati zahteve za standardizacijo. Pri pripravi zahteve za standardizacijo se Komisija posvetuje s svetovalnim forumom in Odborom, da zbere ustrezno strokovno znanje. Ker pa ustrezni sklici na harmonizirane standarde še ne obstajajo, bi morala imeti Komisija možnost, da z izvedbenimi akti in po posvetovanju s svetovalnim forumom določi skupne specifikacije za nekatere zahteve iz te uredbe. Skupna specifikacija bi morala biti izjemna nadomestna rešitev, da se ponudniku olajša izpolnjevanje obveznosti glede skladnosti z zahtevami iz te uredbe, kadar nobena od evropskih organizacij za standardizacijo ne sprejme zahteve za standardizacijo ali kadar ustrezni harmonizirani standardi nezadostno obravnavajo pomisleke glede temeljnih pravic ali kadar harmonizirani standardi niso skladni z zahtevo ali kadar pride do zamud pri sprejetju ustreznega harmoniziranega standarda. Kadar je vzrok za takšno zamudo pri sprejetju harmoniziranega standarda tehnična

⁽⁴¹⁾ 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).

kompleksnost zadevnega standarda, bi morala Komisija to upoštevati preden se odloči za določitev skupnih specifikacij. Komisija naj pri pripravi skupnih specifikacij sodeluje z mednarodnimi partnerji in mednarodnimi organi za standardizacijo.

- (122) Brez poseganja v uporabo harmoniziranih standardov in skupnih specifikacij je primerno, da se za ponudnike visokotveganega sistema UI, ki je bil naučen in testiran na podlagi podatkov, ki odražajo specifično geografsko, vedenjsko, vsebinsko ali funkcionalno okolje, v katerem naj bi se ta sistem uporabljal, domneva, da delujejo skladno z ustreznim ukrepom, določenim na podlagi zahteve glede upravljanja podatkov iz te uredbe. Brez poseganja v zahteve glede robustnosti in točnosti iz te uredbe bi bilo treba v skladu s členom 54(3) Uredbe (EU) 2019/881 domnevati, da so visokotvegani sistemi UI, ki so bili certificirani ali za katere je bila izdana izjava o skladnosti v okviru sheme za kibernetsko varnost na podlagi navedene uredbe, ob tem pa so bili sklici na zadevno shemo objavljeni v *Uradnem listu Evropske unije*, skladni z zahtevo glede kibernetske varnosti iz te uredbe, če certifikat kibernetske varnosti ali izjava o skladnosti ali njen del vključuje zahtevo glede kibernetske varnosti iz te uredbe. To ne posega v prostovoljno naravo navedene sheme za kibernetsko varnost.
- (123) Da bi zagotovili visoko raven zaupanja v visokotvegane sisteme UI, bi bilo treba za te sisteme pred dajanjem na trg ali v uporabo opraviti ugotavljanje skladnosti.
- (124) Da bi čim bolj zmanjšali breme za operaterje in se izognili morebitnemu podvajanju, je primerno, da bi skladnost visokotveganih sistemov UI, povezanih s proizvodi, za katere velja obstoječa harmonizacijska zakonodaja Unije, ki temelji na novem zakonodajnem okviru, z zahtevami te uredbe ocenili v okviru ugotavljanja skladnosti, kot je že določeno navedena zakonodaja. Uporaba zahtev iz te uredbe torej ne bi smela vplivati na posebno logiko, metodologijo ali splošno strukturo ugotavljanja skladnosti na podlagi ustrezne harmonizacijske zakonodaje Unije.
- (125) Zaradi kompleksnosti visokotveganih sistemov UI in z njimi povezanih tveganj je pomembno razviti ustrezen postopek ugotavljanja skladnosti visokotveganih sistemov UI, ki vključuje priglašene organe, tako imenovano ugotavljanje skladnosti s strani tretjih oseb. Glede na sedanje izkušnje poklicnih izdajateljev potrdil pred dajanjem na trg na področju varnosti proizvodov in glede na različno naravo zadevnih tveganj, pa je primerno, da se vsaj v začetni fazi uporabe te uredbe omeji področje uporabe ugotavljanja skladnosti s strani tretjih oseb na visokotvegane sisteme UI, ki niso povezani s proizvodi. Zato bi moral ugotavljanje skladnosti takih sistemov praviloma opraviti ponudnik na lastno odgovornost, z edino izjemo sistemov UI, namenjenih uporabi za biometriko.
- (126) Za izvedbo ugotavljanja skladnosti s strani tretjih oseb, kadar je potrebno, bi morali pristojni nacionalni organi na podlagi te uredbe priglasiti priglašene organe, pod pogojem, da izpolnjujejo vrsto zahtev, zlasti glede neodvisnosti, kompetenc, neobstoja navzkrižja interesov, pa tudi zahtev glede kibernetske varnosti. Pristojni nacionalni organi bi morali prigrasitev teh organov poslati Komisiji in drugim državam članicam prek elektronskega orodja za prigrasitev, ki ga razvije in upravlja Komisija na podlagi člena R23 Priloge I k Sklepu št. 768/2008/ES.
- (127) V skladu z zavezami Unije iz Sporazuma Svetovne trgovinske organizacije o tehničnih ovirah v trgovini je ustrezno olajšati vzajemno priznavanje rezultatov ugotavljanja skladnosti, ki jih pridobijo pristojni organi za ugotavljanje skladnosti ne glede na to, kje imajo sedež, pod pogojem, da navedeni organi za ugotavljanje skladnosti, ustanovljeni na podlagi prava tretje države, izpolnjujejo veljavne zahteve iz te uredbe in če je Unija v ta namen sklenila sporazum. V zvezi s tem bi morala Komisija v ta namen dejavno preučiti morebitne mednarodne instrumente in si zlasti prizadevati za sklenitev sporazumov s tretjimi državami o vzajemnem priznavanju.
- (128) V skladu s skupno uveljavljenim pojmom bistvene spremembe za proizvode, ki jih ureja harmonizacijska zakonodaja Unije, je primerno, da ob vsaki spremembi, ki bi lahko vplivala na skladnost visokotveganega sistema UI s to uredbo (npr. spremembi arhitekture operacijskega sistema ali programske opreme), ali kadar se spremeni predvideni namen sistema, ta sistem UI šteje za nov sistem UI, za katerega bi bilo treba opraviti novo ugotavljanje skladnosti. Vendar spremembe algoritma in zmogljivosti sistemov UI, 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.

- (129) Visokotvegani sistemi UI bi morali imeti oznako CE, ki označuje njihovo skladnost s to uredbo, da se lahko prosto gibljejo na notranjem trgu. Visokotvegani sistemi UI, ki so vgrajeni v proizvod, bi morali biti označeni s fizično oznako CE, ki jo lahko dopolnjuje digitalna oznaka CE. Za visokotvegane sisteme UI, ki se zagotavljajo samo digitalno, bi bilo treba uporabljati digitalno oznako CE. Države članice ne bi smele neupravičeno ovirati dajanja na trg ali v uporabo visokotveganih sistemov UI, ki izpolnjujejo zahteve iz te uredbe in nosijo oznako CE.
- (130) V določenih okoliščinah je lahko hitra razpoložljivost inovativnih tehnologij ključnega pomena za zdravje in varnost ljudi, varstvo okolja in podnebne spremembe ter za družbo kot celoto. Zato je primerno, da bi iz izjemnih razlogov javne varnosti ali varstva življenja in zdravja fizičnih oseb, varstva okolja ter zaščite ključne industrijskih in infrastrukturnih sredstev organi za nadzor trga lahko dovolili dajanje na trg ali v uporabo sistemov UI, za katere ugotavljanje skladnosti ni bilo opravljeno. V ustrezno utemeljenih primerih, kot je določeno v tej uredbi, lahko organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali organi civilne zaščite dajo določen visokotvegani sistem UI v uporabo brez dovoljenja organa za nadzor trga, če se za tako dovoljenje brez nepotrebnega odlašanja zaprosi med uporabo ali po njej.
- (131) Da bi olajšali delo Komisije in držav članic na področju UI ter povečanje preglednosti za javnost, bi bilo treba od ponudnikov visokotveganih sistemov UI, razen tistih, povezanih s proizvodi, ki spadajo na področje uporabe ustreznih obstoječe harmonizacijske zakonodaje Unije, ter ponudnikov, ki menijo, da sistem UI s seznama visokotveganih primerov uporabe iz priloge k tej uredbi, ni visokotvegani na podlagi odstopanja, zahtevati, da se registrirajo v podatkovni zbirki EU, ki jo vzpostavi in upravlja Komisija, in da v tej zbirki beležijo tudi informacije o svojih sistemih UI. Pred uporabo sistema UI s seznama visokotveganih primerov uporabe iz priloge k tej uredbi bi se morali uvajalci visokotveganih sistemov UI, ki so javni organi, agencije ali telesa, registrirati v taki zbirki in izbrati sistem, ki ga nameravajo uporabljati. Drugi uvajalci bi morali imeti pravico do prostovoljne registracije. Ta del podatkovne zbirke EU bi moral biti javno dostopen in brezplačen, informacije pa bi morale biti zlahka dostopne, razumljive in strojno berljive. Podatkovna zbirka EU bi prav tako morala biti prilagojena uporabnikom, na primer z zagotavljanjem funkcije iskanja, tudi s ključnimi besedami, da bi širša javnost lahko našla ustrezne informacije, ki se predložijo ob registraciji visokotveganih sistemov UI in o primeru uporabe visokotveganih sistemov UI iz priloge k tej uredbi za zadevne visokotvegane sisteme UI. V podatkovni zbirki EU bi bilo treba registrirati tudi bistvene spremembe visokotveganih sistemov UI. Za visokotvegane sisteme UI na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, migracij, azila in upravljanja nadzora meja bi bilo treba obveznosti registracije izpolniti v varnem, nejavnem delu podatkovne zbirke EU. Dostop do varnega dela, ki ni dostopen javnosti, bi moral biti strogo omejen na Komisijo in organe za nadzor trga, kar zadeva njihov nacionalni del te podatkovne zbirke. Visokotvegani sistemi UI na področju kritične infrastrukture bi morali biti registrirani le na nacionalni ravni. Komisija bi morala biti upravitelj podatkovne zbirke EU v skladu z Uredbo (EU) 2018/1725. Za zagotovitev polne funkcionalnosti podatkovne zbirke ob njeni uvedbi bi moral postopek za njeno vzpostavitev vključevati razvoj funkcionalnih specifikacij s strani Komisije in neodvisno revizijsko poročilo. Komisija bi morala pri opravljanju nalog upravljalca podatkov v podatkovni zbirki EU upoštevati tveganja, povezana s kibernetsko varnostjo. Podatkovna zbirka EU, vključno z informacijami, ki so prek nje na voljo, bi morala izpolnjevati zahteve iz Direktive (EU) 2019/882, da bi bila javnosti čim bolj dostopna in uporabna.
- (132) Nekateri sistemi UI, namenjeni stikom s fizičnimi osebami ali ustvarjanju vsebine, lahko predstavljajo posebna tveganja izdajanja za drugo osebo ali zavajanja, ne glede na to, ali se uvrščajo med sisteme visokega 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 visokotvegane sisteme UI, in ciljne izjeme, da bi upoštevali posebne potrebe na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Zlasti bi bilo treba fizične osebe obvestiti, da so v interakciji s sistemom UI, 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 te obveznosti bi bilo treba upoštevati značilnosti fizičnih oseb, ki zaradi svoje starosti ali invalidnosti pripadajo ranljivim skupinam, kolikor je namen sistema UI tudi interakcija s temi skupinami. Poleg tega bi bilo treba fizične osebe obvestiti, kadar so izpostavljene sistemom UI, ki lahko s obdelavo njihovih biometričnih podatkov prepoznajo čustva ali namere teh oseb ali sklepajo o njih oziroma te osebe razvrstijo 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. Take informacije in obvestila bi bilo treba zagotoviti v invalidom dostopnih oblikah.

- (133) Različni sistemi UI lahko ustvarijo velike količine sintetičnih vsebin, ki jih ljudje vse težje razlikujejo od vsebin, ki jih ustvari človek, in verodostojnih vsebin. Široka razpoložljivost in večje zmogljivosti teh sistemov pomembno vplivajo na integriteto informacijskega ekosistema in zaupanje vanj, saj se pojavljajo nova tveganja dezinformacij in obsežnega prirejanja, goljufij, izdajanja za drugo osebo in zavajanja potrošnikov. Glede na navedene vplive, hiter tempo tehnološkega razvoja ter potrebo po novih metodah in tehnikah za sledenje izvoru informacij je primerno od ponudnikov navedenih sistemov zahtevati, da vključijo tehnične rešitve, ki v strojno berljivi obliki omogočajo označevanje in zaznavanje, da je izhodne podatke ustvaril ali priredil sistem UI in ne človek. Take tehnike in metode bi morale biti dovolj zanesljive, interoperabilne, učinkovite in robustne, kolikor je to tehnično izvedljivo, ob upoštevanju razpoložljivih tehnik ali kombinacije takih tehnik, kot so vodni žigi, prepoznavanje metapodatkov, kriptografske metode za dokazovanje izvora in pristnosti vsebine, metode beleženja, prstni odtisi ali druge tehnike, kot je ustrezno. Ponudniki bi morali pri izvajanju te obveznosti upoštevati tudi posebnosti in omejitve različnih vrst vsebin ter zadevni tehnološki in tržni razvoj na tem področju, pokazatelj katerega so splošno priznani najsodobnejši tehnološki dosežki. Takšne tehnike in metode se lahko izvajajo na ravni sistema UI ali na ravni modela UI, vključno z modeli UI za splošne namene, ki ustvarjajo vsebino, da se ponudniku sistema UI nižje v verigi omogoči lažje izpolnjevanje te obveznosti. Da bi ta obveznost označevanja ostala sorazmerna, je primerno predvideti, da ne bi smela zajemati sistemov UI, ki zagotavljajo predvsem podporno funkcijo za standardno urejanje, ali sistemov UI, ki ne spreminjajo bistveno vhodnih podatkov, ki jih zagotovi uvajalec, ali njihove semantike.
- (134) Poleg tehničnih rešitev, ki jih uporabljajo ponudniki sistema UI, bi morali uvajalci, ki sistem UI uporabljajo za ustvarjanje ali prirejanje slikovnih, zvočnih ali video vsebin, ki v znatni meri spominjajo na obstoječe osebe, predmete, mesta ali dogodke in bi se osebi zmotno zdele verodostojne ali resnične (globoki ponaredki), na jasn in razpoznaven način tudi razkriti, da je bila vsebina umetno ustvarjena ali prirejena, tako da ustrezno označijo izhodne podatke UI in razkrijejo njihov umetni izvor. Skladnost s to obveznostjo glede preglednosti se ne bi smela razlagati tako, da pomeni, da uporaba sistema UI ali njegovih izhodnih podatkov ovira pravico do svobode izražanja ter pravico do svobode umetnosti in znanosti, ki ju zagotavlja Listina, zlasti kadar je vsebina del očitno ustvarjalnega, satiričnega, umetniškega, izmišljenega ali podobnega dela ali programa, ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine tretjih oseb. V teh primerih je obveznost glede preglednosti za globoke ponaredke iz te uredbe omejena na to, da se obstoj tako ustvarjenih ali prirejenih vsebin ustrezno razkrije na način, ki ne ovira prikazovanja dela ali uživanja v njem, vključno z njegovo običajno eksploatacijo in uporabo, ob ohranjanju uporabnosti in kakovosti dela. Primerno je tudi predvideti podobno obveznost razkritja v zvezi z besedilom, ustvarjenim ali prirejenim z UI, če je objavljeno z namenom obveščanja javnosti o zadevah javnega interesa, razen če je vsebino, ustvarjeno z UI, pregledal človek ali urednik, ob tem pa fizična ali pravna oseba nosi uredniško odgovornost za objavo vsebine.
- (135) Komisija lahko brez poseganja v obvezno naravo in polno uporabo obveznosti glede preglednosti prav tako spodbuja in olajšuje pripravo kodeksov prakse na ravni Unije, da se olajša učinkovito izvajanje obveznosti v zvezi z odkrivanjem in označevanjem umetno ustvarjenih ali prirejenih vsebin, po potrebi vključno s podporo praktičnim ureditvam za omogočanje dostopa do mehanizmov odkrivanja, in olajšanje sodelovanja z drugimi akterji vzdolž verige vrednosti, razširjanje vsebine ali preverjanje njene pristnosti in izvora, da se javnosti omogoči učinkovito razlikovanje vsebin, ustvarjenih z UI.
- (136) Obveznosti za ponudnike in uvajalce nekaterih sistemov UI iz te uredbe, da omogočijo odkrivanje in razkrivanje dejstva, da so izhodni podatki teh sistemov umetno ustvarjeni ali prirejeni, so še zlasti pomembne, da se olajša učinkovito izvajanje Uredbe (EU) 2022/2065. To velja zlasti za obveznosti za ponudnike zelo velikih spletnih platform ali zelo velikih spletnih iskalnikov, da prepoznajo in zmanjšajo sistemska tveganja, ki lahko izhajajo iz razširjanja umetno ustvarjenih ali prirejenih vsebin, zlasti tveganje dejanskih ali predvidljivih negativnih učinkov na demokratične procese, državljansko razpravo in volilne procese, tudi z dezinformacijami. Zahteva za označevanje s sistemi UI ustvarjenih vsebin na podlagi te uredbe ne posega v obveznost iz člena 16(6) Uredbe (EU) 2022/2065, da ponudniki storitev gostovanja obravnavajo prijave nezakonitih vsebin, prejete na podlagi člena 16(1) navedene uredbe, ter ne bi smela vplivati na oceno in odločitve o nezakonitosti določene vsebine. To oceno bi bilo treba opraviti izključno ob upoštevanju pravil, ki urejajo zakonitost vsebine.

- (137) Skladnosti z navedenimi obveznostmi glede preglednosti za sisteme UI iz te uredbe ne bi smeli razlagati tako, da pomeni, da je uporaba sistema UI ali njegovih izhodnih podatkov zakonita na podlagi te uredbe ali drugega prava Unije in prava držav članic, ter ne bi smela posegati v druge obveznosti uvajalcev sistemov UI glede preglednosti, določene v pravu Unije ali nacionalnem pravu.
- (138) UI je hitro razvijajoča se skupina tehnologij, ki zahteva regulativni nadzor ter varen in nadzorovan prostor za eksperimentiranje, ob zagotavljanju odgovornih inovacij ter vključevanja ustreznih zaščitnih ukrepov in ukrepov za zmanjšanje tveganj. Da bi zagotovili pravni okvir, ki spodbuja inovacije ter je primeren za prihodnost in odporen na motnje, bi morale države članice zagotoviti, da njihovi nacionalni pristojni organi na nacionalni ravni vzpostavijo vsaj en regulativni peskovnik za UI, da bi olajšali razvoj in testiranje inovativnih sistemov UI pod strogim regulativnim nadzorom, preden se ti sistemi dajo na trg ali kako drugače v uporabo. Države članice bi lahko to obveznost izpolnile tudi s sodelovanjem v že obstoječih regulativnih peskovnikih ali z vzpostavitvijo peskovnika skupaj s pristojnimi organi ene ali več držav članic, če tako sodelovanje sodelujočim državam članicam zagotavlja enakovredno raven nacionalne pokritosti. Regulativni peskovniki za UI bi lahko bili vzpostavljeni v fizični, digitalni ali hibridni obliki ter za fizične in digitalne izdelke. Organi, ki vzpostavijo regulativne peskovnike za UI, bi morali tudi zagotoviti, da imajo ti peskovniki ustrezne vire za svoje delovanje, vključno s finančnimi in človeškimi viri.
- (139) Cilji regulativnih peskovnikov za UI bi morali biti spodbujanje inovacij na področju UI z vzpostavitvijo nadzorovanega okolja za eksperimentiranje in testiranje v fazi razvoja ter pred trženjem, da se zagotovi skladnost inovativnih sistemov UI s to uredbo ter drugim ustreznim pravom Unije in nacionalnim pravom. Poleg tega bi moral biti cilj regulativnih peskovnikov za UI okrepitev pravne varnosti za inovatorje ter nadzora pristojnih organov in njihovega razumevanja priložnosti, nastajajočih tveganj in vplivov uporabe UI, olajšanje regulativnega učenja za organe in podjetja, tudi zaradi prihodnjih prilagoditev pravnega okvira, podpiranje sodelovanja in izmenjave najboljših praks z organi, vključenimi v regulativni peskovnik za UI, pa tudi pospešitev dostopa do trgov, med drugim z odpravo ovir za MSP, vključno z zagonskimi podjetji. Regulativni peskovniki za UI bi morali biti široko dostopni po vsej Uniji, posebno pozornost pa bi bilo treba nameniti njihovi dostopnosti za MSP, vključno z zagonskimi podjetji. Sodelovanje v regulativnem peskovniku za UI bi moralo biti osredotočeno na vprašanja, ki ustvarjajo pravno negotovost za ponudnike in potencialne ponudnike pri inovacijah, eksperimentiranju z UI v Uniji in prispevanju k regulativnemu učenju, ki temelji na dokazih. Nadzor sistemov UI v regulativnem peskovniku za UI bi zato moral zajemati njihov razvoj, učenje, testiranje in validacijo, 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. Vsa pomembna tveganja, prepoznana med razvojem in testiranjem takih sistemov UI, bi bilo treba ustrezno zmanjšati, če to ni mogoče, pa postopek razvoja in testiranja ustaviti. Kadar je primerno, bi morali pristojni nacionalni organi, ki vzpostavijo regulativne peskovnike za UI, sodelovati z drugimi ustreznimi organi, vključno s tistimi, ki nadzirajo varstvo temeljnih pravic, in bi lahko omogočili sodelovanje drugih akterjev v ekosistemu UI, kot so nacionalne ali evropske organizacije za standardizacijo, priglašeni organi, centri za testiranje in eksperimentiranje, laboratoriji za raziskave in eksperimentiranje, evropska vozlišča za digitalne inovacije 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 za UI in okvir za sodelovanje med ustreznimi organi, vključenimi v nadzor peskovnikov. Regulativni peskovniki za UI, vzpostavljeni na podlagi te uredbe, ne bi smeli posegati v drugo pravo, ki omogoča vzpostavitev drugih peskovnikov, katerih namen je zagotoviti skladnost s pravom, ki ni ta uredba. Ustrezni pristojni organi, odgovorni za te druge regulativne peskovnike, bi morali, kadar je primerno, upoštevati koristi uporabe teh peskovnikov tudi za namen zagotavljanja skladnosti sistemov UI s to uredbo. Po dogovoru med pristojnimi nacionalnimi organi in udeleženci v regulativnem peskovniku za UI se lahko testiranje v realnih razmerah izvaja in nadzira tudi v okviru regulativnega peskovnika za UI.
- (140) Ta uredba bi morala zagotoviti pravno podlago, da ponudniki in potencialni ponudniki v regulativnem peskovniku za UI osebne podatke, zbrane za druge namene, uporabijo za razvoj nekaterih sistemov UI v javnem interesu v okviru regulativnega peskovnika za UI samo pod določenimi pogoji v skladu s členom 6(4) in členom 9(2), točka (g), Uredbe (EU) 2016/679, členi 5, 6 in 10 Uredbe (EU) 2018/1725 ter brez poseganja v člen 4(2) in člen 10 Direktive (EU) 2016/680. Vse druge obveznosti upravljavcev podatkov in pravice posameznikov, na katere se nanašajo osebni podatki, na podlagi uredb (EU) 2016/679 in (EU) 2018/1725 ter Direktive (EU) 2016/680 se še naprej uporabljajo. Ta uredba zlasti ne bi smela zagotavljati pravne podlage v smislu člena 22(2), točka (b), Uredbe (EU) 2016/679 in člena 24(2), točka (b), Uredbe (EU) 2018/1725. Ponudniki in potencialni ponudniki

v regulativnemu peskovniku za UI bi morali zagotoviti ustrezne zaščitne ukrepe in sodelovati s pristojnimi organi, tudi z upoštevanjem njihovih smernic ter hitrim in dobronamernim ukrepanjem, da bi ustrezno zmanjšali vsa prepoznana znatna tveganja za varnost, zdravje in temeljne pravice, ki se lahko pojavijo med razvojem, testiranjem in eksperimentiranjem v tem peskovniku.

- (141) Da bi pospešili proces razvoja visokotveganih sistemov UI s seznama v eni od prilog k tej uredbi in njihovega dajanja na trg, je pomembno, da imajo tudi ponudniki ali potencialni ponudniki takih sistemov koristi od posebne ureditve za testiranje teh sistemov v realnih razmerah brez sodelovanja v regulativnem peskovniku za UI. Vendar bi bilo treba v takih primerih, ob upoštevanju možnih posledic takega testiranja za posameznike zagotoviti, da se s to uredbo za ponudnike ali potencialne ponudnike uvedejo ustrezna in zadostna jamstva in pogoji. Taka jamstva bi morala med drugim vključevati zahtevo, da je za sodelovanje fizičnih oseb pri testiranju v realnih razmerah potrebna informirana privolitev, razen ko gre za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ko bi pridobitev informirane privolitve preprečila testiranje sistema UI. Privolitev posameznikov, da sodelujejo pri takem testiranju na podlagi te uredbe, se razlikuje od privolitve posameznikov, na katere se nanašajo osebni podatki, v obdelavo njihovih osebnih podatkov na podlagi ustrezne zakonodaje o varstvu podatkov in vanjo ne posega. Pomembno je tudi čim bolj zmanjšati tveganja in pristojnim organom omogočiti nadzor ter zato od potencialnih ponudnikov zahtevati, da imajo načrt testiranja v dejanskih razmerah, ki ga predložijo pristojnemu organu za nadzor trga, da testiranje registrirajo v namenskih delih podatkovne zbirke EU, ob upoštevanju nekaterih omejenih izjem, da določijo omejitve obdobja, v katerem je mogoče opraviti testiranje, in da zahtevajo dodatne zaščitne ukrepe za osebe, ki pripadajo določenim ranljivim skupinami, ter da imajo pisni dogovor, v katerem so opredeljene vloge in odgovornosti potencialnih ponudnikov in uvajalcev, ter učinkovit nadzor, ki ga izvaja usposobljeno osebje, vključeno v testiranje v realnih razmerah. Poleg tega je primerno predvideti dodatne zaščitne ukrepe za zagotovitev, da se lahko napovedi, priporočila ali odločitve sistema UI učinkovito izničijo in zanemarijo ter da so osebni podatki zaščiteni in izbrisani, ko posamezniki umaknejo privolitev za sodelovanje v testiranju, brez poseganja v njihove pravice, ki jih imajo kot posamezniki, na katere se nanašajo osebni podatki, na podlagi prava Unije o varstvu podatkov. Kar zadeva prenos podatkov, je primerno predvideti tudi, da bi bilo treba podatke, zbrane in obdelane za namene testiranja v realnih razmerah, prenesti v tretje države le, če se izvajajo ustrezni in veljavni zaščitni ukrepi na podlagi prava Unije, zlasti v skladu z osnovami za prenos osebnih podatkov na podlagi prava Unije o varstvu podatkov, medtem ko so za neosebne podatke ustrezni zaščitni ukrepi vzpostavljeni v skladu s pravom Unije, kot sta uredbi (EU) 2022/868⁽⁴²⁾ in (EU) 2023/2854⁽⁴³⁾ Evropskega parlamenta in Sveta.
- (142) Da bi zagotovili, da bo UI privedla do družbeno in okoljsko koristnih rezultatov, se države članice spodbuja, naj podpirajo in spodbujajo raziskave in razvoj rešitev UI v podporo družbeno in okoljsko koristnim rezultatom, kot so rešitve, ki temeljijo na umetni inteligenci, za povečanje dostopnosti za invalide, odpravo socialno-ekonomskih neenakosti ali doseganje okoljskih ciljev, in sicer z dodelitvijo zadostnih sredstev, vključno z javnimi sredstvi in financiranjem Unije, ter, kadar je ustrezno in pod pogojem, da so izpolnjena merila za upravičenost in izbor, zlasti upoštevajoč projekte, ki vključujejo takšne cilje. Takšni projekti bi morali temeljiti na načelu interdisciplinarnega sodelovanja med razvijalci UI, strokovnjaki za neenakost in nediskriminacijo, dostopnost, potrošnike, okolje in digitalne pravice ter akademskimi krogi.
- (143) Za spodbujanje in zaščito inovacij je pomembno, da se upoštevajo interesi MSP, vključno z zagonskimi podjetji, ki so ponudniki ali uvajalci sistemov UI. V ta namen bi morale države članice razviti pobude, namenjene tem operaterjem, vključno z ozaveščanjem in sporočanjem informacij. Države članice bi morale MSP, vključno z zagonskimi podjetji, ki imajo registrirani sedež ali podružnico v Uniji, zagotoviti prednostni dostop do regulativnih peskovnikov za UI, če ti izpolnjujejo pogoje za upravičenost in merila za izbor, ter drugim ponudnikom in potencialnim ponudnikom ne preprečujejo dostopa do peskovnikov, če so izpolnjeni enaki pogoji in merila. Države članice bi morale uporabljati obstoječe kanale in po potrebi vzpostaviti nove namenske kanale za komunikacijo z MSP, vključno z zagonskimi podjetji, uvajalci, drugimi inovatorji in po potrebi z lokalnimi javnimi organi, da se MSP z zagotavljanjem smernic in odgovarjanjem na vprašanja o izvajanju te uredbe zagotovi podpora v celotnem razvojnem procesu. Ti kanali bi morali po potrebi sodelovati, da bi ustvarili sinergije in zagotovili homogenost svojih smernic za MSP, vključno z zagonskimi podjetji, in uvajalce. Države članice bi poleg tega morale olajševati sodelovanje MSP in drugih ustreznih deležnikov v postopkih razvoja standardizacije. Poleg tega bi se pri določanju pristojbin s strani priglasenih

⁽⁴²⁾ Uredba (EU) 2022/868 Evropskega parlamenta in Sveta z dne 30. maja 2022 o evropskem upravljanju podatkov in spremembi Uredbe (EU) 2018/1724 (Akt o upravljanju podatkov) (UL L 152, 3.6.2022, str. 1).

⁽⁴³⁾ Uredba (EU) 2023/2854 Evropskega parlamenta in Sveta z dne 13. decembra 2023 o harmoniziranih pravilih za pravičen dostop do podatkov in njihovo uporabo ter spremembi Uredbe (EU) 2017/2394 in Direktive (EU) 2020/1828 (akt o podatkih) (UL L, 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).

organov za ugotavljanje skladnosti morali upoštevati posebni interesi in potrebe ponudnikov, ki so MSP, vključno z zagonskimi podjetji. Komisija bi morala stroške certificiranja in skladnosti za MSP, vključno z zagonskimi podjetji, redno ocenjevati, in sicer s preglednimi posvetovanji, ter sodelovati z državami članicami za znižanje teh stroškov. Na primer, 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 uvajalcev. Za obravnavanje posebnih potreb MSP, vključno z zagonskimi podjetji, bi morala Komisija na zahtevo Odbora zagotoviti standardizirane predloge za področja, zajeta v tej uredbi. Poleg tega bi morala Komisija dopolniti prizadevanja držav članic z zagotovitvijo enotne informacijske platforme, ki vsebuje enostavno uporabne informacije v zvezi s to uredbo za vse ponudnike in uvajalce, organiziranjem ustreznih komunikacijskih kampanj za ozaveščanje o obveznostih, ki izhajajo iz te uredbe, ter ocenjevanjem in spodbujanjem zblíževanja najboljših praks v postopkih javnega naročanja v zvezi s sistemi UI. Srednja podjetja, ki so bila do nedavno opredeljena kot mala podjetja v smislu Priloge k Priporočilu Komisije 2003/361/ES⁽⁴⁴⁾, bi morala imeti dostop do teh podpornih ukrepov, saj ta nova srednja podjetja včasih morda nimajo pravnih sredstev in niso pridobila ustreznih usposabljanj, potrebnih za zagotovitev ustreznega razumevanja te uredbe in skladnosti z njo.

- (144) Za spodbujanje in zaščito inovacij bi morali platforma za UI na zahtevo, vsi ustrezni programi in projekti Unije za financiranje, kot sta programa Digitalna Evropa in Obzorje Evropa, ki jih izvajajo Komisija in države članice na ravni Unije ali nacionalni ravni, prispevati k doseganju ciljev te uredbe.
- (145) K izvajanju te uredbe bi morali prispevati platforma za UI na zahtevo, evropska vozlišča za digitalne inovacije ter centri za testiranje in eksperimentiranje, ki so jih vzpostavile Komisija in države članice na ravni Unije ali nacionalni ravni, in sicer da bi čim bolj zmanjšali tveganja za izvajanje, ki so posledica pomanjkanja znanja in strokovnega znanja na trgu, ter da bi ponudnikom, predvsem MSP, vključno z zagonskimi podjetji, in priglašeni organom olajšali izpolnjevanje njihovih obveznosti iz te uredbe. Platforma za UI na zahtevo, evropska vozlišča za digitalne inovacije ter centri za preskušanje in eksperimentiranje lahko ponudnikom in priglašeni organom v okviru svojih mandатов in pristojnosti zagotavljajo zlasti tehnično in znanstveno podporo.
- (146) Poleg tega je zaradi majhnosti nekaterih operaterjev in da se zagotovi sorazmernost, kar zadeva stroške inovacij, primerno, da se mikropodjetjem omogoči izpolnjevanje ene od najdražjih obveznosti, tj. vzpostavitve sistema upravljanja kakovosti, na poenostavljen način, kar bi zmanjšalo upravno breme in stroške za ta podjetja in ne bi vplivalo na raven varstva in potrebo po skladnosti z zahtevami za visokotvegane sisteme UI. Komisija bi morala pripraviti smernice za opredelitev elementov sistema upravljanja kakovosti, ki jih morajo mikropodjetja izpolnjevati na ta poenostavljen način.
- (147) Primerno je, da Komisija organom, skupinam ali laboratorijem, ustanovljenim ali akreditiranim na podlagi katere koli ustrezne harmonizacijske zakonodaje 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 na podlagi uredb (EU) 2017/745 in (EU) 2017/746.
- (148) S to uredbo bi bilo treba vzpostaviti okvir upravljanja, ki bi omogočal tako usklajevanje uporabe te uredbe in podporo uporabi na nacionalni ravni kot tudi krepitev zmogljivosti na ravni Unije in sodelovanje deležnikov s področja UI. Za učinkovito izvajanje in izvrševanje te uredbe je potreben okvir upravljanja, ki omogoča usklajevanje in pridobivanje centraliziranega strokovnega znanja na ravni Unije. Urad za UI je bil ustanovljen s sklepom Komisije⁽⁴⁵⁾ z mandatom razvijati strokovno znanje in zmogljivosti Unije na področju UI ter prispevati k izvajanju prava Unije o umetni inteligenci. Države članice bi morale olajšati naloge Urada za UI, da bi podpirale razvoj strokovnega znanja in zmogljivosti Unije na ravni Unije ter okrepile delovanje enotnega digitalnega trga. Poleg tega bi bilo treba ustanoviti odbor, sestavljen iz predstavnikov držav članic, znanstveni odbor za vključitev znanstvene skupnosti in svetovni forum, da se omogoči prispevanje deležnikov k izvajanju te uredbe na ravni Unije

⁽⁴⁴⁾ Priporočilo Komisije z dne 6. maja 2003 o opredelitvi mikro, malih in srednjih podjetij (UL L 124, 20.5.2003, str. 36).

⁽⁴⁵⁾ Sklep Komisije z dne 24. januarja 2024 o ustanovitvi Evropskega urada za umetno inteligenco C(2024) 390 final.

in nacionalni ravni. Razvoj strokovnega znanja in zmogljivosti Unije bi moral vključevati tudi uporabo obstoječih virov in strokovnega znanja, zlasti s pomočjo sinergij s strukturami, vzpostavljenimi v okviru izvrševanja drugega prava na ravni Unije, in sinergij s povezanimi pobudami na ravni Unije, kot so Skupno podjetje EuroHPC ter centri za testiranje in eksperimentiranje na področju UI v okviru programa Digitalna Evropa.

- (149) Da bi omogočili nemoteno, učinkovito in harmonizirano izvajanje te uredbe, bi bilo treba ustanoviti Odbor. Odbor bi moral odražati različne interese ekosistema UI in sestavljati bi ga morali predstavniki držav članic. Odgovoren bi moral biti za številne svetovalne naloge, med drugim za izdajanje mnenj, priporočil in nasvetov ali za prispevanje k dajanju smernic o zadevah, povezanih z izvajanjem te uredbe, vključno z zadevami glede izvrševanja, tehničnimi specifikacijami ali obstoječimi standardi v zvezi z zahtevami iz te uredbe, ter za svetovanje Komisiji ter državam članicam in njihovim pristojnim nacionalnim organom pri posebnih vprašanjih v zvezi z UI. Da bi državam članicam omogočili nekaj prožnosti pri imenovanju njihovih predstavnikov v Odbor, so lahko ti predstavniki katere koli osebe, ki pripadajo javnim subjektom, ter 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 priglasenimi 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 s členom 33 navedene uredbe bi morala Komisija podpirati dejavnosti stalne podskupine za nadzor trga z ocenjevanji ali študijami trga, zlasti z namenom opredelitve vidikov te uredbe, pri katerih je potrebno posebno in nujno usklajevanje med organi za nadzor trga. Odbor lahko ustanovi druge stalne ali začasne podskupine za preučitev posebnih vprašanj. Po potrebi bi moral sodelovati tudi z ustreznimi organi, strokovnimi skupinami in mrežami Unije, dejavnimi v okviru ustreznega prava Unije, zlasti tudi s tistimi, dejavnimi na podlagi ustreznega prava Unije o podatkih, digitalnih proizvodih in storitvah.
- (150) Za zagotavljanje sodelovanja deležnikov pri izvajanju in uporabi te uredbe, bi bilo treba vzpostaviti svetovalni forum, ki bi Odboru in Komisiji svetoval in jima zagotavljal tehnično strokovno znanje. Da bi zagotovili raznoliko in uravnoteženo zastopanost deležnikov glede na komercialne in nekomercialne interese, znotraj kategorije poslovnih interesov pa v zvezi z MSP in drugimi podjetji, bi moral biti svetovalni forum med drugim sestavljen iz predstavnikov industrije, zagonskih podjetij, MSP, akademskih krogov, civilne družbe, vključno s socialnimi partnerji, pa tudi Agencije za temeljne pravice, ENISA, Evropskega odbora za standardizacijo (CEN), Evropskega odbora za elektrotehniško standardizacijo (CENELEC) in Evropskega inštituta za telekomunikacijske standarde (ETSI).
- (151) Za podporo izvajanju in izvrševanju te uredbe, zlasti dejavnosti spremljanja, ki jih v zvezi z modeli UI za splošne namene izvaja Urad za UI, bi bilo treba ustanoviti znanstveni odbor neodvisnih strokovnjakov. Neodvisni strokovnjaki, ki sestavljajo znanstveni odbor, bi morali biti izbrani zaradi najnovejšega znanstvenega ali tehničnega strokovnega znanja na področju UI in bi morali svoje naloge opravljati nepristransko in objektivno ter zagotavljati zaupnost informacij in podatkov, pridobljenih pri izvajanju njihovih nalog in dejavnosti. Da bi omogočili okrepitev nacionalnih zmogljivosti, potrebnih za učinkovito izvrševanje te uredbe, bi morale imeti države članice možnost, da strokovnjake, ki sestavljajo znanstveni odbor, zaprosijo, da jim pomagajo pri dejavnostih izvrševanja.
- (152) Da bi podprli ustrezno izvrševanje v zvezi s sistemi UI in okrepili zmogljivosti držav članic, bi bilo treba vzpostaviti podporne strukture Unije za testiranje UI in jih dati na voljo državam članicam.
- (153) Države članice imajo ključno vlogo pri uporabi in izvrševanju te uredbe. V zvezi s tem bi morala vsaka država članica za pristojne nacionalne organe za namen nadzora uporabe in izvajanja te uredbe imenovati vsaj en priglasitveni organ in vsaj en organ za nadzor trga. Države članice se lahko v skladu s svojimi specifičnimi nacionalnimi organizacijskimi značilnostmi in potrebami odločijo, da za opravljanje nalog pristojnih nacionalnih organov v smislu te uredbe imenujejo kateri koli javni subjekt. Da bi na strani držav članic izboljšali učinkovitost organizacije ter vzpostavili enotno kontaktno točko za stike z javnostjo in drugimi partnerji na ravni držav članic in Unije, bi morala vsaka država članica imenovati organ za nadzor trga, ki deluje kot enotna kontaktna točka.

- (154) Pristojni nacionalni organi bi svoja pooblastila morali izvajati neodvisno, nepristransko in brez predsodkov, da bi zaščitili objektivnost svojih dejavnosti in nalog ter zagotovili uporabo in izvajanje te uredbe. Člani teh organov bi se morali vzdržati vseh dejanj, ki niso združljiva z njihovimi dolžnostmi, in zanje bi se morala uporabljati pravila o zaupnosti na podlagi te uredbe.
- (155) Da bi zagotovili, da ponudniki visokotveganih sistemov UI izkušnje pri uporabi visokotveganih sistemov UI lahko upoštevajo za izboljšanje svojih sistemov ter postopka zasnovane in razvoja ali da lahko pravočasno izvedejo morebitne popravne ukrepe, bi morali imeti vsi ponudniki vzpostavljen sistem spremljanja po dajanju na trg. Po potrebi bi spremljanje po dajanju na trg moralo vključevati analizo interakcije z drugimi sistemi UI, tudi drugimi napravami in programsko opremo. V spremljanje po dajanju na trg ne bi smeli biti zajeti občutljivi operativni podatki uvalcev, ki so organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Ta sistem je tudi ključen za zagotovitev učinkovitejše in pravočasnejše obravnave morebitnih tveganj, ki izhajajo iz sistemov UI, 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 resnih incidentih, ki so posledica uporabe njihovih sistemov UI, tj. incidentih ali okvarah, ki povzročijo smrt ali resno ogroženost zdravja, hude in nepopravljive motnje v upravljanju in delovanju kritične infrastrukture, kršitve obveznosti na podlagi prava Unije o zaščiti temeljnih pravic ali hudo škodo premoženju ali okolju.
- (156) 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 na podlagi te uredbe, bi morali imeti vsa izvršilna pooblastila, določena v tej uredbi in Uredbi (EU) 2019/1020, ter bi morali svoja pooblastila in dolžnosti izvajati neodvisno, nepristransko in brez predsodkov. Čeprav za večino sistemov UI ne veljajo posebne zahteve in obveznosti iz te uredbe, lahko organi za nadzor trga sprejmejo ukrepe v zvezi z vsemi sistemi UI, če ti predstavljajo tveganje v skladu s to uredbo. Zaradi posebne narave institucij, agencij in organov Unije, ki spadajo na področje uporabe te uredbe, je za organ za nadzor trga, ki bo pristojen zanje, primerno imenovati Evropskega nadzornika za varstvo podatkov. 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 po pravu Unije.
- (157) 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, tudi ne organov za enakost in organov za varstvo podatkov. Kadar je to potrebno za njihov mandat, bi morali imeti navedeni nacionalni javni organi ali telesa tudi dostop do kakršne koli dokumentacije, pripravljene na podlagi te uredbe. Določiti bi bilo treba poseben zaščitni postopek za zagotavljanje ustreznega in pravočasnega izvrševanja v zvezi s sistemi UI, ki predstavljajo tveganje za zdravje, varnost in temeljne pravice. Postopek za take sisteme UI, ki predstavljajo tveganje, bi bilo treba uporabljati za visokotvegane sisteme UI, ki predstavljajo tveganje, prepovedane sisteme, ki so bili dani na trg ali v uporabo oziroma se uporabljajo v skladu s prepovedanimi praksami iz te uredbe, in sisteme UI, ki predstavljajo tveganje in katerih dostopnost je bila omogočena v nasprotju z zahtevami glede preglednosti iz te uredbe.
- (158) Pravo Unije o finančnih storitvah vključuje pravila in zahteve glede notranjega upravljanja in obvladovanja tveganj, ki veljajo za regulirane finančne institucije med opravljanjem teh storitev, tudi kadar uporabljajo sisteme UI. Za zagotovitev usklajene uporabe in izvrševanja obveznosti na podlagi te uredbe ter ustreznih pravil in zahtev iz pravnih aktov Unije o finančnih storitvah bi bilo treba pristojne organe za nadzor in izvrševanje navedenih pravnih aktov, zlasti pristojne organe, opredeljene v Uredbi (EU) št. 575/2013 Evropskega parlamenta in Sveta⁽⁴⁶⁾ ter direktivah 2008/48/ES⁽⁴⁷⁾, 2009/138/ES⁽⁴⁸⁾, 2013/36/EU⁽⁴⁹⁾, 2014/17/EU⁽⁵⁰⁾ in (EU) 2016/97⁽⁵¹⁾ Evropskega

⁽⁴⁶⁾ Uredba (EU) št. 575/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o bonitetnih zahtevah za kreditne institucije in o spremembi Uredbe (EU) št. 648/2012 (UL L 176, 27.6.2013, str. 1).

⁽⁴⁷⁾ Direktiva 2008/48/ES Evropskega parlamenta in Sveta z dne 23. aprila 2008 o potrošniških kreditnih pogodbah in razveljavitvi Direktive Sveta 87/102/EGS (UL L 133, 22.5.2008, str. 66).

⁽⁴⁸⁾ Direktiva 2009/138/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o začetku opravljanja in opravljanju dejavnosti zavarovanja in pozavarovanja (Solventnost II) (UL L 335, 17.12.2009, str. 1).

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

⁽⁵⁰⁾ Direktiva 2014/17/EU Evropskega parlamenta in Sveta z dne 4. februarja 2014 o potrošniških kreditnih pogodbah za stanovanjske nepremičnine in spremembi direktiv 2008/48/ES in 2013/36/EU ter Uredbe (EU) št. 1093/2010 (UL L 60, 28.2.2014, str. 34).

⁽⁵¹⁾ Direktiva (EU) 2016/97 Evropskega parlamenta in Sveta z dne 20. januarja 2016 o distribuciji zavarovalnih produktov (UL L 26, 2.2.2016, str. 19).

parlamenta in Sveta, glede na njihove zadevne pristojnosti imenovati za pristojne organe za namen nadzora izvajanja te uredbe, vključno z dejavnostmi nadzora trga, v zvezi s sistemi UI, ki jih zagotavljajo 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 za izvrševanje zahtev in obveznosti iz te uredbe, vključno s pooblastili za izvajanje naknadnih dejavnosti nadzora trga, ki jih lahko, če je to primerno, vključijo v svoje obstoječe nadzorne mehanizme in postopke na podlagi zadevnega prava Unije o finančnih storitvah. Primerno je predvideti, da bi morali nacionalni organi, ki so odgovorni za nadzor kreditnih institucij, ki jih ureja Direktiva 2013/36/EU, in sodelujejo v enotnem mehanizmu nadzora, vzpostavljenem z Uredbo Sveta (EU) št. 1024/2013⁽⁵²⁾, kadar delujejo kot organi za nadzor trga na podlagi te uredbe, Evropski centralni banki nemudoma sporočiti vse informacije, pridobljene v okviru njihovih dejavnosti 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, je primerno v obstoječe obveznosti in postopke iz Direktive 2013/36/EU vključiti tudi nekatere postopkovne obveznosti ponudnikov v zvezi z obvladovanjem tveganj, spremljanjem po dajanju na trg ter dokumentacijo. Da bi se izognili prekrivanju, bi bilo treba predvideti tudi omejena odstopanja v zvezi s sistemom ponudnikov za upravljanje kakovosti in obveznostjo spremljanja, naloženo uvajalcem visokotveganih sistemov UI, če se ta uporabljajo za kreditne institucije, ki jih ureja Direktiva 2013/36/EU. Isto ureditev bi bilo treba uporabljati za zavarovalnice in pozavarovalnice ter zavarovalne holdinge na podlagi Direktive 2009/138/ES in zavarovalne posrednike na podlagi Direktive (EU) 2016/97 ter druge vrste finančnih institucij, za katere veljajo zahteve glede notranjega upravljanja, ureditev ali postopkov, vzpostavljenih na podlagi ustreznega prava Unije o finančnih storitvah, da se zagotovita doslednost in enaka obravnava v finančnem sektorju.

- (159) Vsak organ za nadzor trga za visokotvegane sisteme UI na področju biometrike, kot so navedeni v eni od prilog k tej uredbi, če se ti sistemi uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, migracij, azila in upravljanja nadzora meja ali za pravosodje in demokratične procese, bi moral imeti pooblastila za preiskovanje in popravne ukrepe, vključno vsaj s pooblastilom za pridobitev dostopa do vseh osebnih podatkov, ki se obdelujejo, in do vseh informacij, potrebnih za opravljanje njegovih nalog. Organi za nadzor trga bi morali imeti možnost, da svoja pooblastila izvajajo popolnoma neodvisno. Morebitne omejitve njihovega dostopa do občutljivih operativnih podatkov na podlagi te uredbe ne bi smele posegati v pooblastila, ki so jim podeljena z Direktivo (EU) 2016/680. Nobena izključitev glede razkritja podatkov nacionalnim organom za varstvo podatkov na podlagi te uredbe ne bi smela vplivati na sedanja ali prihodnja pooblastila teh organov zunaj področja uporabe te uredbe.
- (160) Organom za nadzor trga in Komisiji bi moralo biti omogočeno, da predlagajo skupne dejavnosti – vključno s skupnimi preiskavami, ki jih izvajajo organi za nadzor trga sami ali skupaj s Komisijo –, katerih cilj je spodbujanje skladnosti, odkrivanje neskladnosti, ozaveščanje ali zagotavljanje smernic v zvezi s to uredbo, kar zadeva posebne kategorije visokotveganih sistemov UI, za katere se ugotovi, da predstavljajo resno tveganje v dveh ali več državah članicah. Skupne dejavnosti za spodbujanje skladnosti bi bilo treba izvajati v skladu s členom 9 Uredbe (EU) 2019/1020. Urad za UI bi moral zagotavljati usklajevalno podporo za skupne preiskave.
- (161) Pojasniti je treba odgovornosti in pristojnosti na ravni Unije in nacionalni ravni v zvezi s sistemi UI, ki temeljijo na modelih UI za splošne namene. Da bi se izognili prekrivanju pristojnosti, kadar sistem UI temelji na modelu UI za splošne namene ter kadar model in sistem zagotavlja isti ponudnik, bi moral biti za nadzor na ravni Unije pristojen

⁽⁵²⁾ Uredba Sveta (EU) št. 1024/2013 z dne 15. oktobra 2013 o prenosu posebnih nalog, ki se nanašajo na politike bonitetnega nadzora kreditnih institucij, na Evropsko centralno banko (UL L 287, 29.10.2013, str. 63).

Urad za UI, ki bi moral v ta namen imeti pooblastila organa za nadzor trga v smislu Uredbe (EU) 2019/1020. V vseh drugih primerih so za nadzor sistemov UI še naprej odgovorni nacionalni organi za nadzor trga. Vendar bi morali organi za nadzor trga za sisteme UI za splošne namene, ki jih lahko uvajalci neposredno uporabljajo za vsaj en namen, ki je razvrščen kot visoko tveganje, sodelovati z Uradom za UI pri izvedbi ocen skladnosti ter o tem ustrezno obvestiti Odbor in druge organe za nadzor trga. Poleg tega bi morali imeti organi za nadzor trga možnost, da Urad za UI zaprosijo za pomoč, kadar organ za nadzor trga ne more zaključiti preiskave visokotveganega sistema UI, ker ne more dostopati do nekaterih informacij, ki se nanašajo na model UI za splošne namene, na katerem temelji visokotvegani sistem UI. V takih primerih bi se moral smiselno uporabljati postopek v zvezi s čezmejno medsebojno pomočjo iz poglavja VI Uredbe (EU) 2019/1020.

- (162) Da bi na ravni Unije čim bolj izkoristili centralizirano strokovno znanje in sinergije Unije, bi morala biti pooblastila za nadzor in izvrševanje obveznosti za ponudnike modelov UI za splošne namene v pristojnosti Komisije. Urad za UI bi moral imeti možnost, da izvede vse potrebne ukrepe za spremljanje učinkovitega izvajanja te uredbe v zvezi z modeli UI za splošne namene. Imeti bi moral možnost, da na lastno pobudo na podlagi rezultatov njegovih dejavnosti spremljanja ali na zahtevo organov za nadzor trga v skladu s pogoji iz te uredbe raziše morebitne kršitve pravil o ponudnikih modelov UI za splošne namene. Da bi podprli učinkovito spremljanje Urada za UI, bi bilo treba določiti možnost, da lahko ponudniki nižje v verigi vložijo pritožbe zaradi morebitnih kršitev pravil o ponudnikih modelov UI za splošne namene in sistemov UI.
- (163) Da bi dopolnili sisteme upravljanja modelov UI za splošne namene, bi moral znanstveni odbor prispevati k dejavnostim spremljanja Urada za UI, ki mu v nekaterih primerih lahko pošlje kvalificirana opozorila, ki sprožijo nadaljnje ukrepanje, kot so preiskave. To bi se moralo zgoditi, kadar znanstveni odbor utemeljeno sumi, da model UI za splošne namene predstavlja konkretno in prepoznavno tveganje na ravni Unije. To bi se prav tako moralo zgoditi, kadar znanstveni odbor utemeljeno sumi, da model UI za splošne namene izpolnjuje merila, na podlagi katerih bi moral biti razvrščen kot model UI za splošne namene s sistemskim tveganjem. Da se znanstvenemu svetu zagotovijo informacije, potrebne za opravljanje teh nalog, bi moral obstajati mehanizem, s katerim lahko znanstveni odbor zaprosi Komisijo, da od ponudnika zahteva dokumentacijo ali informacije.
- (164) Urad za UI bi moral imeti možnost, da sprejme potrebne ukrepe za spremljanje učinkovitega izvajanja in izpolnjevanja obveznosti za ponudnike modelov UI za splošne namene iz te uredbe. Urad za UI bi moral imeti možnost, da raziše morebitne kršitve v skladu s pooblastili na podlagi te uredbe, tudi tako, da zahteva dokumentacijo in informacije, izvaja ocenjevanje ter od ponudnikov modelov UI za splošne namene zahteva ukrepe. Pri izvajanju ocenjevanja in zato, da bi uporabili neodvisno strokovno znanje, bi moral Urad za UI imeti možnost vključiti neodvisne strokovnjake, da v njegovem imenu izvedejo ocenjevanje. Izpolnjevanje obveznosti bi moralo biti izvršljivo, med drugim z zahtevami za sprejetje ustreznih ukrepov, vključno z ukrepi za zmanjšanje tveganja v primeru prepoznanih sistemskih tveganj, ter z omejevanjem omogočanja dostopnosti modela na trgu, njegovim umikom ali odpoklicem. Kot zaščitni ukrepi, kadar je to potrebno poleg procesnih pravic iz te uredbe, bi morali imeti ponudniki modelov UI za splošne namene procesne pravice iz člena 18 Uredbe (EU) 2019/1020, ki bi se morale uporabljati smiselno in brez poseganja v bolj specifične procesne pravice iz te uredbe.
- (165) Razvoj sistemov UI, ki niso visokotvegani sistemi UI, v skladu z zahtevami iz te uredbe lahko pripelje do večjega koriščenja etične in zaupanja vredne UI v Uniji. Ponudnike sistemov UI, ki niso sistemi visokega tveganja, bi bilo treba spodbujati k oblikovanju kodeksov ravnanja, vključno s povezanimi mehanizmi upravljanja, ki bodo namenjeni spodbujanju prostovoljne uporabe nekaterih ali vseh obveznih zahtev, ki se uporabljajo za visokotvegane sisteme UI, prilagojeni predvidenemu namenu sistemov in manjšemu tveganju ter bodo v njih upoštevane razpoložljive tehnične rešitve in najboljše prakse v industriji, kot so modeli in podatkovne kartice. Ponudnike in po potrebi uvajalce vseh sistemov UI, ne glede na to, ali so sistemi visokega tveganja ali ne, in modelov UI bi bilo treba spodbujati tudi k prostovoljni uporabi dodatnih zahtev, povezanih na primer z elementi etičnih smernic Unije za

zaupanja vredno UI, okoljsko trajnostnostjo, ukrepi za pismenost na področju UI, zasnovo in razvojem sistemov UI, ki zagotavljata inkluzivnost in raznolikost, vključno s poudarkom na ranljivih osebah in dostopnostjo za invalide, sodelovanjem deležnikov, po potrebi s sodelovanjem ustreznih deležnikov, kot so podjetja in organizacije civilne družbe, akademski krogi, raziskovalne organizacije, sindikati in organizacije za varstvo potrošnikov, pri zasnovi in razvoju sistemov UI, ter z raznolikostjo razvojnih skupin, vključno z uravnoteženo zastopanostjo spolov. Da bi zagotovili učinkovitost prostovoljnih kodeksov ravnanja, bi morali ti temeljiti na jasnih ciljih in ključnih kazalnikih uspešnosti za merjenje doseganja teh ciljev. Prav tako bi jih bilo treba razvijati na inkluziven način, kot je ustrezno, ob sodelovanju ustreznih deležnikov, kot so podjetja in organizacije civilne družbe, akademski krogi, raziskovalne organizacije, sindikati in organizacije za varstvo potrošnikov. Komisija lahko pripravi pobude, tudi sektorske narave, da se omogoči zmanjšanje tehničnih ovir za čezmejno izmenjavo podatkov za razvoj UI, tudi na infrastrukturi za dostop do podatkov, ter semantično in tehnično interoperabilnost različnih vrst podatkov.

- (166) Pomembno je, da so sistemi UI, ki so povezani s proizvodi brez visokega tveganja v skladu s to uredbo in jim zato ni treba izpolnjevati zahtev za visokotvegane sisteme UI, kljub temu varni, ko so dani na trg ali v uporabo. Da bi prispevali k temu cilju, bi se Uredba (EU) 2023/988 Evropskega parlamenta in Sveta ⁽⁵³⁾ uporabljala kot varnostna mreža.
- (167) Za zagotovitev zaupanja vrednega in konstruktivnega sodelovanja pristojnih organov na ravni Unije in nacionalni ravni bi morale vse strani, ki sodelujejo pri uporabi te uredbe, spoštovati zaupnost informacij in podatkov, ki so jih pridobili pri opravljanju svojih nalog, v skladu s pravom Unije ali nacionalnim pravom. Svoje naloge in dejavnosti bi morali opravljati tako, da varujejo zlasti pravice intelektualne lastnine, zaupne poslovne informacije in poslovne skrivnosti, učinkovito izvajanje te uredbe, javne in nacionalne varnostne interese, celovitost kazenskih in upravnih postopkov ter celovitost tajnih podatkov.
- (168) Skladnost s to uredbo bi morala biti izvršljiva z naložitvijo kazni in drugimi izvršilnimi ukrepi. Države članice bi morale sprejeti vse potrebne ukrepe za zagotovitev izvajanja določb te uredbe, tudi z določitvijo učinkovitih, sorazmernih in odvračilnih kazni za njihovo kršitev, in za upoštevanje načela ne bis in idem. Za okrepitev in usklajitev upravnih kazni za kršitev te uredbe bi bilo treba določiti zgornje meje za določitev upravnih glob za nekatere posebne kršitve. Države članice bi morale pri določanju višine glob v vsakem posameznem primeru upoštevati vse ustrezne okoliščine konkretne situacije, zlasti pa naravo, težo in trajanje kršitve ter njene posledice in velikost ponudnika, zlasti če je ponudnik MSP, vključno z zagonskim podjetjem. Evropski nadzornik za varstvo podatkov bi moral biti pooblaščen za naganje glob institucijam, agencijam in organom Unije, ki spadajo na področje uporabe te uredbe.
- (169) Izpolnjevanje obveznosti za ponudnike modelov UI za splošne namene, določenih na podlagi te uredbe, bi moralo med drugim biti izvršljivo z globami. V ta namen bi bilo treba določiti tudi ustrezne ravni glob za kršitev navedenih obveznosti, vključno z neizpolnjevanjem ukrepov, ki jih Komisija zahteva v skladu s to uredbo, ob upoštevanju ustreznih zastaralnih rokov v skladu z načelom sorazmernosti. Vse odločitve, ki jih Komisija sprejme na podlagi te uredbe, so podvržene nadzoru Sodišča Evropske unije v skladu s PDEU, vključno z neomejeno pristojnostjo Sodišča glede kazni na podlagi člena 261 PDEU.
- (170) Pravo Unije in nacionalno pravo fizičnim in pravnim osebam, na pravice in svoboščine katerih negativno vpliva uporaba sistemov UI, že zagotavljata učinkovita pravna sredstva. Brez poseganja v ta pravna sredstva lahko pritožbo pri ustreznem organu za nadzor trga vložijo vsaka fizična ali pravna oseba, ki upravičeno meni, da je prišlo do kršitve te uredbe.
- (171) Osebe, na katere vpliva uporaba sistemov UI, bi morale imeti pravico do pojasnila, kadar odločitev uvajalca temelji predvsem na izhodnih podatkih nekaterih visokotveganih sistemov UI, ki spadajo na področje uporabe te uredbe, in kadar ima ta odločitev pravne učinke za te osebe ali nanje podobno znatno vpliva na način, za katerega menijo, da

⁽⁵³⁾ Uredba (EU) 2023/988 Evropskega parlamenta in Sveta z dne 10. maja 2023 o splošni varnosti proizvodov, spremembi Uredbe (EU) št. 1025/2012 Evropskega parlamenta in Sveta in Direktive (EU) 2020/1828 Evropskega parlamenta in Sveta ter razveljavitvi Direktive 2001/95/ES Evropskega parlamenta in Sveta in Direktive Sveta 87/357/EGS (UL L 135, 23.5.2023, str. 1).

ima negativne učinke na njihovo zdravje, varnost in temeljne pravice. To pojasnilo bi moralo biti jasno in smiselno ter temelj, na podlagi katerega osebe, na katere vpliva uporaba sistemov UI, lahko uveljavljajo svoje pravice. Pravica do pojasnila se ne bi smela uporabljati za uporabo sistemov UI, za katere izjeme ali omejitve izhajajo iz prava Unije ali nacionalnega prava, temveč bi se morala uporabljati le, če ta pravica še ni določena na podlagi prava Unije.

- (172) Osebe, ki kot žvižgači opozarjajo na kršitve te uredbe, bi morale biti zaščitene na podlagi prava Unije. Za prijavo kršitev te uredbe in zaščito oseb, ki te kršitve prijavijo, bi se zato morala uporabljati Direktiva (EU) 2019/1937 Evropskega parlamenta in Sveta ⁽⁵⁴⁾.
- (173) 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 pogojev, pod katerimi se sistem UI ne sme šteti za sistem visokega tveganja, seznama visokotveganih sistemov UI, določb o tehnični dokumentaciji, vsebine EU izjave o skladnosti, določb o postopkih ugotavljanja skladnosti, določb o vzpostavitvi visokotveganih sistemov UI, za katere bi se moral uporabljati postopek ugotavljanja skladnosti na podlagi ocene sistema upravljanja kakovosti in ocene tehnične dokumentacije, praga, meril uspešnosti in kazalnikov, tudi z njihovo dopolnitvijo, kot so opredeljeni v pravilih za razvrščanje modelov UI za splošne namene s sistemskim tveganjem, meril za označevanje modelov UI za splošne namene s sistemskim tveganjem, tehnične dokumentacije za ponudnike modelov UI za splošne namene in informacij o preglednosti za ponudnike modelov UI za splošne namene. Zlasti je pomembno, da se Komisija pri svojem pripravljalnem delu ustrezno posvetuje, tudi na ravni strokovnjakov, in da se ta posvetovanja izvedejo v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje ⁽⁵⁵⁾. Za zagotovitev enakopravnega sodelovanja pri pripravi delegiranih aktov Evropski parlament in Svet zlasti prejemata vse dokumente sočasno s strokovnjaki iz držav članic, njuni strokovnjaki pa se lahko sistematično udeležujejo sestankov strokovnih skupin Komisije, ki zadevajo pripravo delegiranih aktov.
- (174) Glede na hiter tehnološki razvoj in tehnično strokovno znanje, potrebno za učinkovito izvajanje te uredbe bi morala Komisija oceniti in pregledati to uredbo do 2. avgusta 2029 in nato vsaka štiri leta ter poročati Evropskemu parlamentu in Svetu. Poleg tega bi morala Komisija ob upoštevanju posledic za področje uporabe te uredbe enkrat letno oceniti potrebo po spremembi seznama visokotveganih sistemov UI in seznama prepovedanih praks. Komisija bi morala do 2. avgusta 2028 in nato vsaka štiri leta oceniti tudi potrebo po spremembi seznama področij z visokim tveganjem iz ene od prilog k tej uredbi, sisteme UI, ki spadajo na področje uporabe obveznosti glede preglednosti, učinkovitost sistema nadzora in upravljanja ter napredek pri razvoju standardizacijskih dokumentov o energetsko učinkovitem razvoju modelov UI za splošno rabo, vključno s potrebo po nadaljnjih ukrepih ali dejavnostih, ter o tem poročati Evropskemu parlamentu in Svetu. Komisija bi morala do 2. avgusta 2028 ter nato vsaka tri leta oceniti učinek in učinkovitost prostovoljnih kodeksov ravnanja za spodbujanje uporabe zahtev, ki veljajo za visokotvegane sisteme UI, za sisteme UI, ki niso visokotvegani sistemi UI, ter morebitnih drugih dodatnih zahtev za takšne sisteme UI.
- (175) Da se zagotovijo enotni pogoji za izvajanje te uredbe, bi bilo treba na Komisijo prenesti izvedbena pooblastila. Ta pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta ⁽⁵⁶⁾.
- (176) Ker cilja te uredbe, in sicer izboljšati delovanje notranjega trga in spodbujati uvajanje na človeka osredotočene in zaupanja vredne UI, ob zagotavljanju visoke ravni varovanja zdravja, varnosti, temeljnih pravic iz Listine, vključno z demokracijo, pravno državo in varstvom okolja, pred škodljivimi učinki sistemov UI v Uniji ter podpiranju

⁽⁵⁴⁾ Direktiva (EU) 2019/1937 Evropskega parlamenta in Sveta z dne 23. oktobra 2019 o zaščiti oseb, ki prijavijo kršitve prava Unije (UL L 305, 26.11.2019, str. 17).

⁽⁵⁵⁾ UL L 123, 12.5.2016, str. 1.

⁽⁵⁶⁾ 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).

inovacij, države članice ne morejo zadovoljivo doseči, temveč se zaradi obsega ali učinka ukrepa lažje doseže 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.

- (177) Da se zagotovita pravna varnost in ustrezno prilagoditveno obdobje za operaterje ter preprečijo motnje na trgu, vključno z zagotavljanjem neprekinjene uporabe sistemov UI, je primerno, da se ta uredba uporablja za visokotvegane sisteme UI, ki so bili dani na trg ali v uporabo pred splošnim datumom začetka njene uporabe, le, če se pri navedenih sistemih z navedenim datumom bistveno spremeni njihova zasnova ali predvideni namen. Primerno je pojasniti, da bi bilo treba v zvezi s tem koncept bistvene spremembe razumeti kot vsebinsko enakovreden pojmu bistvene spremembe, ki se uporablja samo za visokotvegane sisteme UI na podlagi te uredbe. Tako upravljavci sistemov UI, ki so komponente obsežnih informacijskih sistemov, vzpostavljenih s pravnimi akti iz ene od prilog k tej uredbi, kot tudi operaterji visokotveganih sistemov UI, ki naj bi jih uporabljali javni organi, bi morali izjemoma in glede na javno odgovornost sprejeti potrebne ukrepe za doseg skladnosti z zahtevami iz te uredbe do konca leta 2030 oziroma do 2. avgusta 2030.
- (178) Ponudnike visokotveganih sistemov UI se spodbuja, da že v prehodnem obdobju začnejo prostovoljno izpolnjevati ustrezne obveznosti iz te uredbe.
- (179) Ta uredba se uporablja od 2. avgusta 2026. Vendar bi bilo treba zaradi nesprejemljivega tveganja, povezanega z uporabo UI na določene načine, prepovedi ter splošne določbe te uredbe uporabljati že od 2. februarja 2025. Čeprav bodo te prepovedi polno učinkovale šele po vzpostavitvi upravljanja in izvrševanja te uredbe, je pomembno predvideti uporabo prepovedi, da se upoštevajo nesprejemljiva tveganja in zato, da bi to vplivalo na druge postopke, kot denimo v civilnem pravu. Poleg tega bi morala infrastruktura, povezana z upravljanjem in sistemom ugotavljanja skladnosti, začeti delovati pred 2. avgustom 2026, zato bi bilo treba določbe o priglašeni organih in strukturi upravljanja uporabljati od 2. avgusta 2025. Glede na hiter tehnološki napredek in sprejetje modelov UI za splošne namene bi bilo treba obveznosti za ponudnike modelov UI za splošne namene uporabljati od 2. avgusta 2025. Kodekse prakse bi bilo treba pripraviti najpozneje do 2. maja 2025, da bi ponudniki lahko pravočasno dokazali skladnost. Urad za UI bi moral zagotavljati posodabljanje pravil in postopkov razvrščanja glede na tehnološki razvoj. Poleg tega bi morale države članice določiti pravila o kaznih, vključno z upravnimi globami, in o njih uradno obvestiti Komisijo ter do datuma začetka uporabe te uredbe zagotoviti, da jih bodo učinkovito izvajale. Zato bi bilo treba določbe o kaznih uporabljati od 2. avgusta 2025.
- (180) V skladu s členom 42(1) in (2) Uredbe (EU) 2018/1725 je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov in Evropskim odborom za varstvo podatkov, ki sta dala mnenje 18. junija 2021 –

SPREJELA NASLEDNJO UREDBO:

POGLAVJE I SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja

1. Namen te uredbe je izboljšati delovanje notranjega trga in spodbujati uvajanje na človeka osredotočene in zaupanja vredne umetne inteligence (UI) ter zagotoviti visoko raven varovanja zdravja, varnosti in temeljnih pravic iz Listine, vključno z demokracijo, pravno državo in varstvom okolja, pred škodljivimi učinki sistemov UI v Uniji ter podpirati inovacije.

2. V tej uredbi so določeni:

(a) harmonizirana pravila za dajanje na trg, dajanje v uporabo ter za uporabo sistemov UI v Uniji;

- (b) prepovedi nekaterih praks UI;
- (c) posebne zahteve za visokotvegane sisteme UI in obveznosti za operaterje takih sistemov;
- (d) harmonizirana pravila o preglednosti za nekatere sisteme UI;
- (e) harmonizirana pravila za dajanje na trg modelov UI za splošne namene;
- (f) pravila o spremljanju trga, nadzoru trga, upravljanju in izvrševanju;
- (g) ukrepi v podporo inovacijam s posebnim poudarkom na MSP, vključno z zagonskimi podjetji.

Člen 2

Področje uporabe

1. Ta uredba se uporablja za:

- (a) ponudnike, ki dajejo na trg ali v uporabo sisteme UI ali dajejo na trg modele UI za splošne namene v Uniji, ne glede na to, ali imajo ti ponudniki sedež ali se nahajajo v Uniji ali v tretji državi;
- (b) uvajalce sistemov UI, ki imajo sedež ali se nahajajo v Uniji;
- (c) ponudnike in uvajalce sistemov UI, ki imajo sedež ali se nahajajo v tretji državi, kadar se izhodni podatki, ki jih sistem UI ustvari, uporabljajo v Uniji;
- (d) uvoznike in distributerje sistemov UI;
- (e) proizvajalce proizvodov, ki dajejo sistem UI na trg ali v uporabo skupaj s svojim proizvodom in pod svojim imenom ali znamko;
- (f) pooblaščenec zastopnike ponudnikov, ki nimajo sedeža v Uniji;
- (g) osebe, ki jih zadeva in se nahajajo v Uniji.

2. Za sisteme UI, ki so razvrščeni med visoko tvegane sisteme UI v skladu s členom 6(1) v povezavi s proizvodi, zajetimi v harmonizacijski zakonodaji Unije s seznama v Prilogi I, oddelek B, se uporablja samo člen 6(1), členi 102 do 109 in člen 112. Člen 57 se uporablja le, če so bile zahteve za visokotvegane sisteme UI iz te uredbe vključene v to harmonizacijsko zakonodajo Unije.

3. Ta uredba se ne uporablja za področja, ki ne spadajo na področje uporabe prava Unije, in v nobenem primeru ne vpliva na pristojnosti držav članic v zvezi z nacionalno varnostjo, ne glede na vrsto subjekta, ki ga države članice pooblastijo za opravljanje nalog v zvezi s temi pristojnostmi.

Ta uredba se ne uporablja za sisteme UI, kadar in kolikor so s spremembami ali brez njih dani na trg ali v uporabo oziroma se uporabljajo izključno za vojaške, obrambne ali nacionalne varnostne namene, ne glede na vrsto subjekta, ki izvaja te dejavnosti.

Ta uredba se ne uporablja za sisteme UI, ki niso dani na trg ali v uporabo v Uniji, kadar se izhodni podatki uporabljajo v Uniji izključno za vojaške, obrambne ali nacionalne varnostne namene, 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 na podlagi odstavka 1, kadar ti organi ali organizacije uporabljajo sisteme UI v okviru mednarodnega sodelovanja ali 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, pod pogojem, da ta tretja država ali mednarodna organizacija zagotovi ustrezne zaščitne ukrepe v zvezi z varstvom temeljnih pravic in svoboščin posameznikov.

5. Ta uredba ne vpliva na uporabo določb o odgovornosti ponudnikov posredniških storitev iz poglavja II Uredbe (EU) 2022/2065.

6. Ta uredba se ne uporablja za sisteme UI ali modele UI, vključno z njihovimi izhodnimi podatki, posebej razvite in dane v uporabo zgolj za namene znanstvenih raziskav in razvoja.
7. Pravo Unije o varstvu osebnih podatkov, zasebnosti in zaupnosti komunikacij se uporablja za osebne podatke, ki se obdelujejo v zvezi s pravicami in obveznostmi iz te uredbe. Brez poseganja v člen 10(5) in člen 59 te uredbe ta uredba ne vpliva na Uredbo (EU) 2016/679 ali (EU) 2018/1725 ali Direktivo 2002/58/ES ali (EU) 2016/680.
8. Ta uredba se ne uporablja za raziskovalne dejavnosti, dejavnosti testiranja ali razvojne dejavnosti v zvezi z sistemi UI ali modeli UI, preden se ti dajo na trg ali v uporabo. Te dejavnosti se morajo izvajati v skladu z veljavnim pravom Unije. Ta izključitev ne zajema testiranja v realnih razmerah.
9. Ta uredba ne posega v pravila, določena v drugih pravnih aktih Unije v zvezi z varstvom potrošnikov in varnostjo proizvodov.
10. Ta uredba se ne uporablja za obveznosti uvajalcev, ki so fizične osebe in uporabljajo sisteme UI v okviru povsem osebne nepoklicne dejavnosti.
11. Ta uredba Uniji ali državam članicam ne preprečuje, da ohranijo ali uvedejo zakone ali druge predpise, ki so za delavce ugodnejši v smislu varstva njihovih pravic v zvezi z delodajalčevo uporabo sistemov UI, ali da spodbujajo ali dovolijo uporabo kolektivnih pogodb, ki so za delavce ugodnejše.
12. Ta uredba se ne uporablja za sisteme UI, objavljene na podlagi prostih in odprtokodnih licenc, razen če so dani na trg ali v uporabo kot visokotvegani sistemi UI ali sistem UI iz člena 5 ali 50.

Člen 3

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

- (1) „sistem UI“ pomeni sistem temelječ na napravah, ki je zasnovan za delovanje z različnimi stopnjami avtonomije in lahko po uvedbi izkaže prilagodljivost ter za eksplicitne ali implicitne cilje iz prejetih vhodnih podatkov sklepa, kako ustvariti izhodne podatke, kot so napovedi, vsebine, priporočila ali odločitve, ki lahko vplivajo na fizična ali virtualna okolja;
- (2) „tveganje“ pomeni kombinacijo verjetnosti pojava škode in resnosti te škode;
- (3) „ponudnik“ pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki razvije sistem UI ali model UI za splošne namene ali ima razvit sistem UI ali model UI za splošne namene in ga da na trg ali da sistem UI v uporabo pod svojim imenom ali znamko, za plačilo ali brezplačno;
- (4) „uvajalec“ pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki sistem UI uporablja v svoji pristojnosti, razen kadar se sistem UI uporablja v okviru osebne nepoklicne dejavnosti;
- (5) „pooblaščen zastopnik“ pomeni fizično ali pravno osebo, ki se nahaja ali ima sedež v Uniji in je od ponudnika sistema UI ali modela UI za splošne namene prejela in sprejela pisno pooblastilo, da v njegovem imenu opravlja in izvaja obveznosti in postopke, določene v tej uredbi;
- (6) „uvoznik“ pomeni fizično ali pravno osebo, ki se nahaja ali ima sedež v Uniji, ki da na trg sistem UI, ki nosi ime ali znamko fizične ali pravne osebe s sedežem v tretji državi;
- (7) „distributer“ pomeni fizično ali pravno osebo v dobavni verigi, razen ponudnika ali uvoznika, ki omogoči dostopnost sistema UI na trgu Unije;
- (8) „operater“ pomeni ponudnika, proizvajalca proizvoda, uvajalca, pooblaščenega zastopnika, uvoznika ali distributerja;

- (9) „dajanje na trg“ pomeni, da je sistem UI ali model UI za splošne namene prvič dostopen na trgu Unije;
- (10) „dostopnost na trgu“ pomeni dobavo sistema UI ali modela UI za splošne namene za distribucijo ali uporabo na trgu Unije v okviru gospodarske dejavnosti, bodisi za plačilo ali brezplačno;
- (11) „dajanje v uporabo“ pomeni dobavo sistema UI za prvo uporabo neposredno uvajalcu ali za lastno uporabo v Uniji za predvideni namen;
- (12) „predvideni namen“ pomeni uporabo, za katero je ponudnik namenil sistem UI, vključno s posebnim kontekstom in pogoji uporabe, kot je navedeno v informacijah, ki jih je ponudnik predložil v navodilih za uporabo, v promocijskem ali prodajnem gradivu in izjavah ter v tehnični dokumentaciji;
- (13) „razumno predvidljiva napačna uporaba“ pomeni uporabo sistema UI na način, ki sicer ni v skladu s predvidenim namenom, vendar je lahko posledica razumno predvidljivega človeškega vedenja ali interakcije z drugimi sistemi, vključno z drugimi sistemi UI;
- (14) „varnostna komponenta“ pomeni komponento proizvoda ali sistema UI, ki opravlja varnostno funkcijo za ta proizvod ali sistem UI ali katere nedelovanje ali okvara ogroža zdravje in varnost oseb ali premoženja;
- (15) „navodila za uporabo“ pomeni informacije, ki jih zagotovi ponudnik, da uvajalca obvesti zlasti o predvidenem namenu in pravilni uporabi sistema UI;
- (16) „odpoklic sistema UI“ pomeni vsak ukrep, namenjen zagotovitvi vračila sistema UI, ki je bil na voljo uvajalcem, ponudniku ali namenjen zagotovitvi prenehanja delovanja ali onemogočanja uporabe tega sistema;
- (17) „umik sistema UI“ pomeni vsak ukrep, namenjen preprečevanju dostopnosti sistema UI v dobavni verigi na trgu;
- (18) „zmogljivost sistema UI“ pomeni sposobnost sistema UI, da doseže svoj predvideni namen;
- (19) „priglasitveni organ“ pomeni nacionalni organ, odgovoren za vzpostavitev in izvajanje potrebnih postopkov za ocenjevanje, imenovanje in priglasitev organov za ugotavljanje skladnosti ter za njihovo spremljanje;
- (20) „ugotavljanje skladnosti“ pomeni postopek ugotavljanja, ali so izpolnjene zahteve iz poglavja III, oddelek 2, v zvezi z visokotveganim sistemom UI;
- (21) „organ za ugotavljanje skladnosti“ pomeni organ, ki kot tretja stran izvaja dejavnosti ugotavljanja skladnosti, vključno s testiranjem, certificiranjem in kontrolo;
- (22) „priglašeni organ“ pomeni organ za ugotavljanje skladnosti, priglašen v skladu s to uredbo in drugo ustrezno harmonizacijsko zakonodajo Unije;
- (23) „bistvena sprememba“ pomeni spremembo sistema UI po dajanju na trg ali v uporabo, ki ni predvidena ali načrtovana pri prvotnem ugotavljanju skladnosti, ki jo je izvedel ponudnik, in ki posledično vpliva na skladnost sistema UI z zahtevami iz poglavja III, oddelek 2, ali povzroči spremembo predvidenega namena, za katerega je bila skladnost sistema UI ugotavljana;
- (24) „oznaka CE“ pomeni oznako, s katero ponudnik izjavlja, da je sistem UI skladen z zahtevami iz poglavja III, oddelek 2, in druge veljavne harmonizacijske zakonodaje Unije, ki določa njeno namestitve;
- (25) „sistem spremljanja po dajanju na trg“ pomeni vse dejavnosti, ki jih izvajajo ponudniki sistemov UI, da bi zbirali in pregledovali izkušnje, pridobljene z uporabo sistemov UI, ki jih dajo na trg ali v uporabo, da bi ugotovili, ali so potrebni takojšnji popravni ali preventivni ukrepi;
- (26) „organ za nadzor trga“ pomeni nacionalni organ, ki izvaja dejavnosti in sprejema ukrepe na podlagi Uredbe (EU) 2019/1020;

- (27) „harmonizirani standard“ pomeni harmonizirani standard, kakor je opredeljen v členu 2(1), točka (c), Uredbe (EU) št. 1025/2012;
- (28) „skupna specifikacija“ pomeni sklop tehničnih specifikacij, kakor so opredeljene v členu 2, točka 4, Uredbe (EU) št. 1025/2012 in v katerih je opisano, kako izpolnjevati nekatere zahteve, določene na podlagi te uredbe;
- (29) „učni podatki“ pomeni podatke, ki se uporabljajo za učenje sistema UI s prilagajanjem njegovih učljivih parametrov;
- (30) „validacijski podatki“ pomeni podatke, ki se uporabljajo za ocenjevanje naučenega sistema UI ter za uravnavanje neučljivih parametrov in postopka učenja sistema, med drugim za preprečevanje premajhnega ali prevelikega prilagajanja;
- (31) „nabor validacijskih podatkov“ pomeni ločen nabor podatkov ali fiksni ali spremenljivi del nabora učnih podatkov;
- (32) „testni podatki“ pomeni podatke, ki se uporabljajo za zagotavljanje neodvisne ocene sistema UI za potrditev pričakovane zmogljivosti tega sistema pred dajanjem na trg ali v uporabo;
- (33) „vhodni podatki“ pomeni podatke, ki se vnesejo v sistem UI ali jih ta neposredno pridobi in na podlagi katerih sistem ustvari izhodne podatke;
- (34) „biometrični podatki“ pomeni osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi fizične osebe, kot so podoba obraza ali daktiloskopski podatki;
- (35) „biometrična identifikacija“ pomeni avtomatizirano prepoznavanje fizičnih, fizioloških, vedenjskih ali psiholoških lastnosti človeka z namenom ugotavljanja identitete fizične osebe s primerjavo biometričnih podatkov tega posameznika z biometričnimi podatki posameznikov, shranjenimi v podatkovni zbirki;
- (36) „biometrično preverjanje“ pomeni avtomatizirano „ena proti ena“ preverjanje, vključno z avtentikacijo, identitete fizičnih oseb s primerjavo njihovih biometričnih podatkov s predhodno pridobljenimi biometričnimi podatki;
- (37) „posebne vrste osebnih podatkov“ pomeni 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;
- (38) „občutljivi operativni podatki“ pomeni operativne podatke, povezane z dejavnostmi preprečevanja, odkrivanja, preiskovanja ali pregona kaznivih dejanj, katerih razkritje bi lahko ogrozilo celovitost kazenskih postopkov;
- (39) „sistem za prepoznavanje čustev“ pomeni sistem UI za prepoznavanje čustev ali namenov ali sklepanje o čustvih ali namenih fizičnih oseb na podlagi njihovih biometričnih podatkov;
- (40) „sistem za biometrično kategorizacijo“ pomeni sistem UI za razvrščanje fizičnih oseb v posebne kategorije na podlagi njihovih biometričnih podatkov, razen če gre za pomožni in iz objektivnih tehničnih razlogov nujno potreben sistem druge komercialne storitve;
- (41) „sistem za biometrično identifikacijo na daljavo“ pomeni sistem UI za identifikacijo fizičnih oseb brez njihovega dejavnega sodelovanja, običajno na daljavo, s primerjavo biometričnih podatkov osebe z biometričnimi podatki iz referenčne podatkovne zbirke;
- (42) „sistem za biometrično identifikacijo na daljavo v realnem času“ pomeni sistem za biometrično identifikacijo na daljavo, pri katerem se zajemanje biometričnih podatkov, primerjava in identifikacija izvedejo brez znatnih zamud, ki ne zajema le takojšnje identifikacije, temveč tudi identifikacijo s krajšimi zamiki, da se prepreči izogibanje;
- (43) „sistem za naknadno biometrično identifikacijo na daljavo“ pomeni sistem za biometrično identifikacijo na daljavo, ki ni sistem za biometrično identifikacijo na daljavo v realnem času;
- (44) „javno dostopen prostor“ pomeni vsak fizični prostor v javni ali zasebni lasti, ki je dostopen nedoločenemu številu fizičnih oseb, ne glede na to, ali se lahko uporabljajo določeni pogoji za dostop, in ne glede na morebitne omejitve kapacitete;

- (45) „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 in 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;
- (46) „preprečevanje, odkrivanje in preiskovanje kaznivih dejanj“ pomeni dejavnosti, ki jih organi za preprečevanje, odkrivanje ali preiskovanje 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;
- (47) „Urad za UI“ pomeni funkcijo Komisije, da prispeva k izvajanju, spremljanju in nadzoru sistemov UI in modelov UI za splošne namene ter upravljanju UI, določeno s Sklepom Komisije z dne 24. januarja 2024; v tej uredbi se sklicevanja na Urad za UI razumejo kot sklicevanja na Komisijo;
- (48) „pristojni nacionalni organ“ pomeni priglasitveni organ ali organ za nadzor trga; v zvezi s sistemi UI, ki so dani v uporabo ali jih uporabljajo institucije, agencije, uradi ali organi Unije, se sklicevanje na pristojne nacionalne organe ali organe za nadzor trga v tej uredbi razume kot sklicevanje na Evropskega nadzornika za varstvo podatkov;
- (49) „resen incident“ pomeni incident ali okvaro sistema UI, ki neposredno ali posredno povzroči naslednje:
- (a) smrt osebe ali resno škodo za zdravje osebe;
 - (b) resne in nepopravljive motnje pri upravljanju ali delovanju kritične infrastrukture;
 - (c) kršitev obveznosti iz prava Unije, namenjenih varstvu temeljnih pravic;
 - (d) resno škodo za premoženje ali okolje;
- (50) „osebni podatki“ pomeni osebne podatke, kakor so opredeljeni v členu 4, točka 1, Uredbe (EU) 2016/679;
- (51) „neosebni podatki“ pomeni podatke, ki niso osebni podatki, kakor so opredeljeni v členu 4, točka 1, Uredbe (EU) 2016/679;
- (52) „oblikovanje profilov“ pomeni oblikovanje profilov, kakor je opredeljeno v členu 4, točka 4, Uredbe (EU) 2016/679;
- (53) „načrt testiranja v realnih razmerah“ pomeni dokument, ki opisuje cilje, metodologijo, geografsko, populacijsko in časovno področje uporabe, spremljanje, organizacijo in izvajanje testiranja v realnih razmerah;
- (54) „načrt peskovnika“ pomeni dokument, o katerem se dogovorita sodelujoči ponudnik in pristojni organ in v katerem so opisani cilji, pogoji, časovni okvir, metodologija in zahteve za dejavnosti, ki se izvajajo v peskovniku;
- (55) „regulativni peskovnik za UI“ pomeni nadzorovan okvir, ki ga vzpostavi pristojni nacionalni organ in ki ponudnikom ali potencialnim ponudnikom sistemov UI omogoča, da na podlagi načrta peskovnika za omejen čas in pod regulativnim nadzorom razvijajo, učijo, potrdijo in testirajo, po potrebi v realnih razmerah, inovativen sistem UI;
- (56) „pismenost na področju UI“ pomeni spretnosti, znanje in razumevanje, ki ponudnikom, uvajalcem in zadevnim osebam, ob upoštevanju njihovih pravic in obveznosti v okviru te uredbe, omogočajo, da informirano uvajajo sisteme UI ter se hkrati zavedajo priložnosti in tveganj na področju UI in morebitne škode, ki jo ta lahko povzroči;

- (57) „testiranje v realnih razmerah“ pomeni začasno testiranje sistema UI za predvideni namen v realnih razmerah zunaj laboratorija ali drugače simuliranega okolja z namenom zbiranja zanesljivih in robustnih podatkov ter ugotavljanja in preverjanja skladnosti sistema UI z zahtevami iz te uredbe, pri čemer to ne šteje kot dajanje sistema UI na trg ali v uporabo v smislu te uredbe, če so izpolnjeni vsi pogoji iz člena 57 ali 60;
- (58) „udeleženec“ za namen testiranja v realnih razmerah pomeni fizično osebo, ki sodeluje pri testiranju v realnih razmerah;
- (59) „informirana privolitev“ pomeni svoboden, konkreten, nedvoumen in prostovoljen izraz pripravljenosti udeleženca, da sodeluje pri določenem testiranju v realnih razmerah, potem ko je bil seznanjen z vsemi vidiki testiranja, ki so pomembni za njegovo odločitev za sodelovanje.
- (60) „globoki ponaredek“ pomeni z UI ustvarjeno ali manipulirano slikovno, zvočno ali video vsebino, ki je podobna obstoječim osebam, predmetom, krajem, subjektom ali dogodkom in se uporabniku lažno zdi pristna ali resnična;
- (61) „močno razširjena kršitev“ pomeni vsako dejanje ali opustitev v nasprotju s pravom Unije o varstvu interesov posameznikov:
- (a) ki škoduje ali bi lahko škodovala kolektivnim interesom posameznikov, ki prebivajo v vsaj dveh državah članicah, ki nista država članica:
 - (i) iz katere izvira dejanje ali opustitev, oziroma v kateri je prišlo do dejanja ali opustitve;
 - (ii) v kateri se nahaja ali ima sedež zadevni ponudnik ali, kjer je ustrezno, njegov pooblaščen zastopnik ali
 - (iii) v kateri ima sedež uvajalec, kadar kršitev stori uvajalec;
 - (b) ki je povzročila, povzroča ali bi lahko povzročila škodo kolektivnim interesom posameznikov in ki ima skupne značilnosti, med drugim enako nezakonito prakso ali kršitev istega interesa, stori pa jo isti operater sočasno v vsaj treh državah članicah;
- (62) „kritična infrastruktura“ pomeni kritično infrastrukturo, kakor je opredeljena v členu 2, točka 4, Direktive (EU) 2022/2557;
- (63) „model UI za splošne namene“ pomeni model UI, tudi kadar se takšen model UI uči z veliko količino podatkov z uporabo samonadzora v velikem obsegu, ki kaže znatno splošno uporabnost in je ne glede na to, kako je dan na trg, sposoben kompetentno opravljati širok nabor različnih nalog in ki ga je mogoče vključiti v različne sisteme ali aplikacije nižje v verigi, razen modelov UI, ki se uporabljajo za dejavnosti raziskav, razvoja ali izdelave prototipov, preden se dajo na trg;
- (64) „zmogljivosti z velikim vplivom“ pomeni zmogljivosti, ki so enake ali presegajo zmogljivosti, ki so zabeležene pri najbolj naprednih modelih UI za splošne namene;
- (65) „sistemsko tveganje“ pomeni tveganje, ki je specifično za zmogljivosti modelov UI za splošne namene z velikim vplivom in ima pomemben vpliv na trg Unije zaradi svojega dosega ali dejanskih ali razumno predvidljivih negativnih učinkov na javno zdravje, varnost, javno varnost, temeljne pravice ali družbo kot celoto, ki se lahko v širokem obsegu širijo po vsej verigi vrednosti;
- (66) „sistem UI za splošne namene“ pomeni sistem UI, ki temelji na modelu UI za splošne namene in lahko služi različnim namenom, tako za neposredno uporabo kot za integracijo v druge sisteme UI;
- (67) „operacija s plavajočo vejico“ (floating-point operation) pomeni vsako matematično operacijo ali nalogo, ki vključuje števila s plavajočo vejico, ki so podmnžica realnih števil, na računalnikih običajno predstavljenih s celim številom s fiksno natančnostjo, povečanim za celoštevilski eksponent s fiksno osnovo;
- (68) „ponudnik nižje v verigi“ pomeni ponudnika sistema UI, tudi sistema UI za splošne namene, ki vključuje model UI, ne glede na to, ali model ponuja sam in je vertikalno integriran ali pa ga ponuja drug subjekt na podlagi pogodbenih razmerij.

Člen 4

Pismenost na področju UI

Ponudniki in uvajalci sistemov UI sprejmejo ukrepe, da v najboljši možni meri zagotovijo zadostno raven pismenosti svojega osebja in tudi drugih oseb, ki se v njihovem imenu ukvarjajo z obratovanjem in uporabo sistemov UI, na področju UI, upoštevajoč njihovo tehnično znanje, izkušnje, izobrazbo in usposobljenost ter okolje, v katerem se bodo uporabljali ti sistemi UI, pa tudi osebe ali skupine oseb, v zvezi s katerimi se bodo uporabljali ti sistemi.

POGLAVJE II

PREPOVEDANE PRAKSE UI

Člen 5

Prepovedane prakse UI

1. Prepovedane so naslednje prakse UI:

- (a) dajanje na trg, dajanje v uporabo ali uporaba sistema UI, ki uporablja subliminalne tehnike, ki presegajo zavest osebe, ali namerno manipulativne ali zavajajoče tehnike, s ciljem ali učinkom bistvenega izkrivljanja vedenja osebe ali skupine oseb, tako da se znatno zmanjša njihova sposobnost, da sprejmejo informirano odločitev, zaradi česar sprejmejo odločitev, ki je sicer ne bi sprejeli, na način, ki tej osebi, drugi osebi ali skupini oseb povzroči znatno škodo ali za katerega obstaja razumna verjetnost, da bo povzročil znatno škodo;
- (b) dajanje na trg, dajanje v uporabo ali uporaba sistema UI, ki izkorišča katere koli šibke točke fizične osebe ali določene skupine oseb zaradi njihove starosti, invalidnosti ali posebnega socialnega ali ekonomskega položaja, s ciljem ali učinkom, bistvenega izkrivljanja vedenja te osebe ali osebe iz te skupine na način, ki tej ali drugi osebi povzroči znatno škodo ali za katerega obstaja razumna verjetnost, da bo povzročil znatno škodo;
- (c) dajanje na trg, dajanje v uporabo ali uporaba sistemov UI za ocenjevanje ali razvrščanje fizičnih oseb ali skupin, ki jim pripadajo, v določenem časovnem obdobju na podlagi njihovega družbenega vedenja ali znanih, predpostavljenih ali predvidenih osebnih ali osebnostnih značilnosti, pri čemer število družbenih točk privede do ene ali obeh naslednjih možnosti:
 - (i) škodljiva ali neugodna obravnava nekaterih fizičnih oseb ali skupin oseb 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 skupin oseb, ki je neupravičena ali nesorazmerna z njihovim družbenim vedenjem ali resnostjo njihovega družbenega vedenja;
- (d) dajanje na trg, dajanje v uporabo za ta posebni namen ali uporaba sistema UI za ocenjevanje tveganja v zvezi s fizičnimi osebami, da se oceni ali predvidi, kakšno je tveganje, da bo fizična oseba storila kaznivo dejanje, izključno na podlagi oblikovanja profila fizične osebe ali ocenjevanja njenih osebnostnih lastnosti in značilnosti; ta prepoved se ne uporablja za sisteme UI, ki se uporabljajo za podporo človeški oceni vpletenosti osebe v kriminalno dejavnost, ki že temelji na objektivnih in preverljivih dejstvih, neposredno povezanih s kriminalno dejavnostjo;
- (e) dajanje na trg, dajanje v uporabo za ta posebni namen ali uporaba sistemov UI, ki z neciljnim odvzemom podob obraza z interneta ali s posnetkov kamer CCTV ustvarjajo ali širijo podatkovne zbirke za prepoznavanje obraza;
- (f) dajanje na trg, dajanje v uporabo za ta posebni namen ali uporaba sistemov UI za sklepanje o čustvih fizične osebe na delovnem mestu in v izobraževalnih ustanovah, razen kadar je uporaba sistema UI namenjena uvedbi ali dajanju na trg iz zdravstvenih ali varnostnih razlogov;

- (g) dajanje na trg, dajanje v uporabo za ta posebni namen ali uporaba sistemov za biometrično kategorizacijo, ki posameznike razvrščajo na podlagi njihovih biometričnih podatkov, da bi prišli do sklepov ali ugotovitev glede njihove rase, političnega prepričanja, članstva v sindikatu, verskega ali filozofskega prepričanja, spolnega življenja ali spolne usmerjenosti; ta prepoved ne zajema označevanja ali filtriranja zakonito pridobljenih naborov biometričnih podatkov, kot so slike, na podlagi biometričnih podatkov ali kategorizacije biometričnih podatkov na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj;
- (h) uporaba sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, razen če je taka uporaba nujno potrebna za enega od naslednjih ciljev:
- (i) ciljno usmerjeno iskanje določenih žrtev ugrabitev, trgovine z ljudmi ali spolnega izkoriščanja ljudi ter iskanje pogošenih oseb;
 - (ii) preprečitev konkretne, znatne in neposredne nevarnosti za življenje ali fizično varnost fizičnih oseb ali resnične in sedanje ali resnične in predvidljive grožnje terorističnega napada;
 - (iii) lokalizacija ali identifikacija osebe, osumljene storitve kaznivega dejanja, za namen izvajanja kazenske preiskave ali pregona ali izvršitve kazenske sankcije za kazniva dejanja iz Priloge II, za katera je v zadevni državi članici predpisana zgornja meja zaporne kazni ali ukrepa, vezanega na odvzem prostosti, najmanj štiri leta.

Točka (h) prvega pododstavka ne posega v člen 9 Uredbe (EU) 2016/679 v zvezi z obdelavo biometričnih podatkov za namene, ki niso preprečevanje, odkrivanje in preiskovanje kaznivih dejanj.

2. Sistemi 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 odstavka 1, prvi pododstavek, točka (h), se uporabljajo za namene iz navedene točke, samo da se potrdi identiteta točno določenega posameznika, pri čemer se upoštevajo naslednji elementi:

- (a) narava razmer, ki povzročajo morebitno uporabo, zlasti resnost, verjetnost in obseg škode, ki bi bila povzročena, če se sistem ne bi uporabljal;
- (b) posledice uporabe sistema za pravice in svoboščine vseh zadevnih oseb, zlasti resnost, verjetnost in obseg teh posledic.

Poleg tega mora biti 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 odstavka 1, prvi pododstavek, točka (h), tega člena skladna s potrebnimi in sorazmernimi zaščitnimi ukrepi in pogoji v zvezi z uporabo po nacionalnem pravu, ki dovoljuje njihovo uporabo, zlasti kar zadeva časovne, geografske in osebne omejitve. Uporaba sistema za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih se dovoli le, če je organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj opravil oceno učinka na temeljne pravice iz člena 27 in sistem registriral v podatkovni zbirki EU v skladu s členom 49. Vendar se lahko v ustrezno utemeljenih nujnih primerih uporaba takšnih sistemov začne brez registracije v podatkovni zbirki EU, če se takšna registracija zaključi brez nepotrebnega odlašanja.

3. Za namene odstavka 1, prvi pododstavek, točka (h), in odstavka 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 sodnega organa ali neodvisnega upravnega organa, katerega odločitev je zavezujoča za državo članico, v kateri bo potekala uporaba, izdano na podlagi obrazložene zahteve in v skladu s podrobnimi pravili nacionalnega prava iz odstavka 5. Vendar se lahko v ustrezno utemeljenih nujnih primerih uporaba takšnega sistema začne brez dovoljenja, pod pogojem, da se takšno dovoljenje zahteva brez nepotrebne odlašanja in najpozneje v 24 urah. Če se takšno dovoljenje zavrne, se njegova uporaba takoj ustavi, vsi podatki ter izhodni podatki in izsledki, ki izhajajo iz te uporabe, pa se takoj zavrzijo in izbrišejo.

Pristojni sodni organ ali neodvisni upravni organ, katerega odločitev je zavezujoča, izda dovoljenje samo v primeru, kadar 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 odstavka 1, prvi pododstavek, točka (h), kot je opredeljeno v zahtevi, in zlasti ostaja omejena na to, kar je nujno potrebno v zvezi

z obdobjem ter geografskim in osebnim področjem uporabe. Pri odločanju o zahtevi ta organ upošteva elemente iz odstavka 2. Nobena odločitev, ki ima škodljiv pravni učinek na osebo, se ne sme sprejeti samo na podlagi izhodnih podatkov sistema za biometrično identifikacijo na daljavo v realnem času.

4. Brez poseganja v odstavek 3 je treba o vsaki uporabi sistema za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj uradno obvestiti ustrezni organ za nadzor trga in nacionalni organ za varstvo podatkov v skladu z nacionalnimi pravili iz odstavka 5. Obvestilo vsebuje vsaj informacije iz odstavka 6 in ne vključuje občutljivih operativnih podatkov.

5. Država članica se lahko odloči, da v okviru omejitev in pod pogoji iz odstavka 1, prvi pododstavek, točka (h), 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. Zadevne države članice v svojem nacionalnem pravu določijo potrebna podrobna pravila v zvezi z vložitvijo zahteve za dovoljenja iz odstavka 3, izdajo, izvrševanjem in spremljanjem teh dovoljenj ter poročanjem v zvezi z njimi. V teh pravilih je tudi določeno, za katere od ciljev iz odstavka 1, prvi pododstavek, točka (h), med drugim tudi, za katera kazniva dejanja iz točke (h)(iii) navedenega odstavka, se lahko pristojnim organom dovoli uporaba teh sistemov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Države članice obvestijo Komisijo o teh pravilih najpozneje 30 dni po njihovem sprejetju. Države članice lahko v skladu s pravom Unije uvedejo strožje zakone o uporabi sistemov za biometrično identifikacijo na daljavo.

6. Nacionalni organi za nadzor trga in nacionalni organi za varstvo podatkov držav članic, ki so bili na podlagi odstavka 4 obveščeni o uporabi sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, Komisiji predložijo letna poročila o taki uporabi. V ta namen Komisija državam članicam ter nacionalnim organom za nadzor trga in varstvo podatkov zagotovi predlogo, ki vključuje informacije o številu odločitev, ki jih glede zahtevkov za dovoljenja v skladu z odstavkom 3 sprejmejo pristojni sodni organi ali neodvisni upravni organ, katerega odločitev je zavezujoča, in o njihovih rezultatih.

7. Komisija objavi letna poročila o uporabi sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj na podlagi zbirnih podatkov v državah članicah, ki temeljijo na letnih poročilih iz odstavka 6. Ta letna poročila ne vključujejo občutljivih operativnih podatkov o povezanih dejavnostih preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.

8. Ta člen ne vpliva na prepovedi, ki se uporabljajo, kadar praksa UI krši drugo pravo Unije.

POGLAVJE III

VISOKOTVEGANI SISTEMI UI

ODDELEK 1

Razvrstitev visokotveganih sistemov UI

Člen 6

Pravila razvrstitve za visokotvegane sisteme UI

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

- (a) sistem UI je namenjen uporabi kot varnostna komponenta proizvoda ali pa je sam sistem UI proizvod, ki ga zajema harmonizacijska zakonodaja Unije iz Priloge I;
- (b) za proizvod, katerega varnostna komponenta na podlagi točke (a) je sistem UI, ali za sistem UI, ki je sam proizvod, je treba opraviti ugotavljanje skladnosti s strani tretje osebe zaradi dajanja tega proizvoda na trg ali v uporabo na podlagi harmonizacijske zakonodaje Unije iz Priloge I.

2. Poleg visokotveganih sistemov UI iz odstavka 1 za visokotvegane sisteme UI štejejo tudi sistemi UI iz Priloge III.

3. Z odstopanjem od odstavka 2 sistem UI iz Priloge III ne šteje za visokotvegan, kadar ne predstavlja znatnega tveganja škode za zdravje, varnost ali temeljne pravice fizičnih oseb, tudi s tem, da ne vpliva bistveno na izid odločanja.

Prvi pododstavek se uporablja, kadar je izpolnjen kateri koli od naslednjih pogojev:

- (a) sistem UI naj bi opravljal omejeno postopkovno nalogo;
- (b) namen sistema UI je izboljšati rezultat predhodno zaključene človeške dejavnosti;
- (c) sistem UI je namenjen odkrivanju vzorcev odločanja ali odstopanj od predhodnih vzorcev odločanja in ni namenjen nadomeščanju ali vplivanju na predhodno dokončano človeško oceno brez ustreznega človeškega pregleda ali
- (d) sistem UI je namenjen izvedbi pripravljalne naloge za oceno, ki je pomembna za namene primerov uporabe iz Priloge III.

Ne glede na prvi pododstavek sistem UI iz Priloge III vedno šteje za visokotvegan, kadar izvaja oblikovanje profila fizičnih oseb.

4. Ponudnik, ki meni, da sistem UI iz Priloge III ne pomeni visokega tveganja, dokumentira svojo oceno, preden se ta sistem da na trg ali v uporabo. Za takega ponudnika velja obveznost registracije iz člena 49(2). Ponudnik na zahtevo pristojnih nacionalnih organov predloži dokumentacijo o oceni.

5. Komisija po posvetovanju z Evropskim odborom za umetno inteligenco (v nadaljnjem besedilu: Odbor) in najpozneje do 2. februarja 2026 zagotovi smernice, v katerih določi praktično izvajanje tega člena v skladu s členom 96, skupaj s celovitim seznamom praktičnih primerov uporabe visokotveganih sistemov UI in sistemov UI brez visokega tveganja.

6. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97, da bi spremenila odstavek 3, drugi pododstavek, tega člena, s tem da bi k tam določenim pogojem dodala nove pogoje ali jih spremenila, kadar obstajajo konkretni in zanesljivi dokazi o obstoju sistemov UI, ki spadajo na področje uporabe Priloge III, vendar ne predstavljajo znatnega tveganja škode za zdravje, varnost ali temeljne pravice fizičnih oseb.

7. Komisija sprejme delegirane akte v skladu s členom 97, da bi spremenila kateri koli pogoj iz odstavka 3, drugi pododstavek, tega člena, s črtanjem katerih koli tam določenih pogojev, kadar obstajajo konkretni in zanesljivi dokazi, da je to potrebno za ohranjanje ravni varovanja zdravja, varnosti in temeljnih pravic iz te uredbe.

8. Nobena sprememba pogojev iz odstavka 3, drugi pododstavek, sprejeta v skladu z odstavkoma 6 in 7 tega člena, ne zmanjša splošne ravni varovanja zdravja, varnosti in temeljnih pravic iz te uredbe ter zagotovi skladnost z delegiranimi akti, sprejetimi na podlagi člena 7(1), ter upošteva tržni in tehnološki razvoj.

Člen 7

Spremembe Priloge III

1. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97 za spremembo Priloge III z dodajanjem primerov uporabe visokotveganih sistemov UI ali spreminjanjem njihove uporabe, kadar sta izpolnjena oba naslednja pogoja:

- (a) sistemi UI so namenjeni uporabi na katerem koli področju iz Priloge III;
- (b) sistemi UI predstavljajo tveganje škode za zdravje in varnost ali škodljivega vpliva na temeljne pravice in to tveganje je enakovredno ali večje od tveganja škode ali škodljivega vpliva visokotveganih sistemov UI, ki so že navedeni v Prilogi III.

2. Komisija pri ocenjevanju pogoja iz odstavka 1, točka (b), upošteva naslednja merila:
- (a) predvideni namen sistema UI;
 - (b) obseg, v katerem se sistem UI uporablja ali se bo verjetno uporabljal;
 - (c) naravo in količino podatkov, ki se obdelujejo in uporabljajo v sistemu UI, in zlasti to, ali se obdelujejo posebne vrste osebnih podatkov;
 - (d) obseg, v katerem sistem UI deluje samostojno, in možnost, da človek razveljavi odločitev ali priporočila, ki bi lahko povzročila morebitno škodo;
 - (e) obseg, v katerem je uporaba sistema UI že povzročila škodo za zdravje in varnost, negativno vplivala na temeljne pravice ali povzročila resno zaskrbljenost v zvezi z verjetnostjo take škode ali škodljivega vpliva, kot je razvidno na primer iz poročil ali dokumentiranih trditev, predloženih pristojnim nacionalnim organom, ali drugih poročil, kot je ustrezno;
 - (f) morebitni obseg take škode ali takega škodljivega vpliva, zlasti v smislu njune intenzivnosti in zmožnosti, da vplivata na več oseb ali nesorazmerno vplivata na določeno skupino ljudi;
 - (g) obseg, v katerem so potencialno oškodovane osebe ali osebe, ki bi lahko trpele zaradi škodljivega vpliva, odvisne od izida, ustvarjenega s sistemom UI, zlasti ker iz praktičnih ali pravnih razlogov ni mogoče razumno odstopiti od tega izida;
 - (h) obseg, v katerem obstaja neravnovesje moči ali v katerem so potencialno oškodovane osebe ali osebe, ki bi lahko trpele zaradi škodljivega vpliva, v ranljivem položaju v odnosu do uvajalca sistema UI, zlasti zaradi statusa, avtoritete, znanja, ekonomskih ali socialnih okoliščin ali starosti;
 - (i) obseg, v katerem je rezultat, ki vključuje sistem UI, zlahka popravljiv ali izničitljiv, ob upoštevanju razpoložljivih tehničnih rešitev za njegovo popravljanje ali izničenje, pri čemer rezultati, ki škodljivo vplivajo na zdravje, varnost ali temeljne pravice, ne štejejo za zlahka popravljive ali izničitljive;
 - (j) razsežnost in verjetnost, da bo uvedba sistema UI koristila posameznikom, skupinam ali družbi na splošno, vključno z možnimi izboljšavami glede varnosti proizvodov;
 - (k) obseg, v katerem so v obstoječem pravu Unije določeni:
 - (i) učinkoviti ukrepi sodnega varstva v zvezi s tveganji, ki jih predstavlja sistem UI, razen odškodninskih zahtevkov;
 - (ii) učinkoviti ukrepi za preprečevanje ali bistveno zmanjšanje teh tveganj.
3. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97 za spremembo seznama iz Priloge III z umikom visokotveganih sistemov UI, kadar sta izpolnjena oba naslednja pogoja:
- (a) zadevni visokotvegani sistem UI ob upoštevanju meril iz odstavka 2 ne predstavlja več večjih tveganj za temeljne pravice, zdravje ali varnost;
 - (b) črtanje ne zmanjšuje splošne ravni varovanja zdravja, varnosti in temeljnih pravic na podlagi prava Unije.

ODDELEK 2

Zahteve za visokotvegane sisteme UI

Člen 8

Izpolnjevanje zahtev

1. Visokotvegani sistemi UI izpolnjujejo zahteve iz tega oddelka, pri čemer se upoštevajo njihovi predvideni namen ter splošno priznani najsodobnejši dosežki na področju UI in tehnologij, povezanih z UI. Pri zagotavljanju skladnosti z navedenimi zahtevami se upošteva sistem za obvladovanje tveganja iz člena 9.

2. Kadar proizvod vključuje sistem UI, za katerega se uporabljajo zahteve iz te uredbe in zahteve harmonizacijske zakonodaje Unije iz Priloge I, oddelek A, so ponudniki odgovorni za zagotavljanje popolne usklajenosti njihovega proizvoda z vsemi veljavnimi zahtevami iz veljavne harmonizacijske zakonodaje Unije. Ponudniki imajo pri zagotavljanju skladnosti visokotveganih sistemov UI iz odstavka 1 z zahtevami iz tega oddelka ter za zagotovitev skladnosti, preprečevanje podvajanja in zmanjšanje dodatnih bremen možnost, da po potrebi vključijo potrebne postopke testiranja in poročanja, informacije in dokumentacijo, ki jih predložijo v zvezi s svojim proizvodom, v dokumentacijo in postopke, ki že obstajajo in se zahtevajo na podlagi harmonizacijske zakonodaje Unije iz Priloge I, oddelek A.

Člen 9

Sistem za obvladovanje tveganja

1. V zvezi z visokotveganimi sistemi UI se vzpostavi, izvaja, dokumentira in vzdržuje sistem za obvladovanje tveganja.
2. Sistem za obvladovanje tveganja pomeni neprekinjen in ponavljajoč se proces, ki se načrtuje in izvaja v celotnem življenjskem ciklu visokotvegane sistema UI in ga je treba redno sistematično pregledovati in posodabljati. Vključuje naslednje korake:
 - (a) opredelitev in analizo znanih in razumno predvidljivih tveganj, ki jih lahko visokotvegani sistem UI pomeni za zdravje, varnost ali temeljne pravice, kadar se uporablja v skladu s predvidenim namenom;
 - (b) oceno in ovrednotenje tveganj, ki se lahko pojavijo pri uporabi visokotvegane sistema UI v skladu s predvidenim namenom in v razmerah razumno predvidljive napačne uporabe;
 - (c) ovrednotenje drugih morebitnih tveganj na podlagi analize podatkov, zbranih iz sistema spremljanja po dajanju na trg iz člena 72;
 - (d) sprejetje ustreznih in ciljno usmerjenih ukrepov za obvladovanje tveganja, namenjenih obravnavanju tveganj, opredeljenih na podlagi točke (a).
3. Tveganja iz tega člena se nanašajo samo na tista, ki jih je mogoče razumno zmanjšati ali odpraviti z razvojem ali zasnovo visokotvegane sistema UI ali z zagotovitvijo ustreznih tehničnih informacij.
4. Pri ukrepih za obvladovanje tveganja iz odstavka 2, točka (d), se ustrezno upoštevajo učinki in morebitna interakcija, ki izhajajo iz skupne uporabe zahtev iz tega oddelka 2, da bi učinkoviteje in čim bolj zmanjšali tveganja in hkrati dosegli ustrezno ravnovesje pri izvajanju ukrepov za izpolnjevanje teh zahtev.
5. Ukrepi za obvladovanje tveganja iz odstavka 2, točka (d), so taki, da zadevno preostalo tveganje, povezano z vsako posamezno nevarnostjo, in celotno preostalo tveganje visokotveganih sistemov UI štejeta za sprejemljiva.

Pri določanju najustreznejših ukrepov za obvladovanje tveganja se zagotovi naslednje:

- (a) odpravljanje ali zmanjševanje tveganj ugotovljenih in ocenjenih na podlagi odstavka 2, kolikor je to tehnično izvedljivo z ustrezno zasnovo in razvojem visokotvegane sistema UI;
- (b) po potrebi izvajanje ustreznih ukrepov za zmanjšanje in nadzor tveganj, ki jih ni mogoče odpraviti;
- (c) zagotavljanje zahtevanih informacij na podlagi člena 13 in po potrebi usposabljanje uvajalcev.

Da bi odpravili ali zmanjšali tveganja, povezana z uporabo visokotvegane sistema UI, se ustrezno upoštevajo tehnično znanje, izkušnje, izobraževanje, usposabljanje, ki ga lahko pričakuje uvajalec, in predvideni okvir, v katerem naj bi se sistem uporabljal.

6. Visokotvegani sistemi UI se testirajo, da se določijo najustreznejši in ciljno usmerjeni ukrepi za obvladovanje tveganja. S testiranjem se zagotovi, da visokotvegani sistemi UI dosledno delujejo za predvideni namen in so skladni z zahtevami iz tega oddelka.
7. Postopki testiranja lahko vključujejo testiranje v realnih razmerah v skladu s členom 60.
8. Testiranje visokotveganih sistemov UI se po potrebi izvaja kadar koli med celotnim postopkom razvoja in v vsakem primeru pred njihovim dajanjem na trg ali v uporabo. Testiranje se opravi na podlagi predhodno opredeljenih metrik in verjetnostnih pragov, ki ustrezajo predvidenemu namenu visokotvegane sistema UI.
9. Ponudniki pri izvajanju sistema za obvladovanje tveganja iz odstavkov 1 do 7 preučijo, ali je verjetno, da bo visokotvegani sistem UI glede na predvideni namen negativno vplival na osebe, mlajše od 18 let, in po potrebi na druge ranljive skupine.
10. Pri ponudnikih visokotveganih sistemov UI, za katere veljajo zahteve v zvezi z notranjimi procesi za obvladovanje tveganj v skladu z drugimi ustreznimi določbami prava Unije, so lahko vidiki, opisani v odstavkih 1 do 9, del postopkov za obvladovanje tveganj, vzpostavljenih na podlagi navedenega prava, ali so v kombinaciji s temi postopki.

Člen 10

Podatki in upravljanje podatkov

1. Visokotvegani sistemi UI, ki uporabljajo tehnike, ki vključujejo učenje modelov UI s podatki, se razvijejo na podlagi naborov učnih, validacijskih in testnih podatkov, ki izpolnjujejo merila kakovosti iz odstavkov 2 do 5, kadar se uporabljajo ti nabori podatkov.
2. Za nabore učnih, validacijskih in testnih podatkov veljajo prakse ravnanja s podatki in upravljanja podatkov, ki so primerne za predvideni namen visokotvegane sistema UI. Te prakse se nanašajo zlasti na:
 - (a) ustrezne izbire zasnov;
 - (b) postopke zbiranja podatkov in njihov izvor ter v primeru osebnih podatkov prvotni namen zbiranja podatkov;
 - (c) ustrezne postopke obdelave za pripravo podatkov, kot so dodajanje opomb, označevanje, čiščenje, posodabljanje, obogatitev in združevanje;
 - (d) oblikovanje predpostavk, zlasti v zvezi z informacijami, ki naj bi jih podatki merili in predstavljali;
 - (e) oceno razpoložljivosti, količine in primernosti potrebnih naborov podatkov;
 - (f) preučitev morebitnih pristranskosti, ki bi lahko vplivale na zdravje in varnost oseb, negativno vplivale na temeljne pravice ali privedle do diskriminacije, ki je na podlagi prava Unije prepovedana, zlasti kadar izhodni podatki vplivajo na vhodne podatke za prihodnje operacije;
 - (g) ustrezne ukrepe za odkrivanje, preprečevanje in zmanjševanje morebitnih pristranskosti, opredeljenih v skladu s točko (f);
 - (h) prepoznavanje ustreznih vrzeli ali pomanjkljivosti v podatkih, ki preprečujejo skladnost s to uredbo, ter način za odpravljanje teh vrzeli in pomanjkljivosti.
3. Nabori učnih, validacijskih in testnih podatkov so ustrezni, dovolj reprezentativni in v največji možni meri brez napak in popolni glede na predvideni namen. Imeti morajo tudi ustrezne statistične lastnosti, po potrebi tudi v zvezi z osebami ali skupinami oseb, v zvezi s katerimi naj bi se uporabljal visokotvegani sistem UI. Te značilnosti naborov podatkov se lahko izpolnijo na ravni posameznih naborov podatkov ali na ravni njihovih kombinacij.
4. Nabori podatkov v obsegu, ki se zahteva glede na njihov predvideni namen, upoštevajo značilnosti ali elemente, ki so značilni za posebno geografsko, kontekstualno, vedenjsko ali funkcionalno okolje, v katerem naj bi se visokotvegani sistem UI uporabljal.

5. Če je nujno potrebno za namene zagotavljanja odkrivanja in popravljanja pristranskosti v zvezi z visokotveganimi sistemi UI v skladu z odstavkom 2, točki (f) in (g), tega člena, lahko ponudniki takih sistemov izjemoma obdelujejo posebne vrste osebnih podatkov, ob upoštevanju ustreznih zaščitnih ukrepov za temeljne pravice in svoboščine fizičnih oseb. Poleg določb iz uredb (EU) 2016/679 in (EU) 2018/1725 ter Direktive (EU) 2016/680 morajo biti za tako obdelavo izpolnjeni vsi naslednji pogoji:

- (a) odkrivanja in popravljanja pristranskosti ni mogoče učinkovito doseči z obdelavo drugih podatkov, vključno s sintetičnimi ali anonimiziranimi podatki;
 - (b) za posebne vrste osebnih podatkov veljajo tehnične omejitve glede ponovne uporabe osebnih podatkov ter najodobnejši ukrepi za varnost in ohranjanje zasebnosti, vključno s psevdonimizacijo;
 - (c) za posebne kategorije osebnih podatkov veljajo ukrepi, s katerimi se zagotavlja, da so osebni podatki, ki se obdelujejo, zaščiteni, ob upoštevanju ustreznih zaščitnih ukrepov, vključno s strogim nadzorom in dokumentiranjem dostopa, da se prepreči napačna uporaba in zagotovi, da imajo dostop do teh osebnih podatkov samo pooblaščen osebe z ustreznimi obveznostmi glede zaupnosti;
 - (d) posebne kategorije osebnih podatkov ne smejo biti posredovani, preneseni ali drugače dostopni drugim strankam;
 - (e) posebne kategorije osebnih podatkov se izbrišejo, ko je pristranskost odpravljena ali ko se izteče obdobje njihove hrambe, odvisno od tega, kaj nastopi prej;
 - (f) evidence dejavnosti obdelave na podlagi uredb (EU) 2016/679 in (EU) 2018/1725 ter Direktivo (EU) 2016/680 vključujejo razloge, zakaj je bila obdelava posebnih kategorij osebnih podatkov nujno potrebna za odkrivanje in odpravo pristranskosti ter zakaj tega cilja ni bilo mogoče doseči z obdelavo drugih podatkov.
6. Za razvoj visokotveganih sistemov UI, ki ne uporabljajo tehnik, ki vključujejo učenje modelov s podatki, se odstavki 2 do 5 uporabljajo le za nabore testnih podatkov.

Člen 11

Tehnična dokumentacija

1. Tehnična dokumentacija visokotvegane sistema UI se pripravi pred dajanjem sistema na trg ali v uporabo in se posodablja.

Tehnična dokumentacija se pripravi tako, da izkazuje, da je visokotvegani sistem UI skladen z zahtevami iz tega oddelka, ter pristojnim nacionalnim organom in priglasi organom jasno in celovito zagotavlja potrebne informacije za ugotavljanje skladnosti sistema UI z navedenimi zahtevami. Vsebovati mora vsaj elemente iz Priloge IV. MSP, vključno z zagonskimi podjetji, lahko elemente tehnične dokumentacije iz Priloge IV predložijo na poenostavljen način. V ta namen Komisija pripravi poenostavljen obrazec tehnične dokumentacije, namenjen potrebam malih in mikro podjetij. Kadar se MSP, vključno z zagonskim podjetjem, odloči, da bo informacije, zahtevane v Prilogi IV, zagotovilo na poenostavljen način, uporabi obrazec iz tega odstavka. Priglašeni organi sprejmejo obrazec za namene ugotavljanja skladnosti.

2. Kadar je visokotvegani sistem UI, povezan s proizvodom, za katerega se uporablja harmonizacijska zakonodaja Unije iz Priloge I, oddelek A, dan na trg ali v uporabo, se pripravi enoten sklop tehnične dokumentacije, ki vsebuje vse informacije iz odstavka 1 in informacije, zahtevane v navedenih pravnih aktih.

3. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97 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 oddelka.

Člen 12

Vodenje evidenc

1. Visokotvegani sistemi UI morajo tehnično omogočati samodejno beleženje dogodkov (v nadaljnjem besedilu: dnevniki) v življenjski dobi sistema.
2. Da bi zagotovili raven sledljivosti delovanja visokotveganega sistema UI, ki ustreza predvidenemu namenu sistema, morajo zmogljivosti vodenja dnevnikov omogočati beleženje dogodkov, pomembnih za:
 - (a) prepoznavanje situacij, ki lahko povzročijo, da bi visokotvegani sistem UI predstavljal tveganje v smislu člena 79(1), ali povzročijo bistvene spremembe;
 - (b) olajšanje spremljanja po dajanju na trg iz člena 72 ter
 - (c) spremljanje delovanja visokotveganega sistema UI iz člena 26(5).
3. Za visokotvegane sisteme UI iz Priloge III, točka 1(a), zmogljivosti vodenja dnevnikov zagotavljajo vsaj:
 - (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, ki sodelujejo pri preverjanju rezultatov, iz člena 14(5).

Člen 13

Preglednost in zagotavljanje informacij uvajalcem

1. Visokotvegani sistemi UI morajo biti zasnovani in razviti tako, da je njihovo delovanje dovolj pregledno, da lahko uvajalci razlagajo izhodne podatke sistema in jih ustrezno uporabijo. Treba je zagotoviti ustrezno vrsto in stopnjo preglednosti, da se doseže skladnost z ustreznimi obveznostmi ponudnika in uvajalca iz oddelka 3.
2. Visokotveganim sistemom UI morajo biti 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 uvajalcem.
3. Navodila za uporabo vsebujejo vsaj naslednje informacije:
 - (a) istovetnost in kontaktne podatke ponudnika in po potrebi njegovega pooblaščenega zastopnika, kadar obstaja;
 - (b) značilnosti, zmogljivosti in omejitve zmogljivosti visokotveganega sistema UI, ki vključujejo:
 - (i) njegov predvideni namen;
 - (ii) raven točnosti, vključno s pripadajočimi metrikami, robustnosti in kibernetske varnosti iz člena 15, na podlagi katere je bil visokotvegani sistem UI testiran in potrjen ter ki se lahko pričakuje, pa tudi 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 visokotveganega sistema UI v skladu s predvidenim namenom ali v razmerah razumno predvidljive napačne uporabe, ki lahko povzročijo tveganja za zdravje in varnost ali temeljne pravice iz člena 9(2);
 - (iv) po potrebi tehnične zmogljivosti in značilnosti visokotveganega sistema UI za zagotavljanje informacij, ki so pomembne za pojasnitev njegovih izhodnih podatkov;

- (v) če je primerno, njegova zmogljivost v zvezi z določenimi osebami ali skupinami oseb, na katerih naj bi se sistem uporabljal;
- (vi) če je primerno, specifikacije za vhodne podatke ali katere koli druge ustrezne informacije v zvezi z uporabljenimi nabori učnih, validacijskih in testnih podatkov, ob upoštevanju predvidenega namena visokotveganega sistema UI;
- (vii) po potrebi informacije, da lahko uvajalci razlagajo izhodne podatke visokotveganega sistema UI in jih ustrezno uporabljajo;
- (c) morebitne spremembe visokotveganega sistema UI in njegove zmogljivosti, ki jih je ponudnik vnaprej določil ob začetnem ugotavljanju skladnosti;
- (d) ukrepe za človeški nadzor iz člena 14, vključno z vzpostavljenimi tehničnimi ukrepi, ki uvajalcem olajšajo razlago izhodnih podatkov visokotveganih sistemov UI;
- (e) potrebne računalniške in strojnoopremne vire, življenjsko dobo visokotveganega sistema UI ter vse potrebne vzdrževalne in oskrbovalne ukrepe, vključno z njihovo pogostostjo, za zagotovitev pravilnega delovanja tega sistema UI, tudi kar zadeva posodobitve programske opreme;
- (f) po potrebi opis mehanizmov v visokotveganem sistemu UI, na podlagi katerega lahko uvajalci pravilno zbirajo, hranijo in razlagajo dnevnike v skladu s členom 12.

Člen 14

Človeški nadzor

1. Visokotvegani sistemi UI morajo biti zasnovani in razviti tako, da jih lahko fizične osebe v obdobju njihove uporabe učinkovito nadzorujejo, tudi z ustreznimi vmesniškimi orodji človek-stroj.
2. Namen človeškega nadzora je preprečiti ali čim bolj zmanjšati tveganja za zdravje, varnost ali temeljne pravice, ki se lahko pojavijo pri uporabi visokotveganega sistema UI v skladu s predvidenim namenom ali v razmerah razumno predvidljive napačne uporabe, zlasti kadar taka tveganja niso odpravljena kljub uporabi drugih zahtev iz tega oddelka.
3. Nadzorni ukrepi morajo biti sorazmerni s tveganji, stopnjo samostojnosti in kontekstom uporabe visokotveganega sistema UI in se zagotavljajo z eno ali obema naslednjima vrstama ukrepov:
 - (a) ukrepi, določeni in vgrajeni, če je to tehnično izvedljivo, v visokotvegani sistem UI s strani ponudnika, preden je sistem dan na trg ali v uporabo;
 - (b) ukrepi, ki jih ponudnik določi pred dajanjem visokotveganega sistema UI na trg ali v uporabo in so primerni za izvedbo s strani uvalca.
4. Za namene izvajanja odstavkov 1, 2 in 3 se visokotvegani sistem UI uvajalcu zagotovi tako, da fizične osebe, ki jim je dodeljen človeški nadzor, če je to primerno in sorazmerno:
 - (a) pravilno razumejo ustrezne zmogljivosti in omejitve visokotveganega sistema UI ter ustrezno spremljajo njegovo delovanje, tudi za odkrivanje in obravnavanje nepravilnosti, motenj in nepričakovane zmogljivosti;
 - (b) se zavedajo morebitne težnje po samodejnem zanašanju ali prevelikem zanašanju na izhodne podatke visokotveganega sistema UI (pristranskost zaradi avtomatizacije), zlasti pri visokotveganih sistemih UI, ki se uporabljajo za zagotavljanje informacij ali priporočil za odločitve, ki jih sprejemajo fizične osebe;
 - (c) pravilno razlagajo izhodne podatke visokotveganega sistema UI, zlasti na primer ob upoštevanju razpoložljivih orodij in metod za razlago;

- (d) se v specifičnih situacijah odločijo, da visokotveganega sistema UI ne bodo uporabile ali bodo kako drugače zanemarile, ovrgle ali izničile izhodne podatke visokotveganega sistema UI;
- (e) posegajo v delovanje visokotveganega sistema UI ali ga prekinijo s tipko „stop“ ali podobnim postopkom, ki omogoča varno zaustavitev sistema.

5. Za visokotvegane sisteme UI iz Priloge III, točka 1(a), morajo biti ukrepi iz odstavka 3 takšni, da zagotavljajo, da uvajalec 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 potrdira vsaj dve fizični osebi z ustreznimi kompetencami, usposobljenostjo in pooblastili.

Zahteva o ločeni preverbi s strani vsaj dveh fizičnih oseb se ne uporablja za visokotvegane sisteme UI, ki se uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, migracij, nadzora meje ali azila, v primerih, ko je v skladu s pravom Unije in nacionalnim pravom uporaba te zahteve nesorazmerna.

Člen 15

Točnost, robustnost in kibernetska varnost

1. Visokotvegani sistemi UI morajo biti zasnovani in razviti tako, da dosegajo ustrezno raven točnosti, robustnosti in kibernetske varnosti ter v teh vidikih v vsem svojem življenjskem ciklu delujejo dosledno.
2. Za obravnavo tehničnih vidikov merjenja ustreznih ravni točnosti in robustnosti iz odstavka 1 ter vseh drugih ustreznih metrike učinkovitosti Komisija v sodelovanju z ustreznimi deležniki in organizacijami, kot so meroslovni organi in organi za primerjalno analizo, po potrebi spodbuja razvoj referenčnih vrednosti in metodologij merjenja.
3. Ravni točnosti in ustrezne metrike točnosti visokotveganih sistemov UI se navedejo v priloženih navodilih za uporabo.
4. Visokotvegani sistemi UI morajo biti čim bolj 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. V zvezi s tem se sprejmejo tehnični in organizacijski ukrepi.

Robustnost visokotveganih sistemov UI se lahko doseže s tehničnimi redundantnimi rešitvami, ki lahko vključujejo rezervne načrte ali načrte varne odpovedi.

Visokotvegane sisteme UI, ki se po dajanju na trg ali v uporabo še naprej učijo, je treba razviti tako, da se odpravi ali v največji možni meri zmanjša tveganje morebitnih pristranskih izhodnih podatkov, ki bi vplivali na vhodne podatke za prihodnje operacije (povratne zanke), in zagotovi, da se vse take povratne zanke ustrezno obravnavajo z ustreznimi ukrepi za zmanjšanje tveganj.

5. Visokotvegani sistemi UI morajo biti odporni na poskuse nepooblaščenih tretjih oseb, da z izkoriščanjem šibkih točk sistema spremenijo njihovo uporabo, izhodne podatke ali zmogljivost.

Tehnične rešitve, namenjene zagotavljanju kibernetske varnosti visokotveganih sistemov UI, morajo ustrezati zadevnim okoliščinam in tveganjem.

Tehnične rešitve za odpravljanje šibkih točk, značilnih za UI, po potrebi vključujejo ukrepe za preprečevanje, odkrivanje, odzivanje, reševanje in nadzor v zvezi z napadi, ki poskušajo manipulirati z naborom učnih podatkov (zastrupitev podatkov) ali prednaučenimi komponentami, uporabljenimi pri učenju (zastrupitev modelov), v zvezi z vhodnimi podatki, katerih namen je povzročiti napako modela UI (nasprotovadni primer ali izogibanje modelov), napadi na zaupnost ali pomanjkljivost modela.

ODDELEK 3

Obveznosti ponudnikov in uvajalcev visokotveganih sistemov UI

Člen 16

Obveznosti ponudnikov visokotveganih sistemov UI

Ponudniki visokotveganih sistemov UI:

- (a) zagotovijo, da so njihovi visokotvegani sistemi UI skladni z zahtevami iz oddelka 2;
- (b) na visokotvegane sistem UI ali, kadar to ni mogoče, na embalaži ali spremni dokumentaciji, kot je ustrezno, navedejo svoje ime, registrirano trgovsko ime ali registrirano znamko, in naslov, na katerem so dosegljivi;
- (c) imajo vzpostavljen sistem upravljanja kakovosti, skladen s členom 17;
- (d) hranijo dokumentacijo iz člena 18;
- (e) kadar je to pod njihovim nadzorom, hranijo dnevnike, ki jih samodejno ustvarijo njihovi visokotvegani sistemi UI, kot je navedeno v členu 19;
- (f) zagotovijo, da visokotvegani sistem UI pred dajanjem na trg ali v uporabo opravi ustrezen postopek ugotavljanja skladnosti iz člena 43;
- (g) pripravijo EU izjavo o skladnosti v skladu s členom 47;
- (h) na visokotvegani sistem UI ali, kadar to ni mogoče, na njegovo embalažo ali priloženo dokumentacijo, namestijo oznako CE v skladu s členom 48, da označijo skladnost s to uredbo;
- (i) izpolnjujejo obveznosti registracije iz člena 49(1);
- (j) sprejmejo potrebne korektivne ukrepe in zagotovijo informacije v skladu s členom 20;
- (k) na obrazloženo zahtevo pristojnega nacionalnega organa dokažejo skladnost visokotvegane sistema UI z zahtevami iz oddelka 2;
- (l) zagotovijo, da visokotvegani sistem UI izpolnjuje zahteve glede dostopnosti v skladu z direktivama (EU) 2016/2102 in (EU) 2019/882.

Člen 17

Sistem upravljanja kakovosti

1. Ponudniki visokotveganih sistemov UI 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 visokotvegane sistema UI;
- (b) tehnike, postopke in sistematične ukrepe, ki se uporabljajo za razvoj, nadzor kakovosti in zagotavljanje kakovosti visokotvegane sistema UI;
- (c) tehnike, postopke in sistematične ukrepe, ki se uporabljajo za razvoj, nadzor kakovosti in zagotavljanje kakovosti visokotvegane sistema UI;
- (d) postopke pregledovanja, testiranja in validacije, ki se izvedejo pred razvojem visokotvegane sistema UI, 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 ali ne zajemajo vseh ustreznih zahtev iz oddelka 2, sredstva, ki se uporabijo za zagotovitev, da visokotvegani sistem UI izpolnjuje navedene zahteve;
 - (f) sisteme in postopke za ravnanje s podatki, vključno s pridobivanjem podatkov, 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 visokotveganih sistemov UI na trg ali v uporabo in za namen dajanja na trg ali v uporabo;
 - (g) sistem za obvladovanje tveganj iz člena 9;
 - (h) vzpostavitev, izvajanje in vzdrževanje sistema spremljanja po dajanju na trg v skladu s členom 72;
 - (i) postopke v zvezi s poročanjem o resnih incidentih v skladu s členom 73;
 - (j) vodenje komunikacije s pristojnimi nacionalnimi organi, drugimi ustreznimi organi, tudi s tistimi, ki zagotavljajo ali podpirajo dostop do podatkov, priglašeni 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. V vsakem primeru pa ponudniki spoštujejo stopnjo strogosti in raven zaščite, ki se zahtevata za skladnost njihovih visokotveganih sistemov UI s to uredbo.
3. Ponudniki visokotveganih sistemov UI, za katere veljajo obveznosti v zvezi s sistemi upravljanja kakovosti ali enakovredno funkcijo na podlagi ustreznega sektorskega prava Unije, lahko vključijo vidike, navedene v odstavku 1, kot del sistemov upravljanja kakovosti, vzpostavljenih na podlagi navedenega prava.
4. Za ponudnike, ki so finančne institucije in za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki na podlagi prava Unije o finančnih storitvah, se šteje, da je obveznost vzpostavitve sistema vodenja kakovosti z izjemo odstavka 1, točke (g), (h) in (i) tega člena, izpolnjena z upoštevanjem pravil o ureditvah ali postopkih notranjega upravljanja na podlagi ustreznega prava Unije o finančnih storitvah. V ta namen se upoštevajo vsi harmonizirani standardi iz člena 40.

Člen 18

Vodenje dokumentacije

1. Ponudnik še deset let po tem, ko je bil visokotvegani sistem UI 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, kadar je primerno;
 - (d) odločitve in druge dokumente, ki so jih izdali priglašeni organi, kadar je primerno;
 - (e) EU izjavo o skladnosti iz člena 47.

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

3. Ponudniki, ki so finančne institucije in za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki na podlagi prava Unije o finančnih storitvah, vodijo tehnično dokumentacijo kot del dokumentacije, ki se hrani na podlagi ustreznega prava Unije o finančnih storitvah.

Člen 19

Samodejno ustvarjeni dnevniki

1. Ponudniki visokotveganih sistemov UI vodijo dnevnike iz člena 12(1), ki jih samodejno ustvarijo njihovi visokotvegani sistemi UI, če so ti dnevniki pod njihovim nadzorom. Brez poseganja v pravo Unije ali nacionalno pravo, ki se uporablja, se dnevniki hranijo za obdobje, ki ustreza predvidenemu namenu visokotvegane sistema UI, in sicer najmanj šest mesecev, razen če je v veljavnem pravu Unije ali nacionalnem pravu, zlasti v pravu Unije o varstvu osebnih podatkov, določeno drugače.

2. Ponudniki, ki so finančne institucije in za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki na podlagi prava Unije o finančnih storitvah, vodijo dnevnike, ki jih samodejno ustvarijo njihovi visokotvegani sistemi UI, kot del dokumentacije, ki se hrani na podlagi ustreznega prava Unije o finančnih storitvah.

Člen 20

Korektivni ukrepi in dolžnost obveščanja

1. Ponudniki visokotveganih sistemov UI, ki menijo ali utemeljeno domnevajo, da visokotvegani sistem UI, ki so ga dali na trg ali v uporabo, ni v skladu s to uredbo, nemudoma sprejmejo potrebne popravne ukrepe, da zagotovijo skladnost sistema ali pa ga po potrebi umaknejo, onemogočijo ali preklicajo. O tem obvestijo distributerje zadevnega visokotvegane sistema UI ter, kadar je primerno, uvaljalce, pooblaščenega zastopnika in uvoznike.

2. Kadar visokotvegani sistem UI predstavlja tveganje v smislu člena 79(1) in se ponudnik seznani s tem tveganjem, nemudoma raziše vzroke, po potrebi v sodelovanju z uvaljalcem, ki poroča, ter obvesti organe za nadzor trga, pristojne za zadevni visokotvegani sistem UI, in po potrebi priглаšeni organ, ki je izdal certifikat za visokotvegani sistem UI v skladu s členom 44, zlasti o naravi neskladnosti in vseh ustreznih sprejetih korektivnih ukrepov.

Člen 21

Sodelovanje s pristojnimi organi

1. Ponudniki visokotveganih sistemov UI na obrazloženo zahtevo pristojnega nacionalnega organa temu organu zagotovijo vse informacije in dokumentacijo, potrebne za dokazovanje skladnosti visokotvegane sistema UI z zahtevami iz oddelka 2, v enem od uradnih jezikov Unije, ki ga določi zadevna država članica in ga organ brez težav razume.

2. Ponudniki na obrazloženo zahtevo pristojnega organa pristojnemu organu prosilcu po potrebi omogočijo tudi dostop do samodejno ustvarjenih dnevnikov visokotvegane sistema UI iz člena 12(1), če so ti dnevniki pod njihovim nadzorom.

3. Vse informacije, ki jih pristojni organ pridobi na podlagi tega člena, se obravnavajo v skladu z obveznostmi glede zaupnosti iz člena 78.

Člen 22

Pooblašчени zastopniki ponudnikov visokotveganih sistemov UI

1. Ponudniki s sedežem v tretjih državah pred omogočanjem dostopnosti visokotveganih sistemov UI na trgu Unije s pisnim pooblastilom imenujejo pooblaščenega zastopnika s sedežem v Uniji.
2. Ponudnik svojemu pooblaščenemu zastopniku omogoči, da opravlja naloge, določene v pooblastilu, ki ga prejme od ponudnika.
3. Pooblašчени zastopnik opravlja naloge, določene v pooblastilu, ki ga prejme od ponudnika. Če organi za nadzor trga to zahtevajo, jim predloži izvod pooblastila, in sicer v enem od uradnih jezikov institucij Unije, ki ga navede pristojni organ. Za namene te uredbe pooblastilo pooblaščenemu zastopniku omogoča, da opravlja naslednje naloge:
 - (a) preveri, da je bila pripravljena EU izjava o skladnosti iz člena 47 in tehnična dokumentacija iz člena 11 ter da je ponudnik izvedel ustrezen postopek ugotavljanja skladnosti;
 - (b) daje kontaktne podatke ponudnika, ki je določil pooblaščenega zastopnika, izvod EU izjave o skladnosti iz člena 47, tehnično dokumentacijo in, če je ustrezno, certifikat, ki ga je izdal priglašeni organ, na voljo pristojnim organom in nacionalnim organom ali telesom iz člena 74(10) še deset let po tem, ko je bil visokotvegani sistem UI dan na trg ali v uporabo;
 - (c) pristojnemu organu na podlagi obrazložene zahteve zagotovi vse informacije in dokumentacijo, vključno s tisto, ki se hrani v skladu s točko (b) tega pododstavka, potrebne za dokazovanje skladnosti visokotvegane sistema UI z zahtevami iz oddelka 2, vključno z dostopom do dnevnikov, kakor je navedeno v členu 12(1), ki jih samodejno ustvari visokotvegani sistem UI, če so ti dnevniki pod nadzorom ponudnika;
 - (d) na podlagi obrazložene zahteve sodeluje s pristojnimi organi pri vseh ukrepih, ki jih ti sprejmejo v zvezi z visokotveganim sistemom UI, zlasti za zmanjšanje in omejitev tveganj, ki jih predstavlja visokotvegani sistem UI;
 - (e) po potrebi izpolnjuje obveznosti registracije iz člena 49(1) ali, če registracijo izvede ponudnik sam, zagotovi, da so informacije iz Priloge VIII, oddelek A, točka 3, pravilne.

Na podlagi pooblastila je pooblašчени zastopnik pooblaščen, da lahko pristojni organi nanj, poleg ponudnika ali namesto njega, naslovijo vsa vprašanja, povezana z zagotavljanjem skladnosti s to uredbo.

4. Pooblašчени zastopnik odpove pooblastilo, če meni ali utemeljeno domneva, da ponudnik ravna v nasprotju s svojimi obveznostmi iz te uredbe. V takem primeru o odpovedi pooblastila in razlogih zanjo nemudoma obvesti ustrezní organ za nadzor trga in, kadar je primerno, ustrezní priglašeni organ.

Člen 23

Obveznosti uvoznikov

1. Pred dajanjem visokotvegane sistema UI na trg uvozniki zagotovijo njegovo skladnost s to uredbo tako, da preverijo, da:
 - (a) je ponudnik za ta visokotvegani sistem UI izvedel ustrezen postopek ugotavljanja skladnosti iz člena 43;
 - (b) je ponudnik pripravil tehnično dokumentacijo v skladu s členom 11 in Prilogo IV;
 - (c) je sistem opremljen z zahtevano oznako CE ter so mu priloženi EU izjava o skladnosti iz člena 47 in navodila za uporabo;
 - (d) je ponudnik imenoval pooblaščenega zastopnika v skladu s členom 22(1).

2. Kadar ima uvoznik zadosten razlog za domnevo, da visokotvegani sistem UI ni skladen s to uredbo ali je ponarejen ali mu je priložena ponarejena dokumentacija, tega sistema ne da na trg, dokler ni zagotovljena njegova skladnost. Kadar visokotvegani sistem UI predstavlja tveganje v smislu člena 79(1), uvoznik o tem obvesti ponudnika sistema, pooblaščenega zastopnika in organe za nadzor trga.
3. Uvozniki na visokotveganem sistemu UI in na embalaži ali v spremni dokumentaciji, kadar je ustrezno, navedejo svoje ime, registrirano trgovsko ime ali registrirano znamko in naslov, na katerem so dosegljivi.
4. Uvozniki zagotovijo, da v času, ko so odgovorni za visokotvegani sistem UI, pogoji skladiščenja ali prevoza, kadar je ustrezno, ne ogrožajo skladnosti sistema z zahtevami iz oddelka 2.
5. Uvozniki še deset let po tem, ko je bil visokotvegani sistem UI dan na trg ali v uporabo, hranijo izvod certifikata, ki ga je izdal priglašeni organ, navodil za uporabo, kadar je to primerno, in EU izjave o skladnosti iz člena 47.
6. Uvozniki ustreznim pristojnim organom na podlagi obrazložene zahteve predložijo vse potrebne informacije in dokumentacijo, vključno s tistimi iz odstavka 5, da dokažejo skladnost visokotveganega sistema UI z zahtevami iz oddelka 2, v jeziku, ki ga organi zlahka razumejo. V ta namen zagotovijo tudi, da se tem organom lahko da na voljo tehnična dokumentacija.
7. Uvozniki sodelujejo z ustreznimi pristojnimi organi pri vseh ukrepih, ki jih ti organi sprejmejo v zvezi z visokotveganim sistemom UI, ki so ga uvozniki dali na trg, zlasti za zmanjšanje ali omejitev tveganj, ki jih predstavlja ta sistem.

Člen 24

Obveznosti distributerjev

1. Preden omogočijo dostopnost visokotveganega sistema UI na trgu, distributerji preverijo, ali ima zahtevano oznako CE, ali so mu priloženi izvod EU izjave o skladnosti iz člena 47 in navodila za uporabo ter ali sta ponudnik in uvoznik tega sistema, kot je ustrezno, izpolnila vsak svoje obveznosti iz člena 16, točki (b) in (c), oziroma člena 23(3).
2. Kadar distributer meni ali na podlagi informacij, ki jih ima, utemeljeno domneva, da visokotvegani sistem UI ni skladen z zahtevami iz oddelka 2, za visokotvegani sistem UI ne omogoči dostopnosti na trgu, dokler ni zagotovljena skladnost tega sistema z navedenimi zahtevami. Kadar visokotvegani sistem UI predstavlja tveganje v smislu člena 79(1), distributer o tem obvesti ponudnika oziroma uvoznika sistema, kot je ustrezno.
3. Distributerji zagotovijo, da v času, ko so odgovorni za visokotvegani sistem UI, pogoji skladiščenja ali prevoza, kadar je ustrezno, ne ogrožajo njegove skladnosti z zahtevami iz oddelka 2.
4. Distributer, ki na podlagi informacij, ki jih ima, meni ali utemeljeno domneva, da visokotvegani sistem UI, za katerega je omogočil dostopnost na trgu, ni skladen z zahtevami iz oddelka 2, sprejme popravne ukrepe, potrebne za usklajitev 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 visokotvegani sistem UI predstavlja tveganje v smislu člena 79(1), distributer o tem nemudoma obvesti ponudnika ali uvoznika sistema in organe, pristojne za zadevni visokotvegani sistem UI, ter navede podrobnosti, zlasti o neskladnosti in vseh sprejetih popravnih ukrepih.
5. Distributerji visokotveganega sistema UI ustreznemu pristojnemu organu na podlagi obrazložene zahteve zagotovijo vse informacije in dokumentacijo o svojih ukrepih na podlagi odstavkov 1 do 4, ki so potrebne za dokazovanje skladnosti visokotveganega sistema UI z zahtevami iz oddelka 2.
6. Distributerji sodelujejo z ustreznimi pristojnimi organi pri vseh ukrepih, ki jih ti organi sprejmejo v zvezi z visokotveganim sistemom UI, katerega so distributerji dali na trg, zlasti za zmanjšanje ali omejitev tveganja, ki ga predstavlja visokotvegani sistem UI.

Člen 25

Odgovornosti vzdolž verige vrednosti UI

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

- (a) visokotvegani sistem UI, ki je že bil dan na trg ali v uporabo, označijo s svojim imenom ali znamko, brez poseganja v pogodbene dogovore, ki določajo, da so obveznosti drugače dodeljene;
- (b) bistveno spremenijo visokotvegani sistem UI, ki je že bil dan na trg ali v uporabo, na način, da ostane visokotvegani sistem UI na podlagi člena 6;
- (c) spremenijo predvideni namen sistema UI, vključno s sistemom UI za splošne namene, ki ni bil razvrščen kot sistem visokega tveganja in je že bil dan na trg ali v uporabo na način, da postane visokotvegani sistem UI v skladu s členom 6.

2. Kadar nastopijo okoliščine iz odstavka 1, ponudnik, ki je prvotno dal sistem UI na trg ali v uporabo, za namene te uredbe ne šteje več za ponudnika tega posameznega sistema UI. Ta prvotni ponudnik tesno sodeluje z novimi ponudniki in daje na voljo potrebne informacije ter zagotavlja razumno pričakovani tehnični dostop in drugo pomoč, ki je potrebna za izpolnjevanje obveznosti iz te uredbe, zlasti v zvezi z ugotavljanjem skladnosti visokotveganih sistemov UI. Ta odstavek se ne uporablja v primerih, ko je prvotni ponudnik jasno navedel, da se njegov sistem UI ne sme spremeniti v visokotvegani sistem UI, in zato zanj ne velja obveznost predaje dokumentacije.

3. Za visokotvegane sisteme UI, ki so varnostne komponente proizvodov, za katere se uporablja harmonizacijska zakonodaja Unije iz Priloge I, oddelek A, proizvajalec teh proizvodov šteje za ponudnika visokotveganega sistema UI in zanj veljajo obveznosti iz člena 16 na podlagi enega od naslednjih scenarijev:

- (a) visokotvegani sistem UI se da na trg skupaj s proizvodom pod imenom ali znamko proizvajalca proizvoda;
- (b) visokotvegani sistem UI se da v uporabo pod imenom ali znamko proizvajalca proizvoda, potem ko je bil ta dan na trg.

4. Ponudnik visokotveganega sistema UI in tretja oseba, ki dobavlja sistem UI, orodja, storitve, komponente ali procese, ki se uporabljajo ali integrirajo v visokotvegani sistem UI, s pisnim dogovorom določita potrebne informacije, zmogljivosti, tehnični dostop in drugo pomoč na podlagi splošno priznanih najsodobnejših tehnoloških dosežkov, da lahko ponudnik visokotveganega sistema UI v celoti izpolnjuje obveznosti iz te uredbe. Ta odstavek se ne uporablja za tretje osebe, ki javnosti omogočajo dostop do orodij, storitev, postopkov ali komponent, ki niso modeli UI za splošne namene, na podlagi proste in odprtokodne licence.

Urad za UI lahko pripravi in priporoči prostovoljne vzorčne pogoje za pogodbe med ponudniki visokotveganih sistemov UI in tretjimi osebami, ki zagotavljajo orodja, storitve, komponente ali postopke, ki se uporabljajo za visokotvegane sisteme UI ali so vanje vključeni. Urad za UI pri oblikovanju teh vzorčnih pogojev upošteva morebitne pogodbene zahteve, ki se uporabljajo v posameznih sektorjih ali poslovnih primerih. Prostovoljni vzorčni pogoji se objavijo in so brezplačno na voljo v lahko uporabni elektronski obliki.

5. Odstavka 2 in 3 ne posegata v potrebo po spoštovanju in varstvu pravic intelektualne lastnine, zaupnih poslovnih informacij in poslovnih skrivnosti v skladu s pravom Unije in nacionalnim pravom.

Člen 26

Obveznosti uvajalcev visokotveganih sistemov UI

1. Uvajalci visokotveganih sistemov UI sprejmejo ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovijo, da uporabljajo take sisteme v skladu s priloženimi navodili za uporabo, na podlagi odstavkov 3 in 6.

2. Uvajalci dodelijo človeški nadzor fizičnim osebam, ki imajo potrebne kompetence, usposobljenost in pooblastila ter potrebno podporo.
3. Obveznosti iz odstavkov 1 in 2 ne posegajo v druge obveznosti uvajalca v skladu s pravom Unije ali nacionalnim pravom ter v pravico uvajalca, da organizira lastna sredstva in dejavnosti za izvajanje ukrepov za človeški nadzor, ki jih navede ponudnik.
4. Brez poseganja v odstavek 1 in 2, če uvajalec izvaja nadzor nad vhodnimi podatki, ta uvajalec zagotovi, da so vhodni podatki ustrezni in dovolj reprezentativni glede na predvideni namen visokotveganega sistema UI.
5. Uvajalci spremljajo delovanje visoko tveganega sistema UI na podlagi navodil za uporabo in po potrebi obvestijo ponudnike v skladu s členom 72. Kadar imajo uvajalci razlog za domnevo, da bi uporaba visoko tveganega sistema UI v skladu z navodili lahko povzročila, da bi visokotvegani sistem UI predstavljal tveganje v smislu člena 79(1), o tem brez nepotrebnega odlašanja obvestijo ponudnika ali distributerja in ustrezní organ za nadzor trga ter začasno prekinijo uporabo tega sistema. Kadar uvajalci odkrijejo resen incident, o tem incidentu takoj obvestijo najprej ponudnika in nato uvoznika ali distributerja in ustrezne organe za nadzor trga. Če uvajalec ne more priti v stik s ponudnikom, se smiselno uporablja člen 73. Ta obveznost ne zajema občutljivih operativnih podatkov uvajalcev sistemov UI, ki so organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj.

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

6. Uvajalci visokotveganih sistemov UI vodijo dnevnike, ki jih samodejno ustvari ta visokotvegani sistem UI, če so ti dnevniki pod njihovim nadzorom, v obdobju, ki ustreza predvidenemu namenu visokotveganega sistema UI, in sicer vsaj šest mesecev, razen če je v veljavnem pravu Unije ali nacionalnem pravu, zlasti v pravu Unije o varstvu osebnih podatkov, določeno drugače.

Uvajalci, ki so finančne institucije in za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki na podlagi prava Unije o finančnih storitvah, vodijo dnevnike kot del dokumentacije, ki se hrani na podlagi ustreznega prava Unije o finančnih storitvah.

7. Uvajalci, ki so delodajalci, pred dajanjem v uporabo ali pred uporabo visokotveganega sistema UI na delovnem mestu obvestijo predstavnike delavcev in delavce, na katere se to nanaša, da se bo zanje uporabljal visokotvegani sistem UI. Te informacije se po potrebi zagotovijo v skladu s pravili in postopki, določenimi v pravu Unije in nacionalnem pravu ter praksi v zvezi z obveščanjem delavcev in njihovih predstavnikov.

8. Uvajalci visokotveganih sistemov UI, ki so javni organi ali institucije, organi, uradi in agencije Unije, izpolnjujejo obveznosti registracije iz člena 49. Če ti uvajalci ugotovijo, da visokotvegani sistem UI, ki ga nameravajo uporabljati, ni bil registriran v podatkovni zbirki EU iz člena 71, tega sistema ne uporabljajo in o tem obvestijo ponudnika ali distributerja.

9. Uvajalci visokotveganih sistemov UI po potrebi uporabijo informacije iz člena 13 te uredbe, da izpolnijo svojo obveznost izvedbe ocene učinka v zvezi z varstvom podatkov na podlagi člena 35 Uredbe (EU) 2016/679 ali člena 27 Direktive (EU) 2016/680.

10. Brez poseganja v Direktivo (EU) 2016/680 v okviru preiskave za ciljno iskanje osebe, ki je osumljena ali obsojena storitve kaznivega dejanja, uvajalec visokotveganega sistema UI za naknadno biometrično identifikacijo na daljavo predhodno ali brez nepotrebnega odlašanja in najpozneje v 48 urah zaprosi sodni organ ali upravni organ, katerega odločitev je zavezujoča in je predmet sodnega nadzora, za uporabo tega sistema, razen če se ta uporablja za prvotno identifikacijo morebitnega osumljenca na podlagi objektivnih in preverljivih dejstev, neposredno povezanih s kaznivim dejanjem. Vsaka uporaba mora biti omejena na tisto, kar je nujno potrebno za preiskavo določenega kaznivega dejanja.

Če se dovoljenje, zahtevano na podlagi prvega pododstavka, zavrne, je treba takoj prenehati uporabljati sistem za naknadno biometrično identifikacijo na daljavo, povezan z zahtevanim dovoljenjem, osebni podatki, povezani z uporabo visokotveganega sistema UI, za katerega je bilo zaproseno dovoljenje, pa se izbrišejo.

V nobenem primeru se tak visokotvegani sistem UI za naknadno biometrično identifikacijo na daljavo ne sme uporabljati za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj na neciljen način, brez kakršne koli povezave s kaznivim dejanjem, kazenskim postopkom, resnično in sedanjo ali resnično in predvidljivo grožnjo kaznivega dejanja ali iskanjem določene pogrešane osebe. Zagotovi se, da organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj izključno na podlagi izhodnih podatkov sistema za naknadno biometrično identifikacijo na daljavo ne smejo sprejeti nobene odločitve, ki bi imela negativen pravni učinek na osebo.

Ta odstavek ne posega v člen 9 Uredbe (EU) 2016/679 in člen 10 Direktive (EU) 2016/680 za obdelavo biometričnih podatkov.

Ne glede na namen ali uvajalca se vsaka uporaba takih visokotveganih sistemov UI dokumentira v ustrezni policijski datoteki ter se na zahtevo da na voljo ustreznemu organu za nadzor trga in nacionalnemu organu za varstvo podatkov, razen razkritja občutljivih operativnih podatkov, povezanih s preprečevanjem, odkrivanjem in preiskovanjem kaznivih dejanj. Ta pododstavek ne posega v pooblastila, ki so z Direktivo (EU) 2016/680 dodeljena nadzornim organom.

Uvajalci ustreznim organom za nadzor trga in nacionalnim organom za varstvo podatkov predložijo letna poročila o uporabi sistemov za naknadno biometrično identifikacijo na daljavo, razen razkritja občutljivih operativnih podatkov v zvezi z organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Poročila se lahko združijo tako, da zajemajo več kot eno uvedbo.

Države članice lahko v skladu s pravom Unije uvedejo strožje zakone o uporabi sistemov za naknadno biometrično identifikacijo na daljavo.

11. Brez poseganja v člen 50 te uredbe uvajalci visokotveganih sistemov UI iz Priloge III, ki sprejemajo odločitve ali pomagajo pri njihovem odločanju v zvezi s fizičnimi osebami, slednje obvestijo, da se zanje uporablja visokotvegani sistem UI. Za visokotvegane sisteme UI, ki se uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, se uporablja člen 13 Direktive (EU) 2016/680.

12. Uvajalci sodelujejo z ustreznimi pristojnimi organi pri vseh ukrepih, ki jih ti organi sprejmejo v zvezi z visokotveganim sistemom UI, da bi uresničili to uredbo.

Člen 27

Ocena učinka na temeljne pravice za visokotvegane sisteme UI

1. Pred uvedbo visoko tvegane sistema UI iz člena 6(2), razen visokotveganih sistemov UI, namenjenih uporabi na področju iz Priloge III, točka 2, uvajalci, ki so osebe javnega prava ali zasebni subjekti in zagotavljajo javne storitve, ter uvajalci visokotveganih sistemov UI iz Priloge III, točki 5(b) in (c), izvedejo oceno učinka, ki ga lahko povzroči uporaba takega sistema na temeljne pravice. V ta namen uvajalci izvedejo oceno, ki jo sestavljajo:

- (a) opis postopkov uvajalca, v katerih se bo visokotvegani sistem UI uporabljal v skladu s predvidenim namenom;
- (b) opis obdobja in pogostosti uporabe vsakega visokotvegane sistema UI;
- (c) kategorije fizičnih oseb in skupin, na katere bo verjetno vplivala njegova uporaba v specifičnem kontekstu;
- (d) posebna tveganja škode, ki bi lahko vplivala na kategorije fizičnih oseb ali skupine oseb, opredeljene na podlagi tega odstavka, točka (c), ob upoštevanju informacij, ki jih je ponudnik predložil na podlagi člena 13;
- (e) opis izvajanja ukrepov za človeški nadzor v skladu z navodili za uporabo;
- (f) ukrepi, ki jih je treba sprejeti, v primeru uresničitve teh tveganj, vključno z ureditvami za notranje upravljanje in pritožbene mehanizme.

2. Obveznost iz odstavka 1 se uporablja za prvo uporabo visokotvegane sistema UI. Uvajalec lahko v podobnih primerih uporabi predhodno izvedeno oceno učinka na temeljne pravice ali obstoječo oceno, ki jo je izvedel ponudnik. Če uvajalec med uporabo visokotvegane sistema UI meni, da se je kateri koli element iz odstavka 1 spremenil ali ni več posodobljen, sprejme potrebne ukrepe za posodobitev informacij.
3. Po izvedbi ocene iz odstavka 1 tega člena uvajalec obvesti organ za nadzor trga o svojih rezultatih, s predložitvijo izpolnjene predloge iz odstavka 5 tega člena. V primeru iz člena 46(1) so lahko uvajalci izvzeti iz obveznosti obveščanja.
4. Če je katera od obveznosti iz tega člena že izpolnjena na podlagi ocene učinka v zvezi z varstvom podatkov, izvedene na podlagi člena 35 Uredbe (EU) 2016/679 ali člena 27 Direktive (EU) 2016/680, ocena učinka na temeljne pravice iz odstavka 1 tega člena dopolnjuje to oceno učinka v zvezi z varstvom podatkov.
5. Urad za UI pripravi predlogo vprašalnika, tudi z avtomatiziranim orodjem, da bi se uvajalcem omogočilo, da na poenostavljen način izpolnijo svoje obveznosti iz tega člena.

ODDELEK 4

Priglasitveni organi in priglašeni organi

Člen 28

Priglasitveni organi

1. Vsaka država članica imenuje ali vzpostavi vsaj en priglasitveni organ, odgovoren za vzpostavitev in izvajanje potrebnih postopkov za ocenjevanje, imenovanje in priglasitev organov za ugotavljanje skladnosti ter za njihovo spremljanje. Takšni postopki se oblikujejo v sodelovanju med priglasitvenimi organi vseh držav članic.
2. Države članice lahko odločijo, da mora ocenjevanje in spremljanje iz odstavka 1 izvajati 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, in tudi nobenih storitev svetovanja na komercialni ali konkurenčni podlagi.
6. Priglasitveni organi zagotavljajo zaupnost pridobljenih informacij v skladu s členom 78.
7. Priglasitveni organi morajo imeti na voljo zadostno število strokovnega osebja za pravilno izvajanje svojih nalog. Pristojno osebje mora imeti potrebno strokovno znanje, kadar je ustrezno, za svojo funkcijo na področjih, kot so informacijske tehnologije, UI in pravo, vključno z nadzorom temeljnih pravic.

Člen 29

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 prigrasitev se priložijo opis dejavnosti ugotavljanja skladnosti, opis modula ali modulov za ugotavljanje skladnosti in opis vrst sistemov UI, za katere organ za ugotavljanje skladnosti trdi, da je zanje pristojen, ter morebitni certifikat o akreditaciji, ki ga izda nacionalni akreditacijski organ, ki potrjuje, da organ za ugotavljanje skladnosti izpolnjuje zahteve iz člena 31.

Dodajo se vsi veljavni dokumenti v zvezi z obstoječimi imenovanji priglašene organa vlagatelja na podlagi katere koli druge harmonizacijske zakonodaje Unije.

3. Kadar zadevni organ za ugotavljanje skladnosti ne more zagotoviti certifikata o akreditaciji, prigrasitvenemu organu predloži vsa dokumentarna dokazila, potrebna za preverjanje, priznavanje in redno spremljanje njegove skladnosti z zahtevami iz člena 31.

4. Za priglašene organe, imenovane na podlagi katere koli druge harmonizacijske zakonodaje Unije, se lahko vsi dokumenti in certifikati v zvezi s temi imenovanji uporabijo za podporo njihovem postopku imenovanja na podlagi te uredbe, če je to primerno. Priglašeni organ posodobi dokumentacijo iz odstavkov 2 in 3 tega člena, kadar pride do pomembnih sprememb, da bi organu, pristojnemu za priglašene organe, omogočil spremljanje in preverjanje stalne skladnosti z vsemi zahtevami, določenimi v členu 31.

Člen 30

Postopek prigrasitve

1. Prigrasitveni organi lahko prigrasijo samo tiste organe za ugotavljanje skladnosti, ki izpolnjujejo zahteve iz člena 31.

2. Prigrasitveni organi Komisiji in ostalim državam članicam prigrasijo vsak organ za ugotavljanje skladnosti iz odstavka 1 z uporabo elektronskega orodja za prigrasitev, ki ga je razvila in ga upravlja Komisija.

3. Prigrasitev iz odstavka 2 tega člena vključuje vse podrobnosti o dejavnostih ugotavljanja skladnosti, modulu ali modulih za ugotavljanje skladnosti in zadevnih vrstah sistemov UI ter ustrezno potrdilo o usposobljenosti. Kadar prigrasitev ne temelji na potrdilu o akreditaciji iz člena 29(2), prigrasitveni 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 redno spremljan in bo še naprej izpolnjeval zahteve iz člena 31.

4. Zadevni organ za ugotavljanje skladnosti lahko izvaja dejavnosti priglašene organa le, kadar Komisija ali druge države članice ne vložijo ugovora bodisi v dveh tednih od prigrasitve s strani prigrasitvenega organa, kadar ta vključuje potrdilo o akreditaciji iz člena 29(2), ali v dveh mesecih od prigrasitve s strani prigrasitvenega organa, kadar ta vključuje dokumentarna dokazila iz člena 29(3).

5. Kadar so vloženi ugovori, se Komisija nemudoma posvetuje z zadevnimi državami članicami in organom za ugotavljanje skladnosti. Glede na to, Komisija odloči, ali je dovoljenje upravičeno ali ne. Svojo odločitev naslovi na zadevno državo članico in ustrezeni organ za ugotavljanje skladnosti.

Člen 31

Zahteve v zvezi s priglašenimi organi

1. Priglašeni organ mora biti ustanovljen na podlagi nacionalnega prava države članice in imeti pravno osebnost.

2. Priglašeni organi morajo izpolnjevati organizacijske zahteve, zahteve glede upravljanja kakovosti, virov in procesov, potrebnih za izpolnjevanje njihovih nalog, ter ustrezne zahteve glede kibernetne varnosti.

3. Organizacijska struktura, dodelitev pristojnosti, poročanje in delovanje priglašenih organov morajo zagotavljati zaupanje v učinkovitost priglašenih organov in v rezultate dejavnosti ugotavljanja skladnosti, ki jih izvajajo.

4. Priglašeni organi morajo biti neodvisni od ponudnika visokotveganega sistema UI, v zvezi s katerim izvajajo dejavnosti ugotavljanja skladnosti. Neodvisni morajo biti tudi od vseh drugih operaterjev, ki imajo gospodarski interes pri ocenjevanem visoko tveganem sistemu UI, in od vseh konkurentov ponudnika. To ne izključuje uporabe ocenjenih visokotveganih sistemov UI, nujnih za delovanje organa za ugotavljanje skladnosti, ali uporabe teh sistemov v zasebne namene.
5. Niti organ za ugotavljanje skladnosti in njegovo najvišje vodstvo niti osebje, pristojno za opravljanje nalog ugotavljanja skladnosti, ne smejo neposredno sodelovati pri zasnovi, razvoju, trženju ali uporabi visokotveganih sistemov UI in tudi ne zastopati strani, ki sodelujejo pri teh dejavnostih. Ne smejo sodelovati pri nobeni dejavnosti, ki bi lahko vplivala na njihovo neodvisno presojo ali integriteto v zvezi z dejavnostmi ugotavljanja skladnosti, za katere so priglašeni. To zlasti velja za svetovalne storitve.
6. Priglašeni organi s svojo organizacijo in delovanjem zagotavljajo neodvisnost, objektivnost in nepristranskost pri izvajanju svojih dejavnosti. 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.
7. Priglašeni organi morajo imeti vzpostavljene dokumentirane postopke za zagotovitev, da njihovo osebje, odbori, odvisne družbe, podizvajalci, kateri koli povezan organ ali osebje zunanjih organov v skladu s členom 78 ohranjajo zaupnost informacij, pridobljenih med opravljanjem dejavnosti ugotavljanja skladnosti, razen kadar njihovo razkritje zahteva zakon. Njihovo osebje je zavezano varovanju poklicnih skrivnosti v zvezi z vsemi informacijami, pridobljenimi med izvajanjem nalog na podlagi te uredbe, razen v zvezi s priglasiitvenimi organi države članice, v kateri izvajajo svoje dejavnosti.
8. Priglašeni organi morajo imeti vzpostavljene postopke za izvajanje dejavnosti, pri katerih se ustrezno upoštevajo velikost ponudnika, sektor, v katerem deluje, njegova struktura in stopnja zahtevnosti zadevnega sistema UI.
9. Priglašeni organi sklenejo ustrezno zavarovanje odgovornosti za svoje dejavnosti ugotavljanja skladnosti, razen če odgovornost prevzame država članica, v kateri imajo sedež, v skladu z nacionalnim pravom ali če je ta država članica sama neposredno pristojna za ugotavljanje skladnosti.
10. Priglašeni organi morajo biti sposobni izvajati vse naloge na podlagi te uredbe z najvišjo stopnjo profesionalne integritete in potrebno usposobljenostjo na določenem področju, ne glede na to, ali navedene naloge izvajajo priglašeni organi sami ali se izvajajo v njihovem imenu in pod njihovo odgovornostjo.
11. Priglašeni organi morajo imeti zadostne notranje kompetence, da lahko učinkovito ocenijo naloge, ki jih opravljajo zunanje stranke v njihovem imenu. Stalno morajo imeti na voljo dovolj upravnega, tehničnega, pravnega in znanstvenega osebja, ki ima izkušnje in znanje v zvezi z ustreznimi vrstami sistemov UI, podatki in računalniško obdelavo podatkov ter v zvezi z zahtevami iz oddelka 2.
12. Priglašeni organi sodelujejo v usklajevalnih dejavnostih iz člena 38. Sodelujejo tudi neposredno v evropskih organizacijah za standardizacijo ali so v njih zastopani oziroma zagotavljajo, da so seznanjeni z ustreznimi standardi in na tekočem z njimi.

Člen 32

Domneva o skladnosti z zahtevami v zvezi s priglašnimi 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 31, kolikor so te zajete v veljavnih harmoniziranih standardih.

Člen 33**Odkvisne družbe priglášeni organov in podizvajanje**

1. Kadar priglášeni organ določene naloge, povezane z ugotavljanjem skladnosti, odda v izvajanje podizvajalcu ali jih prenese na odkvisno družbo, zagotovi, da podizvajalec oziroma odkvisna družba izpolnjuje zahteve iz člena 31, ter o tem obvesti prigrlišitveni organ.
2. Priglášeni organi so v celoti odgovorni za naloge, ki jih izvajajo kateri koli podizvajalci ali odkvisne družbe.
3. Dejavnosti se lahko prenesejo na podizvajalca ali odkvisno družbo samo, če ponudnik s tem soglaša. Priglášeni organi objavijo seznam svojih podizvajalcev.
4. Zadevni dokumenti v zvezi z ocenjevanjem usposobljenosti podizvajalca ali odkvisne družbe in delom, ki ga izvaja na podlagi te uredbe, so na voljo prigrlišitvenemu organu pet let od datuma zaključka podizvajanja.

Člen 34**Operativne obveznosti priglášeni organov**

1. Priglášeni organi preverijo skladnost visokotveganih sistemov UI v skladu s postopki ugotavljanja skladnosti iz člena 43.
2. Priglášeni organi se pri opravljanju svojih dejavnosti izogibajo ustvarjanju nepotrebnih bremen za ponudnike ter ustrezno upoštevajo velikost ponudnika, sektor, v katerem deluje, njegovo strukturo in stopnjo kompleksnosti zadevnega visokotvegane sistema UI, zlasti zato, da bi čim bolj zmanjšali upravna bremena in stroške izpolnjevanja obveznosti za mikro in mala podjetja v smislu Priporočila 2003/361/ES. Vendar upoštevajo stopnjo rigoroznosti in raven zaštite, ki sta potrebni za skladnost visokotvegane sistema UI z zahtevami te uredbe.
3. Priglášeni organi dajo prigrlišitvenemu organu iz člena 28 na voljo vso zadevno dokumentacijo – vključno z dokumentacijo ponudnikov –, ki mu jo na zahtevo tudi predložijo, da temu organu omogočijo izvajanje dejavnosti ocenjevanja, imenovanja, prigrlišitve in spremljanja ter da se olajša ocenjevanje, opisano v tem oddelku.

Člen 35**Identifikacijske številke in seznam priglášeni organov**

1. Komisija vsakemu prigrlišenemu organu dodeli enotno identifikacijsko številko, tudi kadar je organ priglášeni na podlagi več kot enega akta Unije.
2. Komisija objavi seznam organov, priglášeni na podlagi te uredbe, vključno z njihovimi identifikacijskimi številkami in dejavnostmi, za katere so bili priglášeni. Komisija skrbi za posodabljanje seznama.

Člen 36**Spremembe prigrlišitev**

1. Prigrlišitveni organ uradno obvesti Komisijo in druge države članice o vseh pomembnih spremembah prigrlišitve priglášene organa z uporabo elektronskega orodja za prigrlišitev iz člena 30(2).
2. Postopki iz členov 29 in 30 se uporabljajo za razširitev področja uporabe prigrlišitve.

Za druge spremembe prigrlišitve, razen za razširitev njenega področja uporabe, se uporabljajo postopki iz odstavkov 3 do 9.

3. Kadar priglašeni organ sklene, da bo prenehal izvajati dejavnosti za ugotavljanje skladnosti, o tem obvesti priglasitveni organ in zadevne ponudnike čim prej, v primeru načrtovanega prenehanja pa vsaj eno leto pred prenehanjem izvajanja svojih dejavnosti. Certifikati priglašenega organa lahko ostanejo veljavni devet mesecev po prenehanju njegovih dejavnosti, pod pogojem da je drug priglašeni organ pisno potrdil, da bo prevzel odgovornost za visokotvegane sisteme UI, na katere se ti certifikati nanašajo. Slednji priglašeni organ opravi celovito oceno zadevnih visokotveganih sistemov UI do konca tega devetmesečnega obdobja, preden izda nove certifikate za te sisteme. Kadar priglašeni organ preneha opravljati svojo dejavnost, priglasitveni organ imenovanje umakne.

4. Kadar ima priglasitveni organ zadosten razlog za domnevo, da priglašeni organ ne izpolnjuje več zahtev iz člena 31 ali da ne izpolnjuje svojih obveznosti, zadevo brez odlašanja raziše z največjo skrbnostjo. V tem okviru obvesti zadevni priglašeni organ o vloženih ugovorih in mu omogoči, da izrazi svoja stališča. Če priglasitveni organ ugotovi, da priglašeni organ ne izpolnjuje več zahtev iz člena 31 ali ne izpolnjuje svojih obveznosti, omeji, začasno prekliče ali umakne imenovanje, odvisno od resnosti neizpolnjevanja navedenih zahtev ali neizpolnjevanja navedenih obveznosti. O tem nemudoma obvesti Komisijo in druge države članice.

5. Kadar se imenovanje priglašenega organa začasno prekliče, omeji oziroma v celoti ali delno umakne, priglašeni organ o tem obvesti zadevne ponudnike v desetih dneh.

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

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

- (a) oceni vpliv na certifikate, ki jih je izdal priglašeni organ;
- (b) Komisiji in drugim državam članicam v treh mesecih od uradnega obvestila o spremembah imenovanja predloži poročilo o svojih ugotovitvah;
- (c) od priglašenega organa zahteva, da v razumnem časovnem roku, ki ga določi organ, začasno prekliče ali umakne vse neupravičeno izdane certifikate, da se zagotovi kontinuirana skladnost visokotveganih sistemov UI na trgu;
- (d) Komisijo in države članice obvesti o certifikatih, katerih začasni preklic ali umik je zahteval;
- (e) pristojnim nacionalnim organom države članice, v kateri ima ponudnik registriran sedež poslovanja, zagotovi vse ustrezne informacije o certifikatih, katerih začasni preklic ali umik je zahteval; ta organ sprejme ustrezne ukrepe za preprečitev morebitnega tveganja za zdravje, varnost ali temeljne pravice, kadar je to potrebno.

8. Razen neupravičeno izdanih certifikatov ostanejo certifikati, kadar je bilo imenovanje začasno preklicano ali omejeno, veljavni v naslednjih okoliščinah:

- (a) priglasitveni organ je v enem mesecu od začasnega preklica ali omejitve potrdil, da v zvezi s certifikati, za katere velja začasni preklic ali omejitev, ni nobenega tveganja za zdravje, varnost ali temeljne pravice, ter določil časovni potek za ukrepe, potrebne za odpravo začasnega preklica ali omejitve, ali
- (b) priglasitveni organ je potrdil, da v obdobju začasnega preklica ali omejitve ne bo izdan, spremenjen ali ponovno izdan noben certifikat, povezan z začasnim preklicem, hkrati pa navedel, ali je priglašeni organ v obdobju začasnega preklica ali omejitve še vedno sposoben spremljati veljavne izdane certifikate in zanje odgovarjati; če priglasitveni organ ugotovi, da priglašeni organ ni sposoben zagotavljati podpore za veljavne izdane certifikate, ponudnik sistema, na katerega se nanaša certifikat, pristojnim nacionalnim organom države članice, v kateri ima registrirani sedež poslovanja, v treh mesecih od začasnega preklica ali omejitve pisno potrdi, da drug kvalificiran priglašeni organ začasno prevzema naloge priglašenega organa v smislu spremljanja certifikatov in odgovarjanja zanje v obdobju začasnega preklica ali omejitve.

9. Razen v primeru neupravičeno izdanih certifikatov in kadar je bilo imenovanje umaknjeno, ostanejo certifikati v naslednjih okoliščinah veljavni še devet mesecev:

- (a) pristojni nacionalni organ države članice, v kateri ima ponudnik visoko tveganega sistema UI, na katerega se nanaša certifikat, registrirani sedež poslovanja, je potrdil, da v povezavi z zadevnimi visokotveganimi sistemi UI ni tveganja za zdravje, varnost ali temeljne pravice, ter
- (b) drug priglašeni organ je pisno potrdil, da bo takoj prevzel odgovornost za te sisteme UI in v 12 mesecih od umika imenovanja zaključi njihovo ocenjevanje.

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

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

Člen 37

Izpodbijanje usposobljenosti priglašениh organov

1. Komisija po potrebi razišče vse primere, v katerih obstajajo razlogi za dvom v usposobljenost priglašene organa oziroma ali priglašeni organ še vedno izpolnjuje zahteve iz člena 31 in svoje veljavne obveznosti.
2. Priglasitveni organ Komisiji na zahtevo predloži vse ustrezne informacije v zvezi s priglasitvijo ali vzdrževanjem usposobljenosti zadevnega priglašene organa.
3. Komisija zagotovi, da se vse občutljive informacije, ki jih pridobi med preiskavami na podlagi tega člena, obravnavajo zaupno v skladu s členom 78.
4. Kadar Komisija ugotovi, da priglašeni organ ne izpolnjuje ali ne izpolnjuje več zahtev za priglasitev, o tem ustrezno obvesti državo članico priglasiteljico in od nje zahteva, da sprejme potrebne popravne ukrepe, po potrebi vključno z začasnim preklicem ali umikom priglasitve. Kadar država članica ne sprejme potrebnih popravnih ukrepov, lahko Komisija z izvedbenim aktom začasno prekliche, omeji ali umakne imenovanje. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 98(2).

Člen 38

Usklajevanje priglašениh organov

1. Komisija zagotovi, da se v zvezi z visokotveganimi sistemi UI vzpostavi ustrezno usklajevanje in sodelovanje med priglasenimi organi, dejavnimi v postopkih ugotavljanja skladnosti na podlagi te uredbe, ter da se to usklajevanje in sodelovanje pravilno izvajata v obliki sektorske skupine priglasenih organov.
2. Vsak priglasitveni organ zagotovi, da organi, ki jih priklasi, neposredno ali prek imenovanih predstavnikov sodelujejo pri delu skupine iz odstavka 1.
3. Komisija omogoči izmenjavo znanja in primerov najboljših praks med priglasitvenimi organi.

Člen 39

Organi za ugotavljanje skladnosti iz tretjih držav

Organi za ugotavljanje skladnosti, ustanovljeni na podlagi prava tretje države, s katero je Unija sklenila sporazum, so lahko pooblaščenici za izvajanje dejavnosti priglasišenih organov na podlagi te uredbe, če izpolnjujejo zahteve iz člena 31 ali zagotavljajo enakovredno raven izpolnjevanja zahtev.

ODDELEK 5

Standardi, ugotavljanje skladnosti, certifikati, registracija

Člen 40

Harmonizirani standardi in standardizacijski dokumenti

1. Za visokotvegane sisteme UI ali modele UI za splošne namene, ki so skladni s harmoniziranimi standardi ali njihovimi deli, katerih sklici so bili objavljeni v *Uradnem listu Evropske unije* v skladu z Uredbo (EU) št. 1025/2012, se domneva, da so skladni z zahtevami iz oddelka 2 tega poglavja ali, kot je ustrezno, z obveznostmi iz poglavja V, oddelka 2 in 3, te uredbe, kolikor ti standardi zajemajo te zahteve ali obveznosti.

2. Komisija v skladu s členom 10 Uredbe (EU) št. 1025/2012 brez nepotrebnega odlašanja izda zahteve za standardizacijo, ki zajemajo vse zahteve iz oddelka 2 tega poglavja in, kot je ustrezno, zahteve za standardizacijo, ki zajemajo obveznosti iz poglavja V, oddelka 2 in 3, te uredbe. V zahtevi za standardizacijo se zahtevajo tudi dokumenti v zvezi s postopki poročanja in dokumentiranja za izboljšanje učinkovitosti virov sistemov UI, kot je zmanjšanje porabe energije in drugih virov visokotvegane sistema UI v njegovem življenjskem ciklu, ter dokumenti v zvezi z energijsko učinkovitim razvojem modelov UI za splošne namene. Komisija se pri pripravi zahteve za standardizacijo posvetuje z Odborom in ustreznimi deležniki, vključno s svetovalnim forumom.

Komisija pri izdaji zahteve za standardizacijo evropskim organizacijam za standardizacijo določi, da morajo biti standardi jasni, skladni, tudi s standardi, razvitimi v različnih sektorjih, za proizvode, za katere velja obstoječa harmonizacijska zakonodaja Unije iz Priloge I, in namenjeni temu, da se zagotovi, da visokotvegani sistemi UI ali modeli UI za splošne namene, ki so dani na trg ali v uporabo v Uniji, izpolnjujejo ustrezne zahteve ali obveznosti iz te uredbe.

Komisija od evropskih organizacij za standardizacijo zahteva, da v skladu s členom 24 Uredbe (EU) št. 1025/2012 predložijo dokaze o svojih najboljših prizadevanjih za izpolnitev ciljev iz prvega in drugega pododstavka tega odstavka.

3. Udeleženci v postopku standardizacije si prizadevajo spodbujati naložbe in inovacije na področju UI, tudi s krepitvijo pravne varnosti, ter konkurenčnost in rast trga Unije, prispevati k izboljšanju globalnega sodelovanja na področju standardizacije ob upoštevanju obstoječih mednarodnih standardov na področju UI, ki so skladni z vrednotami, temeljnimi pravicami in interesi Unije, ter krepiti večdeležniško upravljanje, pri čemer zagotavljajo uravnoteženo zastopanost interesov in učinkovito sodelovanje vseh ustreznih deležnikov v skladu s členi 5, 6 in 7 Uredbe (EU) št. 1025/2012.

Člen 41

Skupne specifikacije

1. Komisija lahko sprejme izvedbene akte o določitvi skupnih specifikacij za zahteve iz oddelka 2 tega poglavja ali, kot je ustrezno, za obveznosti iz oddelkov 2 in 3 poglavja V, kadar so izpolnjeni naslednji pogoji:

(a) Komisija je na podlagi člena 10(1) Uredbe (EU) št. 1025/2012 zahtevala, da ena ali več evropskih organizacij za standardizacijo pripravi osnutek harmoniziranega standarda za zahteve iz oddelka 2 tega poglavja ali, kot je ustrezno, za obveznosti iz oddelkov 2 in 3 poglavja V, in:

(i) zahteve ni sprejela nobena evropska organizacija za standardizacijo ali

(ii) harmonizirani standardi, ki se nanašajo na to zahtevo, niso bili predloženi v roku, določenem v skladu s členom 10 (1) Uredbe (EU) št. 1025/2012, ali

(iii) v ustreznih harmoniziranih standardih so nezadostno obravnavani pomisleki glede temeljnih pravic ali

(iv) harmonizirani standardi niso skladni z zahtevo ter

(b) v *Uradnem listu Evropske unije* v skladu z Uredbo (EU) št. 1025/2012 ni objavljen sklic na harmonizirane standarde, ki zajemajo zahteve iz oddelka 2 tega poglavja ali, kot je ustrezno, obveznosti iz oddelkov 2 in 3 poglavja V, in objava takega sklica se v razumnem roku tudi ne pričakuje.

Pri pripravi skupnih specifikacij se Komisija posvetuje s svetovalnim forumom iz člena 67.

Izvedbeni akti iz prvega pododstavka tega odstavka se sprejmejo v skladu s postopkom pregleda iz člena 98(2).

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

3. Za visokotvegane sisteme UI ali modele UI za splošne namene, ki so v skladu s skupnimi specifikacijami iz odstavka 1 ali deli navedenih specifikacij, se domneva, da so skladni z zahtevami iz oddelka 2 tega poglavja ali, kot je ustrezno, izpolnjujejo zahteve iz oddelkov 2 in 3 poglavja V, kolikor so te zajete v teh skupnih specifikacijah ali teh obveznostih.

4. Kadar evropska organizacija za standardizacijo sprejme harmonizirani standard in ga predloži Komisiji, da se sklic nanj objavi v *Uradnem listu Evropske unije*, Komisija harmonizirani standard oceni v skladu z Uredbo (EU) št. 1025/2012. Ko se sklic na harmonizirani standard objavi v *Uradnem listu Evropske unije*, Komisija razveljavi izvedbene akte iz odstavka 1 ali njihove dele, ki zajemajo zahteve, enake zahtevam iz oddelka 2 tega poglavja ali, kot je ustrezno, iste obveznosti iz oddelkov 2 in 3 poglavja V.

5. Kadar ponudniki visokotveganih sistemov UI ali modelov UI za splošne namene ne izpolnjujejo skupnih specifikacij iz odstavka 1, ustrezno utemeljijo, da so sprejeli tehnične rešitve, ki izpolnjujejo zahteve iz oddelka 2 tega poglavja ali, kot je ustrezno, izpolnjujejo obveznosti iz oddelkov 2 in 3 poglavja V v tolikšni meri, da so jim vsaj enakovredne.

6. Kadar država članica meni, da skupna specifikacija ne izpolnjuje v celoti zahtev iz oddelka 2 ali, kot je ustrezno, ne izpolnjuje obveznosti iz oddelkov 2 in 3 poglavja V, o tem s podrobno obrazložitvijo obvesti Komisijo. Komisija te informacije oceni in po potrebi spremeni izvedbeni akt o določitvi zadevne skupne specifikacije.

Člen 42

Domneva o skladnosti z nekaterimi zahtevami

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

2. Za visokotvegane sisteme UI, ki so prejeli potrdilo ali za katere je bila izdana izjava o skladnosti v okviru sheme za kibernetsko varnost na podlagi Uredbe (EU) 2019/881, sklici na katero so bili objavljeni v *Uradnem listu Evropske unije*, se domneva, da izpolnjujejo zahteve za kibernetsko varnost iz člena 15 te uredbe, kolikor so te zahteve zajete v certifikatu o kibernetski varnosti ali izjavi o skladnosti ali v njunih delih.

Člen 43

Ugotavljanje skladnosti

1. Za visokotvegane sisteme UI iz Priloge III, točka 1, pri katerih je ponudnik pri dokazovanju skladnosti visokotveganega sistema UI z zahtevami iz oddelka 2 uporabil harmonizirane standarde iz člena 40 ali, kadar je to primerno, skupne specifikacije iz člena 41, ponudnik izbere enega od naslednjih postopkov za ugotavljanje skladnosti na podlagi:

- (a) notranjega nadzora iz Priloge VI ali
- (b) ocenjevanja sistema upravljanja kakovosti in ocenjevanja tehnične dokumentacije s sodelovanjem priglasičenega organa iz Priloge VII.

Pri dokazovanju skladnosti visokotveganega sistema UI z zahtevami iz oddelka 2 ponudnik opravi postopek ugotavljanja skladnosti iz Priloge VII, kadar:

- (a) harmonizirani standardi iz člena 40 ne obstajajo in skupne specifikacije iz člena 41 niso na voljo;
- (b) ponudnik ni uporabil harmoniziranega standarda ali ga je uporabil le delno;
- (c) skupne specifikacije iz točke (a) obstajajo, vendar jih ponudnik ni uporabil;
- (d) je bil eden ali več harmoniziranih standardov iz točke (a) objavljen z omejitvijo in samo za tisti del standarda, ki je bil omejen.

Za namene postopka ugotavljanja skladnosti iz Priloge VII lahko ponudnik izbere katerega koli od priglasičenih organov. Kadar pa naj bi visokotvegani sistem UI dali v uporabo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organi, pristojni za priseljevanje, ali azilni organi ali institucije, organi, uradi in agencije Unije, je priglasičen organ organ za nadzor trga iz člena 74(8) ali (9), kot je ustrezno.

2. Za visokotvegane sisteme UI iz Priloge III, točke 2 do 8, ponudniki upoštevajo postopek ugotavljanja skladnosti na podlagi notranje kontrole iz Priloge VI, ki ne predvideva sodelovanja priglasičenega organa.

3. Za visokotvegane sisteme UI, zajete v harmonizacijski zakonodaji Unije iz Priloge I, oddelek A, ponudnik upošteva ustrezeni postopek ugotavljanja skladnosti, kot se zahteva v navedenih pravnih aktih. Za te visokotvegane sisteme UI se uporabljajo zahteve iz oddelka 2 tega poglavja, ki so del te ocene. Uporablja se tudi Priloga VII, točke 4.3, 4.4, 4.5 in peti odstavek točke 4.6.

Za namene te ocene so priglasičeni organi, ki so priglasičeni na podlagi teh pravnih aktov, upravičeni nadzorovati skladnost visokotveganega sistema UI z zahtevami iz oddelka 2, če je bila skladnost teh priglasičenih organov z zahtevami iz člena 31(4), (5), (10) in (11) ocenjena v okviru postopka priglasičitve na podlagi teh pravnih aktov.

Kadar pravni akt iz Priloge I, oddelek A, proizvajalcu proizvoda omogoča, da se odloči za izvzetje iz ugotavljanja skladnosti s strani tretjih oseb, 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 vse zahteve iz oddelka 2 tega poglavja.

4. Pri visokotveganem sistemu UI, pri katerih je bil že opravljen postopek ugotavljanja skladnosti, se v primeru bistvene spremembe opravi nov postopek ugotavljanja skladnosti, ne glede na to, ali je spremenjeni sistem namenjen nadaljnji distribuciji ali ga še naprej uporablja sedanji uvajalec.

Za visokotvegane sisteme UI, ki se po dajanju na trg ali v uporabo še naprej učijo, spremembe visokotveganega sistema UI in njegove zmogljivosti, ki jih je ponudnik vnaprej določil ob začetnem ugotavljanju skladnosti in so del informacij iz tehnične dokumentacije iz Priloge IV, točka 2(f), ne pomenijo bistvene spremembe.

5. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97, da zaradi tehničnega napredka spremeni s posodobitvijo prilogi VI in VII.

6. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97 za spremembo odstavkov 1 in 2 tega člena, da se za visokotvegane sisteme UI iz Priloge III, točke 2 do 8, v celoti ali deloma uvede postopek ugotavljanja skladnosti iz Priloge VII. Komisija take delegirane akte sprejme ob upoštevanju učinkovitosti postopka ugotavljanja skladnosti na podlagi notranje kontrole iz Priloge VI pri preprečevanju ali čim večjem zmanjševanju tveganj za zdravje in varnost ter varstvo temeljnih pravic, ki jih predstavljajo taki sistemi, ter razpoložljivosti ustreznih zmogljivosti in virov med priglasiženimi organi.

Člen 44

Certifikati

1. Certifikati, ki jih izdajo priglasiženi organi v skladu s Prilogo VII, so sestavljeni v jeziku, ki ga ustrezni organi v državi članici, v kateri ima priglasižen organ sedež, zlahka razumejo.
2. Certifikati so veljavni toliko časa, kolikor je navedeno, a ne več kot pet let za sisteme UI iz Priloge I in štiri leta za sisteme UI iz Priloge III. Na zahtevo ponudnika se lahko veljavnost certifikata na podlagi ponovne ocene v skladu z veljavnimi postopki za ugotavljanje skladnosti podaljša za nadaljnja obdobja, ki ne presegajo pet let za sisteme UI iz Priloge I in štirih let za sisteme UI iz Priloge III. Vsako dopolnilo k certifikatu ostane veljavno, če je veljaven certifikat, ki ga to dopolnjuje.
3. Kadar priglasižen organ ugotovi, da sistem UI ne izpolnjuje več zahtev iz oddelka 2, ob upoštevanju načela sorazmernosti začasno prekliče ali umakne izdan certifikat 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 je določil priglasižen organ. Priglasižen organ svojo odločitev obrazloži.

Zoper odločitve priglasiženih organov, tudi o izdanih certifikatih o skladnosti, je na voljo pritožbeni postopek.

Člen 45

Obveznosti obveščanja za priglasižene organe

1. Priglasiženi organi obvestijo priglasitveni organ:
 - (a) o vsakem certifikatu Unije o oceni tehnične dokumentacije, vsakem dodatku k tem certifikatom in vsaki odobritvi sistema upravljanja kakovosti, ki se izdajo v skladu z zahtevami iz Priloge VII;
 - (b) o vsaki zavrnitvi, omejitvi, začasnem preklicu ali umiku certifikata Unije o oceni tehnične dokumentacije ali odobritve sistema upravljanja kakovosti, ki se izda v skladu z zahtevami iz Priloge VII;
 - (c) o vsaki okoliščini, ki vpliva na obseg ali pogoje za priglasiitev;
 - (d) o vsaki zahtevi za informacije, ki so jo prejeli od organov za nadzor trga, v zvezi z dejavnostmi ugotavljanja skladnosti;
 - (e) na zahtevo o dejavnostih ugotavljanja skladnosti, izvedenih v okviru njihove priglasitve, in vsaki drugi izvedeni dejavnosti, vključno s čezmejnimi dejavnostmi in sklepanjem pogodb s podizvajalci.
2. Vsak priglasižen organ obvesti druge priglasižene organe:
 - (a) o odobritvah sistema upravljanja kakovosti, ki jih je zavrnil, začasno preklical ali umaknil, ter na zahtevo o odobritvah sistema upravljanja kakovosti, ki jih je izdal;
 - (b) o certifikatih Unije o oceni tehnične dokumentacije ali njihovih dodatkih, ki jih je zavrnil, začasno preklical, umaknil ali drugače omejil, ter na zahtevo o certifikatih in/ali njihovih dodatkih, ki jih je izdal.

3. Vsak priglašeni organ drugim priglašenim organom, ki izvajajo podobne dejavnosti ugotavljanja skladnosti za iste vrste sistemov UI, predloži ustrezne informacije o vprašanih v zvezi z negativnimi rezultati ugotavljanja skladnosti, na zahtevo pa tudi v zvezi s pozitivnimi.
4. Priglasitveni organi zagotavljajo zaupnost pridobljenih informacij v skladu s členom 78.

Člen 46

Odstopanje od postopka ugotavljanja skladnosti

1. Z odstopanjem od člena 43 in na podlagi ustrezno utemeljene zahteve lahko kateri koli organ za nadzor trga dovoli dajanje posebnih visokotveganih sistemov UI na trg ali v uporabo 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 omejeno obdobje, dokler se izvajajo potrebni postopki ugotavljanja skladnosti, ob upoštevanju izjemnih razlogov, ki upravičujejo odstopanje. Ti postopki se zaključijo brez nepotrebnega odlašanja.
2. 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 določen visokotvegani sistem UI v uporabo brez dovoljenja iz odstavka 1, če se za tako dovoljenje brez nepotrebne odlašanja zaprosi med uporabo ali po njej. Če se dovoljenje iz odstavka 1 zavrne, se uporaba visokotvegane sistema UI takoj ustavi, vsi rezultati in izhodni podatki, ki izhajajo iz take uporabe, pa se takoj zavržejo.
3. Dovoljenje iz odstavka 1 se izda le, če organ za nadzor trga ugotovi, da visokotvegani sistem UI izpolnjuje zahteve iz oddelka 2. Organ za nadzor trga obvesti Komisijo in druge države članice o vseh dovoljenjih, izdanih na podlagi odstavkov 1 in 2. Ta obveznost ne zajema občutljivih operativnih podatkov v zvezi z dejavnostmi organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj.
4. Kadar v 15 koledarskih dneh po prejemu informacij iz odstavka 3 država članica ali Komisija ne poda nobenega ugovora glede dovoljenja, ki ga je izdal organ za nadzor trga države članice v skladu z odstavkom 1, se šteje, da je dovoljenje upravičeno.
5. Kadar v 15 koledarskih dneh po prejemu obvestila iz odstavka 3 država članica poda ugovore zoper dovoljenje, ki ga je izdal organ za nadzor trga druge države članice, ali kadar Komisija meni, da je dovoljenje v nasprotju s pravom Unije ali da je sklep držav članic glede skladnosti sistema iz odstavka 3 neutemeljen, se Komisija brez odlašanja posvetuje z zadevno državo članico. Z zadevnimi operaterji se posvetuje in ti imajo možnost, da predstavijo svoja stališča. Glede na to Komisija odloči, ali je dovoljenje upravičeno. Komisija svojo odločitev sporoči zadevnim državam članicam in ustreznim operaterjem.
6. Kadar Komisija meni, da je dovoljenje neupravičeno, ga organ za nadzor trga zadevne države članice umakne.
7. Za visokotvegane sisteme UI, povezane s proizvodi, zajetimi v harmonizacijski zakonodaji Unije iz Priloge I, oddelek A, se uporabljajo samo odstopanja od ugotavljanja skladnosti, določena v navedeni harmonizacijski zakonodaji Unije.

Člen 47

EU izjava o skladnosti

1. Ponudnik za vsak visokotvegani sistem UI sestavi strojno berljivo, fizično ali elektronsko podpisano pisno EU izjavo o skladnosti in jo hrani za potrebe pristojnih nacionalnih organov ter jim jo daje na voljo še 10 let po tem, ko je bil visokotvegani sistem UI dan na trg ali v uporabo. V EU izjavi o skladnosti se opredeli, za kateri visokotvegani sistem UI je bila sestavljena. Na zahtevo se ustreznim pristojnim nacionalnim organom predloži izvod EU izjave o skladnosti.

2. V EU izjavi o skladnosti se navede, da zadevni visokotvegani sistem UI izpolnjuje zahteve iz oddelka 2. EU izjava o skladnosti vsebuje informacije iz Priloge V in se prevede v jezik, ki ga pristojni nacionalni organi držav članic, v katerih je visokotvegani sistem UI dan na trg ali je omogočena dostopnost do njega, zlahka razumejo.

3. Kadar za visokotvegane sisteme UI velja druga harmonizacijska zakonodaja Unije, v skladu s katero se zahteva tudi EU izjava o skladnosti, se pripravi enotna EU izjava o skladnosti za pravo Unije, ki se uporablja za visokotvegani sistem UI. Ta izjava vsebuje vse informacije, s katerimi se ugotovi, na katero harmonizacijsko zakonodajo Unije se izjava nanaša.

4. S pripravo EU izjave o skladnosti ponudnik prevzame odgovornost za skladnost z zahtevami iz oddelka 2. Ponudnik EU izjavo o skladnosti, če je to primerno, posodablja.

5. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97, da se spremeni Priloga V, s posodobitvijo vsebine EU izjave o skladnosti iz navedene priloge, da se uvedejo elementi, potrebni zaradi tehničnega napredka.

Člen 48

Oznaka CE

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

2. Za visokotvegane sisteme UI, ki se zagotavljajo digitalno, se digitalna oznaka CE uporablja le, če je do nje mogoče enostavno dostopati prek vmesnika, prek katerega se dostopa do tega sistema, ali prek lahko dostopne strojno berljive kode ali drugega elektronskega sredstva.

3. Oznaka CE se vidno, čitljivo in neizbrisno namesti na visokotvegane sisteme UI. Kadar to ni mogoče ali ni upravičeno zaradi značilnosti visokotveganega sistema UI, se oznaka namesti bodisi na embalažo ali na priloženo dokumentacijo.

4. Kadar je to primerno, oznaki CE sledi identifikacijska številka priglašene organa, odgovornega za postopke ugotavljanja skladnosti iz člena 43. Identifikacijsko številko priglašene organa pritrdi organ sam ali pa jo na podlagi njegovih navodil pritrdi ponudnik ali njegov pooblaščen zastopnik. Identifikacijska številka se navede tudi v promocijskem gradivu, v katerem je omenjeno, da visokotvegani sistem UI izpolnjuje zahteve za oznako CE.

5. Kadar visokotvegane sisteme UI ureja drugo pravo Unije, ki prav tako določa namestitvev oznake CE, se na tej oznaki navede, da visokotvegani sistem UI izpolnjuje tudi zahteve tega drugega prava.

Člen 49

Registracija

1. Pred dajanjem visokotveganega sistema UI iz Priloge III, z izjemo visokotveganih sistemov UI iz Priloge III, točka 2, na trg ali v uporabo ponudnik ali, kadar je to ustrezno, pooblaščen zastopnik sebe in svoj sistem registrira v podatkovni zbirki EU iz člena 71.

2. Pred dajanjem sistema UI, za katerega je ponudnik ugotovil, da v skladu s členom 6(3) ne šteje za visokotvegane, na trg ali v uporabo ponudnik ali, kadar je to ustrezno, pooblaščen zastopnik sebe in navedeni sistem registrira v podatkovni zbirki EU iz člena 71.

3. Pred dajanjem v uporabo ali pred uporabo visokotveganega sistema UI iz Priloge III, z izjemo visokotveganih sistemov UI iz Priloge III, točka 2, se uvajalci, ki so javni organi, institucije, organi, uradi ali agencije Unije ali osebe, ki delujejo v njihovem imenu, registrirajo, izberejo sistem in registrirajo njegovo uporabo v podatkovni zbirki EU iz člena 71.

4. Za visokotvegane sisteme UI iz Priloge III, točke 1, 6 in 7, na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, migracij, azila in upravljanja nadzora meja se registracija iz odstavkov 1, 2 in 3 tega člena izvede v varnem nejavnem delu podatkovne zbirke EU iz člena 71 in vključuje le naslednje informacije, kot je ustrezno, iz:

(a) Priloge VIII, oddelek A, točke 1 do 10, razen točk 6, 8 in 9;

(b) Priloge VIII, oddelek B, točke 1 do 5 ter točki 8 in 9;

(c) Priloge VIII, oddelek C, točke 1 do 3;

(d) Priloge IX, točke 1, 2, 3 in 5.

Dostop do ustreznih omejenih delov podatkovne zbirke EU iz prvega pododstavka tega odstavka imajo samo Komisija in nacionalni organi iz člena 74(8).

5. Visokotvegani sistemi UI iz Priloge III, točka 2, se registrirajo na nacionalni ravni.

POGLAVJE IV

OBVEZNOSTI PONUDNIKOV IN UVAJALCEV NEKATERIH SISTEMOV UI GLEDE PREGLEDNOSTI

Člen 50

Obveznosti ponudnikov in uvajalcev nekaterih sistemov UI glede preglednosti

1. Ponudniki zagotovijo, da so sistemi UI, namenjeni neposredni interakciji s fizičnimi osebami, zasnovani in razviti tako, da so zadevne fizične osebe obveščene, da so v interakciji s sistemom UI, razen če je to očitno z vidika razmeroma dobro obveščene, pozorne in preudarne fizične osebe ob upoštevanju okoliščin in konteksta uporabe. Ta obveznost se ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine tretjih oseb ne uporablja za sisteme UI, ki so z zakonom odobreni za odkrivanje, preprečevanje, preiskovanje ali pregon kaznivih dejanj, razen če so ti sistemi na voljo javnosti za prijavo kaznivega dejanja.

2. Ponudniki sistemov UI, vključno s sistemi UI za splošne namene, ki ustvarjajo sintetično zvočno, slikovno, video ali besedilno vsebino, zagotovijo, da so izhodni podatki sistema UI označeni v strojno berljivi obliki in jih je mogoče prepoznati kot umetno ustvarjene ali prirejene. Ponudniki zagotovijo, da so njihove tehnične rešitve učinkovite, interoperabilne, robustne in zanesljive, kolikor je to tehnično izvedljivo, pri čemer upoštevajo posebnosti in omejitve različnih vrst vsebin, stroške izvajanja in splošno priznane najsodobnejše tehnološke dosežke, kar se lahko odraža v ustreznih tehničnih standardih. Ta obveznost se ne uporablja, kolikor sistemi UI zagotavljajo podporno funkcijo za standardno urejanje ali ne spreminjajo bistveno vhodnih podatkov, ki jih zagotovi uvajalec, ali njihove semantike ali kadar so z zakonom dovoljeni za odkrivanje, preprečevanje, preiskovanje ali pregon kaznivih dejanj.

3. Uvajalci sistema za prepoznavanje čustev ali sistema za biometrično kategorizacijo o delovanju sistema obvestijo fizične osebe, ki so mu izpostavljene, in obdelujejo osebne podatke v skladu z uredbama (EU) 2016/679 in (EU) 2018/1725 ter Direktivo (EU) 2016/680, kot je ustrezno. Ta obveznost se ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine tretjih oseb ter v skladu s pravom Unije ne uporablja za sisteme UI, ki se uporabljajo za biometrično kategorizacijo in prepoznavanje čustev ter so z zakonom dovoljeni za odkrivanje, preprečevanje ali preiskovanje kaznivih dejanj.

4. Uvajalci sistema UI, ki ustvarja ali prireja slikovno, zvočno ali video vsebino, ki je globoki ponaredek, morajo razkriti, da je bila vsebina umetno ustvarjena ali prirejena. Ta obveznost se ne uporablja, kadar je uporaba zakonsko dovoljena za odkrivanje, preprečevanje, preiskovanje ali pregon kaznivih dejanj. Kadar je vsebina del očitno umetniškega, ustvarjalnega, satiričnega, fiktivnega ali podobnega dela ali programa, so obveznosti glede preglednosti iz tega odstavka omejene na razkritje obstoja take ustvarjene ali prirejene vsebine na ustrezen način, ki ne ovira prikazovanja ali uživanja dela.

Uvajalci sistema UI, ki ustvarja ali prireja besedilo, ki se objavi z namenom obveščanja javnosti o zadevah javnega interesa, morajo razkriti, da je bilo besedilo umetno ustvarjeno ali prirejeno. Ta obveznost se ne uporablja, kadar je uporaba zakonsko dovoljena za odkrivanje, preprečevanje, preiskovanje ali pregon kaznivih dejanj ali kadar je bila vsebina, ustvarjena z UI, predmet človeške preverbe ali uredniškega pregleda in kadar ima fizična ali pravna oseba uredniško odgovornost za objavo vsebine.

5. Informacije iz odstavkov 1 do 4 se dajo na voljo zadevnim fizičnim osebam na jasen in razpoznaven način ter najpozneje ob prvi interakciji ali izpostavljenosti. Informacije morajo biti skladne z veljavnimi zahtevami glede dostopnosti.

6. Odstavki 1 do 4 ne vplivajo na zahteve in obveznosti iz poglavja III in ne posegajo v druge obveznosti glede preglednosti, ki so za uvajalce sistemov UI določene v pravu Unije ali nacionalnem pravu.

7. Urad za UI spodbuja in olajšuje pripravo kodeksov prakse na ravni Unije, da se omogoči učinkovito izvajanje obveznosti glede odkrivanja in označevanja umetno ustvarjenih ali prirejenih vsebin. Komisija lahko sprejme izvedbene akte za odobritev teh kodeksov prakse v skladu s postopkom iz člena 56(6). Če meni, da kodeks ni ustrezen, lahko Komisija sprejme izvedbeni akt, s katerim določi skupna pravila za izvajanje navedenih obveznosti v skladu s postopkom pregleda iz člena 98(2).

POGLAVJE V

MODELI UI ZA SPLOŠNE NAMENE

ODDELEK 1

Pravila za razvrščanje

Člen 51

Razvrstitev modelov UI za splošne namene kot modelov UI za splošne namene s sistemskim tveganjem

1. Model UI za splošne namene se razvrsti kot model UI za splošne namene s sistemskim tveganjem, če izpolnjuje katerega od naslednjih pogojev:

- (a) ima zmogljivosti z visoko učinkovitostjo, ocenjene na podlagi ustreznih tehničnih orodij in metodologij, vključno s kazalniki in merili uspešnosti;
- (b) ima zmogljivosti ali učinek, ki so enakovredni tistim iz točke (a), ob upoštevanju meril iz Priloge XIII, na podlagi odločitve Komisije, in sicer po uradni dolžnosti ali na podlagi kvalificiranega opozorila znanstvenega odbora.

2. Za model UI za splošne namene se predpostavlja, da ima zmogljivosti z visoko učinkovitostjo na podlagi odstavka 1, točka (a), kadar je skupna količina izračuna, uporabljena za njegovo učenje, merjeno z operacijami s plavajočo vejico, večja od 10^{25} .

3. Komisija sprejme delegirane akte v skladu s členom 97 za spremembo pragov iz odstavkov 1 in 2 tega člena ter dopolnitev meril uspešnosti in kazalnikov glede na tehnološki razvoj, ki zadeva na primer algoritemsko izboljšavo ali večjo učinkovitost strojne opreme, kadar je to potrebno, da bi bili v teh pragovih upoštevani najsodobnejši tehnološki dosežki.

Člen 52

Postopek

1. Kadar model UI za splošne namene izpolnjuje pogoj iz člena 51(1), točka (a), zadevni ponudnik o tem nemudoma, v vsakem primeru pa v dveh tednih po izpolnitvi te zahteve ali po tem, ko je znano, da bo izpolnjena, uradno obvesti Komisijo. To uradno obvestilo vključuje informacije, iz katerih je razvidno, da je ustrezna zahteva izpolnjena. Če Komisija ugotovi, da model UI za splošne namene predstavlja sistemska tveganja, o katerih ni bila uradno obveščena, se lahko odloči, da ga bo označila za model s sistemskim tveganjem.

2. Ponudnik modela UI za splošne namene, ki izpolnjuje pogoj iz člena 51(1), točka (a), lahko ob uradnem obvestilu predloži dovolj utemeljene argumente, s katerimi dokaže, da model UI za splošne namene izjemoma, čeprav izpolnjuje navedeno zahtevo, zaradi svojih posebnih značilnosti ne predstavlja sistemskih tveganj in zato ne bi smel biti razvrščen kot model UI za splošne namene s sistemskim tveganjem.

3. Kadar Komisija ugotovi, da argumenti, predloženi na podlagi odstavka 2, niso dovolj utemeljeni in da zadevni ponudnik ni mogel dokazati, da model UI za splošne namene zaradi svojih posebnih značilnosti ne predstavlja sistemskih tveganj, te argumente zavrne, model UI za splošne namene pa se šteje za model UI za splošne namene s sistemskim tveganjem.

4. Komisija lahko na podlagi meril iz Priloge XIII po uradni dolžnosti ali na podlagi kvalificiranega opozorila znanstvenega odbora na podlagi člena 90(1), točka (a), model UI za splošne namene označi za model, ki predstavlja sistemska tveganja.

Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97, da spremeni Prilogo XIII, s tem da določi in posodobi merila iz navedene priloge.

5. Komisija na obrazloženo zahtevo ponudnika, katerega model je bil označen za model UI za splošne namene s sistemskim tveganjem na podlagi odstavka 4, upošteva zahtevo in se lahko odloči, da ponovno oceni, ali se lahko za model UI za splošne namene še vedno šteje, da predstavlja sistemska tveganja na podlagi meril iz Priloge XIII. Taka zahteva vsebuje objektivne, podrobne in nove razloge, ki so se pojavili po odločitvi glede označitve. Ponudniki ponovne ocene ne morejo zahtevati prej kot šest mesecev po odločitvi glede označitve. Kadar se Komisija po ponovni oceni odloči, da bo ohranila označitev modela UI za splošne namene s sistemskim tveganjem, ponudniki ponovne zahteve ne morejo zahtevati prej kot šest mesecev po tej odločitvi.

6. Komisija zagotovi objavo seznama modelov UI za splošne namene s sistemskim tveganjem in ga posodablja, ne da bi pri tem posegala v potrebo po spoštovanju in varstvu pravic intelektualne lastnine in zaupnih poslovnih informacij ali poslovnih skrivnosti v skladu s pravom Unije in nacionalnim pravom.

ODDELEK 2

Obveznosti, naložene ponudnikom modelov UI za splošne namene

Člen 53

Obveznosti, naložene ponudnikom modelov UI za splošne namene

1. Ponudniki modelov UI za splošne namene:

(a) pripravijo in posodablajo tehnično dokumentacijo modela, vključno s postopkom učenja in testiranja ter rezultati njegovega ocenjevanja, ki vsebuje vsaj informacije iz Priloge XI, da se na zahtevo predloži Uradu za UI in pristojnim nacionalnim organom;

(b) pripravijo, posodablajo in dajejo na voljo informacije in dokumentacijo za ponudnike sistemov UI, ki nameravajo model UI za splošne namene integrirati v svoje sisteme UI. Brez poseganja v potrebo po spoštovanju in varstvu pravic intelektualne lastnine in zaupnih poslovnih informacij ali poslovnih skrivnosti v skladu s pravom Unije in nacionalnim pravom informacije in dokumentacija:

(i) ponudnikom sistemov UI omogočajo, da dobro razumejo zmogljivosti in omejitve modela UI za splošne namene ter izpolnjujejo svoje obveznosti na podlagi te uredbe, ter

(ii) vsebujejo vsaj elemente iz Priloge XII;

(c) vzpostavijo politiko za doseganje skladnosti s pravom Unije o avtorskih in sorodnih pravicah, zlasti za opredelitev in spoštovanje, tudi z najsodobnejšimi tehnologijami, pridržanjam pravic, izraženih na podlagi člena 4(3) Direktive (EU) 2019/790;

(d) v skladu s predlogo, ki jo zagotovi Urad za UI, pripravijo in objavijo dovolj podroben povzetek vsebine, ki se uporablja za učenje modela UI za splošne namene.

2. Obveznosti iz odstavka 1, točki (a) in (b), ne veljajo za ponudnike modelov UI, ki so bili objavljeni na podlagi proste in odprtokodne licence, ki omogoča dostop do modela, njegovo uporabo, spreminjanje in distribucijo ter katere parametri, vključno z utežmi, informacijami o strukturi modela in informacijami o uporabi modela, so javno dostopni. Ta izjema se ne uporablja za modele UI za splošne namene s sistemskimi tveganji.
3. Ponudniki modelov UI za splošne namene pri izvajanju svojih pristojnosti in pooblastil na podlagi te uredbe po potrebi sodelujejo s Komisijo in pristojnimi nacionalnimi organi.
4. Ponudniki modelov UI za splošne namene se lahko do objave harmoniziranega standarda zanašajo na kodekse prakse v smislu člena 56, da dokažejo skladnost z obveznostmi iz odstavka 1 tega člena. Izpolnjevanje evropskih harmoniziranih standardov zagotavlja ponudnikom domnevo o skladnosti, kadar ti standardi zajemajo te obveznosti. Ponudniki modelov UI za splošne namene, ki ne upoštevajo odobrenega kodeksa prakse ali ne izpolnjujejo evropskega harmoniziranega standarda, dokažejo, da imajo druge ustrezne načine za zagotavljanje skladnosti, ki jih oceni Komisija.
5. Da se olajša skladnost s Prilogo XI, zlasti s točko 2(d) in (e) navedene priloge, se na Komisijo prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97, v katerih se podrobno opredelijo metodologije merjenja in izračunavanja, da se omogoči primerljiva in preverljiva dokumentacija.
6. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97(2) za spremembo prilog XI in XII glede na hiter tehnološki razvoj.
7. Vse informacije ali dokumentacija, pridobljene na podlagi tega člena, vključno s poslovnimi skrivnostmi, se obravnavajo v skladu z obveznostmi glede zaupnosti iz člena 78.

Člen 54

Pooblašчени zastopniki ponudnikov modelov UI za splošne namene

1. Ponudniki s sedežem v tretji državi pred dajanjem modela UI za splošne namene na trg Unije s pisnim pooblastilom imenujejo pooblaščenega zastopnika s sedežem v Uniji.
2. Ponudnik svojemu pooblaščenemu zastopniku omogoči, da opravlja naloge, določene v pooblastilu, ki ga prejme od ponudnika.
3. Pooblaščen zastopnik opravlja naloge, določene v pooblastilu, ki ga prejme od ponudnika. Uradu za UI na njegovo zahtevo predloži izvod pooblastila, in sicer v enem od uradnih jezikov institucij Unije. Za namene te uredbe pooblastilo pooblaščenemu zastopniku omogoča, da opravlja naslednje naloge:
 - (a) preveri, ali je bila tehnična dokumentacija, določena v Prilogi XI, pripravljena in ali je ponudnik izpolnil vse obveznosti iz člena 53 in, kadar je ustrezno, člena 55;
 - (b) hrani izvod tehnične dokumentacije, določene v Prilogi XI, da je za obdobje 10 let po tem, ko je bil model UI za splošne namene dan na trg, na voljo Uradu za UI in pristojnim nacionalnim organom, ter kontaktne podatke ponudnika, ki je imenoval pooblaščenega zastopnika;
 - (c) Uradu za UI na obrazloženo zahtevo zagotovi vse informacije in dokumentacijo, vključno s tistimi iz točke (b), s katerimi dokaže, da izpolnjuje obveznosti iz tega poglavja;
 - (d) na obrazloženo zahtevo sodeluje z Uradom za UI in pristojnimi nacionalnimi organi pri vseh ukrepih, ki jih slednji sprejmejo v zvezi z modelom UI za splošne namene s sistemskimi tveganji, tudi kadar je model vključen v sisteme UI, dane na trg ali v uporabo v Uniji.
4. Na podlagi pooblastila je pooblaščen zastopnik pooblaščen, da lahko Urad za UI ali pristojni organi nanj, poleg ponudnika ali namesto njega, naslovijo vsa vprašanja, povezana z zagotavljanjem skladnosti s to uredbo.

5. Pooblaščen zastopnik odpove pooblastilo, če meni ali utemeljeno domneva, da ponudnik ravna v nasprotju s svojimi obveznostmi na podlagi te uredbe. V takem primeru tudi nemudoma obvesti Urad za UI o odpovedi pooblastila in o razlogih zanj.

6. Obveznost iz tega člena ne velja za ponudnike modelov UI za splošne namene, ki so bili objavljeni na podlagi proste in odprtokodne licence, ki omogoča dostop do modela, njegovo uporabo, spreminjanje in distribucijo ter katere parametri, vključno z utežmi, informacijami o strukturi modela in informacijami o uporabi modela, so javno dostopni, razen če modeli UI za splošne namene predstavljajo sistemska tveganja.

ODDELEK 3

Obveznosti ponudnikov modelov UI za splošne namene s sistemskim tveganjem

Člen 55

Obveznosti ponudnikov modelov UI za splošne namene s sistemskim tveganjem

1. Poleg obveznosti iz členov 53 in 54 ponudniki modelov UI za splošne namene s sistemskim tveganjem:
 - (a) izvedejo ocene modelov v skladu s standardiziranimi protokoli in orodji, ki upoštevajo najsodobnejše tehnološke dosežke, vključno z izvajanjem in dokumentiranjem testiranja modelov po načelu kontradiktornosti z namenom prepoznavanja in zmanjšanja sistemskega tveganja;
 - (b) ocenijo in zmanjšajo morebitna sistemska tveganja na ravni Unije, vključno z njihovimi viri, ki lahko izhajajo iz razvoja, dajanja na trg ali uporabe modelov UI za splošne namene s sistemskim tveganjem;
 - (c) spremljajo in dokumentirajo resne incidente ter informacije o njih in morebitne popravne ukrepe za njihovo odpravo brez nepotrebnega odlašanja sporočajo Uradu za UI in po potrebi pristojnim nacionalnim organom;
 - (d) zagotavljajo ustrezno raven kibernetske zaščite za model UI za splošne namene s sistemskim tveganjem in fizično infrastrukturo modela.
2. Ponudniki modelov UI za splošne namene s sistemskim tveganjem se lahko do objave harmoniziranega standarda zanašajo na kodekse prakse v smislu člena 56, da dokažejo skladnost z obveznostmi iz odstavka 1 tega člena. Izpolnjevanje evropskih harmoniziranih standardov zagotavlja ponudnikom domnevo o skladnosti, kadar ti standardi zajemajo te obveznosti. Ponudniki modelov UI za splošne namene s sistemskim tveganjem, ki ne upoštevajo odobrenega kodeksa prakse ali ne izpolnjujejo evropskega harmoniziranega standarda, dokažejo, da imajo druge ustrezne načine za zagotavljanje skladnosti, ki jih oceni Komisija.
3. Vse informacije ali dokumentacija, pridobljene na podlagi tega člena, vključno s poslovnimi skrivnostmi, se obravnavajo v skladu z obveznostmi glede zaupnosti iz člena 78.

ODDELEK 4

Kodeksi prakse

Člen 56

Kodeksi prakse

1. Urad za UI spodbuja in olajšuje pripravo kodeksov prakse na ravni Unije, da bi prispeval k pravilni uporabi te uredbe ob upoštevanju mednarodnih pristopov.
2. Urad za UI in Odbor si prizadevata zagotoviti, da kodeksi prakse zajemajo vsaj obveznosti iz členov 53 in 55, vključno z naslednjimi elementi:

- (a) načini za zagotavljanje, da se informacije iz člena 53(1), točki (a) in (b), posodablajo glede na tržni in tehnološki razvoj;
- (b) ustrezno ravno podrobnosti za povzetek o vsebini, ki se uporablja za učenje;
- (c) opredelitvijo vrste in narave sistemskih tveganj na ravni Unije, po potrebi vključno z njihovimi viri;
- (d) ukrepi, postopki in načini za oceno in obvladovanje sistemskih tveganj na ravni Unije, vključno s pripadajočo dokumentacijo, ki so sorazmerni s tveganji, upoštevajo njihovo resnost in verjetnost ter upoštevajo posebne izzive pri obvladovanju teh tveganj glede na možne načine, na katere se lahko taka tveganja pojavijo in udejanijo vzdolž verige vrednosti UI.

3. Urad za UI lahko k sodelovanju pri pripravi kodeksov prakse povabi vse ponudnike modelov UI za splošne namene in ustrezne pristojne nacionalne organe. V procesu lahko sodelujejo organizacije civilne družbe, industrija, akademski krogi in drugi ustrezni deležniki, kot so ponudniki nižje v verigi in neodvisni strokovnjaki.

4. Urad za UI in Odbor si prizadevata zagotoviti, da kodeksi prakse jasno določajo njune posebne cilje in vsebujejo zaveze ali ukrepe, po potrebi tudi ključne kazalnike uspešnosti, da se zagotovi doseganje teh ciljev, ter da so v njih ustrezno upoštevani potrebe in interesi vseh zainteresiranih strani na ravni Unije, tudi oseb, ki jih to zadeva.

5. Urad za UI si prizadeva zagotoviti, da mu sodelujoči pri kodeksu prakse redno poročajo o uresničevanju zavez in sprejetih ukrepov ter posledičnih rezultatih, po potrebi tudi glede na ključne kazalnike uspešnosti. V ključnih kazalnikih uspešnosti in obveznostih poročanja se odražajo razlike v velikosti in zmogljivosti različnih sodelujočih.

6. Urad za UI in Odbor redno spremljata in ocenjujeta, kako sodelujoči dosegajo cilje kodeksov prakse in kako prispevajo k pravilni uporabi te uredbe. Urad za UI in Odbor ocenita, ali kodeksi prakse zajemajo obveznosti iz členov 53 in 55, ter redno spremljata in ocenjujeta doseganje ciljev v zvezi s tem. Svojo oceno ustreznosti kodeksov prakse objaviata.

Komisija lahko z izvedbenim aktom odobri kodeks prakse in mu da splošno veljavnost v Uniji. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 98(2).

7. Urad za UI lahko povabi vse ponudnike modelov UI za splošne namene, da pristopijo h kodeksom prakse. Za ponudnike modelov UI za splošne namene, ki ne predstavljajo sistemskih tveganj, je pristop lahko omejen na obveznosti iz člena 53, razen če izrecno izrazijo svoj interes za pristop k celotnemu kodeksu.

8. Urad za UI po potrebi spodbuja in olajšuje pregled in prilagoditev kodeksov prakse, zlasti glede na nastajajoče standarde. Urad za UI pomaga ocenjevati razpoložljive standarde.

9. Kodeksi prakse se pripravijo najpozneje do 2. maja 2025. Urad za UI sprejme potrebne ukrepe, vključno s povabilom ponudnikom na podlagi odstavka 7.

Če kodeksa prakse do 2. avgusta 2025 ni mogoče dokončati ali če Urad za UI na podlagi svoje ocene na podlagi odstavka 6 tega člena meni, da ni ustrezen, lahko Komisija z izvedbenimi akti določi skupna pravila za izvajanje obveznosti iz členov 53 in 55, vključno z elementi iz odstavka 2 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 98(2).

POGLAVJE VI
UKREPI V PODPORO INOVACIJAM

Člen 57

Regulativni peskovniki za UI

1. Države članice zagotovijo, da njihovi pristojni organi na nacionalni ravni vzpostavijo vsaj en regulativni peskovnik za UI, ki začne delovati najpozneje 2. avgusta 2026. Ta peskovnik se lahko vzpostavi skupaj s pristojnimi organi drugih držav članic. Komisija lahko za vzpostavitev in delovanje regulativnih peskovnikov za UI zagotovi tehnično podporo, svetovanje in orodja.

Obveznost iz prvega pododstavka se lahko izpolni tudi s sodelovanjem v obstoječem peskovniku, če tako sodelovanje zagotavlja enakovredno nacionalno zastopanost sodelujočih držav članic.

2. Na regionalni ali lokalni ravni ali skupaj s pristojnimi organi drugih držav članic se lahko vzpostavijo tudi dodatni regulativni peskovniki za UI.

3. Evropski nadzornik za varstvo podatkov lahko vzpostavi tudi regulativni peskovnik za UI za institucije, organe, urade in agencije Unije ter lahko opravlja vloge in naloge pristojnih nacionalnih organov v skladu s tem poglavjem.

4. Države članice zagotovijo, da pristojni organi iz odstavkov 1 in 2 dodelijo zadostna sredstva za učinkovito in pravočasno izpolnjevanje tega člena. Kadar je primerno, pristojni nacionalni organi sodelujejo z drugimi ustreznimi organi in lahko dopustijo udeležnost drugih akterjev ekosistema UI. Ta člen ne vpliva na druge regulativne peskovnike, vzpostavljene na podlagi prava Unije ali nacionalnega prava. Države članice zagotovijo ustrezno raven sodelovanja med organi, ki nadzorujejo te druge peskovnike, in pristojnimi nacionalnimi organi.

5. Regulativni peskovniki za UI, vzpostavljeni na podlagi odstavka 1, zagotavljajo nadzorovano okolje, ki spodbuja inovacije ter omogoča razvoj, učenje, testiranje in validacijo inovativnih sistemov UI za določen čas, preden se dajo na trg ali v uporabo, v skladu s posebnim načrtom peskovnika, o katerem se dogovorijo ponudniki ali potencialni ponudniki in pristojni organ. Taki peskovniki lahko vključujejo testiranje v realnih razmerah, ki se v njih nadzoruje.

6. Pristojni organi v regulativnem peskovniku za UI po potrebi zagotovijo smernice, nadzor in podporo, kar zadeva opredeljevanje tveganja – zlasti za temeljne pravice, zdravje in varnost –, testiranje, ukrepe za zmanjšanje tveganj in njihovo učinkovitost glede na obveznosti in zahteve iz te uredbe ter po potrebi iz drugega prava Unije in nacionalnega prava, katerih upoštevanje se nadzoruje v peskovniku.

7. Pristojni organi ponudnikom in potencialnim ponudnikom, ki sodelujejo v regulativnem peskovniku za UI, zagotovijo smernice o regulativnih pričakovanjih ter o tem, kako izpolniti zahteve in obveznosti iz te uredbe.

Pristojni organ na zahtevo ponudnika ali potencialnega ponudnika sistema UI predloži pisno dokazilo o dejavnostih, ki so bile uspešno izvedene v peskovniku. Predloži tudi poročilo o izstopu, v katerem podrobno opiše dejavnosti, izvedene v peskovniku, ter povezane rezultate in učne izide. Ponudniki lahko tako dokumentacijo uporabijo za to, da s postopkom ugotavljanja skladnosti ali z ustreznimi dejavnostmi nadzora trga dokažejo skladnost s to uredbo. V zvezi s tem organi za nadzor trga in priglašeni organi pozitivno upoštevajo poročila o izstopu in pisna dokazila, ki jih predloži pristojni nacionalni organ, da bi v razumni meri pospešili postopke ugotavljanja skladnosti.

8. Komisija in Odbor sta ob upoštevanju določb o zaupnosti iz člena 78 in s soglasjem ponudnika ali potencialnega ponudnika pooblaščen za dostop do poročil o izstopu in jih, če je to primerno, upoštevata pri izvajanju svojih nalog na podlagi te uredbe. Če se ponudnik ali potencialni ponudnik in pristojni nacionalni organ izrecno strinjata, se lahko poročilo o izstopu objavi na enotni informacijski platformi iz tega člena.

9. Namen vzpostavitve regulativnih peskovnikov za UI je prispevati k naslednjim ciljem:

(a) izboljšanju pravne varnosti, da se doseže regulativna skladnost s to uredbo ali po potrebi z drugim veljavnim pravom Unije in nacionalnim pravom;

- (b) podpiranju izmenjave najboljših praks s sodelovanjem z organi, vključenimi v regulativni peskovnik za UI;
- (c) spodbujanju inovacij in konkurenčnosti ter olajšanju razvoja ekosistema UI;
- (d) prispevanju k regulativnemu učenju, ki temelji na dokazih;
- (e) olajšanju in pospežitvi dostopa sistemov UI do trga Unije, zlasti če so njihovi ponudniki MSP, vključno z zagonskimi podjetji.

10. Če inovativni sistemi UI vključujejo obdelavo osebnih podatkov ali kako drugače spadajo v nadzorno pristojnost drugih nacionalnih organov ali pristojnih organov, ki zagotavljajo ali podpirajo dostop do podatkov, nacionalni pristojni organi zagotovijo, da so nacionalni organi za varstvo podatkov in ti drugi nacionalni ali pristojni organi povezani z delovanjem regulativnega peskovnika za UI in vključeni v nadzor omenjenih vidikov v okviru svojih nalog in pooblastil.

11. Regulativni peskovniki za UI ne vplivajo na pooblastila pristojnih organov, ki nadzirajo peskovnike, za nadzor ali popravne ukrepe, tudi na regionalni ali lokalni ravni ne. Vsa pomembna tveganja za zdravje in varnost ter temeljne pravice, prepoznana med razvojem in testiranjem takih sistemov UI, se ustrezno zmanjšajo. Nacionalni pristojni organi so pooblaščen, da začasno ali trajno prekinajo postopek testiranja ali sodelovanje v peskovniku, če tveganj ni mogoče učinkovito zmanjšati, in o taki odločitvi obvestijo Urad za UI. Nacionalni pristojni organi svoja nadzorna pooblastila izvajajo v mejah ustreznega prava in pri izvajanju pravnih določb v zvezi z določenim projektom peskovnika za UI uporabljajo svoja diskrecijska pooblastila, da bi podprli inovacije na področju UI v Uniji.

12. Ponudniki in potencialni ponudniki, ki sodelujejo v regulativnem peskovniku za UI, so na podlagi veljavnega prava Unije in nacionalnega prava o odgovornosti še naprej odgovorni za škodo, povzročeno tretjim osebam zaradi eksperimentov, ki se izvajajo v peskovniku. Kadar pa potencialni ponudniki spoštujejo posebni načrt in pogoje za sodelovanje ter v dobri veri sledijo smernicam nacionalnih pristojnih organov, organi ne naložijo upravnih kazni za kršitev te uredbe. Kadar so bili v nadzor sistema UI v peskovniku dejavno vključeni drugi pristojni organi, odgovorni za drugo pravo Unije in nacionalno pravo, in so zagotovili smernice za skladnost, se v zvezi s tem pravom ne naložijo upravne kazni.

13. Regulativni peskovniki za UI so zasnovani in se izvajajo tako, da po potrebi olajšujejo čezmejno sodelovanje med pristojnimi nacionalnimi organi.

14. Nacionalni pristojni organi usklajujejo svoje dejavnosti in sodelujejo v okviru Odbora.

15. Pristojni nacionalni organi o vzpostavitvi peskovnika obvestijo Urad za UI in Odbor ter ju lahko zaprosijo za podporo in smernice. Urad za UI objavi seznam načrtovanih in obstoječih peskovnikov ter ga posodablja, da bi spodbudil večjo interakcijo v regulativnih peskovnikih za UI in čezmejno sodelovanje.

16. Pristojni nacionalni organi Uradu za UI in Odboru predložijo letna poročila, najprej eno leto po vzpostavitvi regulativnega peskovnika za UI, nato pa vsako leto do njegove ukinitve, tako kot tudi končno poročilo. Ta poročila vsebujejo informacije o napredku in rezultatih izvajanja teh peskovnikov, vključno z najboljšimi praksami, incidenti, pridobljenimi izkušnjami in priporočili o njihovi vzpostavitvi ter po potrebi o uporabi in morebitni reviziji te uredbe, vključno s povezanimi delegiranimi in izvedbenimi akti, in o uporabi drugega prava Unije, ki ga v peskovniku nadzorujejo pristojni organi. Pristojni nacionalni organi ta letna poročila ali njihove povzetke objavijo na spletu. Komisija pri izvajanju svojih nalog na podlagi te uredbe, kadar je primerno, upošteva ta letna poročila.

17. Komisija razvije enotni in namenski vmesnik, ki vsebuje vse ustrezne informacije v zvezi z regulativnimi peskovniki za UI, da bi lahko deležniki vstopali v interakcijo z regulativnimi peskovniki za UI in vlagali poizvedbe pri pristojnih organih ter zaprosili za nezavezujoče smernice glede skladnosti inovativnih proizvodov, storitev in poslovnih modelov, ki vključujejo tehnologije UI, v skladu s členom 62(1), točka (c). Komisija se po potrebi proaktivno usklajuje s pristojnimi nacionalnimi organi.

Člen 58

Podrobnosti v zvezi z regulativnimi peskovniki za UI in njihovo delovanje

1. Da bi se izognili razdrobljenosti po Uniji, Komisija sprejme izvedbene akte, v katerih določi podrobnosti za vzpostavitev, razvoj, izvajanje, delovanje in nadzor regulativnih peskovnikov za UI. Ti izvedbeni akti med drugim vsebujejo skupna načela o naslednjih elementih:

- (a) merilih za upravičenost in izbor za sodelovanje v regulativnem peskovniku za UI;
- (b) postopkih za vlogo, sodelovanje, spremljanje, izstop iz regulativnega peskovnika za UI in njegovo prenehanje, vključno z načrtom peskovnika in poročilom o izstopu;
- (c) pogojih, ki veljajo za udeležence.

Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 98(2).

2. Z izvedbenim aktom iz odstavka 1 se zagotovi:

- (a) da so regulativni peskovniki za UI odprti za vse ponudnike in potencialne ponudnike sistema UI, ki izpolnjujejo pregledna in pravična merila za upravičenost in izbor, in da pristojni nacionalni organi vlagatelje obvestijo o svoji odločitvi v treh mesecih od vložitve vloge;
- (b) da regulativni peskovniki za UI omogočajo širok in enak dostop ter sledijo povpraševanju po sodelovanju; ponudniki ali potencialni ponudniki lahko vloge predložijo tudi v partnerstvih z uvajalci in drugimi ustreznimi tretjimi osebami;
- (c) da se s podrobnostmi in pogoji v zvezi z regulativnimi peskovniki za UI v največji možni meri podpira prožnost, ki pristojnim nacionalnim organom omogoča vzpostavitev in upravljanje njihovih regulativnih peskovnikov za UI;
- (d) da je dostop do regulativnih peskovnikov za UI za MSP, vključno z zagonskimi podjetji, brezplačen, brez poseganja v izredne stroške, ki jih lahko pristojni nacionalni organi izterjajo na pošten in sorazmeren način;
- (e) da se ponudnikom ali potencialnim ponudnikom z učnimi izidi regulativnih peskovnikov za UI pomaga pri izpolnjevanju obveznosti glede ugotavljanja skladnosti iz te uredbe in prostovoljni uporabi kodeksov ravnanja iz člena 95;
- (f) da regulativni peskovniki za UI olajšujejo vključevanje drugih ustreznih akterjev v ekosistem UI, na primer priglašeni organov in organizacij za standardizacijo, MSP, vključno z zagonskimi podjetji, podjetij, inovatorjev, centrov za testiranje in eksperimentiranje, raziskovalnih in eksperimentalnih laboratorijev ter evropskih vozlišč za digitalne inovacije, centrov odličnosti, posameznih raziskovalcev, da bi omogočili in olajšali sodelovanje z javnim in zasebnimi sektorji;
- (g) da so postopki, procesi in upravne zahteve za vlogo, izbiro, sodelovanje in izstop iz regulativnega peskovnika za UI preprosti, lahko razumljivi in jasno predstavljeni, da bi olajšali udeležbo MSP, vključno z zagonskimi podjetji, z omejenimi pravnimi in upravnimi zmogljivostmi, ter da so racionalizirani po vsej Uniji, da bi preprečili razdrobljenost in da bi bila udeležba v regulativnem peskovniku za UI, ki ga vzpostavi država članica ali evropski nadzornik za varstvo podatkov, vzajemno in enotno priznana ter da bi imela enake pravne učinke po vsej Uniji;
- (h) da je sodelovanje v regulativnem peskovniku za UI omejeno na obdobje, ki je primerno glede na kompleksnost in obseg projekta in ki ga lahko pristojni nacionalni organ podaljša;
- (i) da regulativni peskovniki za UI olajšujejo razvoj orodij in infrastrukture za testiranje, primerjalno analizo, ocenjevanje in razlago razsežnosti sistemov UI, ki so pomembne za regulativno učenje, na primer točnosti, robustnosti in kibernetske varnosti, pa tudi ukrepov za zmanjšanje tveganj, kar zadeva temeljne pravice in družbo na splošno.

3. Potencialni ponudniki v regulativnih peskovnikih za UI, zlasti MSP in zagonska podjetja, so po potrebi usmerjeni k storitvam pred uvedbo, kot so smernice o izvajanju te uredbe, k drugim storitvam z dodano vrednostjo, kot so pomoč pri dokumentih za standardizacijo in certificiranju, centri za testiranje in eksperimentiranje, evropska vozlišča za digitalne inovacije in centri odličnosti.

4. Kadar pristojni nacionalni organi presoja o odobritvi testiranja v realnih razmerah, ki se nadzoruje v okviru regulativnega peskovnika za UI, ki se vzpostavi na podlagi tega člena, se z udeleženci izrecno dogovorijo o pogojih takega testiranja in zlasti o ustreznih zaščitnih ukrepih za varovanje temeljnih pravic, zdravja in varnosti. Kadar je primerno, sodelujejo z drugimi pristojnimi nacionalnimi organi, da bi zagotovili dosledne prakse po vsej Uniji.

Člen 59

Nadaljnja obdelava osebnih podatkov za razvoj določenih sistemov UI v javnem interesu v regulativnem peskovniku za UI

1. V regulativnem peskovniku za UI se osebni podatki, zakonito zbrani za druge namene, lahko obdelujejo izključno za namene razvoja, učenja in testiranja nekaterih sistemov UI v peskovniku, če so izpolnjeni vsi naslednji pogoji:

- (a) javni organ ali druga fizična ali pravna oseba razvije sisteme UI za zaščito bistvenega javnega interesa na enem ali več naslednjih področjih:
 - (i) javna varnost in javno zdravje, vključno z odkrivanjem, diagnosticiranjem, preprečevanjem, obvladovanjem in zdravljenjem bolezni ter izboljšanjem sistemov zdravstvenega varstva;
 - (ii) visoka raven varstva in izboljšanje kakovosti okolja, ohranjanje biotske raznovrstnosti, varstvo pred onesnaževanjem, ukrepi za zeleni prehod ter blažitev podnebnih sprememb in prilagajanje nanje;
 - (iii) trajnostna energija;
 - (iv) varnost in odpornost prometnih sistemov in mobilnosti, kritične infrastrukture in omrežij;
 - (v) učinkovitost in kakovost javne uprave in javnih storitev;
- (b) obdelani podatki so potrebni za izpolnjevanje ene ali več zahtev iz poglavja III, oddelek 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 se 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 potencialnih ponudnikov, dostop do teh podatkov pa imajo le pooblaščen osebe;
- (e) ponudniki lahko prvotno zbrane podatke delijo naprej le v skladu s pravom Unije o varstvu podatkov; osebnih podatkov ustvarjenih v peskovniku, ni mogoče deliti zunaj peskovnika;
- (f) nobena obdelava osebnih podatkov v okviru peskovnika ne sme biti podlaga za sprejetje ukrepov ali odločitev, ki bi vplivali na posameznike, na katere se nanašajo osebni podatki, niti ne sme vplivati na uveljavljanje njihovih pravic, določenih v pravu Unije o varstvu osebnih podatkov;
- (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 logike, na katerih temeljijo učenje, testiranje in validacija sistema UI, se skupaj z rezultati testiranja hrani kot del tehnične dokumentacije iz Priloge IV;

- (j) kratek povzetek projekta UI, 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 mejne kontrole in organov, pristojnih za priseljevanje, ali azilnih organov.

2. 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 UI temelji na posebnem pravu Unije ali nacionalnem pravu in zanjo veljajo enaki kumulativni pogoji, kot so navedeni v odstavku 1.

3. Odstavek 1 ne posega v pravo Unije ali nacionalno pravo, ki izključuje obdelavo osebnih podatkov za druge namene, kot so izrecno navedeni v tem pravu, pa tudi ne v pravo Unije ali nacionalno pravo, ki določa podlago za obdelavo osebnih podatkov, potrebno za namene razvoja, testiranja ali učenja inovativnih sistemov UI, ali katero koli drugo pravno podlago, skladno s pravom Unije o varstvu osebnih podatkov.

Člen 60

Testiranje visokotveganih sistemov UI v realnih razmerah zunaj regulativnih peskovnikov za UI

1. Testiranje visokotveganih sistemov UI v realnih razmerah zunaj regulativnih peskovnikov za UI lahko izvajajo ponudniki ali potencialni ponudniki visokotveganih sistemov UI s seznama v Prilogi III v skladu s tem členom in načrtom testiranja v realnih razmerah iz tega člena, brez poseganja v prepovedi na podlagi člena 5.

Komisija z izvedbenimi akti določi podrobne elemente načrta testiranja v realnih razmerah. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 98(2).

Ta odstavek ne posega v pravo Unije ali nacionalno pravo za testiranje visokotveganih sistemov UI, povezanih s proizvodi, zajetimi v harmonizacijski zakonodaji Unije iz Priloge I, v realnih razmerah.

2. Ponudniki ali potencialni ponudniki lahko testiranje visokotveganih sistemov UI iz Priloge III v realnih razmerah izvedejo kadar koli, preden dajo sistem UI na trg ali v uporabo, bodisi sami bodisi v partnerstvu z enim ali več uvajalci ali potencialnimi uvajalci.

3. Testiranje visokotveganih sistemov UI v realnih razmerah na podlagi tega člena ne posega v nobeno etično presojo, ki se zahteva v skladu s pravom Unije ali nacionalnim pravom.

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

- (a) ponudnik ali potencialni ponudnik je pripravil načrt testiranja v realnih razmerah in ga predložil organu za nadzor trga v državi članici, v kateri se bo testiranje v realnih razmerah izvajalo;
- (b) organ za nadzor trga v državi članici, v kateri se testiranje v realnih razmerah izvaja, je odobril testiranje v realnih razmerah in načrt testiranja v realnih razmerah; kadar organ za nadzor trga ne odgovori v 30 dneh, se šteje, da sta testiranje v realnih razmerah in načrt testiranja v realnih razmerah odobrena; kadar nacionalno pravo ne določa tihe odobritve, je za testiranje v realnih razmerah še naprej potrebno dovoljenje;
- (c) ponudnik ali potencialni ponudnik, z izjemo ponudnikov ali potencialnih ponudnikov visokotveganih sistemov UI iz Priloge III, točke 1, 6 in 7, na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, migracij, azila in upravljanja nadzora meja ter visokotveganih sistemov UI iz Priloge III, točka 2, je registriral testiranje v realnih razmerah v skladu s členom 71(4) z vseevropsko enotno identifikacijsko številko in informacijami, določenimi v Prilogi IX; ponudnik ali potencialni ponudnik visokotveganih sistemov UI iz točk 1, 6 in 7 Priloge III je na področjih preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, migracij, azila in upravljanja mejnega nadzora registriral testiranje v realnih razmerah v varnem nejavnem delu podatkovne zbirke EU skladno s členom 49(4), točka (d), z vseevropsko enotno identifikacijsko številko in informacijami, določenimi v njej; ponudnik ali potencialni ponudnik visokotveganih sistemov UI iz točke 2 Priloge III je registriral testiranje v realnih razmerah v skladu s členom 49(5);

- (d) ponudnik ali potencialni ponudnik, ki izvaja testiranje v realnih razmerah, ima sedež v Uniji ali je imenoval pravnega zastopnika, ki ima sedež v Uniji;
- (e) podatki, zbrani in obdelani za namen testiranja v realnih razmerah, se v tretje države prenesejo le, če se izvajajo ustrezni in veljavni zaščitni ukrepi na podlagi prava Unije;
- (f) testiranje v realnih razmerah ne traja dlje, kot je potrebno, da se dosežejo zadani cilji, v nobenem primeru pa ne presega šestmesečnega obdobja, ki se lahko podaljša za dodatnih šest mesecev, če ponudnik ali potencialni ponudnik o tem predhodno uradno obvesti organ za nadzor trga in uradnemu obvestilu doda obrazložitev potrebe po takem podaljšanju;
- (g) udeleženci testiranja v realnih razmerah, ki so osebe, ki pripadajo ranljivim skupinam zaradi svoje starosti ali invalidnosti, so ustrezno zaščiteni;
- (h) kadar ponudnik ali potencialni ponudnik testiranje v realnih razmerah organizira v sodelovanju z enim ali več uvajalci ali potencialnimi uvajalci, so bili slednji obveščeni o vseh vidikih testiranja, ki so pomembni za njihovo odločitev za sodelovanje, in so prejeli ustrezna navodila za uporabo sistema UI iz člena 13; ponudnik ali potencialni ponudnik in uvajalec ali potencialni uvajalec sklenejo sporazum, ki določa njihove vloge in odgovornosti, da se zagotovi skladnost z določbami za testiranje v realnih razmerah na podlagi te uredbe ter na podlagi drugega veljavnega prava Unije in nacionalnega prava;
- (i) udeleženci testiranja v realnih razmerah so dali informirano privolitev v skladu s členom 61, v primeru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ko bi pridobitev informirane privolitve preprečila testiranje sistema UI, pa samo testiranje in rezultati testiranja v realnih razmerah ne smejo negativno vplivati na udeležence, njihovi osebni podatki pa se po koncu testiranja izbrišejo;
- (j) testiranje v realnih razmerah učinkovito nadzorujejo ponudnik ali potencialni ponudnik, pa tudi uvajalci ali potencialni uvajalci, z osebami, ki so ustrezno kvalificirane na zadevnem področju in imajo potrebne zmogljivosti, usposobljenost in pooblastila za opravljanje svojih nalog;
- (k) napovedi, priporočila ali odločitve sistema UI je mogoče učinkovito izničiti in zanemariti.

5. Vsi udeleženci testiranja v realnih razmerah ali njihov zakonito imenovani zastopnik, kot je primerno, se lahko brez kakršne koli škode in brez obrazložitve kadar koli umaknejo iz testiranja, tako, da prekličejo svojo informirano privolitev, in lahko zahtevajo, da se njihovi osebni podatki nemudoma in stalno izbrišejo. Preklic informirane privolitve ne vpliva na že izvedene dejavnosti.

6. Države članice v skladu s členom 75 na svoje organe za nadzor trga prenesejo pooblastila, na podlagi katerih od ponudnikov in potencialnih ponudnikov zahtevajo predložitev informacij, izvajajo nenapovedane inšpekcijske preglede na daljavo ali na kraju samem ter preverjajo opravljanje testiranja v realnih razmerah in z njimi povezane visoko tvegane sisteme UI. Organi za nadzor trga ta pooblastila uporabljajo za zagotovitev varnega poteka testiranja v realnih razmerah.

7. Vsak resen incident, ugotovljen med testiranjem v realnih razmerah, se sporoči nacionalnemu organu za nadzor trga v skladu s členom 73. Ponudnik ali potencialni ponudnik sprejme takojšnje ukrepe za zmanjšanje tveganj ali, če to ni mogoče, testiranje v realnih razmerah začasno ustavi, dokler ne pride do tovrstnega zmanjšanja, v nasprotnem primeru pa ga dokončno ustavi. Po taki dokončni ustavitvi testiranja v realnih razmerah vzpostavi postopek za takojšnji odpoklic sistema UI.

8. Ponudniki ali potencialni ponudniki obvestijo nacionalni organ za nadzor trga v državi članici, v kateri se testiranje v realnih razmerah izvaja, o začasni ali dokončni ustavitvi testiranja v realnih razmerah in o končnih rezultatih.

9. Ponudnik ali potencialni ponudnik je na podlagi veljavnega prava Unije in nacionalnega prava o odgovornosti odgovoren za vsakršno škodo, povzročeno med njegovim testiranjem v realnih razmerah.

Člen 61

Informirana privolitev za sodelovanje pri testiranju v realnih razmerah zunaj regulativnih peskovnikov za UI

1. Za namen testiranja v realnih razmerah na podlagi člena 60 udeleženci testiranja dajo prostovoljno informirano privolitev, preden začnejo sodelovati pri takem testiranju in po tem, ko so bili z jedrnatimi, jasnimi, ustreznimi in razumljivimi informacijami ustrezno obveščeni o:
 - (a) naravi in ciljih testiranja v realnih razmerah ter morebitnih nevšečnostih, ki so lahko povezane z njihovim sodelovanjem;
 - (b) pogojih, pod katerimi se bo testiranje v realnih razmerah izvajalo, vključno s pričakovanim trajanjem sodelovanja udeležencev;
 - (c) svojih pravicah in zagotovilih v zvezi s sodelovanjem, zlasti o pravici, da zavrnejo sodelovanje in se lahko brez kakršne koli škode in brez obrazložitve kadar koli umaknejo iz testiranja v realnih razmerah;
 - (d) tem, kako se vloži zahteva za to, da se napovedi, priporočila ali odločitve sistema UI izničijo ali zanemarijo;
 - (e) vseevropski enotni identifikacijski številki testiranja v realnih razmerah v skladu s členom 60(4), točka (c), in kontaktnih podatkih ponudnika ali njegovega pravnega zastopnika, od katerega je mogoče pridobiti dodatne informacije.
2. Informirana privolitev se datira in dokumentira, udeleženci testiranja ali njihov zakoniti zastopnik pa prejmejo kopijo.

Člen 62

Ukrepi za ponudnike in uvajalce, zlasti MSP, vključno z zagonskimi podjetji

1. Države članice sprejmejo naslednje ukrepe:
 - (a) MSP, vključno z zagonskimi podjetji, ki imajo statutarni sedež ali podružnico v Uniji, zagotovijo prednostni dostop do regulativnih peskovnikov za UI, če izpolnjujejo pogoje za upravičenost in merila za izbor; prednostni dostop drugim MSP, vključno z zagonskimi podjetji, razen tistih iz tega odstavka, ne preprečuje dostopa do regulativnega peskovnika za UI, če izpolnjujejo tudi pogoje za upravičenost in merila za izbor;
 - (b) organizirajo posebne dejavnosti ozaveščanja in usposabljanja o uporabi te uredbe, prilagojene potrebam MSP, vključno z zagonskimi podjetji, uvajalcev in, če je to primerno, lokalnih javnih organov;
 - (c) uporabijo obstoječe in, kadar je primerno, vzpostavijo nove posebne kanale za komunikacijo z MSP, vključno z zagonskimi podjetji, uvajalci, drugimi inovatorji in, če je to primerno, lokalnimi javnimi organi, da jim svetujejo in odgovarjajo na vprašanja o izvajanju te uredbe, tudi kar zadeva sodelovanje v regulativnih peskovnikih za UI;
 - (d) olajšujejo sodelovanje MSP in drugih ustreznih deležnikov v postopku razvoja standardizacije.
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. Urad za UI sprejme naslednje ukrepe:
 - (a) zagotovi standardizirane predloge za področja, ki jih zajema ta uredba, kot jih določi Odbor v svoji zahtevi;
 - (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 najboljših praks v postopkih javnega naročanja v zvezi s sistemi UI.

Člen 63

Odstopanja za določene operaterje

1. Mikropodjetja v smislu Priporočila 2003/361/ES lahko nekatere elemente sistema vodenja kakovosti iz člena 17 te uredbe izpolnjujejo na poenostavljen način, če nimajo partnerskih podjetij ali povezanih podjetij v smislu navedenega priporočila. V ta namen Komisija pripravi smernice o elementih sistema vodenja kakovosti, ki se lahko upoštevajo na poenostavljen način ob upoštevanju potreb mikropodjetij, ne da bi to vplivalo na raven zaščite ali potrebo po skladnosti z zahtevami v zvezi z visokotveganimi sistemi UI.
2. Odstavek 1 tega člena se ne razlaga tako, da so ti operaterji oproščeni izpolnjevanja katerih koli drugih zahtev ali obveznosti iz te uredbe, tudi tistih ne iz členov 9, 10, 11, 12, 13, 14, 15, 72 in 73.

POGLAVJE VII

UPRAVLJANJE

ODDELEK 1

Upravljanje na ravni Unije

Člen 64

Urad za UI

1. Komisija prek Urada za UI razvija strokovno znanje in zmogljivosti Unije na področju UI.
2. Države članice olajšujejo naloge, zaupane Uradu za UI, kot je razvidno iz te uredbe.

Člen 65

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 Urad za UI, pri glasovanju pa ne sodeluje. Odbor se lahko vsakič posebej odloči, da na sestanek povabi druge organe, telesa ali strokovnjake iz Unije in držav članic, kadar so obravnavana vprašanja zanje pomembna.
3. Države članice imenujejo svojega predstavnika za obdobje treh let z možnostjo enkratnega podaljšanja.
4. Države članice zagotovijo, da njihovi predstavniki v Odboru:
 - (a) imajo v svoji državi članici ustrezne pristojnosti in pooblastila, da dejavno prispevajo k izpolnjevanju nalog Odbora iz člena 66;
 - (b) so določeni kot enotna kontaktna točka v odnosu do Odbora in, kadar je primerno, ob upoštevanju potreb držav članic kot enotna kontaktna točka za deležnike;

(c) so pooblaščen za spodbujanje doslednosti in usklajevanja med pristojnimi nacionalnimi organi v svoji državi članici glede izvajanja te uredbe, vključno z zbiranjem ustreznih podatkov in informacij za namene opravljanja njihovih nalog v Odboru.

5. Imenovani predstavniki držav članic z dvotretjinsko večino sprejmejo poslovnik Odbora. V poslovniku se določijo zlasti potek izbirnega postopka, trajanje mandata predsednika in specifikacije njegovih nalog, podrobnosti glede glasovanja ter organizacija dejavnosti Odbora in dejavnosti njegovih podskupin.

6. Odbor ustanovi dve stalni podskupini, da bi zagotavljali platformo za sodelovanje in izmenjavo med organi za nadzor trga ter uradno obveščali organe o vprašanjih, povezanih z nadzorom trga oziroma priglašeni 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.

Odbor lahko ustanovi druge bodisi stalne ali začasne podskupine za preučitev posebnih vprašanj. Po potrebi so lahko predstavniki svetovalnega foruma iz člena 67 povabljeni k sodelovanju v takih podskupinah ali na posebne sestanke teh podskupin kot opazovalci.

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

8. Odboru predseduje eden od predstavnikov držav članic. Urad za UI je sekretariat Odbora, na zahtevo predsednika sklicuje sestanke in pripravi njihov dnevni red v skladu z nalogami Odbora na podlagi te uredbe in njegovega poslovnika.

Člen 66

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) prispeva k usklajevanju med pristojnimi nacionalnimi organi, odgovornimi za uporabo te uredbe, ter v sodelovanju z zadevnimi organi za nadzor trga in v dogovoru z njimi podpira skupne dejavnosti organov za nadzor trga iz člena 74(11);
- (b) zbira in izmenjuje tehnično in regulativno strokovno znanje in najboljše prakse med državami članicami;
- (c) svetuje o izvajanju te uredbe, zlasti v zvezi z izvrševanjem pravil o modelih UI za splošne namene;
- (d) prispeva k harmonizaciji upravnih praks v državah članicah, tudi v zvezi z odstopanjem od postopkov ugotavljanja skladnosti iz člena 46, delovanjem regulativnih peskovnikov za UI ter testiranjem v realnih razmerah iz členov 57, 59 in 60;
- (e) 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, tudi:
 - (i) o razvoju in uporabi kodeksov ravnanja in kodeksov prakse na podlagi te uredbe ter smernic Komisije;
 - (ii) o oceni in pregledu te uredbe na podlagi člena 112, tudi kar zadeva poročila o resnih incidentih iz člena 73 in delovanje podatkovne zbirke EU iz člena 71, o pripravi delegiranih ali izvedbenih aktov ter morebitnih uskladitvah te uredbe s pravnimi akti iz Priloge I;
 - (iii) o tehničnih specifikacijah ali obstoječih standardih v zvezi z zahtevami iz poglavja III, oddelek 2,

- (iv) o uporabi harmoniziranih standardov ali skupnih specifikacij iz členov 40 in 41;
- (v) o trendih, kot so svetovna konkurenčnost Evrope na področju UI, uvajanje UI v Uniji ter razvoj digitalnih spretnosti;
- (vi) o trendih v zvezi z razvijajočo se tipologijo verig vrednosti UI, zlasti glede iz tega izhajajočih posledic v smislu odgovornosti;
- (vii) o morebitni potrebi po spremembi Priloge III v skladu s členom 7 in o morebitni potrebi po morebitni reviziji člena 5 na podlagi člena 112, ob upoštevanju ustreznih razpoložljivih dokazov in najnovejšega tehnološkega razvoja;
- (f) podpira Komisijo pri spodbujanju pismenosti na področju UI ter ozaveščanja in razumevanja javnosti o prednostih, tveganjih, zaščitnih ukrepih ter pravicah in obveznostih, povezanih z uporabo sistemov UI;
- (g) spodbuja oblikovanje skupnih meril in skupnega razumevanja ustreznih konceptov iz te uredbe med udeleženci na trgu in pristojnimi organi, tudi s prispevanjem k razvoju meril uspešnosti;
- (h) sodeluje, če je to primerno, z drugimi institucijami, organi, uradi in agencijami Unije, pa tudi z ustreznimi strokovnimi skupinami in mrežami Unije, zlasti na področju varnosti proizvodov, kibernetske varnosti, konkurence, digitalnih in medijskih storitev, finančnih storitev, varstva potrošnikov ter varstva podatkov in temeljnih pravic;
- (i) prispeva k učinkovitemu sodelovanju s pristojnimi organi tretjih držav in mednarodnimi organizacijami;
- (j) pomaga pristojnim nacionalnim organom in Komisiji pri razvoju organizacijskega in tehničnega strokovnega znanja, potrebnega za izvajanje te uredbe, vključno s prispevanjem k oceni potreb po usposabljanju osebja držav članic, ki sodeluje pri izvajanju te uredbe;
- (k) pomaga Uradu za UI pri podpiranju pristojnih nacionalnih organov pri vzpostavitvi in razvoju regulativnih peskovnikov za UI ter olajšuje sodelovanje in izmenjavo informacij med regulativnimi peskovniki za UI;
- (l) prispeva k pripravi smernic in zagotavlja ustrezno svetovanje v zvezi z njim;
- (m) svetuje Komisiji v zvezi z mednarodnimi zadevami na področju UI;
- (n) Komisiji daje mnenja o kvalificiranih opozorilih v zvezi z modeli UI za splošne namene;
- (o) prejema mnenja držav članic o kvalificiranih opozorilih v zvezi z modeli UI za splošne namene ter o nacionalnih izkušnjah in praksah v zvezi s spremljanjem in izvrševanjem sistemov UI, zlasti sistemov, v katere so vgrajeni modeli UI za splošne namene.

Člen 67

Svetovalni forum

1. Ustanovi se svetovalni forum, ki zagotavlja tehnično strokovno znanje in svetuje Odboru in Komisiji ter prispeva k njunim nalogam iz te uredbe.
2. Članstvo svetovalnega foruma je sestavljeno iz uravnovešenega izbora deležnikov, vključno z industrijo, zagonskimi podjetji, MSP, civilno družbo in akademskimi krogi. Članstvo v svetovalnem forumu je uravnoveženo z vidika komercialnih in nekomercialnih interesov, v kategoriji poslovnih interesov pa z vidika MSP in drugih podjetij.
3. Komisija člane svetovalnega foruma imenuje med deležniki s priznanim strokovnim znanjem na področju UI v skladu z merili iz odstavka 2.

4. Mandat članov svetovalnega foruma traja dve leti in se lahko podaljša še za največ štiri leta.
5. Stalni člani svetovalnega foruma so Agencija Evropske unije za temeljne pravice, ENISA, Evropski odbor za standardizacijo (CEN), Evropski odbor za elektrotehniško standardizacijo (CENELEC) in Evropski inštitut za telekomunikacijske standarde (ETSI).
6. Svetovalni odbor sestavi svoj poslovnik. Med svojimi člani izvoli dva sopredsednika v skladu z merili iz odstavka 2. Mandat sopredsednikov traja dve leti z možnostjo enkratnega podaljšanja.
7. Svetovalni forum se sestane najmanj dvakrat na leto. Na svoje sestanke lahko povabi strokovnjake in druge deležnike.
8. Svetovalni forum lahko na zahtevo Odbora ali Komisije pripravi mnenja, priporočila in pisne prispevke.
9. Svetovalni forum lahko po potrebi ustanovi stalne ali začasne podskupine za preučitev posebnih vprašanj, povezanih s cilji te uredbe.
10. Svetovalni forum pripravi letno poročilo o svojih dejavnostih. To poročilo se objavi.

Člen 68

Znanstveni odbor neodvisnih strokovnjakov

1. Komisija z izvedbenim aktom sprejme določbe o ustanovitvi znanstvenega odbora neodvisnih strokovnjakov (v nadaljnjem besedilu: znanstveni odbor), ki bo podpiral dejavnosti izvrševanja iz te uredbe. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 98(2).
 2. Znanstveni odbor sestavljajo strokovnjaki, ki jih Komisija izbere na podlagi najnovejšega znanstvenega ali tehničnega strokovnega znanja na področju UI, potrebnega za naloge iz odstavka 3, in so sposobni dokazati, da izpolnjujejo vse naslednje pogoje:
 - (a) imajo posebno strokovno znanje in kompetence ter znanstveno ali tehnično strokovno znanje na področju UI;
 - (b) neodvisnost od katerega koli ponudnika sistemov UI ali modelov UI za splošne namene;
 - (c) sposobnost skrbnega, natančnega in objektivnega izvajanja dejavnosti.
- Komisija v posvetovanju z Odborom in v skladu z zahtevanimi potrebami določi število strokovnjakov v znanstvenem odboru ter zagotovi pravično zastopanost spolov in geografsko zastopanost.
3. Znanstveni odbor svetuje Uradu za UI in mu zagotavlja podporo, zlasti v zvezi z naslednjimi nalogami:
 - (a) podpiranje izvajanja in izvrševanja te uredbe v zvezi z modeli UI in sistemi za splošne namene, zlasti z:
 - (i) opozarjanjem Urada za UI na morebitna sistemska tveganja, ki jih lahko na ravni Unije povzročajo modeli UI za splošne namene, v skladu s členom 90;
 - (ii) prispevanjem k razvoju orodij in metodologij za ocenjevanje zmogljivosti modelov UI in sistemov za splošne namene, vključno z merili uspešnosti;
 - (iii) svetovanjem o razvrstitvi modelov UI za splošne namene s sistemskim tveganjem;
 - (iv) svetovanjem o razvrstitvi različnih modelov UI in sistemov za splošne namene;

- (v) prispevanjem k razvoju orodij in predlog;
 - (b) podpiranje dela organov za nadzor trga na njihovo zahtevo;
 - (c) podpiranje čezmejnih dejavnosti nadzora trga iz člena 74(11), brez poseganja v pooblastila organov za nadzor trga;
 - (d) podpiranje Urada za UI pri opravljanju njegovih nalog v okviru zaščitnega postopka Unije na podlagi člena 81.
4. Strokovnjaki znanstvenega odbora svoje naloge opravljajo nepristransko in objektivno ter zagotavljajo zaupnost informacij in podatkov, pridobljenih pri izvajanju njihovih nalog in dejavnosti. Pri opravljanju svojih nalog iz odstavka 3 ne smejo zahtevati ali sprejemati navodil od nikogar. Vsak strokovnjak predloži izjavo o interesih, ki se tudi objavi. Urad za UI vzpostavi sisteme in postopke za aktivno obvladovanje in preprečevanje morebitnih nasprotij interesov.
5. Izvedbeni akt iz odstavka 1 vključuje določbe o pogojih, postopkih in podrobnostih, v skladu s katerimi znanstveni odbor in njegovi člani izdajajo opozorila in zaprosajo Urad za UI za pomoč pri opravljanju svojih nalog.

Člen 69

Dostop držav članic do nabora strokovnjakov

1. Države članice lahko strokovnjake znanstvenega sveta zaprosijo, da jim pomagajo pri dejavnostih izvrševanja iz te uredbe.
2. Od držav članic se lahko zahteva, da plačajo pristojbine za svetovanje in podporo strokovnjakov. Struktura in višina pristojbin ter višina in struktura povračljivih stroškov se določi v izvedbenem aktu iz člena 68(1), pri čemer se upoštevajo cilji ustreznega izvajanja te uredbe, stroškovna učinkovitost in potreba, da se vsem državam članicam zagotovi učinkovit dostop do strokovnjakov.
3. Komisija državam članicam po potrebi omogoči pravočasen dostop do strokovnjakov in zagotovi, da je kombinacija podpornih dejavnosti, ki jih izvajajo podporne strukture Unije za testiranje UI na podlagi člena 84, in strokovnjakov na podlagi tega člena učinkovito organizirana in zagotavlja največjo možno dodano vrednost.

ODDELEK 2

Pristojni nacionalni organi

Člen 70

Imenovanje pristojnih nacionalnih organov in enotne kontaktne točke

1. Za namene te uredbe vsaka država članica kot pristojne nacionalne organe ustanovi ali imenuje vsaj en priglasitveni organ in vsaj en organ za nadzor trga. Ti pristojni nacionalni organi svoja pooblastila izvajajo neodvisno, nepristransko in brez predsodkov, da bi zaščitili objektivnost svojih dejavnosti in nalog ter zagotovili uporabo in izvajanje te uredbe. Člani teh organov se vzdržijo vseh dejanj, ki niso združljiva z njihovimi dolžnostmi. Če se ta načela spoštujejo, lahko take dejavnosti in naloge izvaja eden ali več imenovanih organov v skladu z organizacijskimi potrebami države članice.
2. Države članice Komisiji sporočijo identiteto priglasitvenih organov in organov za nadzor trga ter njihove naloge in vse naknadne spremembe v zvezi s tem. Države članice do 2. avgusta 2025 prek elektronskih komunikacijskih sredstev objavijo informacije o tem, kako je mogoče stopiti v stik s pristojnimi organi in enotnimi kontaktnimi točkami. Države članice imenujejo organ za nadzor trga, ki deluje kot enotna kontaktna točka za to uredbo, in Komisijo uradno obvestijo o identiteti enotne kontaktne točke. Komisija seznam enotnih kontaktnih točk objavi.

3. Države članice zagotovijo, da imajo njihovi pristojni nacionalni organi na voljo ustrezne tehnične, finančne in človeške vire ter infrastrukturo za učinkovito izpolnjevanje svojih nalog na podlagi te uredbe. Pristojni nacionalni organi morajo imeti zlasti zadostno število stalno razpoložljivega osebja, katerega kompetence in strokovno znanje vključujejo poglobljeno razumevanje tehnologij UI, podatkov in računalniške obdelave podatkov, varstva osebnih podatkov, kibernetске varnosti, temeljnih pravic, zdravstvenih in varnostnih tveganj ter poznavanje obstoječih standardov in pravnih zahtev. Države članice vsako leto ocenijo in po potrebi posodobijo zahteve glede usposobljenosti in virov iz tega odstavka.
4. Pristojni nacionalni organi sprejmejo ustrezne ukrepe, da se zagotovi ustrezna raven kibernetске varnosti.
5. Pristojni nacionalni organi pri opravljanju svojih nalog delujejo v skladu z obveznostmi glede zaupnosti iz člena 78.
6. Države članice do 2. avgusta 2025 in nato vsaki dve leti poročajo Komisiji o stanju finančnih in človeških virov, ki so na voljo pristojnim nacionalnim organom, z oceno njihove ustreznosti. Komisija navedene informacije posreduje Odboru v razpravo in morebitna priporočila.
7. Komisija olajšuje izmenjavo izkušenj med pristojnimi nacionalnimi organi.
8. Pristojni nacionalni organi lahko zagotovijo smernice in nasvete o izvajanju te uredbe, zlasti za MSP, vključno z zagonskimi podjetji, pri čemer po potrebi upoštevajo smernice in nasvete Odbora in Komisije. Kadar nameravajo pristojni nacionalni organi zagotoviti smernice in nasvete v zvezi s sistemom UI na področjih, ki jih zajema drugo pravo Unije, se, če je to primerno, posvetujejo s pristojnimi nacionalnimi organi, ki delujejo na podlagi navedenega prava Unije.
9. Kadar institucije, organi, uradi in agencije Unije spadajo na področje uporabe te uredbe, Evropski nadzornik za varstvo podatkov deluje kot pristojni organ za njihov nadzor.

POGLAVJE VIII

PODATKOVNA ZBIRKA EU ZA VISOKOTVEGANE SISTEME UI

Člen 71

Podatkovna zbirka EU za visokotvegane sisteme UI s seznama v Prilogi III

1. Komisija v sodelovanju z državami članicami vzpostavi in vzdržuje podatkovno zbirko EU, ki vsebuje informacije iz odstavkov 2 in 3 tega člena o visokotveganih sistemih UI iz člena 6(2), registriranih v skladu s členoma 49 in 60, ter sisteme UI, ki se ne štejejo za visokotvegane na podlagi člena 6(3) in ki so registrirani v skladu s členom 6(4) in členom 49. Komisija se pri določanju funkcionalnih specifikacij take podatkovne zbirke posvetuje z ustreznimi strokovnjaki, pri posodabljanju funkcionalnih specifikacij take podatkovne zbirke pa z Odborom.
2. Podatke iz Priloge VIII, oddelka A in B, v podatkovno zbirko EU vnese ponudnik ali po potrebi pooblaščen zastopnik.
3. Podatke iz Priloge VIII, oddelek C, v podatkovno zbirko EU vnese uvajalec, ki je javni organ, agencija ali telo ali deluje v njegovem imenu, v skladu s členom 49(3) in (4).
4. Z izjemo oddelka iz člena 49(4) in člena 60(4), točka (c), so informacije v podatkovni zbirki EU, registrirane v skladu s členom 49, dostopne in na voljo javnosti na uporabniku prijazen način. Po informacijah bi se morale dati enostavno iskati in morale bi biti strojno berljive. Informacije, registrirane v skladu s členom 60, 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.
5. Podatkovna zbirka EU vsebuje osebne podatke le, kolikor je to potrebno za zbiranje in obdelavo informacij v skladu s to uredbo. Te informacije vključujejo imena in kontaktne podatke fizičnih oseb, ki so odgovorne za registracijo sistema in imajo pravno pooblastilo za zastopanje ponudnika ali uvajalca, kakor je ustrezno.

6. Komisija je upravljavec podatkovne zbirke EU. Ponudnikom, potencialnim ponudnikom in uvajalcem zagotavlja ustrezno tehnično in upravno podporo. Podatkovna zbirka EU mora biti skladna z veljavnimi zahtevami glede dostopnosti.

POGLAVJE IX

SPREMLJANJE PO DAJANJU NA TRG, IZMENJAVA INFORMACIJ IN NADZOR TRGA

ODDELEK 1

Spremljanje po dajanju na trg

Člen 72

Spremljanje po dajanju na trg s strani ponudnikov in načrt spremljanja po dajanju na trg za visokotvegane sisteme UI

1. Ponudniki vzpostavijo in dokumentirajo sistem spremljanja po dajanju na trg na način, ki je sorazmeren z naravo tehnologij UI in tveganji visokotveganega sistema UI.

2. Sistem spremljanja po dajanju na trg aktivno in sistematično zbira, dokumentira in analizira ustrezne podatke o učinkovitosti visokotveganih sistemov UI skozi celotno življenjsko dobo, ki jih lahko zagotovijo uvajalci ali ki se lahko zberejo prek drugih virov ter ki ponudniku omogočajo, da oceni, ali sistemi UI stalno izpolnjujejo zahteve iz poglavja III, oddelek 2. Kadar je ustrezno, spremljanje po dajanju na trg vključuje analizo interakcije z drugimi sistemi UI. Ta obveznost ne zajema občutljivih operativnih podatkov uvajalcev, 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 s podrobnimi določbami o predlogi za načrt spremljanja po dajanju na trg in s seznamom elementov, ki jih je treba do 2. februarja 2026 vključiti v načrt. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 98(2).

4. Za visokotvegane sisteme UI, zajete v harmonizacijski zakonodaji Unije iz Priloge I, oddelek A – kadar sta sistem in načrt spremljanja po dajanju na trg že vzpostavljena na podlagi navedene zakonodaje in da se zagotovi skladnost, prepreči podvajanje in čim bolj zmanjšajo dodatna bremena – imajo ponudniki možnost, da v sisteme in načrte, ki že obstajajo na podlagi navedene zakonodaje, po potrebi vključijo potrebne elemente, opisane v odstavkih 1, 2 in 3, pri čemer uporabijo predlogo iz odstavka 3, če se s tem doseže enakovredna raven zaščite.

Prvi pododstavek tega odstavka se uporablja tudi za visokotvegane sisteme UI iz Priloge III, točka 5, ki jih dajo na trg ali v uporabo finančne institucije, za katere veljajo zahteve na podlagi prava Unije o finančnih storitvah v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki.

ODDELEK 2

Izmenjava informacij o resnih incidentih

Člen 73

Poročanje o resnih incidentih

1. Ponudniki visokotveganih sistemov UI, ki so dani na trg Unije, organom za nadzor trga držav članic, v katerih je prišlo do navedenega incidenta, poročajo o vsakem resnem incidentu.

2. Poročilo iz odstavka 1 se sestavi takoj, ko ponudnik ugotovi obstoj vzročne zveze med sistemom UI in resnim incidentom ali razumno verjetnost take zveze, v vsakem primeru pa najpozneje 15 dni po tem, ko ponudnik ali, kadar je ustrezno, uvajalec izve za resen incident.

Pri roku za poročanje iz prvega pododstavka se upošteva resnost incidenta.

3. Ne glede na odstavek 2 tega člena se v primeru močno razširjene kršitve ali resnega incidenta, kakor je opredeljen v členu 3, točka 49(b), poročilo iz odstavka 1 predloži nemudoma, najpozneje pa dva dni po tem, ko ponudnik ali, kadar je ustrezno, uvajalec izve za ta incident.

4. Ne glede na odstavek 2 se v primeru smrti osebe poročilo predloži takoj, ko ponudnik ali uvajalec ugotovi ali posumi, da obstaja vzročna zveza med visokotveganim sistemom UI in resnim incidentom, vendar najpozneje 10 dni po datumu, ko ponudnik ali, kadar je ustrezno, uvajalec izve za resen incident.

5. Kadar je to potrebno zaradi pravočasnega poročanja, lahko ponudnik ali, kadar je ustrezno, uvajalec najprej predloži nepopolno začetno poročilo, nato pa predloži še popolnega.

6. Po poročanju o resnem incidentu na podlagi odstavka 1 ponudnik nemudoma izvede potrebne preiskave v zvezi z resnim incidentom in zadevnim sistemom UI. To vključuje oceno tveganja incidenta in popravne ukrepe.

Ponudnik med preiskavami iz prvega pododstavka sodeluje s pristojnimi organi in po potrebi z zadevnim priglašnim organom ter brez predhodne obvestitve pristojnih organov ne izvede nobene raziskave, ki vključuje spremembo zadevnega sistema UI na način, ki bi lahko vplival na poznejšo oceno vzrokov za incident.

7. Zadevni organ za nadzor trga po prejemu uradnega obvestila o resnem incidentu iz člena 3, točka 49(c), obvesti nacionalne javne organe ali telesa iz člena 77(1). Komisija pripravi posebne smernice za lažje izpolnjevanje obveznosti iz odstavka 1 tega člena. Navedene smernice se izdajo do 2. avgusta 2025 in se redno ocenjujejo.

8. Organ za nadzor trga sprejme ustrezne ukrepe, kot je določeno v členu 19 Uredbe (EU) 2019/1020, v sedmih dneh od datuma prejema uradnega obvestila iz odstavka 1 tega člena in upošteva postopke uradnega obveščanja iz navedene uredbe.

9. Za visokotvegane sisteme UI iz Priloge III, ki jih dajejo na trg ali v uporabo ponudniki, za katere veljajo zakonodajni instrumenti Unije, v katerih so določene obveznosti glede poročanja, enakovredne tistim iz te uredbe, se uradno obveščanje o resnih incidentih zahteva le za incidente iz člena 3, točka 49(c).

10. Za visokotvegane sisteme UI, ki so varnostne komponente pripomočkov ali so sami pripomočki, zajeti v uredbah (EU) 2017/745 in (EU) 2017/746, je uradno obvestilo o resnih incidentih omejeno na tiste iz člena 3, točka 49(c), te uredbe in se pošlje pristojnemu nacionalnemu organu, ki ga v ta namen izberejo države članice, v katerih se je navedeni incident zgodil.

11. Pristojni nacionalni organi v skladu s členom 20 Uredbe (EU) 2019/1020 nemudoma uradno obvestijo Komisijo o vsakem resnem incidentu, ne glede na to, ali so v zvezi z njim ukrepali ali ne.

ODDELEK 3

Izvrševanje

Člen 74

Nadzor trga in nadzor sistemov UI na trgu Unije

1. Za sisteme UI, zajete s to uredbo, se uporablja Uredba (EU) 2019/1020. 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(1) te uredbe;
- (b) vsako sklicevanje na proizvod na podlagi Uredbe (EU) 2019/1020 se razume kot sklicevanje na vse sisteme UI, ki spadajo na področje uporabe te uredbe.

2. Organi za nadzor trga v okviru svojih obveznosti poročanja na podlagi člena 34(4) Uredbe (EU) 2019/1020 Komisiji in ustreznim nacionalnim organom za konkurenco vsako leto poročajo o vseh informacijah, ugotovljenih med dejavnostmi nadzora trga, ki bi lahko bile zanimive za uporabo prava Unije o pravilih konkurence. Komisiji vsako leto poročajo tudi o primerih uporabe prepovedanih praks, do katerih je prišlo v zadevnem letu, in o sprejetih ukrepih.

3. Za visokotvegane sisteme UI, ki so povezani s proizvodi, zajetimi v harmonizacijski zakonodaji Unije iz Priloge I, oddelek A, je organ za nadzor trga za namene te uredbe organ, odgovoren za dejavnosti nadzora trga in imenovan v skladu z navedenimi pravnimi akti.

Z odstopanjem od prvega pododstavka in v ustreznih okoliščinah lahko države članice imenujejo drug ustrezen organ, ki deluje kot organ za nadzor trga, če zagotovijo usklajevanje z ustreznimi sektorskimi organi za nadzor trga, odgovornimi za izvrševanje harmonizacijske zakonodaje Unije iz Priloge I.

4. Postopki iz členov 79 do 83 te uredbe se ne uporabljajo za sisteme UI, ki so povezani s proizvodi, zajetimi v harmonizacijski zakonodaji Unije iz Priloge I, oddelek A, če so v takih pravnih aktih že določeni postopki, na podlagi katerih se zagotovi enakovredna raven zaščite in ki imajo isti cilj. V takih primerih se namesto tega uporabijo ustrezni sektorski postopki.

5. Brez poseganja v pooblastila organov za nadzor trga na podlagi člena 14 Uredbe (EU) 2019/1020 lahko organi za nadzor trga, da se zagotovi učinkovito izvrševanje te uredbe, pooblastila iz člena 14(4), točki (d) in (j), navedene uredbe po potrebi izvajajo na daljavo.

6. Za visokotvegane sisteme UI, ki jih dajo na trg ali v uporabo oziroma jih uporabljajo finančne institucije, ki jih ureja pravo Unije o finančnih storitvah, je organ za nadzor trga za namene te uredbe zadevni nacionalni organ, odgovoren za finančni nadzor navedenih institucij na podlagi navedene zakonodaje, če je dajanje sistema UI na trg ali v uporabo oziroma njegova uporaba neposredno povezana z zagotavljanjem navedenih finančnih storitev.

7. Z odstopanjem od odstavka 6 lahko država članica v ustreznih 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, ki jih ureja Direktiva 2013/36/EU, in sodelujejo v enotnem mehanizmu nadzora, vzpostavljenem z Uredbo (EU) št. 1024/2013, bi morali Evropski centralni banki brez odlašanja sporočiti vse informacije, ugotovljene v okviru svojih dejavnosti nadzora trga, ki bi lahko bile zanimive za naloge bonitetnega nadzora Evropske centralne banke, kot so določene v navedeni uredbi.

8. Za visokotvegane sisteme UI iz točke 1 Priloge III k tej uredbi, če se sistemi uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, upravljanja meja ter pravosodja in demokracije, in za visokotvegane sisteme UI iz Priloge III, točke 6, 7 in 8, k tej uredbi države članice kot organe za nadzor trga za namene te uredbe imenujejo bodisi pristojne nadzorne organe za varstvo podatkov na podlagi Uredbe (EU) 2016/679 ali Direktive (EU) 2016/680 bodisi kateri koli drugi organ, ki je imenovan na podlagi enakih pogojev iz členov 41 do 44 Direktive (EU) 2016/680. Dejavnosti nadzora trga nikakor ne vplivajo na neodvisnost pravosodnih organov in tudi drugače ne posegajo v njihove dejavnosti, kadar delujejo v okviru svoje sodne pristojnosti.

9. Kadar institucije, organi, uradi in agencije Unije spadajo na področje uporabe te uredbe, Evropski nadzornik za varstvo podatkov deluje kot njihov organ za nadzor trga, razen v zvezi s Sodiščem Evropske unije, kadar to izvaja svojo sodno pristojnost.

10. Države članice olajšujejo usklajevanje med organi za nadzor trga, imenovanimi na podlagi te uredbe, in drugimi ustreznimi nacionalnimi organi ali telesi, ki nadzorujejo uporabo harmonizacijske zakonodaje Unije iz Priloge I ali drugega prava Unije, ki bi lahko bilo pomembno za visokotvegane sisteme UI iz Priloge III.

11. Organi za nadzor trga in Komisija lahko predlagajo skupne dejavnosti – vključno s skupnimi preiskavami, ki jih izvajajo organi za nadzor trga sami ali skupaj s Komisijo –, katerih cilj je spodbujanje skladnosti, odkrivanje neskladnosti, ozaveščanje ali zagotavljanje smernic v zvezi s to uredbo, kar zadeva posebne kategorije visokotveganih sistemov UI, za katere se ugotovi, da predstavljajo resno tveganje v dveh ali več državah članicah v skladu s členom 9 Uredbe (EU) 2019/1020. Urad za UI zagotavlja usklajevalno podporo za skupne preiskave.

12. 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, ponudniki organom za nadzor trga omogočijo polni dostop do dokumentacije ter naborov učnih, testnih in validacijskih podatkov, ki se uporabljajo za razvoj visokotveganih sistemov UI, vključno z vmesniki za aplikacijsko programiranje (API) ali drugimi ustreznimi tehničnimi sredstvi in orodji, ki omogočajo oddaljeni dostop, kadar je to primerno in ob upoštevanju varnostnih zaščitnih ukrepov.

13. Organom za nadzor trga se dostop do izvirne kode visokotvegane sistema UI odobri na podlagi obrazložene zahteve in samo, če sta izpolnjena oba naslednja pogoja:

- (a) dostop do izvirne kode je potreben za oceno skladnosti visokotvegane sistema UI z zahtevami iz poglavja III, oddelek 2, in
- (b) postopki testiranja ali revizije in preverjanja na podlagi podatkov in dokumentacije, ki jih je predložil ponudnik, so bili izčrpani ali so se izkazali za nezadostne.

14. Vse informacije ali dokumentacija, ki jih pridobijo organi za nadzor trga, se obravnavajo v skladu z obveznostmi glede zaupnosti iz člena 78.

Člen 75

Medsebojna pomoč, nadzor trga in nadzor sistemov UI za splošne namene

1. Kadar sistem UI temelji na modelu UI za splošne namene ter model in sistem razvije isti ponudnik, ima Urad za UI pooblastila za spremljanje in nadzor skladnosti tega sistema UI z obveznostmi iz te uredbe. Urad za UI ima za izvajanje svojih nalog spremljanja in nadzora vsa pooblastila organa za nadzor trga iz tega oddelka in Uredbe (EU) 2019/1020.

2. Kadar imajo ustrezni organi za nadzor trga zadosten razlog, da sisteme UI za splošne namene, ki jih lahko uvajalci neposredno uporabljajo za vsaj en namen, ki je na podlagi te uredbe razvrščen kot veliko tveganje, štejejo za neskladne z zahtevami iz te uredbe, pri izvajanju ocen skladnosti sodelujejo z Uradom za UI ter o tem ustrezno obvestijo Odbor in druge organe za nadzor trga.

3. Kadar organ za nadzor trga ne more zaključiti preiskave visokotvegane sistema UI, ker ne more dostopati do nekaterih informacij, povezanih z modelom UI za splošne namene, čeprav si je ustrezno prizadeval, da bi jih pridobil, lahko Uradu za UI predloži obrazloženo zahtevo, na podlagi katere se zagotovi dostop do teh informacij. V tem primeru Urad za UI organu prosilcu brez odlašanja, v vsakem primeru pa v 30 dneh, zagotovi vse informacije, za katere meni, da so pomembne za ugotovitev, ali je visokotvegani sistem UI neskladen. Organi za nadzor trga zagotavljajo zaupnost informacij, ki jih pridobijo v skladu s členom 78 te uredbe. Smiselno se uporablja postopek iz poglavja VI Uredbe (EU) 2019/1020.

Člen 76

Nadzor testiranja v realnih razmerah s strani organov za nadzor trga

1. Organi za nadzor trga imajo pristojnosti in pooblastila za zagotavljanje, da je testiranje v realnih razmerah skladno s to uredbo.

2. Kadar se testiranje v realnih razmerah izvaja za sisteme UI, ki se nadzorujejo v regulativnem peskovniku za UI na podlagi člena 58, organi za nadzor trga skladnost s členom 60 preverijo v okviru svoje nadzorne vloge za regulativni peskovnik za UI. Ti organi lahko po potrebi dovolijo, da ponudnik ali potencialni ponudnik opravi testiranje v realnih razmerah z odstopanjem od pogojev iz člena 60(4), točki (f) in (g).

3. Kadar potencialni ponudnik, ponudnik ali katera koli tretja oseba obvesti organ za nadzor trga o resnem incidentu ali ima druge razloge za domnevo, da pogoji iz členov 60 in 61 niso izpolnjeni, lahko na svojem ozemlju sprejme katero koli od naslednjih odločitev:

(a) začasno ali dokončno ustavi testiranje v realnih razmerah;

(b) od ponudnika ali potencialnega ponudnika in uvajalca ali potencialnega uvajalca zahteva, da spremenijo katerega od vidikov testiranja v realnih razmerah.

4. Kadar organ za nadzor trga sprejme odločitev iz odstavka 3 tega člena ali izda ugovor v smislu člena 60(4), točka (b), se v odločitvi ali ugovoru navedejo razlogi zanj ali zanj ter kako lahko ponudnik ali potencialni ponudnik izpodbija odločitev ali ugovor.

5. Kadar je ustrezno, kadar organ za nadzor trga sprejme odločitev iz odstavka 3, razloge zanj sporoči organom za nadzor trga iz drugih držav članic, v katerih je bil sistem UI testiran v skladu z načrtom za testiranje.

Člen 77

Pooblastila organov, pristojnih za varstvo temeljnih pravic

1. Nacionalni javni organi ali telesa, ki nadzorujejo ali uveljavljajo spoštovanje obveznosti na podlagi prava Unije o varstvu temeljnih pravic, vključno s pravico do nediskriminacije, so v zvezi z uporabo visokotveganih sistemov UI iz Priloge III pooblašteni, da zahtevajo vso dokumentacijo, ustvarjeno ali hranjeno na podlagi te uredbe, in da v dostopnem jeziku in obliki dostopajo do nje, kadar je dostop do navedene dokumentacije potreben za učinkovito izvrševanje njihovih pooblastil v mejah njihove jurisdikcije. Zadevni javni organ ali telo o vsaki taki zahtevi obvesti organ za nadzor trga zadevne države članice.

2. Vsaka država članica do 2. novembra 2024 določi javne organe ali telesa iz odstavka 1 in seznam teh organov ali teles objavi. Države članice o seznamu uradno obvestijo Komisijo in druge države članice ter seznam redno posodablja.

3. Kadar dokumentacija iz odstavka 1 ne zadošča za ugotovitev, ali je prišlo do kršitve obveznosti na podlagi prava Unije o varstvu temeljnih pravic, lahko javni organ ali telo iz odstavka 1 na podlagi obrazložene zahteve od organa za nadzor trga zahteva, da organizira testiranje visokotvegane sistema UI s tehničnimi sredstvi. Organ za nadzor trga v razumnem času po prejemu zahteve organizira testiranje v tesnem sodelovanju z javnim organom ali telesom, ki je vložilo zahtevo.

4. Vse informacije ali dokumentacija, ki jo nacionalni javni organi ali telesa iz odstavka 1 tega člena pridobijo na podlagi tega člena, se obravnavajo v skladu z obveznostmi glede zaupnosti iz člena 78.

Člen 78

Zaupnost

1. Komisija, organi za nadzor trga in priglasi organi ter vse druge fizične ali pravne osebe, ki sodelujejo pri uporabi te uredbe, v skladu s pravom Unije ali nacionalnim pravom spoštujejo zaupnost informacij in podatkov, pridobljenih pri opravljanju svojih nalog in dejavnosti, tako da varujejo zlasti:

- (a) pravice intelektualne lastnine in zaupne poslovne informacije ali poslovne skrivnosti fizične ali pravne osebe, vključno z izvirno kodo, razen v primerih iz člena 5 Direktive (EU) 2016/943 Evropskega parlamenta in Sveta ⁽⁵⁷⁾;
- (b) učinkovito izvajanje te uredbe, zlasti za namene inšpekcijskih pregledov, preiskav ali revizij;
- (c) javne interese in interese nacionalne varnosti;
- (d) izvedbo kazenskih ali upravnih postopkov;
- (e) podatke, ki so tajni na podlagi prava Unije ali nacionalnega prava.

2. Organi, ki sodelujejo pri uporabi te uredbe na podlagi odstavka 1, zahtevajo samo podatke, ki so nujno potrebni za oceno tveganja, ki ga predstavljajo sistemi UI, in za izvajanje svojih pooblastil v skladu s to uredbo in Uredbo (EU) 2019/1020. V skladu z veljavnim pravom Unije ali nacionalnim pravom uvedejo ustrezne in učinkovite ukrepe za kibernetsko varnost, da zaščitijo varnost in zaupnost pridobljenih informacij in podatkov, ter zbrane podatke izbrišejo takoj, ko niso več potrebni za namen, za katerega so bili pridobljeni.

3. Brez poseganja v odstavka 1 in 2 se informacije, ki se zaupno izmenjujejo med pristojnimi nacionalnimi organi ali med pristojnimi nacionalnimi organi in Komisijo, ne razkrijejo brez predhodnega posvetovanja z izvirnim pristojnim nacionalnim organom in uvajalcem, kadar visokotvegane sisteme UI iz Priloge III, točke 1, 6 ali 7, uporabljajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organi mejne kontrole, organi, pristojni za priseljevanje, ali azilni organi, kadar bi tako razkritje ogrozilo javne in nacionalne varnostne interese. Ta izmenjava informacij ne zajema občutljivih operativnih podatkov v zvezi z dejavnostmi organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organov mejne kontrole in organov, pristojnih za priseljevanje, ali azilnih organov.

Kadar so organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organi, pristojni za priseljevanje, ali azilni organi ponudniki visokotveganih sistemov UI iz Priloge III, točke 1, 6 ali 7, ostane tehnična dokumentacija iz Priloge IV v prostorih teh organov. Ti organi zagotovijo, da lahko organi za nadzor trga iz člena 74(8) in (9), kot je ustrezno, na zahtevo nemudoma dostopajo do dokumentacije ali pridobijo njeno kopijo. Dostop do te dokumentacije ali njene kopije je dovoljen samo osebu organa za nadzor trga, ki ima ustrezno stopnjo varnostnega preverjanja.

4. Odstavki 1, 2 in 3 ne vplivajo na pravice ali obveznosti Komisije, držav članic in njihovih zadevnih organov ter priglašeni organov v zvezi z izmenjavo informacij in razširjanjem opozoril, tudi v okviru čezmejnega sodelovanja, niti ne vplivajo na obveznosti zadevnih strani, da zagotovijo informacije na podlagi kazenskega prava držav članic.

5. Komisija in države članice lahko po potrebi in v skladu z ustreznimi določbami mednarodnih in trgovinskih sporazumov zaupne informacije izmenjajo z regulativnimi organi tretjih držav, s katerimi so sklenile dvostranske ali večstranske dogovore o zaupnosti, ki zagotavljajo ustrezno raven zaupnosti.

Člen 79

Nacionalni postopek za obravnavo sistemov UI, ki predstavljajo tveganje

1. Sistemi UI, ki predstavljajo tveganje, se štejejo za „proizvod, ki predstavlja tveganje“, kot je opredeljen v členu 3, točka 19, Uredbe (EU) 2019/1020, če predstavljajo tveganje za zdravje, varnost ali temeljne pravice oseb.
2. Kadar ima organ za nadzor trga države članice zadosten razlog za domnevo, da sistem UI predstavlja tveganje iz odstavka 1 tega člena, izvede ocenjevanje skladnosti zadevnega sistema UI z vsemi zahtevami in obveznostmi iz te uredbe. Posebno pozornost nameni sistemom UI, ki predstavljajo tveganje za ranljive skupine. Kadar so ugotovljena tveganja za temeljne pravice, organ za nadzor trga obvesti tudi ustrezne nacionalne javne organe ali telesa iz člena 77(1) in z njimi polno sodeluje. Zadevni operaterji po potrebi sodelujejo z organom za nadzor trga in drugimi nacionalnimi javnimi organi ali telesi iz člena 77(1).

⁽⁵⁷⁾ Direktiva (EU) 2016/943 Evropskega parlamenta in Sveta z dne 8. junija 2016 o varstvu nerazkritega strokovnega znanja in izkušenj ter poslovnih informacij (poslovnih skrivnosti) pred njihovo protipravno pridobitvijo, uporabo in razkritjem (UL L 157, 15.6.2016, str. 1).

Kadar organ za nadzor trga sam ali, kadar je ustrezno, v sodelovanju z nacionalnim javnim organom iz člena 77(1) med navedenim ocenjevanjem ugotovi, da sistem UI 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 sistema UI, ga umakne s trga ali odpokliče v roku, ki ga lahko določi organ za nadzor trga, v vsakem primeru pa najpozneje v 15 delovnih dneh ali kot je določeno v ustrezni harmonizacijski zakonodaji Unije.

Organ za nadzor trga o tem obvesti zadevni priglašeni organ. Za ukrepe iz drugega pododstavka tega odstavka 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 sprejetje vseh ustreznih popravnih ukrepov glede vseh zadevnih sistemov UI, katerih dostopnost je omogočil na trgu Unije.

5. Kadar operater sistema UI ne sprejme ustreznih popravnih ukrepov v roku iz odstavka 2, organ za nadzor trga sprejme vse ustreznečasne ukrepe za prepoved ali omejitev dostopnosti sistema UI na svojem nacionalnem trgu ali njegovega dajanja v uporabo, za umik proizvoda ali samostojnega sistema UI z navedenega trga ali za njegov odpoklic. Zadevni organ brez nepotrebnega odlašanja uradno obvesti Komisijo in druge države članice o teh ukrepih.

6. Uradno obvestilo iz odstavka 5 vsebuje vse razpoložljive podrobnosti, zlasti informacije, potrebne za identifikacijo neskladnega sistema UI, poreklo sistema UI in dobavno verigo, 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 enega ali več naslednjih elementov:

(a) neupoštevanja prepovedi praks UI iz člena 5;

(b) neizpolnjevanja zahtev iz poglavja III, oddelek 2, s strani visokotveganega sistema UI;

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

(d) neskladnosti s členom 50.

7. Organi za nadzor trga, 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 sistema UI, v primeru nestrinjanja s priglašnim nacionalnim ukrepom pa tudi o svojih ugovorih.

8. Kadar organ za nadzor trga države članice ali Komisija v treh mesecih po prejemu uradnega obvestila iz odstavka 5 ne poda ugovora glede začasnega ukrepa, ki ga je sprejel organ za nadzor trga druge države članice, se šteje, da je ukrep upravičen. To ne posega v postopkovne pravice zadevnega operaterja v skladu s členom 18 Uredbe (EU) 2019/1020. Trimesečno obdobje iz tega odstavka se skrajša na 30 dni v primeru neupoštevanja prepovedi praks UI iz člena 5 te uredbe.

9. Organi za nadzor trga zagotovijo, da so ustrezni omejevalni ukrepi v zvezi z zadevnim proizvodom ali sistemom UI, kot je umik proizvoda ali sistema UI s trga, sprejeti brez nepotrebnega odlašanja.

Člen 80

Postopek za obravnavo sistemov UI, ki jih je ponudnik v skladu s Prilogo III razvrstil kot sisteme UI brez visokega tveganja

1. Kadar ima organ za nadzor trga zadosten razlog za domnevo, da je sistem UI, ki ga je ponudnik na podlagi člena 6(3) razvrstil kot sistem UI, ki ni visokotvegan, dejansko visokotvegani sistem UI, izvede ocenjevanje zadevnega sistema UI z vidika njegove razvrstitve kot visokotveganega sistema UI na podlagi pogojev iz člena 6(3) in smernic Komisije.

2. Kadar organ za nadzor trga med navedenim ocenjevanjem ugotovi, da gre za visokotvegani sistem UI, od zadevnega ponudnika brez nepotrebne odlašanja zahteva, da sprejme vse potrebne ukrepe za uskladitev sistema UI z zahtevami in obveznostmi iz te uredbe ter da sprejme ustrezne popravne ukrepe v roku, ki ga lahko določi organ za nadzor trga.
3. Kadar organ za nadzor trga meni, da uporaba zadevnega sistema UI ni omejena na njegovo nacionalno ozemlje, Komisijo in druge države članice brez nepotrebne odlašanja obvesti o rezultatih ocenjevanja in ukrepih, ki jih je zahteval od ponudnika.
4. Ponudnik zagotovi sprejetje vseh potrebnih ukrepov za uskladitev sistema UI z zahtevami in obveznostmi iz te uredbe. Kadar ponudnik zadevnega sistema UI v roku iz odstavka 2 tega člena ne uskladi sistema UI z zahtevami in obveznostmi, se ponudniku naložijo globe v skladu s členom 99.
5. Ponudnik zagotovi sprejetje vseh ustreznih popravnih ukrepov glede vseh zadevnih sistemov UI, katerih dostopnost je omogočil na trgu Unije.
6. Kadar ponudnik zadevnega sistema UI ne sprejme ustreznih popravnih ukrepov v roku iz odstavka 2 tega člena, se uporablja člen 79(5) do (9).
7. Kadar organ za nadzor trga med ocenjevanjem na podlagi odstavka 1 tega člena ugotovi, da je ponudnik sistem UI napačno razvrstil kot sistem UI, ki ni visokotvegani, da bi se izognil uporabi zahtev iz poglavja III, oddelek 2, se ponudniku naložijo globe v skladu s členom 99.
8. Organi za nadzor trga lahko pri izvajanju svojih pooblastil za spremljanje uporabe tega člena in v skladu s členom 11 Uredbe (EU) 2019/1020 izvajajo ustrezne preglede, pri čemer upoštevajo zlasti informacije, shranjene v podatkovni zbirki EU iz člena 71 te uredbe.

Člen 81

Zaščitni postopek Unije

1. Kadar organ za nadzor trga države članice v treh mesecih od prejema uradnega obvestila iz člena 79(5) ali v 30 dneh v primeru neupoštevanja prepovedi praks UI iz člena 5 poda ugovor proti ukrepu, ki ga je sprejel drug organ za nadzor trga, ali kadar Komisija meni, da je ukrep v nasprotju s pravom Unije, se Komisija brez nepotrebne odlašanja posvetuje z organom za nadzor trga zadevne države članice in operaterjem ali operaterji ter oceni nacionalni ukrep. Komisija na podlagi rezultatov navedenega ocenjevanja v šestih mesecih ali v 60 dneh v primeru neupoštevanja prepovedi praks UI iz člena 5 od uradnega obvestila iz člena 79(5) odloči, ali je nacionalni ukrep upravičen, in o taki odločitvi uradno obvesti organ za nadzor trga zadevne države članice. Komisija o svoji odločitvi tudi obvesti vse druge organe za nadzor trga.
2. Kadar Komisija meni, da je ukrep, ki ga je sprejela zadevna država članica, upravičen, vse države članice zagotovijo, da v zvezi z zadevnim sistemom UI sprejmejo ustrezne omejevalne ukrepe, kot je zahteva za umik sistema UI z njihovega trga brez nepotrebne odlašanja, in o tem obvestijo Komisijo. Kadar Komisija meni, da nacionalni ukrep ni upravičen, zadevna država članica ukrep preklic in o tem obvesti Komisijo.
3. Kadar se nacionalni ukrep šteje za upravičenega, neskladnost sistema UI pa je pripisana 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 82

Skladni sistemi UI, ki predstavljajo tveganje

1. Kadar organ za nadzor trga države članice po opravljenem ocenjevanju iz člena 79 in posvetovanju z zadevnim nacionalnim javnim organom iz člena 77(1) ugotovi, da visokotvegani sistem UI, ki je skladen s to uredbo, kljub temu predstavlja tveganje za zdravje ali varnost oseb, temeljne pravice ali druge vidike zaščite javnih interesov, od zadevnega operaterja zahteva, da brez nepotrebne odlašanja v roku, ki ga lahko določi organ za nadzor trga, sprejme vse ustrezne ukrepe, s katerimi zagotovi, da zadevni sistem UI, ko je dan na trg ali v uporabo, tega tveganja ne predstavlja več.

2. Ponudnik ali drugi zadevni operater zagotovi sprejetje popravilnih ukrepov glede vseh zadevnih sistemov UI, katerih dostopnost na trgu Unije je omogočil, v roku, ki ga določi organ za nadzor trga države članice iz odstavka 1.
3. Države članice o ugotovitvi na podlagi odstavka 1 nemudoma obvestijo Komisijo in druge države članice. Navedene informacije vključujejo vse razpoložljive podrobnosti, zlasti podatke, potrebne za identifikacijo zadevnega sistema UI, poreklo in dobavno verigo sistema UI, 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. Na podlagi rezultatov navedenega ocenjevanja odloči, ali je ukrep upravičen, in po potrebi predlaga druge ustrezne ukrepe.
5. Komisija svojo odločitev nemudoma sporoči zadevnim državam članicam in ustreznim operaterjem. Obvesti tudi vse druge države članice.

Člen 83

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 določi organ za nadzor trga:
 - (a) oznaka CE ni nameščena v skladu s členom 48;
 - (b) oznaka CE ni bila nameščena;
 - (c) EU izjava o skladnosti iz člena 47 ni pripravljena;
 - (d) EU izjava o skladnosti iz člena 47 ni pravilno pripravljena;
 - (e) registracija v podatkovni zbirki EU iz člena 71 ni bila opravljena;
 - (f) kadar je ustrezno, pooblaščen predstavnik ni bil imenovan;
 - (g) tehnična dokumentacija ni na voljo.
2. Kadar se neskladnost iz odstavka 1 nadaljuje, organ za nadzor trga zadevne države članice nemudoma sprejme vse ustrezne in sorazmerne ukrepe za to, da se omogočanje dostopnosti visokotveganega sistema UI na trgu omeji ali prepove oziroma da se tak sistem brez odlašanja prekliče ali umakne s trga.

Člen 84

Podporne strukture Unije za testiranje UI

1. Komisija za opravljanje nalog na podlagi člena 21(6) Uredbe (EU) 2019/1020 na področju UI imenuje eno ali več podpornih struktur Unije za testiranje UI.
2. Brez poseganja v naloge iz odstavka 1 podporne strukture Unije za testiranje UI na zahtevo Odbora, Komisije ali organov za nadzor trga zagotavljajo tudi neodvisno tehnično ali znanstveno svetovanje.

ODDELEK 4
Pravna sredstva

Člen 85

Pravica do vložitve pritožbe pri organu za nadzor trga

Brez poseganja v druga upravna ali pravna sredstva lahko pritožbe pri ustreznem organu za nadzor trga vloži vsaka fizična ali pravna oseba, ki utemeljeno meni, da je prišlo do kršitve določb te uredbe.

V skladu z Uredbo (EU) 2019/1020 se pritožbe upoštevajo za namen izvajanja dejavnosti nadzora trga in se obravnavajo v skladu z namenskimi postopki, ki jih za to vzpostavijo organi za nadzor trga.

Člen 86

Pravica do obrazložitve postopka odločanja za posamične primere

1. Vsaka prizadeta oseba, za katero velja odločitev, ki jo uvajalec sprejme na podlagi izhodnih podatkov visokotvegane sistema UI iz Priloge III, razen sistemov iz točke 2 Priloge III, in ki ima pravne učinke ali na to osebo podobno znatno vpliva na način, ki ima po njenem mnenju negativne učinke na njeno zdravje, varnost in temeljne pravice, ima pravico od uvajalca pridobiti jasna in smiselna pojasnila o vlogi sistema UI v postopku odločanja in glavnih elementih sprejete odločitve.
2. Odstavek 1 se ne uporablja za uporabo sistemov UI, za katere izjeme od obveznosti iz navedenega odstavka ali omejitve teh obveznosti izhajajo iz prava Unije ali nacionalnega prava v skladu s pravom Unije.
3. Ta člen se uporablja le, če pravica iz odstavka 1 še ni drugje določena na podlagi prava Unije.

Člen 87

Prijava kršitev in zaščita prijaviteljev

Za prijavo kršitev te uredbe in zaščito oseb, ki prijavijo take kršitve, se uporablja Direktiva (EU) 2019/1937.

ODDELEK 5

Nadzor, preiskovanje, izvrševanje in spremljanje v zvezi s ponudniki modelov UI za splošne namene

Člen 88

Izvrševanje obveznosti ponudnikov modelov UI za splošne namene

1. Komisija ima izključne pristojnosti za nadzor in izvrševanje poglavja V, pri čemer upošteva procesna jamstva na podlagi člena 94. Izvajanje teh nalog zaupa Uradu za UI, brez poseganja v organizacijska pooblastila Komisije ter delitev pristojnosti med državami članicami in Unijo na podlagi Pogodb.
2. Brez poseganja v člen 75(3) lahko organi za nadzor trga od Komisije zahtevajo, da izvaja pooblastila iz tega oddelka, kadar je to potrebno in sorazmerno za pomoč pri izpolnjevanju njihovih nalog na podlagi te uredbe.

*Člen 89***Ukrepi spremljanja**

1. Urad za UI lahko za namen opravljanja nalog, ki jih ima na podlagi tega oddelka, sprejme ukrepe, potrebne za spremljanje učinkovitega izvajanja te uredbe in skladnosti z njo s strani ponudnikov modelov UI za splošne namene, vključno z upoštevanjem odobrenih kodeksov prakse.
2. Ponudniki nižje v verigi imajo pravico vložiti pritožbo o domnevni kršitvi te uredbe. Pritožba mora biti ustrezno obrazložena in vsebuje vsaj:
 - (a) kontaktno točko zadevnega ponudnika modela UI za splošne namene;
 - (b) opis relevantnih dejstev, zadevnih določb te uredbe in razloga, zakaj ponudnik nižje v verigi meni, da je zadevni ponudnik modela UI za splošne namene kršil to uredbo;
 - (c) vse druge informacije, za katere ponudnik nižje v verigi, ki je poslal zahtevo, meni, da so pomembne, po potrebi tudi informacije, ki jih je zbral na lastno pobudo.

*Člen 90***Opozorila znanstvenega odbora o sistemskih tveganjih**

1. Znanstveni odbor lahko Uradu za UI pošlje kvalificirano opozorilo, kadar ima razlog za sum, da:
 - (a) model UI za splošne namene predstavlja konkretno prepoznavno tveganje na ravni Unije ali
 - (b) model UI za splošne namene izpolnjuje pogoje iz člena 51.
2. Po takem kvalificiranem opozorilu lahko Komisija prek Urada za UI in po obvestitvi Odbora izvaja pooblastila iz tega oddelka, da bi ocenila zadevo. Urad za UI obvesti Odbor o vseh ukrepih v skladu s členi 91 do 94.
3. Kvalificirano opozorilo mora biti ustrezno obrazloženo in vsebuje vsaj:
 - (a) kontaktno točko ponudnika zadevnega modela UI za splošne namene s sistemskim tveganjem;
 - (b) opis relevantnih dejstev in razlogov za obvestilo znanstvenega odbora;
 - (c) vse druge informacije, za katere znanstveni odbor meni, da so pomembne, po potrebi tudi informacije, ki jih je zbral na lastno pobudo.

*Člen 91***Pooblastilo za zahtevanje dokumentacije in informacij**

1. Komisija lahko od zadevnega ponudnika modela UI za splošne namene zahteva, da predloži dokumentacijo, ki jo je pripravil v skladu s členoma 53 in 55, ali vse dodatne informacije, ki so potrebne za oceno skladnosti ponudnika s to uredbo.
2. Preden se pošlje zahteva za informacije, lahko Urad za UI začne strukturiran dialog s ponudnikom modela UI za splošne namene.
3. Komisija lahko na ustrezno utemeljeno zahtevo znanstvenega odbora ponudniku modela UI za splošne namene pošlje zahtevo za informacije, kadar je dostop do informacij potreben in sorazmeren za izpolnjevanje nalog znanstvenega odbora na podlagi člena 68(2).

4. V zahtevi za informacije se navedeta pravna podlaga in namen zahteve, navedejo se informacije, ki se zahtevajo, določi rok, v katerem je treba informacije predložiti, pa tudi globe iz člena 101 za predložitev nepravilnih, nepopolnih ali zavajajočih informacij.

5. Ponudnik zadevnega modela UI za splošne namene ali njegov zastopnik zagotovi zahtevane informacije. V primeru pravnih oseb, podjetij ali družb ali kadar ponudnik nima pravne osebnosti, zahtevane informacije v imenu zadevnega ponudnika modela UI za splošne namene predložijo osebe, ki so z zakonom ali statutom pooblaščen, da jih zastopajo. Pooblaščen odvjetniki lahko predložijo informacije v imenu svojih strank. Stranke so kljub temu v celoti odgovorne, če so predložene informacije nepopolne, napačne ali zavajajoče.

Člen 92

Pooblastilo za izvajanje ocenjevanja

1. Urad za UI lahko po posvetovanju z Odborom izvede ocenjevanje zadevnega modela UI za splošne namene, da:
 - (a) oceni, ali ponudnik izpolnjuje obveznosti iz te uredbe, kadar informacije, zbrane na podlagi člena 91, niso zadostne, ali
 - (b) razišče sistemska tveganja modelov UI za splošne namene s sistemskim tveganjem na ravni Unije, zlasti na podlagi kvalificiranega obvestila znanstvenega odbora v skladu s členom 90(1), točka (a).
2. Komisija se lahko odloči, da imenuje neodvisne strokovnjake, tudi iz znanstvenega odbora, ustanovljenega na podlagi člena 68, da v njenem imenu izvedejo ocenjevanje. Neodvisni strokovnjaki, imenovani za to nalogo, morajo izpolnjevati merila iz člena 68(2).
3. Za namene odstavka 1 lahko Komisija zahteva dostop do zadevnega modela UI za splošne namene prek API ali drugih ustreznih tehničnih sredstev in orodij, vključno z izvirno kodo.
4. V zahtevi za dostop se navedejo pravna podlaga, namen zahteve in razlogi zanj ter določi rok, v katerem je treba zagotoviti dostop, pa tudi globe iz člena 101, če se dostop ne zagotovi.
5. Zadevni ponudnik modela UI za splošne namene ali njegov predstavnik zagotovi zahtevane informacije. V primeru pravnih oseb pa podjetja ali družbe ali, kadar ponudnik nima pravne osebnosti, osebe, ki so z zakonom ali statutom pooblaščen, da jih zastopajo, zagotovijo zahtevani dostop v imenu zadevnega ponudnika modela UI za splošne namene.
6. Komisija sprejme izvedbene akte, v katerih določi podrobnosti in pogoje ocenjevanja, vključno s podrobnostmi glede vključevanja neodvisnih strokovnjakov, ter postopek za njihov izbor. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 98(2).
7. Preden Urad za UI zaprosi za dostop do zadevnega modela UI za splošne namene, lahko začne strukturiran dialog s ponudnikom modela UI za splošne namene, da bi zbral več informacij o notranjem testiranju modela, notranjih zaščitnih ukrepih za preprečevanje sistemskih tveganj ter drugih notranjih postopkih in ukrepov, ki jih je ponudnik sprejel za zmanjšanje takih tveganj.

Člen 93

Pooblastilo za zahtevanje ukrepov

1. Kadar je to potrebno in primerno, lahko Komisija od ponudnikov zahteva, da:
 - (a) sprejmejo ustrezne ukrepe za izpolnjevanje obveznosti iz členov 53 in 54;

- (b) izvedejo ukrepe za zmanjšanje tveganj, kadar je ocena, izvedena v skladu s členom 92, vzbudila resne in utemeljene pomisleke glede sistemskega tveganja na ravni Unije;
 - (c) omejijo omogočanje dostopnosti modela na trgu, ga umaknejo s trga ali odpokličejo.
2. Preden se zahteva ukrep, lahko Urad za UI začne strukturiran dialog s ponudnikom modela UI za splošne namene.
 3. Če ponudnik modela UI za splošne namene s sistemskim tveganjem med strukturiranim dialogom iz odstavka 2 ponudi zaveze za izvajanje ukrepov za zmanjšanje sistemskih tveganj na ravni Unije, lahko Komisija s sklepom določi, da so te zaveze zavezujoče, in izjavi, da ni nadaljnjih razlogov za ukrepanje.

Člen 94

Postopkovne pravice gospodarskih subjektov v zvezi z modelom UI za splošne namene

Člen 18 Uredbe (EU) 2019/1020 se smiselno uporablja za ponudnike modela UI za splošne namene brez poseganja v bolj specifične postopkovne pravice iz te uredbe.

POGLAVJE X

KODEKSI RAVNANJA IN SMERNICE

Člen 95

Kodeksi ravnanja za prostovoljno uporabo posebnih zahtev

1. Urad za UI in države članice spodbujajo in olajšujejo pripravo kodeksov ravnanja, vključno s pripadajočimi mehanizmi upravljanja, namenjenih spodbujanju prostovoljne uporabe nekaterih ali vseh zahtev iz poglavja III, oddelek 2, za sisteme UI, ki niso visokotvegani sistemi UI, pri čemer upoštevajo razpoložljive tehnične rešitve in najboljše prakse v tem sektorju, ki omogočajo uporabo takih zahtev.
2. Urad za UI in države članice olajšujejo pripravo kodeksov ravnanja v zvezi s prostovoljno uporabo posebnih zahtev za vse sisteme UI, tudi s strani uvajalcev, na podlagi jasnih ciljev in ključnih kazalnikov uspešnosti za merjenje doseganja teh ciljev, vključno z elementi, kot so med drugim:
 - (a) veljavni elementi, določeni v etičnih smernicah Unije za zaupanja vredno umetno inteligenco;
 - (b) ocenjevanje in zmanjšanje vpliva sistemov UI na okoljsko trajnostnost, tudi v zvezi z načrtovanjem in tehnikami energetske učinkovitosti za učinkovito snovanje, učenje in uporabo UI;
 - (c) spodbujanje pismenosti na področju UI, zlasti oseb, ki se ukvarjajo z razvijanjem, delovanjem in uporabo UI;
 - (d) spodbujanje vključujoče in raznolike zasnove sistemov UI, tudi z ustanovitvijo vključujočih in raznolikih skupin razvijalcev ter spodbujanjem vključevanja deležnikov v ta proces;
 - (e) ocenjevanje in preprečevanje negativnega vpliva sistemov UI na ranljive osebe ali skupine ranljivih oseb, tudi kar zadeva dostopnost za invalide, pa tudi na enakost spolov.
3. Kodekse ravnanja lahko pripravijo posamezni ponudniki ali uvajalci sistemov UI ali organizacije, ki jih zastopajo, ali oboji, pri tem pa lahko sodelujejo vsi deležniki ter njihove predstavniške organizacije, vključno z organizacijami civilne družbe in akademskimi krogi. Kodeksi ravnanja lahko zajemajo enega ali več sistemov UI ob upoštevanju podobnosti predvidenega namena zadevnih sistemov.
4. Urad za UI in države članice pri spodbujanju in olajševanju priprave kodeksov ravnanja upoštevajo posebne interese in potrebe MSP, vključno z zagonskimi podjetji.

Člen 96

Smernice Komisije za izvajanje te uredbe

1. Komisija pripravi smernice za praktično izvajanje te uredbe, zlasti glede:
 - (a) izpolnjevanja zahtev in obveznosti iz členov 8 do 15 in člena 25;
 - (b) prepovedanih praks iz člena 5;
 - (c) praktičnega izvajanja določb v zvezi z bistveno spremembo;
 - (d) praktičnega izvajanja obveznosti glede preglednosti iz člena 50;
 - (e) podrobnih informacij o razmerju te uredbe do harmonizacijske zakonodaje Unije iz Priloge I ter drugega ustreznega prava Unije, tudi kar zadeva doslednost pri njihovem izvrševanju;
 - (f) uporabe opredelitve sistema UI iz člena 3, točka 1.

Komisija pri izdaji takih smernic posebno pozornost nameni potrebam MSP, vključno z zagonskimi podjetji, ter lokalnih javnih organov in sektorjev, na katere bo ta uredba najverjetneje vplivala.

Smernice iz prvega pododstavka tega odstavka ustrezno upoštevajo splošno priznane najsodobnejše tehnološke dosežke na področju UI ter ustrezne harmonizirane standarde in skupne specifikacije iz členov 40 in 41 oziroma harmonizirane standarde ali tehnične specifikacije, ki so določeni na podlagi harmonizacijskega prava Unije.

2. Komisija na zahtevo držav članic ali Urada za UI ali na lastno pobudo po potrebi posodobi že sprejete smernice.

POGLAVJE XI

PRENOS POOBLASTIL IN POSTOPEK V ODBORU

Člen 97

Izvajanje prenosa pooblastila

1. Pooblastilo za sprejemanje delegiranih aktov je preneseno na Komisijo pod pogoji, določenimi v tem členu.
2. Pooblastilo za sprejemanje delegiranih aktov iz člena 6(6) in (7), člena 7(1) in (3), člena 11(3), člena 43(5) in (6), člena 47(5), člena 51(3), člena 52(4) ter člena 53(5) in (6) se prenese na Komisijo za obdobje pet let od 1. avgusta 2024. 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. Prenos pooblastila iz člena 6(6) in (7), člena 7(1) in (3), člena 11(3), člena 43(5) in (6), člena 47(5), člena 51(3), člena 52(4) ter člena 53(5) in (6) lahko kadarkoli 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 se pred sprejetjem delegiranega akta posvetuje s strokovnjaki, ki jih imenujejo države članice, v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje.

5. Komisija takoj po sprejetju delegiranega akta o njem sočasno uradno obvesti Evropski parlament in Svet.
6. Delegirani akt, sprejet na podlagi člena 6(6) ali (7), člena 7(1) ali (3), člena 11(3), člena 43(5) ali (6), člena 47(5), člena 51(3), člena 52(4) ali člena 53(5) ali (6), 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 98

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.

POGLAVJE XII

KAZNI

Člen 99

Kazni

1. Države članice v skladu s pogoji iz te uredbe določijo pravila o kaznih in drugih izvršilnih ukrepih, ki lahko vključujejo tudi opozorila in nadenarne ukrepe, ki se uporabljajo za kršitve te uredbe s strani operaterjev, ter sprejmejo vse potrebne ukrepe za zagotovitev njihovega pravnega in učinkovitega izvajanja, pri čemer upoštevajo smernice, ki jih izda Komisija na podlagi člena 96. Te kazni morajo biti učinkovite, sorazmerne in odvračilne. Upoštevajo interese MSP, vključno z zagonskimi podjetji, in njihovo ekonomsko sposobnost.
2. Države članice brez odlašanja in najpozneje do datuma začetka uporabe uradno obvestijo Komisijo o pravilih o kaznih in drugih izvršilnih ukrepih iz odstavka 1 ter o vseh naknadnih spremembah teh pravil.
3. Neupoštevanje prepovedi praks UI iz člena 5 se kaznuje z upravnimi globami v višini do 35 000 000 EUR ali, če je kršitelj podjetje, do 7 % njegovega skupnega svetovnega letnega prometa za preteklo poslovno leto, odvisno od tega, kateri znesek je višji.
4. Neskladnost s katero koli od naslednjih določb, ki se nanašajo na operaterje in priglase organe, razen tistih iz člena 5, se kaznuje z upravnimi globami v višini do 15 000 000 EUR ali, če je kršitelj podjetje, do 3 % njegovega skupnega svetovnega letnega prometa za preteklo poslovno leto, odvisno od tega, kateri znesek je višji:
 - (a) obveznosti ponudnikov na podlagi člena 16;
 - (b) obveznosti pooblaščenih zastopnikov na podlagi člena 22;
 - (c) obveznosti uvoznikov na podlagi člena 23;
 - (d) obveznosti distributerjev na podlagi člena 24;
 - (e) obveznosti uvajalcev na podlagi člena 26;
 - (f) zahteve in obveznosti priglasi organov na podlagi člena 31, člena 33(1), (3) in (4) ali člena 34;
 - (g) obveznosti ponudnikov in uvajalcev glede preglednosti na podlagi člena 50.

5. Če se priglašeni organ ali pristojni nacionalni organ v odgovor na zahtevo predloži nepravilne, nepopolne ali zavajajoče informacije, se izrečejo upravne globe do 7 500 000 EUR ali, če je kršitelj podjetje, do 1 % njegovega skupnega svetovnega letnega prometa za preteklo poslovno leto, odvisno od tega, kateri znesek je višji.
6. V primeru MSP, vključno z zagonskimi podjetji, višina vsake globe iz tega člena ne presega višine odstotkov ali zneska iz odstavkov 3, 4 in 5, odvisno od tega, kateri znesek je nižji.
7. Pri odločanju o naložitvi upravne globe in o znesku upravne globe v vsakem posameznem primeru se upoštevajo vse zadevne okoliščine konkretnega primera, po potrebi pa tudi naslednje:
- (a) vrsta, resnost in trajanje kršitve ter njene posledice, pri čemer se upoštevajo namen sistema UI ter po potrebi število prizadetih oseb in raven škode, ki so jo utrpeli;
 - (b) ali so drugi organi za nadzor trga že naložili upravne globe istemu operaterju za isto kršitev;
 - (c) ali so drugi organi istemu operaterju že naložili upravne globe za kršitve drugega prava Unije ali nacionalnega prava, kadar so take kršitve posledica iste dejavnosti ali opustitve dejanja, ki pomeni zadevno kršitev te uredbe;
 - (d) velikost, letni promet in tržni delež operaterja, ki je storil kršitev;
 - (e) morebitni drugi obteževalni ali olajševalni dejavniki v zvezi z okoliščinami primera, kot so pridobljene finančne koristi ali preprečene izgube, ki neposredno ali posredno izhajajo iz kršitve;
 - (f) stopnja sodelovanja z nacionalnimi pristojnimi organi za odpravo kršitve in zmanjšanje morebitnih škodljivih učinkov kršitve;
 - (g) stopnja odgovornosti operaterja ob upoštevanju tehničnih in organizacijskih ukrepov, ki jih izvaja;
 - (h) način, na katerega so nacionalni pristojni organi seznanjeni s kršitvijo, zlasti pa, ali in v kakšnem obsegu operater kršitev prihlasi;
 - (i) ali je kršitev naklepna ali posledica malomarnosti;
 - (j) ukrepi, ki jih operater sprejme za zmanjšanje škode, ki so jo utrpeli prizadete osebe.
8. Vsaka država članica določi pravila o tem, v kolikšni meri se lahko javnim organom in telesom s sedežem v zadevni državi članici naložijo upravne globe.
9. 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.
10. Za izvajanje pooblastil na podlagi tega člena veljajo ustrezna postopkovna jamstva v skladu s pravom Unije in nacionalnim pravom, vključno z učinkovitimi pravnimi sredstvi in ustreznim pravnim postopkom.
11. Države članice Komisiji vsako leto poročajo o upravnih globah, ki so jih v skladu s tem členom naložile v tistem letu, in o vseh povezanih pravnih sporih ali sodnih postopkih.

Člen 100

Upravne globe za institucije, organe, urade in agencije Unije

1. Evropski nadzornik za varstvo podatkov lahko naloži upravne globe institucijam, organom, uradom in agencijam 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, pri čemer se upoštevajo namen zadevnega sistema UI ter, kadar je ustrezno, število prizadetih oseb in raven škode, ki so jo utrpeli;
- (b) stopnja odgovornosti institucije, organa, urada ali agencije Unije, ob upoštevanju tehničnih in organizacijskih ukrepov, ki jih izvaja;
- (c) ukrepi, ki jih institucija, organ, urad ali agencija Unije sprejme za zmanjšanje škode, ki so jo utrpeli prizadete osebe;
- (d) obseg sodelovanja z Evropskim nadzornikom za varstvo podatkov za odpravo kršitve in zmanjšanje morebitnih škodljivih učinkov kršitve, vključno z upoštevanjem katerega koli ukrepa, ki ga je Evropski nadzornik za varstvo podatkov predhodno odredil zoper zadevno institucijo, organ, urad ali agencijo Unije v zvezi z isto vsebino;
- (e) vse podobne prejšnje kršitve institucije, organa, urada ali agencije Unije;
- (f) kako je Evropski nadzornik za varstvo podatkov izvedel za kršitev, zlasti če in v kakšnem obsegu ga je institucija, organ, urad ali agencija Unije uradno obvestila o kršitvi;
- (g) letni proračun institucije, organa, urada ali agencije Unije.

2. Za neupoštevanje prepovedi praks UI iz člena 5 se kaznuje z upravnimi globami v višini do 1 500 000 EUR.

3. Neskladnost sistema UI s katerimi koli zahtevami ali obveznostmi iz te uredbe, razen tistih iz člena 5, se kaznuje z upravnimi globami v višini do 750 000 EUR.

4. Evropski nadzornik za varstvo podatkov pred sprejetjem odločitev na podlagi tega člena instituciji, organu, uradu ali agenciji 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 zgolj na podlagi elementov in okoliščin, na katere so lahko zadevne strani podale pripombe. Morebitni pritožniki so tesno povezani s postopki.

5. V postopkih se v celoti spoštujejo pravice zadevnih strani do obrambe. Zagotovljena jim je tudi pravica do vpogleda v spis Evropskega nadzornika za varstvo podatkov, pri čemer se upošteva zakonit interes posameznikov ali podjetij za varstvo njihovih osebnih podatkov ali poslovnih skrivnosti.

6. Sredstva, zbrana z naložitvijo glob iz tega člena, pripadajo splošnemu proračunu Unije. Globe ne smejo vplivati na učinkovito delovanje oglobljene institucije, organa, urada ali agencije Unije.

7. Evropski nadzornik za varstvo podatkov Komisijo vsako leto uradno obvesti o upravnih globah, ki jih je naložil na podlagi tega člena, in o vseh pravnih sporih ali sodnih postopkih, ki jih je začel.

Člen 101

Globe, naložene ponudnikom modelov UI za splošne namene

1. Komisija lahko ponudnikom modelov UI za splošne namene naloži globe, ki ne presegajo 3 % njihovega letnega skupnega svetovnega prometa v predhodnem poslovnem letu ali 15 000 000 EUR, odvisno od tega, kateri znesek je višji, če ugotovi, da je ponudnik naklepno ali iz malomarnosti:

- (a) kršil ustrezne določbe te uredbe;
- (b) ni izpolnil zahteve za dokumentacijo ali informacije na podlagi člena 91 ali da je naklepno ali iz malomarnosti predložil nepravilne, nepopolne ali zavajajoče informacije;
- (c) ni ravnal v skladu z ukrepom, zahtevanim na podlagi člena 93;

- (d) Komisiji ni omogočil dostopa do modela UI za splošne namene ali modela UI za splošne namene s sistemskim tveganjem, da bi izvedla ocenjevanje na podlagi člena 92.

Pri določanju zneska globe ali periodične denarne kazni se upoštevajo narava, teža in trajanje kršitve, ustrezno pa se upoštevata tudi načeli sorazmernosti in primernosti. Komisija upošteva tudi zaveze, sprejete v skladu s členom 93(3) ali sprejete v ustreznih kodeksih prakse v skladu s členom 56.

2. Komisija pred sprejetjem odločitve na podlagi odstavka 1 sporoči svoje predhodne ugotovitve ponudniku modela UI za splošne namene tveganjem in mu da priložnost, da se o njih opredeli.
3. Globe, naložene v skladu s tem členom, morajo biti učinkovite, sorazmerne in odvračilne.
4. Informacije o globah, naloženih na podlagi tega člena, se po potrebi sporočijo tudi Odboru.
5. Sodišče Evropske unije ima neomejeno pristojnost za pregled odločitev Komisije o določitvi globe na podlagi tega člena. Naloženo globo lahko prekliče, zniža ali zviša.
6. Komisija sprejme izvedbene akte, v katerih določi podrobne ureditve in postopkovna jamstva za postopke z vidika morebitnega sprejemanja odločitev na podlagi odstavka 1 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 98(2).

POGLAVJE XIII

KONČNE DOLOČBE

Člen 102

Sprememba 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) 2024/1689 Evropskega parlamenta in Sveta (*) se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.

(*) Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).“

Člen 103

Sprememba Uredbe (EU) št. 167/2013

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

„Pri sprejemanju delegiranih aktov na podlagi prvega pododstavka o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/1689 Evropskega parlamenta in Sveta (*), se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.

(*) Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).“

Člen 104

Sprememba Uredbe (EU) št. 168/2013

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

„Pri sprejemanju delegiranih aktov na podlagi prvega pododstavka o umetnointeligentnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/1689 Evropskega parlamenta in Sveta (*), se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.

(*) Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).“

Člen 105

Sprememba Direktive 2014/90/EU

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

„5. Za umetnointeligentne sisteme, ki so varnostne komponente v smislu Uredbe (EU) 2024/1689 Evropskega parlamenta in Sveta (*), Komisija pri izvajanju svojih dejavnosti na podlagi odstavka 1 ter pri sprejemanju tehničnih specifikacij in standardov preskušanja v skladu z odstavkoma 2 in 3 upošteva zahteve iz poglavja III, oddelek 2, navedene uredbe.

(*) Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).“

Člen 106

Sprememba Direktive (EU) 2016/797

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

„12. Pri sprejemanju delegiranih aktov na podlagi odstavka 1 in izvedbenih aktov na podlagi odstavka 11 o umetnointeligentnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/1689 Evropskega parlamenta in Sveta (*), se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.

(*) Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).“

Člen 107

Sprememba Uredbe (EU) 2018/858

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

„4. Pri sprejemanju delegiranih aktov na podlagi odstavka 3 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/1689 Evropskega parlamenta in Sveta (*), se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.

(*) Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).“

Člen 108

Spremembe Uredbe (EU) 2018/1139

Uredba (EU) 2018/1139 se spremeni:

(1) v členu 17 se doda naslednji odstavek:

„3. Brez poseganja v odstavek 2 se pri sprejemanju izvedbenih aktov na podlagi odstavka 1 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/1689 Evropskega parlamenta in Sveta (*), upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.

(*) Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).“;

(2) v členu 19 se doda naslednji odstavek:

„4. Pri sprejemanju delegiranih aktov na podlagi odstavkov 1 in 2 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/1689, se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.“;

(3) v členu 43 se doda naslednji odstavek:

„4. Pri sprejemanju izvedbenih aktov na podlagi odstavka 1 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/1689, se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.“;

(4) v členu 47 se doda naslednji odstavek:

„3. Pri sprejemanju delegiranih aktov na podlagi odstavkov 1 in 2 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/1689, se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.“;

(5) v členu 57 se doda naslednji pododstavek:

„Pri sprejemanju teh izvedbenih aktov o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/1689, se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.“;

(6) v členu 58 se doda naslednji odstavek:

„3. Pri sprejemanju delegiranih aktov na podlagi odstavkov 1 in 2 o umetnointeligentnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/1689, se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.“

Člen 109

Sprememba Uredbe (EU) 2019/2144

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

„3. Pri sprejemanju izvedbenih aktov na podlagi odstavka 2 o umetnointeligentnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/1689 Evropskega parlamenta in Sveta (*), se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.

(*) Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).“

Člen 110

Sprememba Direktive (EU) 2020/1828

V Prilogi I k Direktivi (EU) 2020/1828 Evropskega parlamenta in Sveta ⁽⁵⁸⁾ se doda naslednja točka:

„(68) Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).“

Člen 111

Sistemi UI, ki so že dani na trg ali v uporabo, in modeli UI za splošne namene, ki so že dani na trg

1. Brez poseganja v uporabo člena 5, kakor je predvidena v členu 113(3), točka (a), se sistemi UI, ki so komponente obsežnih informacijskih sistemov, vzpostavljenih s pravnimi akti iz Priloge X, in ki so bili dani na trg ali v uporabo pred 2. avgustom 2027, uskladijo s to uredbo do 31. decembra 2030.

Zahteve iz te uredbe se upoštevajo pri ocenjevanju vsakega obsežnega informacijskega sistema, vzpostavljenega s pravnimi akti iz Priloge X, ki ga je treba izvesti, kot je določeno v teh pravnih aktih in kadar se ti pravni akti nadomestijo ali spremenijo.

2. Brez poseganja v uporabo člena 5, kakor je predvidena v členu 113(3), točka (a), se ta uredba uporablja za operaterje visokotveganih sistemov UI, razen sistemov iz odstavka 1 tega člena, ki so bili dani na trg ali v uporabo pred 2. avgustom 2026, le, če se je pri navedenih sistemih od navedenega datuma bistveno spremenila njihova zasnova. V vsakem primeru ponudniki in uvajalci visokotveganih sistemov UI, ki naj bi jih uporabljali javni organi, sprejmejo potrebne ukrepe za izpolnitev zahtev in obveznosti iz te uredbe do 2. avgusta 2030.

3. Ponudniki modelov UI za splošne namene, ki so bili dani na trg pred 2. avgustom 2025, sprejmejo potrebne ukrepe za izpolnitev obveznosti iz te uredbe do 2. avgusta 2027.

⁽⁵⁸⁾ Direktiva (EU) 2020/1828 Evropskega parlamenta in Sveta z dne 25. novembra 2020 o zastopniških tožbah za varstvo kolektivnih interesov potrošnikov in razveljavitvi Direktive 2009/22/ES (UL L 409, 4.12.2020, str. 1).

Člen 112

Ocena in pregled

1. Komisija enkrat letno po začetku veljavnosti te uredbe in do konca trajanja prenosa pooblastila iz člena 97 oceni potrebo po spremembi seznama iz Priloge III in seznama prepovedanih praks UI iz člena 5. Komisija ugotovitve te ocene predloži Evropskemu parlamentu in Svetu.
2. Komisija do 2. avgusta 2028 in nato vsaka štiri leta oceni ter Evropskemu parlament in Svetu poroča o naslednjem:
 - (a) potrebi po spremembah za razširitev obstoječih razdelkov področij ali dodajanje novih razdelkov področij v Prilogi III;
 - (b) spremembah seznama sistemov UI, pri katerih so potrebni dodatni ukrepi za preglednost, iz člena 50;
 - (c) spremembah za povečanje učinkovitosti sistema nadzora in upravljanja.
3. Komisija do 2. avgusta 2029 ter nato vsaka štiri leta Evropskemu parlamentu in Svetu predloži poročilo o oceni in pregledu te uredbe. Poročilo vključuje oceno strukture izvrševanja in morebitno potrebo, da agencija Unije odpravi vse ugotovljene pomanjkljivosti. Temu poročilu na podlagi ugotovitev po potrebi priloži predlog za spremembo te uredbe. Poročila se objavijo.
4. V poročilih iz odstavka 2 se posebna pozornost nameni naslednjemu:
 - (a) stanju finančnih, tehničnih in človeških virov pristojnih nacionalnih organov, da se zagotovi učinkovito izvajanje nalog, dodeljenih s to uredbo;
 - (b) stanju kazni, zlasti upravnih glob iz člena 99(1), ki jih države članice uporabljajo za kršitve te uredbe;
 - (c) sprejetim harmoniziranim standardom in skupnim specifikacijam, razvitim v podporo tej uredbi;
 - (d) številu podjetij, ki vstopijo na trg po začetku uporabe te uredbe, in koliko od njih je MSP.
5. Komisija do 2. avgusta 2028 oceni delovanje Urada za UI, ali je Urad za UI dobil zadostna pooblastila in pristojnosti za izpolnjevanje svojih nalog ter ali bi bilo ustrezno in potrebno za pravilno izvajanje in izvrševanje te uredbe nadgraditi Urad za UI in njegove pristojnosti izvrševanja ter povečati njegove vire. Komisija poročilo o svoji oceni predloži Evropskemu parlamentu in Svetu.
6. Komisija do 2. avgusta 2028 in nato vsaka štiri leta predloži poročilo o pregledu napredka pri razvoju standardizacijskih dokumentov o energetske učinkovitosti razvoju modelov UI za splošne namene in oceni potrebo po nadaljnjih ukrepih ali dejavnostih, vključno z zavezujočimi ukrepi ali dejavnostmi. Poročilo predloži Evropskemu parlamentu in Svetu ter ga objavi.
7. Komisija do 2. avgusta 2028 ter nato vsaka tri leta oceni vpliv in učinkovitost prostovoljnih kodeksov ravnanja za spodbujanje uporabe zahtev iz poglavja III, oddelek 2, za sisteme UI, ki niso visokotvegani sistemi UI, in morebitnih drugih dodatnih zahtev za sisteme UI, ki niso visokotvegani sistemi UI, tudi kar zadeva okoljsko trajnostnost.
8. Za namene odstavkov 1 do 7 Odbor, države članice in pristojni nacionalni organi Komisiji na njeno zahtevo in brez nepotrebnega odlašanja zagotovijo informacije.
9. Komisija pri izvajanju ocenjevanj in pregledov iz odstavkov 1 do 7 upošteva stališča in ugotovitve Odbora, Evropskega parlamenta, Sveta ter drugih ustreznih organov ali virov.

10. Komisija po potrebi predloži ustrezne predloge za spremembo te uredbe, zlasti ob upoštevanju razvoja tehnologije, učinkov sistemov UI na zdravje in varnost ter na temeljne pravice in glede na stanje napredka v informacijski družbi.

11. Urad za UI se zaveže, da bo za usmerjanje ocenjevanj in pregledov iz odstavkov 1 do 7 tega člena razvil objektivno in participativno metodologijo za ocenjevanje stopenj tveganja na podlagi meril iz ustreznih členov ter za vključitev novih sistemov na:

- (a) seznam iz Priloge III, vključno z razširitvijo obstoječih razdelkov področij ali dodajanjem novih razdelkov področij v navedeni prilogi;
- (b) seznam prepovedanih praks iz člena 5 in
- (c) seznam sistemov UI, pri katerih so potrebni dodatni ukrepi za preglednost na podlagi člena 50.

12. Pri vsaki spremembi te uredbe na podlagi odstavka 10 ali zadevnih delegiranih ali izvedbenih aktov, ki se nanašajo na sektorsko harmonizacijsko zakonodajo Unije iz oddelka B Priloge I se upoštevajo regulativne posebnosti vsakega sektorja in obstoječi mehanizmi upravljanja, ugotavljanja skladnosti in izvrševanja ter organi, ki so določeni v njih.

13. Komisija do 2. avgusta 2031 oceni izvajanje te uredbe, pri čemer upošteva prva leta njene uporabe, ter o tem poroča Evropskemu parlamentu, Svetu in Evropskemu ekonomsko-socialnemu odboru. Na podlagi ugotovitev se navedenemu poročilu po potrebi priloži predlog za spremembo te uredbe v zvezi s strukturo izvrševanja in potrebo, da agencija Unije odpravi vse ugotovljene pomanjkljivosti.

Člen 113

Začetek veljavnosti in uporaba

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Uporablja se od 2. avgusta 2026.

Vendar se:

- (a) poglavji I in II začneta uporabljati od 2. februarja 2025;
- (b) poglavje III, oddelek 4, poglavje V, poglavje VII in poglavje XII ter člen 78 uporabljajo od 2. avgusta 2025, razen člena 101;
- (c) člen 6(1) in ustrezne obveznosti iz te uredbe uporabljajo od 2. avgusta 2027.

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

V Bruslju, 13. junija 2024

Za Evropski parlament
predsednica
R. METSOLA

Za Svet
predsednik
M. MICHEL

PRILOGA I

Seznam harmonizacijske zakonodaje Unije

Oddelek A. Seznam harmonizacijske zakonodaje Unije, ki temelji na novem zakonodajnem okviru

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);
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

13. 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);
14. 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);
15. 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);

16. 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);
17. 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);
18. 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);
19. 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);
20. 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 člena 2(1), točki (a) in (b), navedene uredbe, kar zadeva brezpilotne zrakoplove in njihove motorje, propelerje, dele in opremo za njihovo daljinsko upravljanje.

PRILOGA II

Seznam kaznivih dejanj iz člena 5(1), prvi pododstavek, točka (h)(iii)

Kazniva dejanja iz člena 5(1), prvi pododstavek, točka (h)(iii):

- terorizem,
 - trgovina z ljudmi,
 - spolno izkoriščanje otrok in otroška pornografija,
 - nedovoljena trgovina s prepovedanimi drogami ali psihotropnimi snovmi,
 - nedovoljena trgovina z orožjem, strelivom ali eksplozivi,
 - umor, huda telesna poškodba,
 - nedovoljena trgovina s človeškimi organi ali tkivi,
 - nedovoljena trgovina z jedrskimi ali radioaktivnimi snovmi,
 - ugrabitev, protipraven odvzem prostosti ali zajetje talcev,
 - kazniva dejanja v pristojnosti Mednarodnega kazenskega sodišča,
 - nezakonit zaseg zrakoplova ali plovila,
 - posilstvo,
 - okoljska kriminaliteta,
 - organiziran ali oborožen rop,
 - sabotaža,
 - sodelovanje v hudodelski združbi, ki je vpletena v eno ali več zgoraj navedenih kaznivih dejanj.
-

PRILOGA III

Visokotvegani sistemi UI iz člena 6(2)

Visokotvegani sistemi UI na podlagi člena 6(2) so sistemi UI, navedeni na seznamu za katero koli od naslednjih področij:

1. biometrika, kolikor je njena uporaba dovoljena na podlagi ustreznega prava Unije ali nacionalnega prava:
 - (a) sistemi za biometrično identifikacijo na daljavo.

To ne vključuje sistemov UI za biometrično preverjanje, katerih edini namen je potrditi, da je določena fizična oseba res ta, za katero se predstavlja;
 - (b) sistemi UI za biometrično kategorizacijo glede na občutljive ali zaščitene lastnosti ali značilnosti na podlagi sklepanja na te lastnosti ali značilnosti;
 - (c) sistemi UI za prepoznavanje čustev;
2. kritična infrastruktura: sistemi UI za uporabo kot varnostne komponente pri upravljanju in delovanju kritične digitalne infrastrukture, cestnega prometa ali pri oskrbi z vodo, plinom, ogrevanjem ali električno energijo;
3. izobraževanje in poklicno usposabljanje:
 - (a) sistemi UI za določanje dostopa ali sprejema ali za razvrščanje fizičnih oseb v izobraževalne ustanove in ustanove za poklicno usposabljanje na vseh ravneh;
 - (b) sistemi UI za evalvacijo učnih izidov, tudi kadar se ti izidi uporabljajo za usmerjanje učnega procesa fizičnih oseb v izobraževalnih ustanovah in ustanovah za poklicno usposabljanje na vseh ravneh;
 - (c) sistemi UI za ocenjevanje ustrezne ravni izobrazbe, ki jo bo posameznik prejel ali do katere bo lahko dostopal v okviru ali znotraj izobraževalnih ustanov in ustanov za poklicno usposabljanje na vseh ravneh;
 - (d) sistemi UI za spremljanje in ugotavljanje prepovedanega vedenja učencev in študentov med opravljanjem preizkusov znanja v okviru ali znotraj izobraževalnih ustanov in ustanov za poklicno usposabljanje na vseh ravneh;
4. zaposlovanje, upravljanje delavcev in dostop do samozaposlitve:
 - (a) sistemi UI za zaposlovanje ali izbor fizičnih oseb, zlasti za ciljno oglaševanje delovnih mest, analizo in filtriranje prijav za zaposlitev ter ocenjevanje kandidatov;
 - (b) sistemi UI za odločanje o pogojih delovnih razmerij, napredovanju ali prenehanju delovnih 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:
 - (a) sistemi UI, 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, vključno z zdravstvenimi storitvami, ter za dodelitev, zmanjšanje, preklic ali povračilo takih ugodnosti in storitev;
 - (b) sistemi UI za ocenjevanje kreditne sposobnosti fizičnih oseb ali določanje njihove kreditne ocene, razen sistemov UI, ki se uporabljajo za odkrivanje finančnih goljufij;
 - (c) sistemi UI za oceno tveganja in oblikovanje cen v zvezi s fizičnimi osebami v primeru življenjskega in zdravstvenega zavarovanja;

- (d) sistemi UI za ocenjevanje in razvrščanje nujnih klicev fizičnih oseb ali za napotitev služb za ukrepanje ob nesrečah, vključno s policijo, gasilci in medicinsko pomočjo, ali določanje prednosti pri njihovi napotitvi, ter sistemi za nujno zdravstveno triažo pacientov;
6. preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, kolikor je njihova uporaba dovoljena na podlagi zadevnega prava Unije ali nacionalnega prava:
- (a) sistemi UI, ki naj bi jih uporabljali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije v podporo organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali v njihovem imenu za oceno tveganja, da fizična oseba postane žrtev kaznivih dejanj;
- (b) sistemi UI, ki naj bi jih kot poligrafe ali podobna orodja uporabljali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije v podporo organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj;
- (c) sistemi UI, ki naj bi jih uporabljali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije v podporo organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj za ocenjevanje zanesljivosti dokazov med preiskavo ali pregonom kaznivih dejanj;
- (d) sistemi UI, ki naj bi jih uporabljali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije v podporo organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj za oceno tveganja, ali bi fizična oseba storila ali ponovila kaznivo dejanje, ne samo na podlagi oblikovanja profilov fizičnih oseb iz člena 3(4) Direktive (EU) 2016/680, ali za oceno osebnostnih lastnosti in značilnosti ali preteklega kriminalnega ravnanja fizičnih oseb ali skupin;
- (e) sistemi UI, ki naj bi jih uporabljali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije v podporo organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj za oblikovanje profilov fizičnih oseb iz člena 3(4) Direktive (EU) 2016/680;
7. migracije, azil in upravljanje nadzora meje, kolikor je njihova uporaba dovoljena na podlagi zadevnega prava Unije ali nacionalnega prava:
- (a) sistemi UI, ki naj bi jih uporabljali pristojni javni organi ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije kot poligrafe ali podobna orodja;
- (b) sistemi UI, ki naj bi jih uporabljali pristojni javni organi ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije 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;
- (c) sistemi UI, ki naj bi jih uporabljali pristojni javni organi ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije za pomoč pristojnim javnim organom pri preučitvi prošenj za azil, vizume in dovoljenja za prebivanje ter s tem povezanih pritožb glede upravičenosti fizičnih oseb, ki so zaprosile za status, vključno s pripadajočimi ocenami zanesljivosti dokazov;
- (d) sistemi UI, ki naj bi jih uporabljali pristojni javni organi ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije, v okviru migracij, azila in upravljanja nadzora meja za namene odkrivanja, prepoznavanja ali identifikacije fizičnih oseb, z izjemo preverjanja potnih listin;
8. pravosodje in demokratični procesi:
- (a) sistemi UI, ki naj bi jih uporabljal sodni organ ali naj bi se uporabljali v njegovem imenu za pomoč sodnemu organu pri raziskovanju in razlagi dejstev in prava ter pri uporabi prava za konkreten sklop dejstev ali ki naj bi se uporabljali na podoben način pri alternativnem reševanju sporov;

- (b) sistemi UI za vplivanje na izid volitev ali referendumov ali na volilno vedenje fizičnih oseb pri glasovanju na volitvah ali referendumih. To ne vključuje sistemov UI, katerih izhodnim podatkom fizične osebe niso neposredno izpostavljene, kot so orodja, ki se uporabljajo za organizacijo, optimizacijo ali strukturiranje političnih kampanj z upravnega in logističnega vidika.
-

PRILOGA IV

Tehnična dokumentacija iz člena 11(1)

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

1. splošni opis sistema UI, vključno z:
 - (a) njegovim predvidenim namenom, imenom ponudnika in različico sistema, ki odraža njegovo razmerje do prejšnjih različic;
 - (b) opisom, na kakšen način je sistem UI v interakciji s strojno ali programsko opremo, vključno z drugimi sistemi UI, ki niso del samega sistema UI, ali na kakšen način bi se lahko uporabljal za takšno interakcijo, kadar je ustrezno;
 - (c) različicami ustrezne programske opreme ali strojne programske opreme in morebitnimi zahtevami v zvezi s posodobitvami različice;
 - (d) opisom vseh oblik, v katerih je sistem UI dan na trg ali v uporabo, kot so programski paketi, vgrajeni v strojno opremo, prenosi ali API;
 - (e) opisom strojne opreme, na kateri naj bi sistem UI deloval;
 - (f) kadar je sistem UI sestavni del proizvodov, fotografijami ali ilustracijami, ki prikazujejo zunanje značilnosti, oznake in notranjo razporeditev teh proizvodov;
 - (g) osnovnim opisom uporabniškega vmesnika, ki se zagotovi uvajalcu;
 - (h) navodili za uvajalca za uporabo in, kadar je ustrezno, osnovnim opisom uporabniškega vmesnika, ki se zagotovi uvajalcu;
2. podroben opis elementov sistema UI in postopka za njegov razvoj, vključno z:
 - (a) metodami in ukrepi, izvedenimi za razvoj sistema UI, 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;
 - (b) specifikacijami zasnove sistema, in sicer splošno logiko sistema UI 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 razvrstitve; informacijami o tem, kaj naj bi sistem optimiziral in kako pomembni so različni parametri; opisom pričakovanih izhodnih podatkov sistema in njihovo kakovostjo; odločitvami o morebitnih kompromisih glede tehničnih rešitev, sprejetih za izpolnitev zahtev iz poglavja III, oddelek 2;
 - (c) opisom arhitekture sistema, ki pojasnjuje, kako se sestavni deli programske opreme medsebojno nadgrajujejo ali navezujejo in kako so vključeni v celotno obdelavo; računalniškimi viri, uporabljenimi za razvoj, učenje, testiranje in validacijo sistema UI;
 - (d) 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);
 - (e) oceno potrebnih ukrepov za človeški nadzor v skladu s členom 14, vključno z oceno tehničnih ukrepov, ki jih uvajalci potrebujejo za lažjo razlago izhodnih podatkov sistemov UI, v skladu s členom 13(3), točka (d);
 - (f) kadar je ustrezno, podrobnim opisom vnaprej določenih sprememb sistema UI in njegove zmogljivosti skupaj z vsemi ustreznimi informacijami v zvezi s tehničnimi rešitvami, sprejetimi za zagotovitev stalne skladnosti sistema UI z ustreznimi zahtevami iz poglavja III, oddelek 2;
 - (g) uporabljenimi postopki validacije in testiranja, vključno z informacijami o uporabljenih validacijskih in testnih podatkih ter njihovih glavnih značilnostih; metrikami, uporabljenimi za merjenje točnosti, robustnosti in skladnosti z drugimi ustreznimi zahtevami iz poglavja III, oddelek 2, pa tudi za merjenje potencialno diskriminatornih vplivov; dnevnik testiranj in vsemi poročili o testiranjih z datumi in podpisi odgovornih oseb, tudi v zvezi z vnaprej določenimi spremembami iz točke (f);

- (h) sprejetimi ukrepi za kibernetско varnost;
3. podrobne informacije o spremljanju, delovanju in nadzoru sistema UI, zlasti glede: njegovih kapacitet in omejitev zmogljivosti, 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 sistema UI; potrebnih ukrepov za človeški nadzor v skladu s členom 14, vključno s sprejetimi tehničnimi ukrepi, ki uvajalcem omogočajo lažjo razlago izhodnih podatkov sistemov UI; specifikacij o vhodnih podatkih, če je to primerno;
 4. opis ustreznosti metrik zmogljivosti za posamezni sistem UI;
 5. podroben opis sistema obvladovanja tveganja v skladu s členom 9;
 6. opis pomembnih sprememb sistema, ki jih je v njegovem življenjskem ciklu naredil ponudnik;
 7. seznam harmoniziranih standardov, ki so bili delno ali v celoti uporabljeni in katerih sklici so bili objavljeni v *Uradnem listu Evropske unije*; kadar taki harmonizirani standardi niso bili uporabljeni, podroben opis rešitev, sprejetih za izpolnitev zahtev iz poglavja III, oddelek 2, vključno s seznamom drugih uporabljenih ustreznih standardov in tehničnih specifikacij;
 8. izvod EU izjave o skladnosti iz člena 47;
 9. podroben opis vzpostavljenega sistema za ocenjevanje zmogljivosti sistema UI v obdobju po dajanju na trg v skladu s členom 72, vključno z načrtom spremljanja po dajanju na trg iz člena 72(3).
-

PRILOGA V

EU izjava o skladnosti

EU izjava o skladnosti iz člena 47 vsebuje vse naslednje podatke:

1. ime in vrsto sistema UI ter morebitne dodatne nedvoumne navedbe, ki omogočajo identifikacijo in sledljivost sistema UI;
2. ime in naslov ponudnika ali, kadar je ustrezno, njegovega pooblaščenega zastopnika;
3. izjavo, da je za izdajo EU izjave o skladnosti iz člena 47 odgovoren izključno ponudnik;
4. izjavo, da je sistem UI v skladu s to uredbo in po potrebi z drugimi določbami ustreznega prava Unije, ki določa izdajanje EU izjave o skladnosti iz člena 47;
5. kadar sistem UI vključuje obdelavo osebnih podatkov, izjavo, da je sistem UI skladen z uredbama (EU) 2016/679 in (EU) 2018/1725 ter Direktivo (EU) 2016/680;
6. sklice na morebitne uporabljene ustrezne harmonizirane standarde ali druge skupne specifikacije, v zvezi s katerimi je navedena skladnost;
7. kadar je ustrezno, ime in identifikacijsko številko priglašene organa, opis postopka ugotavljanja skladnosti in identifikacijo izdanega certifikata;
8. kraj in datum izdaje izjave, ime in funkcijo podpisnika ter navedbo, za koga ali 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, 3 in 4.
 2. Ponudnik preveri, ali je vzpostavljeni sistem upravljanja kakovosti usklajen z zahtevami iz člena 17.
 3. Ponudnik preuči informacije iz tehnične dokumentacije, da bi ocenil skladnost sistema UI z ustreznimi bistvenimi zahtevami iz poglavja III, oddelek 2.
 4. Ponudnik tudi preveri, ali sta postopek zasnov in razvoja sistema UI ter njegovo spremljanje po dajanju na trg iz člena 72 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 do 5.

2. Pregled

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

3. Sistem upravljanja kakovosti

3.1. Zahtevek ponudnika vključuje:

- (a) ime in naslov ponudnika in, če je zahtevek vložil pooblaščen zastopnik, tudi njegovo ime in naslov;
- (b) seznam sistemov UI, zajetih v istem sistemu upravljanja kakovosti;
- (c) tehnično dokumentacijo za vse sisteme UI, zajete v istem sistemu upravljanja kakovosti;
- (d) dokumentacijo v zvezi s sistemom upravljanja kakovosti, ki zajema vse vidike iz člena 17;
- (e) opis postopkov, ki so vzpostavljeni za ohranjanje ustreznosti in učinkovitosti sistema upravljanja kakovosti;
- (f) 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 obvesti priglašeni organ o vseh načrtovanih spremembah odobrenega sistema upravljanja kakovosti ali seznamu sistemov UI, 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 obrazloženo odločitev o oceni.

4. Pregled tehnične dokumentacije

4.1. Ponudnik poleg zahtevka iz točke 3 pri priglašenem organu, ki ga izbere sam, vloži zahtevek za oceno tehnične dokumentacije v zvezi s sistemom UI, ki ga namerava dati na trg ali v uporabo in ki je zajet v sistemu upravljanja kakovosti iz točke 3.

4.2. Zahtevek vključuje:

- (a) ime in naslov ponudnika;
- (b) pisno izjavo, da enak zahtevek ni bil predložen nobenemu drugemu priglašenemu organu;
- (c) tehnično dokumentacijo iz Priloge IV.

- 4.3. Priglašeni organ pregleda tehnično dokumentacijo. Kadar je primerno in omejeno na to, kar je potrebno za izpolnjevanje njegovih nalog, se priglašenemu organu omogoči neomejen dostop do uporabljenih naborov učnih, validacijskih in testnih podatkov, tudi, kadar je ustrezno in ob uporabi ustreznih varoval, prek API ali z drugimi ustreznimi tehničnimi 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 dodatna testiranja, da se omogoči ustrezna ocena skladnosti sistema UI z zahtevami iz poglavja III, oddelek 2. Kadar priglašeni organ ni zadovoljen s testiranjem, ki jih je opravil ponudnik, neposredno sam opravi ustrezna testiranja, če je to primerno.
- 4.5. Potem ko so bili izkoriščeni in so se izkazali za nezadostne vsi drugi razumni načini preverjanja skladnosti, se priglašenemu organu na obrazloženo zahtevo dovoli tudi dostop do učnih in naučenih modelov sistema UI, vključno z njegovimi relevantnimi parametri, kadar je to potrebno za oceno skladnosti visokotvegane sistema UI z zahtevami iz naslova III, poglavje 2. Za tak dostop se uporablja veljavno pravo Unije in nacionalno pravo o intelektualni lastnini in poslovnih skrivnostih.
- 4.6. Odločitev priglašene organa se uradno sporoči ponudniku ali njegovemu pooblaščenemu zastopniku. Obvestilo vsebuje ugotovitve ocenjevanja tehnične dokumentacije in obrazloženo odločitev o oceni.

Kadar je sistem UI skladen z zahtevami iz poglavja III, oddelek 2, priglašeni organ izda certifikat Unije o oceni tehnične dokumentacije. V certifikatu so navedeni ime in naslov ponudnika, ugotovitve pregleda, morebitni pogoji za njegovo veljavnost in podatki, potrebni za identifikacijo sistema UI.

V certifikatu in njegovih prilogah so navedene vse potrebne informacije za oceno skladnosti sistema UI in, kadar je ustrezno, nadzor sistema UI med uporabo.

Kadar sistem UI ni skladen z zahtevami iz poglavja III, oddelek 2, priglašeni organ zavrne izdajo certifikata Unije o oceni tehnične dokumentacije ter o tem obvesti vlagatelja in svojo zavrnitev podrobno utemelji.

Kadar sistem UI ne izpolnjuje zahtev glede podatkov, uporabljenih za njegovo učenje, bo pred zahtevkom za novo ugotavljanje skladnosti potrebno ponovno učenje sistema UI. V tem primeru obrazložena odločitev priglašene organa o oceni, s katero zavrne izdajo certifikata Unije o oceni tehnične dokumentacije, vsebuje specifične premisleke glede kakovosti podatkov, uporabljenih za učenje sistema UI, zlasti glede razlogov za neskladnost.
- 4.7. Vsako spremembo sistema UI, ki bi lahko vplivala na njegovo skladnost z zahtevami ali predvidenim namenom, oceni priglašeni organ, ki je izdal certifikat Unije o oceni tehnične dokumentacije. Ponudnik obvesti ta priglašeni organ o svoji nameri, da bo uvedel katero koli od navedenih sprememb, obvesti pa ga 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 certifikata Unije o oceni tehnične dokumentacije. V slednjem primeru priglašeni organ oceni spremembe, uradno obvesti ponudnika o svoji odločitvi in mu, kadar so spremembe odobrene, izda dopolnilo certifikata Unije 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 ocene ponudnik priglašenemu organu omogoči dostop do prostorov, v katerih potekajo zasnova, razvoj in testiranje sistemov UI. Poleg tega mu posreduje vse potrebne informacije.
 - 5.3. Priglašeni organ opravlja redne revizije, s čimer zagotovi, da ponudnik vzdržuje in izvaja sistem upravljanja kakovosti, poročila o teh revizijah pa predloži ponudniku. V okviru teh revizij lahko priglašeni organ izvede dodatna testiranja sistemov UI, za katere je bil izdan certifikat Unije o oceni tehnične dokumentacije.

PRILOGA VIII

Informacije, ki se predložijo ob registraciji visokotveganih sistemov UI v skladu s členom 49

Oddelek A – Informacije, ki jih predložijo ponudniki visokotveganih sistemov UI v skladu s členom 49(1)

V zvezi z visokotveganimi sistemi UI, ki se registrirajo v skladu s členom 49(1), se predložijo in nato posodablajo naslednje informacije:

1. ime, naslov in kontaktni podatki ponudnika;
2. kadar informacije predloži druga oseba v imenu ponudnika: ime, naslov in kontaktni podatki te osebe;
3. ime, naslov in kontaktni podatki pooblaščenega zastopnika, kadar je ustrezno;
4. trgovsko ime sistema UI ter morebitne dodatne nedvoumne navedbe, ki omogočajo identifikacijo in sledljivost sistema UI;
5. opis predvidenega namena sistema UI ter komponent in funkcij, podprtih s tem sistemom UI;
6. kratek in jedrnat opis informacij, ki jih uporablja sistem (podatki, vhodni podatki), in logike delovanja sistema;
7. status sistema UI (na trgu ali v uporabi; ni več na trgu/v uporabi, odpoklican);
8. vrsta, številka in datum izteka veljavnosti certifikata, ki ga je izdal priglašeni organ, ter ime ali identifikacijska številka tega priglašene organa, kadar je ustrezno;
9. skeniran izvod certifikata iz točke 8, kadar je ustrezno;
10. imena vse držav članic, v katerih je bil sistem UI dan na trg ali v uporabo oziroma je bila omogočena njegova dostopnost v Uniji;
11. izvod EU izjave o skladnosti iz člena 47;
12. elektronska navodila za uporabo; te informacije se ne predložijo za visokotvegane sisteme UI na področjih preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali migracij, azila in upravljanja nadzora meje iz Priloge III, točke 1, 6 in 7;
13. URL za dodatne informacije (neobvezno).

Oddelek B – Informacije, ki jih predložijo ponudniki visokotveganih sistemov UI v skladu s členom 49(2)

V zvezi z visokotveganimi sistemi UI, ki se registrirajo v skladu s členom 49(2), se predložijo in nato posodablajo naslednje informacije:

1. ime, naslov in kontaktni podatki ponudnika;
2. kadar informacije predloži druga oseba v imenu ponudnika: ime, naslov in kontaktni podatki te osebe;
3. ime, naslov in kontaktni podatki pooblaščenega zastopnika, kadar je ustrezno;
4. trgovsko ime sistema UI ter morebitne dodatne nedvoumne navedbe, ki omogočajo identifikacijo in sledljivost sistema UI;
5. opis predvidenega namena sistema UI;
6. pogoj ali pogoji iz člena 6(3), na podlagi katerih sistem UI ne šteje za visokotvegani;
7. kratek povzetek razlogov, na podlagi katerih sistem UI pri uporabi postopka iz člena 6(3) ne šteje za visokotvegani;
8. status sistema UI (na trgu ali v uporabi; ni več na trgu/v uporabi, odpoklican);
9. imena vseh držav članic, v katerih je bil sistem UI dan na trg ali v uporabo oziroma je bila omogočena njegova dostopnost v Uniji.

Oddelek C – Informacije, ki jih predložijo uvajalci visokotveganih sistemov UI v skladu s členom 49(3)

V zvezi z visokotveganimi sistemi UI, ki se registrirajo v skladu s členom 49(3), se predložijo in nato posodablajo naslednje informacije:

1. ime, naslov in kontaktni podatki uvajalca;
 2. ime, naslov in kontaktni podatki osebe, ki posreduje informacije v imenu uvajalca;
 3. URL naslov vnosa sistema UI v podatkovno zbirko EU, za katerega poskrbi njegov ponudnik;
 4. povzetek ugotovitev ocene učinka v zvezi s temeljnimi pravicami, ki se opravi v skladu s členom 27;
 5. kadar je ustrezno, povzetek ocene učinka v zvezi z varstvom podatkov, izvedene v skladu s členom 35 Uredbe (EU) 2016/679 ali členom 27 Direktive (EU) 2016/680, kot je določeno v členu 26(8) te uredbe.
-

PRILOGA IX

Informacije, ki se predložijo ob registraciji visokotveganih sistemov UI v zvezi s testiranjem v realnih razmerah v skladu s členom 60

V zvezi s testiranjem v realnih razmerah, ki se registrira v skladu s členom 60, se predložijo in nato posodablajo naslednje informacije:

1. vseevropska enotna identifikacijska številka testiranja v realnih razmerah;
 2. ime in kontaktni podatki ponudnika ali potencialnega ponudnika in uvajalcev, ki sodelujejo pri testiranju v realnih razmerah;
 3. kratek opis sistema UI, njegov predvideni namen in druge informacije, potrebne za identifikacijo sistema;
 4. povzetek glavnih značilnosti načrta za testiranje v realnih razmerah;
 5. informacije o začasni ali dokončni ustavitvi testiranja v realnih razmerah.
-

PRILOGA X

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

1. Schengenski informacijski sistem

- (a) 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);
- (b) 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);
- (c) 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

- (a) Uredba (EU) 2021/1133 Evropskega parlamenta in Sveta z dne 7. julija 2021 o spremembi uredb (EU) št. 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 in (EU) 2019/818 v zvezi z določitvijo pogojev za dostop do drugih informacijskih sistemov EU za namene Vizumskega informacijskega sistema (UL L 248, 13.7.2021, str. 1).
- (b) Uredba (EU) 2021/1134 Evropskega parlamenta in Sveta z dne 7. julija 2021 o spremembi uredb (ES) št. 767/2008, (ES) št. 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 in (EU) 2019/1896 Evropskega parlamenta in Sveta ter razveljavitvi Odločbe Sveta 2004/512/ES in Sklepa Sveta 2008/633/PNZ zaradi reforme Vizumskega informacijskega sistema (UL L 248, 13.7.2021, str. 11).

3. Eurodac

Uredba (EU) 2024/1358 Evropskega parlamenta in Sveta z dne 14. maja 2024 o vzpostavitvi sistema Eurodac za primerjavo biometričnih podatkov zaradi učinkovite uporabe Uredbe (EU) 2024/1315 [uredba o upravljanju azila in migracij], Uredbe (EU) 2024/1350 [uredba o preselitvi] in Direktive 2001/55/ES [Direktiva o začasni zaščiti] 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 ter razveljavitvi Uredbe (EU) št. 603/2013 Evropskega parlamenta in Sveta (UL L, 2024/1358, 22.5.2024, ELI: <http://data.europa.eu/eli/reg/2024/1358/oj>).

4. Sistem vstopa/izstopa

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

- (a) 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);
- (b) 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

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

(a) 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 ter spremembi uredb (ES) št. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 in (EU) 2018/1861 Evropskega parlamenta in Sveta ter Odločbe Sveta 2004/512/ES in Sklepa Sveta 2008/633/PNZ (UL L 135, 22.5.2019, str. 27);

(b) 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 in spremembi uredb (EU) 2018/1726, (EU) 2018/1862 ter (EU) 2019/816 (UL L 135, 22.5.2019, str. 85).

PRILOGA XI

Tehnična dokumentacija iz člena 53(1), točka (a) – tehnična dokumentacija za ponudnike modelov UI za splošne namene

Oddelek 1

Informacije, ki jih predložijo vsi ponudniki modelov UI za splošne namene

Tehnična dokumentacija iz člena 53(1), točka (a), vsebuje vsaj naslednje informacije, odvisno od velikosti in profila tveganja modela:

1. splošni opis modela UI za splošne namene, vključno z:
 - (a) nalogami, ki naj bi jih model opravljal, ter vrsto in naravo sistemov UI, v katere se lahko vključi;
 - (b) veljavnimi politikami glede sprejemljive uporabe;
 - (c) datumom, na katerega je bil objavljen, in metodami distribucije;
 - (d) arhitekturo in številom parametrov;
 - (e) načinom (npr. besedilo, slika) ter obliko vhodnih in izhodnih podatkov;
 - (f) licenco;
2. podrobni opis elementov modela iz točke 1 in ustrezne informacije o postopku razvoja, vključno z naslednjimi elementi:
 - (a) tehničnimi sredstvi (npr. navodila za uporabo, infrastruktura, orodja), potrebnimi za vključitev modela UI za splošne namene v sisteme UI;
 - (b) specifikacijami zasnove modela in postopkom učenja, vključno z metodologijami in tehnikami učenja, ključnimi odločitvami glede zasnove, tudi utemeljitev in predpostavke; informacijami o tem, kaj naj bi model optimiziral in kako pomembni so različni parametri, kot je ustrezno;
 - (c) informacijami o podatkih, uporabljenih za učenje, testiranje in validacijo, kadar je primerno, vključno z vrsto in izvorom podatkov ter metodologijami urejanja (npr. čiščenje, filtriranje itd.), številom podatkovnih točk, njihovim obsegom in glavnimi značilnostmi; načinom pridobitve in izbire podatkov ter po potrebi vsemi drugimi ukrepi za odkrivanje neprimernosti virov podatkov in metod za zaznavanje prepoznavnih pristranskosti;
 - (d) računalniškimi viri, ki se uporabljajo za učenje modela (npr. število operacij s plavajočo vejico), čas učenja in druge pomembne podrobnosti v zvezi z učenjem;
 - (e) znano ali ocenjeno energetska poraba modela.

Kadar energetska poraba modela iz točke (e) ni znana, lahko energetska poraba temelji na informacijah o uporabljenih računalniških virih.

Oddelek 2

Dodatne informacije, ki jih predložijo ponudniki modelov UI za splošne namene s sistemskim tveganjem

1. podrobni opis strategij ocenjevanja, vključno z rezultati ocenjevanja, na podlagi razpoložljivih javnih protokolov in orodij za ocenjevanje ali drugih metodologij za ocenjevanje. Strategije ocenjevanja vključujejo merila za ocenjevanje, metrike in metodologijo za opredelitev omejitev;
2. kadar je ustrezno, podrobni opis ukrepov, sprejetih za izvajanje notranjega in/ali zunanega preskušanja po načelu kontradiktornosti (npr. etični heking) in prilagoditve modela, vključno z uskladitvami in izpopolnitvami;

3. kadar je ustrezno, podrobni opis arhitekture sistema, ki pojasnjuje, kako se sestavni deli programske opreme medsebojno nadgrajujejo ali navezujejo in kako so vključeni v celotno obdelavo.
-

PRILOGA XII

Informacije o preglednosti iz člena 53(1), točka (b) – tehnična dokumentacija, ki jo ponudniki modelov UI za splošne namene dajo na razpolago ponudnikom nižje v verigi, ki model vključijo v svoj sistem UI

Informacije iz člena 53(1), točka (b), vsebujejo vsaj naslednje:

1. splošni opis modela UI za splošne namene, vključno z:
 - (a) nalogami, ki naj bi jih model opravljal, ter vrsto in naravo sistemov UI, v katere se lahko vključi;
 - (b) veljavnimi politikami glede sprejemljive uporabe;
 - (c) datumom, na katerega je bil objavljen, in metodami distribucije;
 - (d) opisom, na kakšen način je model v interakciji s strojno ali programsko opremo, ki ni del samega modela, ali na kakšen način bi se lahko uporabljal za takšno interakcijo, kadar je ustrezno;
 - (e) različicami ustrezne programske opreme, povezane z uporabo modela UI za splošne namene, kadar je to ustrezno;
 - (f) arhitekturo in številom parametrov;
 - (g) načinom (npr. besedilo, slika) ter obliko vhodnih in izhodnih podatkov;
 - (h) licenco za model;
2. opis elementov modela in postopka za njegov razvoj, vključno s:
 - (a) tehničnimi sredstvi (npr. navodila za uporabo, infrastruktura, orodja), potrebnimi za vključitev modela UI za splošne namene v sisteme UI;
 - (b) načinom (npr. besedilo, slika itd.) ter obliko vhodnih in izhodnih podatkov, pa tudi njihovo največjo velikostjo (npr. dolžina vsebinskega okna itd.);
 - (c) informacijami o podatkih, uporabljenih za učenje, testiranje in validacijo, kadar je primerno, vključno z vrsto in izvorom podatkov ter metodologijami urejanja.

PRILOGA XIII

Merila za označitev modelov UI za splošne namene s sistemskim tveganjem iz člena 51

Pri ugotavljanju, ali ima model UI za splošne namene zmogljivosti ali vpliv, enakovredne tistim iz člena 51(1), točka (a), Komisija upošteva naslednja merila:

- (a) število parametrov modela;
 - (b) kakovost ali velikost nabora podatkov, merjeno na primer z žetoni;
 - (c) količino izračuna, uporabljeno za učenje modela, merjeno z operacijami s plavajočo vejico ali izraženo s kombinacijo drugih spremenljivk, kot so ocenjeni stroški učenja, predvideni čas, potreben za učenje, ali ocenjena poraba energije za učenje;
 - (d) vhodne in izhodne načine modela, kot so besedilo v besedilo (veliki jezikovni modeli), besedilo v podobo, večmodalnost in najsodobnejši pragovi za določanje zmogljivosti z visoko učinkovitostjo za vsak način, ter posebna vrsta vhodnih in izhodnih podatkov (npr. biološka zaporedja);
 - (e) merila uspešnosti in ocenjevanja zmogljivosti modela, vključno z upoštevanjem števila nalog brez dodatnega učenja, prilagodljivostjo za učenje novih, različnih nalog, njegovo stopnjo avtonomije in nadgradljivosti ter orodji, do katerih ima dostop;
 - (f) ali ima velik vpliv na notranji trg zaradi svojega dosega, na katerega se domneva, ko je bil dan na voljo vsaj 10 000 registriranim poslovnim uporabnikom s sedežem v Uniji;
 - (g) število registriranih končnih uporabnikov.
-