



2024/1689

12.7.2024.

UREDBA (EU) 2024/1689 EUROPSKOG PARLAMENTA I VIJEĆA

od 13. lipnja 2024.

o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji)

(Tekst značajan za EGP)

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegove članke 16. i 114.,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrtu zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora ⁽¹⁾,

uzimajući u obzir mišljenje Europske središnje banke ⁽²⁾,

uzimajući u obzir mišljenje Odbora regija ⁽³⁾,

u skladu s redovnim zakonodavnim postupkom ⁽⁴⁾,

budući da:

- (1) Svrha je ove Uredbe poboljšati funkcioniranje unutarnjeg tržišta utvrđivanjem ujednačenog pravnog okvira, osobito za razvoj, stavljanje na tržište, stavljanje u upotrebu i korištenje sustava umjetne inteligencije („UI sustavi”) u Uniji, u skladu s vrijednostima Unije, promicati prihvaćanje antropocentrične i pouzdane umjetne inteligencije uz istodobno jamčenje visoke razine zaštite zdravlja, sigurnosti i temeljnih prava kako su sadržana u Povelji Europske unije o temeljnim pravima („Povelja”), uključujući demokraciju, vladavinu prava i zaštitu okoliša, zaštitu od štetnih učinaka UI sustava u Uniji, te podupirati inovacije. Ovom se Uredbom osigurava slobodno prekogranično kretanje robe i usluga temeljenih na umjetnoj inteligenciji, čime se države članice sprečava da nametnu ograničenja razvoju, stavljanju na tržište i korištenju UI sustava, osim ako je to izričito odobreno ovom Uredbom.
- (2) Ova bi se Uredba trebala primjenjivati u skladu s vrijednostima Unije sadržanima u Povelji i trebala bi olakšati zaštitu fizičkih osoba, poduzeća, demokracije, vladavine prava i okoliša, a istodobno poticati inovacije i zapošljavanje te učiniti Uniju predvodnikom u prihvaćanju pouzdane umjetne inteligencije.
- (3) UI sustavi mogu se lako uvesti u brojne različite sektore gospodarstva i mnoge dijelove društva, među ostalim i preko granica, te lako cirkulirati u cijeloj Uniji. Neke su države članice već razmotrile donošenje nacionalnih pravila kojima bi se zajamčilo da umjetna inteligencija bude pouzdana i sigurna te da se razvija i upotrebljava u skladu s obvezama u području temeljnih prava. Divergentna nacionalna pravila mogu dovesti do fragmentacije unutarnjeg tržišta i smanjiti pravnu sigurnost za operatere koji razvijaju, uvoze ili upotrebljavaju UI sustave. Stoga bi za postizanje pouzdane umjetne inteligencije trebalo osigurati dosljednu i visoku razinu zaštite u cijeloj Uniji, dok bi divergencije koje otežavaju slobodnu cirkulaciju, inovacije te uvođenje i prihvaćanje UI sustava i povezanih

⁽¹⁾ SL C 517, 22.12.2021., str. 56.

⁽²⁾ SL C 115, 11.3.2022., str. 5.

⁽³⁾ SL C 97, 28.2.2022., str. 60.

⁽⁴⁾ Stajalište Europskog parlamenta od 13. ožujka 2024. (još nije objavljeno u Službenom listu) i Odluka Vijeća od 21. svibnja 2024.

proizvoda i usluga na unutarnjem tržištu trebalo spriječiti utvrđivanjem ujednačenih obveza za operatere i jamčenjem ujednačene zaštite prevladavajućih razloga od javnog interesa i prava osoba na cijelom unutarnjem tržištu na temelju članka 114. Ugovora o funkcioniranju Europske unije (UFEU). U mjeri u kojoj ova Uredba sadržava specifična pravila o zaštiti pojedinaca u pogledu obrade osobnih podataka u vezi s ograničenjima korištenja UI sustavâ za daljinsku biometrijsku identifikaciju u svrhu kaznenog progona, korištenja UI sustavâ za procjene rizika u pogledu fizičkih osoba u svrhu kaznenog progona i korištenja UI sustavâ za biometrijsku kategorizaciju u svrhu kaznenog progona, primjereno je ovu Uredbu, u mjeri u kojoj se odnosi na ta specifična pravila, temeljiti na članku 16. UFEU-a. S obzirom na ta specifična pravila i pozivanje na članak 16. UFEU-a, primjereno je zatražiti mišljenje Europskog odbora za zaštitu podataka.

- (4) Umjetna inteligencija skup je tehnologija koji se brzo razvija i doprinosi širokom spektru gospodarskih, okolišnih i društvenih koristi u cijelom nizu industrija i društvenih aktivnosti. Zahvaljujući boljem predviđanju, optimizaciji operacija i dodjeli resursa te personalizaciji digitalnih rješenja dostupnih pojedincima i organizacijama, korištenje umjetne inteligencije može poduzećima pružiti ključne konkurentske prednosti te podupirati društveno i okolišno korisne ishode, na primjer u zdravstvu, poljoprivredi, sigurnosti hrane, obrazovanju i osposobljavanju, medijima, sportu, kulturi, upravljanju infrastrukturom, energetici, prometu i logistici, javnim uslugama, sigurnosti, pravosuđu, resursnoj i energetske učinkovitosti, praćenju stanja okoliša, očuvanju i obnovi bioraznolikosti i ekosustavâ te ublažavanju klimatskih promjena i prilagodbi njima.
- (5) Istodobno, ovisno o okolnostima njezine specifične primjene, korištenja i razine tehnološkog razvoja, umjetna inteligencija može stvoriti rizike i uzrokovati štetu javnim interesima i temeljnim pravima zaštićenima pravom Unije. Ta šteta može biti materijalna ili nematerijalna, uključujući tjelesnu, psihološku, društvenu ili ekonomsku štetu.
- (6) S obzirom na velik učinak koji umjetna inteligencija može imati na društvo i potrebu za izgradnjom povjerenja, ključno je da se umjetna inteligencija i njezin regulatorni okvir razvijaju u skladu s vrijednostima Unije sadržanima u članku 2. Ugovora o Europskoj uniji (UEU), temeljnim pravima i slobodama sadržanima u Ugovorima i, na temelju članka 6. UEU-a, u Povelji. Umjetna inteligencija neophodno bi trebala biti antropocentrična tehnologija. Trebala bi služiti kao alat namijenjen ljudima s krajnjim ciljem povećanja njihove dobrobiti.
- (7) Kako bi se osigurala dosljedna i visoka razina zaštite javnih interesa u smislu zdravlja, sigurnosti i temeljnih prava, trebalo bi utvrditi zajednička pravila za visokorizične UI sustave. Ta bi pravila trebala biti dosljedna s Poveljom, nediskriminirajuća i usklađena s međunarodnim trgovinskim obvezama Unije. Njima bi se ujedno trebalo uzeti u obzir Europsku deklaraciju o digitalnim pravima i načelima za digitalno desetljeće i Etičke smjernice za pouzdanu umjetnu inteligenciju koje je sastavila Stručna skupina na visokoj razini za umjetnu inteligenciju.
- (8) Stoga je potreban pravni okvir Unije kojim se utvrđuju usklađena pravila o umjetnoj inteligenciji kako bi se poticali razvoj, korištenje i prihvaćanje umjetne inteligencije na unutarnjem tržištu i istodobno ostvarila visoka razina zaštite javnih interesa, kao što su zdravlje i sigurnost te zaštita temeljnih prava, uključujući demokraciju, vladavinu prava i zaštitu okoliša, kako su priznata i zaštićena pravom Unije. Da bi se postigao taj cilj, trebalo bi utvrditi pravila kojima se uređuju stavljanje na tržište, stavljanje u upotrebu i korištenje određenih UI sustava, te tako osigurati neometano funkcioniranje unutarnjeg tržišta i omogućiti da ti sustavi ostvaruju koristi od načela slobodnog kretanja robe i usluga pogoduju. Ta bi pravila trebala biti jasna i snažna u zaštiti temeljnih prava, podupirati nova inovativna rješenja i pogodovati europskom ekosustavu javnih i privatnih aktera koji stvaraju UI sustave u skladu s vrijednostima Unije te ostvariti potencijal digitalne transformacije u svim regijama Unije. Utvrđivanjem tih pravila i mjera za potporu inovacijama s osobitim naglaskom na malim i srednjim poduzećima (MSP-ovi), uključujući *start-up* poduzeća, ovom se Uredbom doprinosi cilju promicanja europskog antropocentričnog pristupa umjetnoj inteligenciji i globalnog vodstva u razvoju sigurne, pouzdane i etične umjetne inteligencije kako je navelo Europsko vijeće ⁽⁵⁾ te se osigurava zaštita etičkih načela u skladu s izričitim zahtjevom Europskog parlamenta ⁽⁶⁾.

⁽⁵⁾ Europsko vijeće, izvanredni sastanak Europskog vijeća (1. i 2. listopada 2020.) – zaključci, EUCO 13/20, 2020., str. 6.

⁽⁶⁾ Rezolucija Europskog parlamenta od 20. listopada 2020. s preporukama Komisiji o okviru etičkih aspekata umjetne inteligencije, robotike i s njima povezanih tehnologija, 2020/2012(INL).

- (9) Usklađena pravila koja se primjenjuju na stavljanje na tržište, stavljanje u upotrebu i korištenje visokorizičnih UI sustava trebala bi biti utvrđena u skladu s Uredbom (EZ) br. 765/2008 Europskog parlamenta i Vijeća ⁽⁷⁾, Odlukom br. 768/2008/EZ Europskog parlamenta i Vijeća ⁽⁸⁾ i Uredbom (EU) 2019/1020 Europskog parlamenta i Vijeća ⁽⁹⁾ (novi zakonodavni okvir). Usklađena pravila utvrđena u ovoj Uredbi trebala bi se primjenjivati u svim sektorima i, u skladu s novim zakonodavnim okvirom, ne bi trebala dovoditi u pitanje postojeće pravo Unije, osobito ono u području zaštite podataka, zaštite potrošača, temeljnih prava, zapošljavanja, zaštite radnika i sigurnosti proizvoda, koje ova Uredba dopunjuje. Kao posljedica toga sva prava i pravna sredstva predviđena tim pravom Unije za potrošače i druge osobe na koje UI sustavi mogu imati negativan učinak, među ostalim i u pogledu naknade potencijalne štete na temelju Direktive Vijeća 85/374/EEZ ⁽¹⁰⁾, i dalje su nepromijenjeni i u potpunosti se primjenjuju. Nadalje, u kontekstu zapošljavanja i zaštite radnika, ova Uredba stoga ne bi trebala utjecati na pravo Unije o socijalnoj politici i nacionalno radno pravo, u skladu s pravom Unije, koje se odnosi na zapošljavanje i radne uvjete, uključujući zdravlje i sigurnost na radu te odnos između poslodavaca i radnika. Ova Uredba ne bi trebala utjecati ni na ostvarivanje temeljnih prava priznatih u državama članicama i na razini Unije, uključujući pravo ili slobodu štrajka ili poduzimanja drugih mjera obuhvaćenih specifičnim sustavima država članica u području radnih odnosa, kao i pravo na dogovaranje, kroz pregovore, na sklapanje i provedbu kolektivnih ugovora ili na poduzimanje kolektivnih mjera u skladu s nacionalnim pravom. Ova Uredba ne bi trebala utjecati na odredbe čiji je cilj poboljšanje radnih uvjeta u radu putem platformi utvrđene u direktivi Europskog parlamenta i Vijeća o poboljšanju radnih uvjeta u radu putem platformi. Usto, cilj je ove Uredbe ojačati djelotvornost tih postojećih prava i pravnih sredstava utvrđivanjem posebnih zahtjeva i obveza, među ostalim i u pogledu transparentnosti, tehničke dokumentacije i vođenja evidencije o UI sustavima. Nadalje, obveze koje su na temelju ove Uredbe nametnute različitim operaterima uključenima u lanac vrijednosti umjetne inteligencije trebale bi se primjenjivati ne dovodeći u pitanje nacionalno pravo, u skladu s pravom Unije, koje ima učinak ograničavanja korištenja određenih UI sustava ako takvo pravo nije obuhvaćeno područjem primjene ove Uredbe ili ako se njime žele ostvariti drugi legitimni ciljevi od javnog interesa koji nisu ciljevi koji se nastoje ostvariti ovom Uredbom. Na primjer, ova Uredba ne bi trebala utjecati na nacionalno radno pravo ni na pravo o zaštiti maloljetnika, odnosno osoba mlađih od 18 godina, uzimajući u obzir Opću napomenu Ujedinjenih naroda br. 25 (2021.) o pravima djece u pogledu digitalnog okružja, u mjeri u kojoj ono nije specifično za UI sustave i njime se žele ostvariti drugi legitimni ciljevi od javnog interesa.
- (10) Temeljno pravo na zaštitu osobnih podataka osobito je zajamčeno uredbama (EU) 2016/679 ⁽¹¹⁾ i (EU) 2018/1725 ⁽¹²⁾ Europskog parlamenta i Vijeća te Direktivom (EU) 2016/680 Europskog parlamenta i Vijeća ⁽¹³⁾. Direktivom 2002/58/EZ Europskog parlamenta i Vijeća ⁽¹⁴⁾ dodatno se štiti privatni život i povjerljivost komunikacija, među ostalim i pružanjem uvjeta za svu pohranu osobnih i neosobnih podataka u terminalnoj opremi te pristup tim podacima s terminalne opreme. Ti su pravni akti Unije temelj za održivu i odgovornu obradu podataka, među ostalim i onda kada skupovi podataka uključuju kombinaciju osobnih i neosobnih podataka. Ovom se Uredbom ne nastoji utjecati na primjenu postojećeg prava Unije kojim se uređuje obrada osobnih podataka, uključujući zadaće i ovlasti neovisnih nadzornih tijela nadležnih za praćenje usklađenosti s tim instrumentima. Ona usto ne utječe na obveze dobavljača UI sustava i subjekata koji uvode te sustave u njihovu ulogu voditelja obrade podataka ili izvršitelja obrade podataka koje proizlaze iz prava Unije o zaštiti osobnih podataka ili nacionalnog prava o zaštiti osobnih podataka u mjeri u kojoj dizajniranje, razvoj ili korištenje UI sustava uključuje obradu osobnih
-
- (7) Uredba (EZ) br. 765/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o utvrđivanju zahtjeva za akreditaciju i o stavljanju izvan snage Uredbe (EEZ) br. 339/93 (SL L 218, 13.8.2008., str. 30.).
- (8) Odluka br. 768/2008/EZ Europskog parlamenta i Vijeća od 9. srpnja 2008. o zajedničkom okviru za stavljanje na tržište proizvoda i o stavljanju izvan snage Odluke Vijeća 93/465/EEZ (SL L 218, 13.8.2008., str. 82.).
- (9) Uredba (EU) 2019/1020 Europskog parlamenta i Vijeća od 20. lipnja 2019. o nadzoru tržišta i sukladnosti proizvoda i o izmjeni Direktive 2004/42/EZ i uredbi (EZ) br. 765/2008 i (EU) br. 305/2011 (SL L 169, 25.6.2019., str. 1.).
- (10) Direktiva Vijeća 85/374/EEZ od 25. srpnja 1985. o približavanju zakona i drugih propisa država članica u vezi s odgovornošću za neispravne proizvode (SL L 210, 7.8.1985., str. 29.).
- (11) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).
- (12) Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39.).
- (13) Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL L 119, 4.5.2016., str. 89.).
- (14) Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37.).

podataka. Također je primjereno pojasniti da ispitanici i dalje uživaju sva prava i jamstva koja su im dodijeljena tim pravom Unije, među ostalim i prava povezana s isključivo automatiziranim pojedinačnim donošenjem odluka, uključujući izradu profila. Usklađena pravila o stavljanju na tržište, stavljanju u upotrebu i korištenju UI sustava uspostavljena ovom Uredbom trebala bi olakšati djelotvornu provedbu i omogućiti ostvarivanje prava ispitanika i drugih pravnih sredstava zajamčenih na temelju prava Unije o zaštiti osobnih podataka i drugih temeljnih prava.

- (11) Ovom se Uredbom ne bi trebale dovoditi u pitanje odredbe o odgovornosti pružatelja usluga posredovanja kako su utvrđene u Uredbi (EU) 2022/2065 Europskog parlamenta i Vijeća ⁽¹⁵⁾.
- (12) Pojam „UI sustav” u ovoj bi Uredbi trebalo jasno definirati i usko ga uskladiti s radom međunarodnih organizacija koje se bave umjetnom inteligencijom kako bi se zajamčila pravna sigurnost te olakšala međunarodna konvergencija i široka prihvaćenost i pritom omogućila fleksibilnost za prilagođavanje brzom tehnološkom napretku u tom području. Nadalje, ta bi se definicija trebala temeljiti na ključnim značajkama UI sustava po kojima se razlikuje od jednostavnijih tradicionalnih softverskih sustava ili pristupa programiranju te ne bi trebao obuhvaćati sustave koji se temelje na pravilima koja su definirale isključivo fizičke osobe za automatsko izvršavanje operacija. Ključna značajka UI sustava njihova je sposobnost zaključivanja. Ta sposobnost zaključivanja odnosi se na proces dobivanja izlaznih vrijednosti, kao što su predviđanja, sadržaj, preporuke ili odluke, koje mogu utjecati na fizička i virtualna okružja, te na sposobnost UI sustava da izvode modele ili algoritme, ili i modele i algoritme, iz ulaznih vrijednosti ili podataka. Tehnike koje omogućuju zaključivanje pri izgradnji UI sustava uključuju pristupe strojnog učenja koji s pomoću podataka uče kako postići određene ciljeve te pristupe temeljene na logici i znanju koji izvode zaključke iz kodiranog znanja ili simboličkog prikaza zadatka koji treba riješiti. Sposobnost UI sustava da zaključuje nadilazi osnovnu obradu podataka omogućujući učenje, rezoniranje ili modeliranje. Pojam „strojni” odnosi se na činjenicu da je rad UI sustava pogonjen strojevima. Upućivanjem na eksplicitne ili implicitne ciljeve ističe se da UI sustavi mogu raditi u skladu s eksplicitno definiranim ciljevima ili implicitnim ciljevima. Ciljevi UI sustava mogu se u specifičnom kontekstu razlikovati od namjene UI sustava. Za potrebe ove Uredbe okružja bi trebalo razumjeti kao kontekste u kojima UI sustavi rade, a izlazne vrijednosti koje UI sustav generira odražavaju različite funkcije UI sustava i uključuju predviđanja, sadržaj, preporuke ili odluke. UI sustavi dizajnirani su tako da rade s promjenjivim razinama autonomije, što znači da imaju određeni stupanj neovisnosti djelovanja od ljudske uključenosti i sposobnosti rada bez ljudske intervencije. Prilagodljivost koju bi UI sustav mogao pokazati nakon uvođenja odnosi se na sposobnosti samostalnog učenja, koje sustavu omogućuju da se mijenja dok je u upotrebi. UI sustavi mogu se upotrebljavati samostalno ili kao komponenta nekog proizvoda, neovisno o tome je li sustav fizički integriran u proizvod (ugrađen) ili služi funkcionalnosti proizvoda, a da nije integriran u njega (neugrađen).
- (13) Pojam „subjekt koji uvodi sustav” iz ove Uredbe trebalo bi tumačiti kao svaku fizičku ili pravnu osobu, uključujući tijelo javne vlasti, javnu agenciju ili drugo javno tijelo, koja upotrebljava UI sustav u okviru svoje nadležnosti, osim ako se UI sustav upotrebljava u osobnoj neprofesionalnoj djelatnosti. Ovisno o vrsti UI sustava, njegovo korištenje može utjecati na osobe koje nisu subjekt koji ga uvodi.
- (14) Pojam „biometrijski podaci” koji se upotrebljava u ovoj Uredbi trebalo bi tumačiti s obzirom na pojam biometrijskih podataka kako je definiran u članku 4. točki 14. Uredbe (EU) 2016/679, članku 3. točki 18. Uredbe (EU) 2018/1725 i članku 3. točki 13. Direktive (EU) 2016/680. Biometrijski podaci mogu omogućiti autentifikaciju, identifikaciju ili kategorizaciju fizičkih osoba i prepoznavanje njihovih emocija.
- (15) Pojam „biometrijska identifikacija” iz ove Uredbe trebalo bi definirati kao automatizirano prepoznavanje fizičkih, fizioloških i biheviornalnih obilježja ljudi, kao što su lice, pokreti očiju, izrazi lica, oblik tijela, glas, govor, hod, držanje, srčani ritam, krvni tlak, miris i način tipkanja, u svrhu utvrđivanja identiteta pojedinca usporedbom njegovih biometrijskih podataka s biometrijskim podacima pojedinaca pohranjenima u referentnoj bazi podataka, neovisno o tome je li dotični pojedinac dao privolu. To isključuje UI sustave namijenjene za biometrijsku provjeru, uključujući autentifikaciju, čija je jedina svrha potvrditi da je određena fizička osoba doista ona kojom se predstavlja i potvrditi identitet fizičke osobe isključivo radi pristupa usluzi, otključavanja uređaja ili sigurnog pristupa prostorijama.

⁽¹⁵⁾ Uredba (EU) 2022/2065 Europskog parlamenta i Vijeća od 19. listopada 2022. o jedinstvenom tržištu digitalnih usluga i izmjeni Direktive 2000/31/EZ (Akt o digitalnim uslugama) (SL L 277, 27.10.2022., str. 1.).

- (16) Pojam „biometrijska kategorizacija” iz ove Uredbe trebalo bi definirati kao razvrstavanje fizičkih osoba u određene kategorije na temelju njihovih biometrijskih podataka. Te specifične kategorije mogu se odnositi na aspekte kao što su spol, dob, boja kose, boja očiju, tetovaže, značajke ponašanja ili osobnosti, jezik, vjera, pripadnost nacionalnoj manjini, spolna ili politička orijentacija. To ne uključuje sustave za biometrijsku kategorizaciju koji su isključivo pomoćni element intrinzično povezan s drugom komercijalnom uslugom, što znači da se taj element iz objektivnih tehničkih razloga ne može upotrebljavati bez glavne usluge i da integracija tog elementa ili funkcionalnosti nije sredstvo za zaobilaženje primjenjivosti pravila ove Uredbe. Na primjer, filtri za kategorizaciju značajki lica ili tijela koji se upotrebljavaju na internetskim tržištima mogli bi biti takav pomoćni element jer se mogu upotrebljavati samo u vezi s glavnom uslugom koja se sastoji od prodaje proizvoda tako što se potrošaču omogućuje da pregleda prikaz proizvoda na sebi i tako što pomaže u donošenju odluke o kupnji. Filtri koji se upotrebljavaju na internetskim društvenim mrežama i kojima se kategoriziraju značajke lica ili tijela kako bi se korisnicima omogućilo dodavanje ili izmjena slika ili videozapisa također bi se mogli smatrati pomoćnim elementom jer se takvi filtri ne mogu upotrebljavati bez glavne usluge društvenih mreža koja se sastoji od dijeljenja sadržaja na internetu.
- (17) Pojam „sustav za daljinsku biometrijsku identifikaciju” iz ove Uredbe trebalo bi definirati funkcionalno kao UI sustav namijenjen identifikaciji fizičkih osoba bez njihova aktivnog sudjelovanja, obično na daljinu, usporedbom biometrijskih podataka dotične osobe s biometrijskim podacima iz referentne baze podataka, bez obzira na specifičnu tehnologiju, specifične postupke ili specifične vrste biometrijskih podataka koji se upotrebljavaju. Takvi sustavi za daljinsku biometrijsku identifikaciju obično se upotrebljavaju za istodobno percipiranje više osoba ili njihova ponašanja kako bi se znatno olakšala identifikacija fizičkih osoba bez njihova aktivnog sudjelovanja. To isključuje UI sustave namijenjene za biometrijsku provjeru, uključujući autentifikaciju, čija je jedina svrha potvrditi da je određena fizička osoba doista ona kojom se predstavlja i potvrditi identitet fizičke osobe isključivo radi pristupa usluzi, otključavanja uređaja ili sigurnog pristupa prostorijama. To je isključenje opravdano činjenicom da će takvi sustavi vjerojatno manje utjecati na temeljna prava fizičkih osoba nego sustavi za daljinsku biometrijsku identifikaciju koji se mogu upotrebljavati za obradu biometrijskih podataka velikog broja osoba bez njihova aktivnog sudjelovanja. U slučaju sustava u stvarnom vremenu prikupljanje biometrijskih podataka, usporedba i identifikacija odvijaju se trenutačno, gotovo trenutačno ili u svakom slučaju bez znatnog vremenskog odmaka. U tom pogledu ne bi trebao postojati prostor za zaobilaženje pravila iz ove Uredbe o korištenju dotičnih UI sustava u stvarnom vremenu predviđanjem kratkih vremenskih odmaka. Sustavi u stvarnom vremenu uključuju korištenje materijala snimljenog „uživo” ili „gotovo uživo”, kao što je videozapis, zabilježenog kamerom ili drugim uređajem sa sličnom funkcijom. S druge strane, u slučaju sustava za naknadnu identifikaciju biometrijski su podaci već prethodno prikupljeni te se usporedba i identifikacija provode tek nakon znatnog vremenskog odmaka. To uključuje materijal, kao što su fotografije ili videozapisi zabilježeni nadzornim kamerama ili privatnim uređajima, snimljen prije nego što je sustav upotrijebljen za identifikaciju dotičnih fizičkih osoba.
- (18) Pojam „sustav za prepoznavanje emocija” iz ove Uredbe trebalo bi definirati kao UI sustav namijenjen prepoznavanju emocija ili namjera fizičkih osoba ili izvođenju zaključaka o njihovim emocijama ili namjerama na temelju njihovih biometrijskih podataka. Taj se pojam odnosi na emocije ili namjere kao što su sreća, tuga, ljutnja, iznenađenje, gađenje, osramoćenost, uzbuđenje, sram, prijezir, zadovoljstvo i zabavljenost. Ne uključuje fizička stanja, kao što su bol ili umor, među ostalim, primjerice, sustave koji se upotrebljavaju za otkrivanje stanja umora kod profesionalnih pilota ili vozača u svrhu sprečavanja nesreća. To također ne uključuje samo otkrivanje lako vidljivih izraza, gesta ili pokreta, osim ako se upotrebljavaju za identifikaciju ili izvođenje zaključaka o emocijama. Ti izrazi mogu biti osnovni izrazi lica, kao što su namrštenost ili osmijeh, ili geste kao što su pokreti ruku ili glave, ili značajke glasa osobe, kao što su podignut glas ili šaptanje.
- (19) Za potrebe ove Uredbe pojam „javno mjesto” trebalo bi razumjeti kao svako fizičko mjesto koje je dostupno neodređenom broju fizičkih osoba, bez obzira na to je li dotično mjesto u privatnom ili javnom vlasništvu i na aktivnost za koju se to mjesto može upotrebljavati, kao što su trgovina npr. trgovine, restorani, kafići, usluge npr. banke, profesionalne aktivnosti, ugostiteljstvo, sport npr. bazeni, teretane, stadioni, prijevoz npr. autobusne i željezničke postaje, postaje podzemne željeznice, zračne luke, prijevozna sredstva, zabava npr. kina, kazališta, muzeji, koncertne i konferencijske dvorane odnosno aktivnosti u slobodno vrijeme ili druge svrhe npr. javne ceste i trgovi, parkovi, šume, igrališta. Mjesto bi trebalo klasificirati kao javno i ako, bez obzira na potencijalni kapacitet ili sigurnosna ograničenja, pristup tom mjestu podliježe određenim unaprijed utvrđenim uvjetima koje može ispuniti neodređen broj osoba, kao što su kupnja ulaznice ili prijevozne karte, prethodna registracija ili određena dob. S druge strane, mjesto se ne bi trebalo smatrati javnim ako je pristup ograničen na specifične i definirane fizičke osobe putem prava Unije ili nacionalnog prava koje je izravno povezano s javnom sigurnošću ili zaštitom odnosno putem jasnog iskaza volje osobe koja ima odgovarajuće ovlasti na tom mjestu. Sama činjenična mogućnost pristupa

kao što su otključana vrata ili otvoreni ulaz u ogradu ne znači da je mjesto javno ako postoje naznake ili okolnosti koje upućuju na suprotno kao što su znakovi kojima se zabranjuje ili ograničava pristup. Poslovni prostori poduzeća i tvornica te uredi i mjesta rada kojima mogu pristupiti samo relevantni zaposlenici i pružatelji usluga nisu javna mjesta. Javna mjesta ne bi trebala uključivati zatvore ili graničnu kontrolu. Neka druga mjesta mogu se sastojati i od mjesta koja su javna mjesta i od mjesta koja to nisu, kao što je hodnik privatne stambene zgrade potreban za pristup liječničkoj ordinaciji ili zračna luka. Nisu obuhvaćeni internetski prostori jer oni nisu fizički prostori. Ipak, činjenicu je li određeno mjesto javno trebalo bi utvrditi na pojedinačnoj osnovi i pritom uzeti u obzir specifične okolnosti konkretne situacije.

- (20) Kako bi se ostvarile najveće koristi od UI sustava i istodobno zaštitila temeljna prava, zdravlje i sigurnost te omogućila demokratska kontrola, pismenost u području umjetne inteligencije trebala bi dobavljačima, subjektima koji uvode sustav i osobama na koje utječe umjetna inteligencija osigurati vladanje potrebnim pojmovima kako bi mogli donositi informirane odluke o UI sustavima. Ti se pojmovi mogu razlikovati s obzirom na relevantni kontekst i mogu uključivati razumijevanje pravilne primjene tehničkih elemenata tijekom faze razvoja UI sustava, mjera koje treba primijeniti tijekom njegova korištenja, prikladnih načina tumačenja izlaznih vrijednosti UI sustava i, u slučaju osoba na koje utječe umjetna inteligencija, znanje potrebno za razumijevanje načina na koji će odluke donesene uz pomoć umjetne inteligencije utjecati na njih. U kontekstu primjene ove Uredbe pismenost u području umjetne inteligencije trebala bi svim relevantnim akterima u vrijednosnom lancu umjetne inteligencije pružiti uvide potrebne za osiguravanje odgovarajuće usklađenosti i njezina pravilnog izvršavanja. Nadalje, široka provedba mjera pismenosti u području umjetne inteligencije i uvođenje odgovarajućih daljnjih mjera mogli bi doprinijeti poboljšanju radnih uvjeta i u konačnici podržati konsolidaciju i inovacijski put pouzdane umjetne inteligencije u Uniji. Europsko vijeće za umjetnu inteligenciju („Vijeće za umjetnu inteligenciju”) trebalo bi podupirati Komisiju u promicanju alata za pismenost u području umjetne inteligencije, javne svijesti te razumijevanja koristi, rizika, zaštitnih mjera, prava i obveza povezanih s korištenjem UI sustava. U suradnji s relevantnim dionicima Komisija i države članice trebale bi olakšati izradu dobrovoljnih kodeksa ponašanja kako bi se unaprijedila pismenost u području umjetne inteligencije među osobama koje se bave razvojem, radom i korištenjem umjetne inteligencije.
- (21) Kako bi se osigurali jednaki uvjeti i djelotvorna zaštita prava i sloboda pojedinaca u cijeloj Uniji, pravila utvrđena ovom Uredbom trebala bi se primjenjivati na dobavljače UI sustava na nediskriminirajući način, bez obzira na to imaju li poslovni nastan u Uniji ili trećoj zemlji, i na subjekte koji uvode UI sustave s poslovnim nastanom u Uniji.
- (22) Određeni bi UI sustavi s obzirom na njihov digitalni karakter trebali biti obuhvaćeni područjem primjene ove Uredbe čak i ako nisu stavljeni na tržište ni u upotrebu niti se upotrebljavaju u Uniji. To se, primjerice, odnosi na operatera s poslovnim nastanom u Uniji koji od operatera s poslovnim nastanom u trećoj zemlji naruči određene usluge povezane s aktivnošću koju obavlja UI sustav koji bi se smatrao visokorizičnim. U tim bi okolnostima UI sustav kojim se služi operater u trećoj zemlji mogao obrađivati podatke koji su zakonito prikupljeni u Uniji i preneseni iz nje te operateru ugovaratelju u Uniji dostaviti izlazne podatke UI sustava koje su rezultat te obrade, a da taj UI sustav nije stavljen ni na tržište ni u upotrebu niti se upotrebljava u Uniji. Kako bi se spriječilo zaobilaženje ove Uredbe i osigurala djelotvorna zaštita fizičkih osoba koje se nalaze u Uniji, ova bi se Uredba trebala primjenjivati i na dobavljače UI sustava i subjekte koji ih uvode koji imaju poslovni nastan u trećoj zemlji, u mjeri u kojoj se u Uniji namjeravaju upotrebljavati izlazni podaci tih sustava. Međutim, kako bi se uzeli u obzir postojeći aranžmani i posebne potrebe za budućom suradnjom sa stranim partnerima s kojima se razmjenjuju informacije i dokazi, ova se Uredba ne bi trebala primjenjivati na tijela javne vlasti treće zemlje ni na međunarodne organizacije kada djeluju u okviru suradnje ili međunarodnih sporazuma koji su na razini Unije ili na nacionalnoj razini sklopljeni s Unijom ili državama članicama radi suradnje u područjima kaznenog progona i pravosuđa, pod uvjetom da relevantna treća zemlja ili međunarodna organizacija osigura odgovarajuće zaštitne mjere u pogledu zaštite temeljnih prava i sloboda pojedinaca. To prema potrebi može obuhvaćati aktivnosti subjekata kojima su treće zemlje povjerile izvršavanje posebnih zadaća za potporu takvoj suradnji u područjima kaznenog progona i pravosuđa. Takvi okviri za suradnju ili sporazumi uspostavljeni su bilateralno između država članica i trećih zemalja ili između Europske unije, Europolu i drugih agencija Unije te trećih zemalja i međunarodnih organizacija. Tijela nadležna za nadzor tijela kaznenog progona i pravosudnih tijela na temelju ove Uredbe trebala bi procijeniti uključuju li ti okviri za suradnju ili međunarodni sporazumi odgovarajuće zaštitne mjere u pogledu zaštite temeljnih prava i sloboda

pojedinaца. Nacionalna tijela primatelji i institucije, tijela, uredi i agencije Unije koji se služe takvim izlaznim podacima u Uniji i dalje snose odgovornost za osiguravanje usklađenosti njihova korištenja s pravom Unije. Pri reviziji tih međunarodnih sporazuma ili sklapanju novih sporazuma u budućnosti ugovorne stranke trebale bi uložiti najveće moguće napore u usklađivanje tih sporazuma sa zahtjevima ove Uredbe.

- (23) Ova bi se Uredba trebala primjenjivati i na institucije, tijela, urede i agencije Unije kada djeluju kao dobavljač UI sustava ili subjekt koji ga uvodi.
- (24) Ako se i u mjeri u kojoj se UI sustavi stavljaju na tržište, stavljaju u upotrebu ili se upotrebljavaju, s izmjenama ili bez njih, u vojne svrhe, obrambene svrhe ili u svrhe povezane s nacionalnom sigurnošću, te bi sustave trebalo isključiti iz područja primjene ove Uredbe neovisno o tome koja vrsta subjekta obavlja te aktivnosti, primjerice bez obzira na to radi li se o javnom ili privatnom subjektu. Kad je riječ o vojnim i obrambenim svrhama, takvo je isključenje opravdano i člankom 4. stavkom 2. UEU-a i posebnostima obrambene politike država članica i zajedničke obrambene politike Unije obuhvaćene glavom V. poglavljem 2. UEU-a koje podliježu međunarodnom javnom pravu, koje je stoga primjereniji pravni okvir za reguliranje UI sustava u kontekstu korištenja smrtonosne sile i drugih UI sustava u kontekstu vojnih i obrambenih aktivnosti. Kad je riječ o nacionalnoj sigurnosti, isključenje je opravdano kako činjenicom da nacionalna sigurnost ostaje isključiva odgovornost država članica, u skladu s člankom 4. stavkom 2. UEU-a, tako i posebnom prirodom i operativnim potrebama aktivnosti povezanih s nacionalnom sigurnošću i posebnim nacionalnim pravilima koja se primjenjuju na te aktivnosti. Međutim, ako se UI sustav koji je razvijen, stavljen na tržište, stavljen u upotrebu ili se njime služi u vojne svrhe, obrambene svrhe ili u svrhe povezane s nacionalnom sigurnošću privremeno ili trajno upotrebljava u druge svrhe, na primjer civilne ili humanitarne, u svrhu kaznenog progona ili za potrebe javne sigurnosti, takav bi sustav bio obuhvaćen područjem primjene ove Uredbe. U tom bi slučaju subjekt koji UI sustav upotrebljava u svrhe koje nisu vojne svrhe, obrambene svrhe ili svrhe povezane s nacionalnom sigurnošću trebao osigurati usklađenost UI sustava s ovom Uredbom, osim ako je sustav s njome već usklađen. UI sustavi koji se stavljaju na tržište ili u upotrebu u isključene svrhe, odnosno vojne svrhe, obrambene svrhe ili svrhe povezane s nacionalnom sigurnošću, i u jednu ili više svrha koje nisu isključene, kao što su civilne svrhe ili kazneni progon, obuhvaćeni su područjem primjene ove Uredbe i dobavljači tih sustava trebali bi osigurati usklađenost s ovom Uredbom. U tim slučajevima činjenica da UI sustav može biti obuhvaćen područjem primjene ove Uredbe ne bi trebala utjecati na mogućnost da subjekti koji provode aktivnosti povezane s nacionalnom sigurnošću te obrambene i vojne aktivnosti, bez obzira na vrstu subjekta koji te aktivnosti obavlja, upotrebljavaju UI sustave čija je upotreba isključena iz područja primjene ove Uredbe u svrhe povezane s nacionalnom sigurnošću te vojne i obrambene svrhe. UI sustav koji se stavlja na tržište u civilne svrhe ili u svrhu kaznenog progona i koji se, s izmjenama ili bez njih, upotrebljava u vojne svrhe, obrambene svrhe ili u svrhe povezane s nacionalnom sigurnošću ne bi trebao biti obuhvaćen područjem primjene ove Uredbe, bez obzira na vrstu subjekta koji obavlja te aktivnosti.
- (25) Ovom bi se Uredbom trebale podupirati inovacije, trebala bi se poštovati sloboda znanosti te se njome ne bi smjele ugrožavati aktivnosti istraživanja i razvoja. Stoga je iz njezina područja primjene potrebno isključiti UI sustave i modele koji su posebno razvijeni i stavljeni u upotrebu isključivo u svrhu znanstvenog istraživanja i razvoja. Nadalje, potrebno je osigurati da ova Uredba na drugi način ne utječe na aktivnosti znanstvenog istraživanja i razvoja UI sustava ili modela prije njihova stavljanja na tržište ili u upotrebu. Kad je riječ o aktivnostima istraživanja, testiranja i razvoja u vezi s UI sustavima ili modelima usmjerenima na proizvode, odredbe ove Uredbe ne bi se trebale primjenjivati ni prije nego što se ti sustavi i modeli stave u upotrebu ili na tržište. Tim isključenjem ne dovodi se u pitanje obveza usklađivanja s ovom Uredbom ako se UI sustav obuhvaćen područjem primjene ove Uredbe stavlja na tržište ili u upotrebu kao rezultat takve aktivnosti istraživanja i razvoja niti se dovodi u pitanje primjena odredaba o regulatornim izoliranim okruženjima za umjetnu inteligenciju i testiranju u stvarnim uvjetima. Nadalje, ne dovodeći u pitanje isključenje UI sustava koji su posebno razvijeni i stavljeni u upotrebu isključivo u svrhu znanstvenog istraživanja i razvoja, svi ostali UI sustavi koji se mogu upotrebljavati za obavljanje bilo kakvih aktivnosti istraživanja i razvoja trebali bi i dalje podlijeagati odredbama ove Uredbe. U svakom slučaju, aktivnosti istraživanja i razvoja trebale bi se provoditi u skladu s priznatim etičkim i profesionalnim standardima za znanstvena istraživanja i u skladu s primjenjivim pravom Unije.
- (26) Kako bi se uveo proporcionalan i djelotvoran skup obvezujućih pravila za UI sustave, trebalo bi slijediti jasno definiran pristup temeljen na riziku. Vrsta i sadržaj tih pravila u tom bi pristupu trebali biti primjereni intenzitetu i opsegu rizika koje mogu stvoriti UI sustavi. Stoga je potrebno zabraniti određene neprihvatljive prakse u području umjetne inteligencije te utvrditi zahtjeve za visokorizične UI sustave i obveze za relevantne operatere te obveze u pogledu transparentnosti za određene UI sustave.

- (27) Iako je pristup temeljen na riziku osnova za razmjernan i djelotvoran skup obvezujućih pravila, važno je podsjetiti na Etičke smjernice za pouzdanu umjetnu inteligenciju iz 2019. koje je izradila neovisna Stručna skupina za umjetnu inteligenciju koju je imenovala Komisija. U tim je smjernicama Stručna skupina za umjetnu inteligenciju razvila sedam neobvezujućih etičkih načela za umjetnu inteligenciju kojima se nastoji osigurati pouzdanost i etička prihvatljivost umjetne inteligencije. Tih sedam načela uključuju ljudsko djelovanje i nadzor; tehničku otpornost i sigurnost; privatnost i upravljanje podacima; transparentnost; raznolikost, nediskriminaciju i pravednost; dobrobit društva i okoliša te odgovornost. Ne dovodeći u pitanje pravno obvezujuće zahtjeve iz ove Uredbe i bilo koje drugo primjenjivo pravo Unije, te smjernice doprinose dizajniranju koherentne, pouzdane i antropocentrične umjetne inteligencije, u skladu s Poveljom i vrijednostima na kojima se Unija temelji. Prema smjernicama Stručne skupine za umjetnu inteligenciju, „ljudsko djelovanje i nadzor” znači da se UI sustavi razvijaju i upotrebljavaju kao alat koji služi ljudima, poštuje ljudsko dostojanstvo i osobnu autonomiju te funkcionira na način koji ljudi mogu na odgovarajući način kontrolirati i nadzirati. Tehnička otpornost i sigurnost znači da se UI sustavi razvijaju i upotrebljavaju na način kojim se omogućuje otpornost u slučaju problema i odupiranje pokušajima promjene korištenja ili učinkovitosti UI sustava s ciljem da se trećim stranama omogući nezakonita upotreba, te kojim se nenamjerna šteta svodi na najmanju moguću mjeru. Privatnost i upravljanje podacima znači da se UI sustavi razvijaju i upotrebljavaju u skladu s pravilima o privatnosti i zaštiti podataka, pri čemu se obrađuju podaci koji ispunjavaju visoke standarde u pogledu kvalitete i cjelovitosti. Transparentnost znači da se UI sustavi razvijaju i upotrebljavaju na način kojim se omogućuje odgovarajuća sljedivost i objašnjivost, uz istodobno informiranje ljudi o tome da komuniciraju ili su u interakciji s UI sustavom te propisno obavješćivanje subjekata koji uvode sustav o sposobnostima i ograničenjima tog UI sustava, a osoba na koje utječe UI sustav o njihovim pravima. Raznolikost, nediskriminacija i pravednost znači da se UI sustavi razvijaju i upotrebljavaju na način koji uključuje različite aktere i kojim se promiču jednak pristup, rodna ravnopravnost i kulturna raznolikost, pri čemu se izbjegavaju diskriminirajući učinci i nepravedne pristranosti koji su zabranjeni pravom Unije ili nacionalnim pravom. Dobrobit društva i okoliša znači da se UI sustavi razvijaju i upotrebljavaju na održiv i okolišno prihvatljiv način i u korist svih ljudi, uz istodobno praćenje i procjenu dugoročnih učinaka na pojedinca, društvo i demokraciju. Ta bi se načela trebala primjenjivati i pri dizajniranju i korištenju UI modela, kada je to moguće. Ona bi u svakom slučaju trebala služiti kao osnova za izradu kodeksa ponašanja na temelju ove Uredbe. Sve dionike, uključujući industriju, akademsku zajednicu, civilno društvo i organizacije za normizaciju, potiče se da prema potrebi uzmu u obzir etička načela za razvoj dobrovoljnih najboljih praksi i normi.
- (28) Osim brojnih korisnih primjena umjetne inteligencije, ona se može i zloupotrijebiti te omogućiti nove i moćne alate za manipulativne i izrabljivačke prakse te prakse društvene kontrole. Takve su prakse osobito štetne i predstavljaju zlouporabu te bi ih trebalo zabraniti jer su protivne Unijanim vrijednostima poštovanja ljudskog dostojanstva, slobode, ravnopravnosti, demokracije i vladavine prava te temeljnih prava sadržanih u Povelji, uključujući pravo na nediskriminaciju, zaštitu podataka i privatnost te prava djeteta.
- (29) Manipulativne tehnike omogućene umjetnom inteligencijom mogu se upotrebljavati kako bi se osobe navelo na neželjeno ponašanje ili kako bi ih se obmanulo tako da ih se potiče na odluke na način kojim se podriva i narušava njihova autonomija, donošenje odluka i slobodan izbor. Stavljanje na tržište, stavljanje u upotrebu ili korištenje određenih UI sustava s ciljem ili učinkom bitnog iskrivljavanja ljudskog ponašanja, pri čemu je vjerojatno da će nastati znatna šteta, osobito ona koja ima dovoljno velike štetne učinke na fizičko ili psihološko zdravlje odnosno financijske interese, osobito su opasni te bi ih stoga trebalo zabraniti. U takvim se UI sustavima upotrebljavaju subliminalne komponente kao što su zvučni i slikovni podražaji te videopodražaji koje osobe ne mogu percipirati jer nadilaze ljudsku percepciju ili se upotrebljavaju druge manipulativne ili prijevorne tehnike kojima se podriva ili narušava autonomija, donošenje odluka ili slobodan izbor osobe na način da ljudi svjesno ne percipiraju te tehnike ili zbog kojih su, ako ih i jesu svjesni, svejedno prevareni ili ih ne mogu kontrolirati niti im se oduprijeti. To bi se, na primjer, moglo olakšati sučeljima mozak-računalo ili virtualnom stvarnošću jer se njima omogućuje viši stupanj kontrole toga koji se podražaji prikazuju osobama, u mjeri u kojoj bi oni mogli bitno iskriviti njihovo ponašanje na znatno štetan način. Osim toga, UI sustavi mogu na drugi način iskorištavati ranjivosti osobe ili određene skupine osoba zbog njihove dobi, invaliditeta u smislu Direktive (EU) 2019/882 Europskog parlamenta i Vijeća⁽¹⁶⁾ ili određene socijalne ili gospodarske situacije zbog kojih bi te osobe mogle biti izložene iskorištavanju, kao što su osobe koje žive u ekstremnom siromaštvu i etničke ili vjerske manjine. Takvi UI sustavi mogu se staviti na tržište, staviti u upotrebu ili se upotrebljavati s ciljem ili učinkom bitnog iskrivljavanja ponašanja osobe i to na način kojim se toj osobi ili drugoj osobi ili skupinama osoba uzrokuje znatan šteta ili je se može razumno očekivati da će se prouzročiti takva šteta, što uključuje štetu koja se može akumulirati s vremenom, te bi ih stoga trebalo zabraniti.

⁽¹⁶⁾ Direktiva (EU) 2019/882 Europskog parlamenta i Vijeća od 17. travnja 2019. o zahtjevima za pristupačnost proizvoda i usluga (SL L 151, 7.6.2019., str. 70.).

Možda nije moguće pretpostaviti postojanje namjere da se iskrivi ponašanje ako je to iskrivljavanje ponašanja posljedica čimbenika izvan UI sustava koji su izvan kontrole dobavljača ili subjekta koji uvodi sustav, odnosno čimbenika koje dobavljač UI sustava ili subjekt koji ga uvodi ne mogu u razumnoj mjeri predvidjeti i stoga ublažiti. U svakom slučaju, nije potrebno da dobavljač UI sustava ili subjekt koji ga uvodi ima namjeru prouzročiti znatnu štetu pod uvjetom da ta šteta proizlazi iz manipulativne ili izrabljivačke prakse omogućene umjetnom inteligencijom. Zabrane takvih praksi u području umjetne inteligencije komplementarne su odredbama sadržanima u Direktivi 2005/29/EZ Europskog parlamenta i Vijeća ⁽¹⁷⁾, osobito u pogledu toga da su nepošteno poslovne prakse koje dovode do gospodarske ili financijske štete potrošačima zabranjene u svim okolnostima, bez obzira na to provode li se putem UI sustava ili na drugi način. Zabrane manipulativnih i izrabljivačkih praksi iz ove Uredbe ne bi trebale utjecati na zakonite prakse u kontekstu liječenja, kao što je psihološko liječenje mentalnih bolesti ili fizička rehabilitacija, ako se te prakse provode u skladu s primjenjivim pravom i medicinskim standardima, kao što su izričita privola pojedinaca ili njihovih zakonskih zastupnika. Osim toga, uobičajene i zakonite poslovne prakse, primjerice u području oglašavanja, koje su u skladu s primjenjivim pravom ne bi same po sebi trebalo smatrati štetnom manipulativnom praksom omogućenom umjetnom inteligencijom.

- (30) Trebalo bi zabraniti sustave biometrijske kategorizacije koji se temelje na biometrijskim podacima fizičkih osoba, kao što su lice ili otisak prstiju pojedinca, kako bi se deduciralo ili izvelo zaključke o njegovim političkim mišljenjima, članstvu u sindikatima, vjerskim ili filozofskim uvjerenjima, rasi, spolnom životu ili seksualnoj orijentaciji. Ta zabrana ne bi trebala obuhvaćati zakonito označivanje, filtriranje ili kategorizaciju skupova biometrijskih podataka prikupljenih u skladu s pravom Unije ili nacionalnim pravom na temelju biometrijskih podataka, kao što je razvrstavanje slika prema boji kose ili boji očiju, koji se, primjerice, mogu upotrebljavati u području kaznenog progona.
- (31) UI sustavi koji omogućuju društveno vrednovanje fizičkih osoba koje upotrebljavaju javni ili privatni akteri mogu rezultirati diskriminatornim ishodima i isključivanjem određenih skupina. Njima se može prekršiti pravo na dostojanstvo i nediskriminaciju te vrijednosti kao što su ravnopravnost i pravda. Takvi UI sustavi evaluiraju ili klasificiraju fizičke osobe ili skupine fizičkih osoba na temelju višestrukih podataka povezanih s njihovim društvenim ponašanjem u višestrukim kontekstima ili poznatih, izvedenih ili predviđenih osobnih značajki ili značajki osobnosti tijekom određenih razdoblja. Društveni rejting dobiven takvim UI sustavima može rezultirati štetnim ili nepovoljnim tretmanom fizičkih osoba ili cijelih skupina fizičkih osoba u društvenim kontekstima koji nisu povezani s kontekstom u kojima su podaci izvorno generirani ili prikupljeni odnosno štetnim tretmanom koji je nerazmjeran ili neopravdan u odnosu na težinu posljedica njihova društvenog ponašanja. Stoga bi UI sustave koji uključuju takve neprihvatljive prakse vrednovanja i koji rezultiraju takvim štetnim ili nepovoljnim ishodima trebalo zabraniti. Ta zabrana ne bi trebala utjecati na zakonite prakse evaluacije fizičkih osoba koje se provode u specifičnu svrhu u skladu s pravom Unije i nacionalnim pravom.
- (32) Korištenje UI sustava za daljinsku biometrijsku identifikaciju fizičkih osoba u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona osobito je intruzivno za prava i slobode dotičnih osoba, u onoj mjeri u kojoj može utjecati na privatni život velikog dijela stanovništva, pobuditi doživljaj stalnog nadzora i neizravno odvratiti od ostvarivanja slobode okupljanja i drugih temeljnih prava. Tehničke netočnosti UI sustava namijenjenih daljinskoj biometrijskoj identifikaciji fizičkih osoba mogu rezultirati pristranim rezultatima i imati diskriminacijske učinke. Takvi potencijalni pristrani rezultati i diskriminacijski učinci osobito su relevantni s obzirom na dob, etničku pripadnost, rasu, spol ili invaliditet. Osim toga, neposrednost učinka i ograničene mogućnosti za dodatne provjere ili ispravke u pogledu korištenja takvih sustava koji funkcioniraju u stvarnom vremenu nose povećane rizike za prava i slobode dotičnih osoba u kontekstu aktivnosti kaznenog progona ili na koje aktivnosti kaznenog progona utječu.
- (33) Stoga bi trebalo zabraniti korištenje tih sustava u svrhu kaznenog progona, osim u taksativno popisanim i usko definiranim situacijama u kojima je ono nužno za ostvarenje znatnog javnog interesa, čija važnost premašuje rizike. Te situacije uključuju potragu za određenim žrtvama kaznenih djela, uključujući nestale osobe, određene prijetnje životu ili tjelesnoj sigurnosti fizičkih osoba ili prijetnje od terorističkih napada i lociranje ili identifikaciju počinitelja kaznenih djela ili osumnjičenika za kaznena djela iz priloga ovoj Uredbi, ako je za ta kaznena djela u dotičnoj državi

⁽¹⁷⁾ Direktiva 2005/29/EZ Europskog parlamenta i Vijeća od 11. svibnja 2005. o nepoštenoj poslovnoj praksi poslovnog subjekta u odnosu prema potrošaču na unutarnjem tržištu i o izmjeni Direktive Vijeća 84/450/EEZ, direktiva 97/7/EZ, 98/27/EZ i 2002/65/EZ Europskog parlamenta i Vijeća, kao i Uredbe (EZ) br. 2006/2004 Europskog parlamenta i Vijeća („Direktiva o nepoštenoj poslovnoj praksi”) (SL L 149, 11.6.2005., str. 22.).

članici zapriječena kazna zatvora ili oduzimanja slobode u maksimalnom trajanju od najmanje četiri godine i kako su definirana u pravu te države članice. Takvim pragom za kaznu zatvora ili oduzimanje slobode u skladu s nacionalnim pravom doprinosi se osiguravanju toga da kazneno djelo bude dovoljno teško da bi se moglo opravdati korištenje sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu. Nadalje, popis kaznenih djela naveden u prilogu ovoj Uredbi temelji se na 32 kaznena djela navedena u Okvirnoj odluci Vijeća 2002/584/PUP⁽¹⁸⁾, uzimajući u obzir da su neka od tih kaznenih djela u praksi vjerojatno relevantnija od drugih, u smislu da bi primjena daljinske biometrijske identifikacije u stvarnom vremenu mogla biti predvidljivo potrebna i proporcionalna u vrlo promjenjivim opsezima za praktičnu provedbu lokalizacije ili identifikacije počinitelja različitih navedenih kaznenih djela ili osumnjičenika za ta kaznena djela i s obzirom na vjerojatne razlike u težini, vjerojatnosti i razmjeru štete ili mogućih negativnih posljedica. Izravna prijetnja životu ili tjelesnoj sigurnosti fizičkih osoba mogla bi također rezultirati iz ozbiljnog poremećaja kritične infrastrukture, kako je definirana u članku 2. točki 4. Direktive (EU) 2022/2557 Europskog parlamenta i Vijeća⁽¹⁹⁾, ako bi poremećaj u radu ili uništenje takve kritične infrastrukture prouzročili izravnu prijetnju životu ili tjelesnoj sigurnosti osobe, među ostalim i putem teške štete pružanju osnovne opskrbe stanovništva ili izvršavanju temeljne funkcije države. Osim toga, ovom bi se Uredbom trebala očuvati sposobnost tijela kaznenog progona, tijela nadležnih za nadzor granica, tijela nadležnih za imigraciju ili tijela nadležnih za azil da provode provjere identiteta u prisutnosti dotične osobe, u skladu s uvjetima utvrđenima za takve provjere u pravu Unije i nacionalnom pravu. Tijela kaznenog progona, tijela nadležna za nadzor granica, tijela nadležna za imigraciju ili tijela nadležna za azil osobito bi se trebala moći koristiti informacijskim sustavima, u skladu s pravom Unije ili nacionalnim pravom, za identifikaciju osoba koje se tijekom provjere identiteta odbijaju identificirati ili nisu u stanju navesti ili dokazati svoj identitet, a da pritom ne moraju pribaviti prethodno odobrenje na temelju ove Uredbe. To bi, na primjer, mogla biti osoba uključena u kazneno djelo, koja nije voljna ili koja zbog nesreće ili zdravstvenog stanja nije u stanju otkriti svoj identitet tijelima kaznenog progona.

- (34) Kako bi se osiguralo odgovorno i proporcionalno korištenje tih sustava, važno je i utvrditi da bi u svakoj od tih taksativno popisanih i usko definiranih situacija trebalo uzeti u obzir određene elemente, osobito u pogledu prirode situacije zbog koje se zahtijeva njihova upotreba i posljedica te upotrebe za prava i slobode svih dotičnih osoba te u pogledu zaštitnih mjera i uvjeta propisanih za tu upotrebu. Osim toga, sustavi za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona trebali bi se upotrebljavati samo za potvrđivanje identiteta konkretno ciljanog pojedinca i ta bi upotreba trebala biti ograničena na ono što je nužno kad je riječ o razdoblju te zemljopisnom i personalnom području primjene, uzimajući osobito u obzir dokaze ili naznake u vezi s prijetnjama, žrtvama ili počiniteljem. Upotrebu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima trebalo bi odobriti samo ako je relevantno tijelo kaznenog progona dovršilo procjenu učinka na temeljna prava i, osim ako je drukčije predviđeno u ovoj Uredbi, registriralo sustav u bazi podataka kako je utvrđeno u ovoj Uredbi. Referentna baza podataka osoba trebala bi biti primjerena za svaki slučaj korištenja u svakoj od gore navedenih situacija.

- (35) Uvjet za svaku upotrebu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona trebalo bi biti izričito i specifično odobrenje pravosudnog tijela ili neovisnog upravnog tijela države članice čija je odluka obvezujuća. Takvo bi odobrenje u načelu trebalo pribaviti prije upotrebe UI sustava radi identifikacije jedne ili više osoba. Iznimke od tog pravila trebalo bi dopustiti u propisno opravdanim situacijama na temelju hitnosti, odnosno u situacijama u kojima je potreba za upotrebom dotičnih sustava takva da je praktično i objektivno nemoguće pribaviti odobrenje prije početka upotrebe UI sustava. U takvim hitnim situacijama upotreba UI sustava trebala bi biti ograničena na apsolutno nužni minimum te podlijezati odgovarajućim zaštitnim mjerama i uvjetima, kako je utvrđeno u nacionalnom pravu i kako je odredilo samo tijelo kaznenog progona u kontekstu svakog pojedinačnog hitnog slučaja upotrebe. Osim toga, tijelo kaznenog progona trebalo bi u takvim situacijama zatražiti takvo odobrenje uz navođenje razloga zbog kojih ga nije moglo zatražiti ranije, bez nepotrebne odgode, a najkasnije u roku od 24 sata. Ako je takvo odobrenje odbijeno, upotrebu sustava za biometrijsku identifikaciju u stvarnom vremenu povezanu s tim odobrenjem trebalo bi smjesti zaustaviti te bi sve podatke povezane s takvom upotrebom trebalo odbaciti i izbrisati. Takvi podaci uključuju ulazne podatke koje je UI sustav izravno prikupio

⁽¹⁸⁾ Okvirna odluka Vijeća 2002/584/PUP od 13. lipnja 2002. o Europskom uhiđenom nalogu i postupcima predaje između država članica (SL L 190, 18.7.2002., str. 1.).

⁽¹⁹⁾ Direktiva (EU) 2022/2557 Europskog parlamenta i Vijeća od 14. prosinca 2022. o otpornosti kritičnih subjekata i o stavljanju izvan snage Direktive Vijeća 2008/114/EZ (SL L 333, 27.12.2022., str. 164.).

tijekom upotrebe takvog sustava te rezultate i izlazne podatke upotrebe povezane s tim odobrenjem. Ne bi trebali uključivati ulazne podatke koji su zakonito pribavljeni u skladu s drugim pravom Unije ili nacionalnim pravom. U svakom slučaju, odluku koja proizvodi negativan pravni učinak na osobu ne bi trebalo donijeti isključivo na temelju izlaznih podataka sustava za daljinsku biometrijsku identifikaciju.

- (36) Kako bi obavljali svoje zadaće u skladu sa zahtjevima utvrđenima u ovoj Uredbi i nacionalnim pravilima, relevantno tijelo za nadzor tržišta i nacionalno tijelo za zaštitu podataka trebali bi biti obaviješteni o svakom korištenju sustava za biometrijsku identifikaciju u stvarnom vremenu. Tijela za nadzor tržišta i prijavljena nacionalna tijela za zaštitu podataka trebala bi Komisiji podnositi godišnje izvješće o korištenju sustava za biometrijsku identifikaciju u stvarnom vremenu.
- (37) Nadalje, primjereno je u kontekstu iscrpnog okvira utvrđenog ovom Uredbom predvidjeti da bi takvo korištenje na državnom području države članice u skladu s ovom Uredbom trebalo biti moguće samo ako i u mjeri u kojoj je dotična država članica odlučila izričito predvidjeti mogućnost odobravanja takvog korištenja u svojim podrobnim pravilima nacionalnog prava. Stoga države članice na temelju ove Uredbe i dalje mogu slobodno odlučiti da neće uopće predvidjeti takvu mogućnost ili mogu predvidjeti takvu mogućnost samo u odnosu na neke od ciljeva kojima se može opravdati odobreno korištenje utvrđeno u ovoj Uredbi. O takvim nacionalnim pravilima trebalo bi obavijestiti Komisiju u roku od 30 dana od njihova donošenja.
- (38) Korištenje UI sustavâ za daljinsku biometrijsku identifikaciju pojedinaca u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona nužno uključuje obradu biometrijskih podataka. Pravila iz ove Uredbe kojima se, podložno određenim iznimkama, zabranjuje takvo korištenje, koja se temelje na članku 16. UFEU-a, trebala bi se primjenjivati kao *lex specialis* u odnosu na pravila o obradi biometrijskih podataka iz članka 10. Direktive (EU) 2016/680, čime se na iscrpan način uređuje takvo korištenje i obrada biometrijskih podataka. Stoga bi takvo korištenje i obrada trebali biti mogući samo u onoj mjeri u kojoj su u skladu s okvirom utvrđenim ovom Uredbom, pri čemu ne bi trebao postojati prostor, izvan tog okvira, da nadležna tijela koja djeluju u svrhu kaznenog progona upotrebljavaju takve sustave i obrađuju takve povezane podatke na temelju razloga navedenih u članku 10. Direktive (EU) 2016/680. U tom kontekstu svrha ove Uredbe nije pružanje pravne osnove za obradu osobnih podataka na temelju članka 8. Direktive (EU) 2016/680. Međutim, korištenje sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u druge svrhe osim kaznenog progona, među ostalim kad ih upotrebljavaju nadležna tijela, ne bi trebalo biti obuhvaćeno posebnim okvirom o takvom korištenju u svrhu kaznenog progona utvrđenim ovom Uredbom. Takvo korištenje u druge svrhe osim kaznenog progona stoga ne bi trebalo podlijeći zahtjevu za odobrenje na temelju ove Uredbe te važećim podrobnim pravilima nacionalnog prava kojima se daje učinak tom odobrenju.
- (39) Svaka obrada biometrijskih podataka i drugih osobnih podataka povezana s korištenjem UI sustavâ za biometrijsku identifikaciju, osim obrade povezane s korištenjem sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona kako je uređeno ovom Uredbom, i dalje bi trebala ispunjavati sve zahtjeve koji proizlaze iz članka 10. Direktive (EU) 2016/680. U svrhe koje nisu kazneni progon, člankom 9. stavkom 1. Uredbe (EU) 2016/679 i člankom 10. stavkom 1. Uredbe (EU) 2018/1725 zabranjuje se obrada biometrijskih podataka koji podliježu ograničenim iznimkama kako je predviđeno u tim člancima. Primjenom članka 9. stavka 1. Uredbe (EU) 2016/679 nacionalna tijela za zaštitu podataka već su donijela odluke o zabrani upotrebe daljinske biometrijske identifikacije u svrhe koje nisu kazneni progon.
- (40) U skladu s člankom 6.a Protokola br. 21 o stajalištu Ujedinjene Kraljevine i Irske s obzirom na područje slobode, sigurnosti i pravde, priloženog UEU-u i UFEU-u, Irsku ne obvezuju pravila utvrđena u članku 5. stavku 1. prvom podstavku točki (g), u mjeri u kojoj se primjenjuje na korištenje sustavâ biometrijske kategorizacije za aktivnosti u području policijske suradnje i pravosudne suradnje u kaznenim stvarima, u članku 5. stavku 1. prvom podstavku točki (d), u mjeri u kojoj se primjenjuje na korištenje UI sustava obuhvaćenih tom odredbom, u članku 5. stavku 1. prvom podstavku točki (h), u članku 5. stavicama od 2. do 6. i u članku 26. stavku 10. ove Uredbe, donesena na temelju članka 16. UFEU-a, koja se odnose na obradu osobnih podataka koju vrše države članice pri obavljanju aktivnosti koje su obuhvaćene dijelom trećim glavom V. poglavljem 4. ili poglavljem 5. UFEU-a ako Irsku ne obvezuju pravila koja uređuju oblike pravosudne suradnje u kaznenim stvarima ili policijske suradnje za koja se zahtijeva usklađenost s odredbama utvrđenima na temelju članka 16. UFEU-a.
- (41) U skladu s člancima 2. i 2.a Protokola br. 22 o stajalištu Danske, priloženog UEU-u i UFEU-u, Dansku ne obvezuju pravila utvrđena u članku 5. stavku 1. točki (g), u mjeri u kojoj se primjenjuje na korištenje sustavâ biometrijske kategorizacije za aktivnosti u području policijske suradnje i pravosudne suradnje u kaznenim stvarima, u članku 5. stavku 1. prvom podstavku točki (d), u mjeri u kojoj se primjenjuje na korištenje UI sustava obuhvaćenih tom odredbom, u članku 5. stavku 1. prvom podstavku točki (h), u članku 5. stavicama od 2. do 6. i u članku 26.

stavku 10. ove Uredbe, donesena na temelju članka 16. UFEU-a, niti ona podliježe primjeni tih pravila koja se odnose na obradu osobnih podataka koju vrše države članice pri obavljanju aktivnosti koje su obuhvaćene dijelom trećim glavom V. poglavljem 4. ili poglavljem 5. UFEU-a.

- (42) U skladu s pretpostavkom nedužnosti, fizičke osobe u Uniji uvijek bi trebalo prosuđivati na temelju njihova stvarnog ponašanja. Fizičke osobe nikada ne se bi trebale prosuđivati na temelju ponašanja koje je umjetna inteligencija predviđela isključivo na temelju njihova profiliranja, obilježja osobnosti ili značajki kao što su državljanstvo, mjesto rođenja, mjesto boravišta, broj djece, razina duga ili vrsta automobila, bez opravdane sumnje da je ta osoba uključena u kriminalnu aktivnost na temelju objektivnih provjerljivih činjenica i bez ljudske procjene tih činjenica. Stoga bi trebalo zabraniti procjene rizika u pogledu fizičkih osoba u svrhu procjene vjerojatnosti da će počiniti kaznena djela ili u svrhu predviđanja počinjenja stvarnog ili potencijalnog kaznenog djela isključivo na temelju profiliranja tih osoba ili procjene njihovih obilježja osobnosti i značajki. U svakom slučaju, ta se zabrana ne odnosi niti se dotiče analitike rizika koja se ne temelji na profiliranju pojedinaca ili na obilježjima osobnosti i značajkama pojedinaca, kao što su UI sustavi koji upotrebljavaju analitiku rizika u svrhu procjene vjerojatnosti počinjenja financijskih prijevara od strane poduzeća na temelju sumnjivih transakcija ili alate za analizu rizika kako bi predviđeli vjerojatnost lokalizacije narkotika ili nezakonite robe od strane carinskih tijela, primjerice na temelju poznatih krijumčarskih ruta.
- (43) Trebalo bi zabraniti stavljanje na tržište, stavljanje u upotrebu u tu specifičnu svrhu ili korištenje UI sustava koji stvaraju ili proširuju baze podataka za prepoznavanje lica neciljanim prikupljanjem prikaza lica s interneta ili iz snimaka CCTV-a jer ta praksa doprinosi osjećaju masovnog nadzora i može dovesti do teških kršenja temeljnih prava, uključujući pravo na privatnost.
- (44) Postoji ozbiljna zabrinutost u pogledu znanstvene osnove UI sustavâ čiji je cilj utvrđivanje emocija ili izvođenje zaključaka o njima, osobito s obzirom na to da se izražavanje emocija znatno razlikuje među kulturama i situacijama, pa čak kod istog pojedinca. Među ključnim su nedostacima takvih sustava ograničena pouzdanost, nedostatak specifičnosti i ograničena mogućnost generalizacije. Stoga UI sustavi koji identificiraju emocije ili namjere fizičkih osoba ili izvođe zaključke o njihovim emocijama ili namjerama na temelju njihovih biometrijskih podataka mogu dovesti do diskriminatornih ishoda te biti intruzivni za prava i slobode dotičnih osoba. S obzirom na neravnotežu moći u kontekstu rada ili obrazovanja, u kombinaciji s intruzivnom prirodom tih sustava, takvi bi sustavi mogli dovesti do štetnog ili nepovoljnog tretmana određenih fizičkih osoba ili cijelih skupina određenih fizičkih osoba. Stoga bi trebalo zabraniti stavljanje na tržište, stavljanje u upotrebu ili korištenje UI sustava namijenjenih za otkrivanje emocionalnog stanja pojedinaca u situacijama povezanim s radnim mjestom i obrazovanjem. Ta zabrana ne bi trebala obuhvaćati UI sustave koji se stavljaju na tržište isključivo iz medicinskih ili sigurnosnih razloga, kao što su sustavi namijenjeni terapijskoj upotrebi.
- (45) Ova Uredba ne bi trebala utjecati na prakse koje su zabranjene pravom Unije, među ostalim u okviru prava o zaštiti podataka, nediskriminacijskog prava, prava o zaštiti potrošača i prava tržišnog natjecanja.
- (46) Visokorizični UI sustavi trebali bi se stavljati na tržište Unije ili u upotrebu odnosno upotrebljavati se samo ako ispunjavaju određene obvezne zahtjeve. Tim bi se zahtjevima trebalo osigurati da visokorizični UI sustavi koji su dostupni u Uniji ili čije se izlazne vrijednosti na drugi način upotrebljavaju u Uniji ne predstavljaju neprihvatljiv rizik za važne javne interese Unije koji su priznati i zaštićeni pravom Unije. Na temelju novog zakonodavnog okvira, kako je pojašnjeno u obavijesti Komisije pod nazivom „Plavi vodič” o provedbi pravila EU-a o proizvodima 2022.”⁽²⁰⁾, opće je pravilo da se više od jednog pravnog akta zakonodavstva Unije o usklađivanju, kao što su uredbe (EU) 2017/745⁽²¹⁾ i (EU) 2017/746⁽²²⁾ Europskog parlamenta i Vijeća ili Direktiva 2006/42/EZ Europskog parlamenta i Vijeća⁽²³⁾, može primjenjivati na jedan proizvod jer se stavljanje na raspolaganje ili u upotrebu može provesti samo ako je proizvod u skladu sa svim primjenjivim zakonodavstvom Unije o usklađivanju. Kako bi se osigurala

⁽²⁰⁾ SL C 247, 29.6.2022., str. 1.

⁽²¹⁾ Uredba (EU) 2017/745 Europskog parlamenta i Vijeća od 5. travnja 2017. o medicinskim proizvodima, o izmjeni Direktive 2001/83/EZ, Uredbe (EZ) br. 178/2002 i Uredbe (EZ) br. 1223/2009 te o stavljanju izvan snage direktiva Vijeća 90/385/EEZ i 93/42/EEZ (SL L 117, 5.5.2017., str. 1.).

⁽²²⁾ Uredba (EU) 2017/746 Europskog parlamenta i Vijeća od 5. travnja 2017. o *in vitro* dijagnostičkim medicinskim proizvodima te o stavljanju izvan snage Direktive 98/79/EZ i Odluke Komisije 2010/227/EU (SL L 117, 5.5.2017., str. 176.).

⁽²³⁾ Direktiva 2006/42/EZ Europskog parlamenta i Vijeća od 17. svibnja 2006. o strojevima o izmjeni Direktive 95/16/EZ (SL L 157, 9.6.2006., str. 24.).

dosljednost i izbjegla nepotrebna administrativna opterećenja ili troškovi, dobavljači proizvoda koji sadržava jedan ili više visokorizičnih UI sustava, na koje se primjenjuju zahtjevi iz ove Uredbe i zahtjevi iz zakonodavstva Unije o usklađivanju navedeni u prilogu ovoj Uredbi, trebali bi biti fleksibilni u pogledu operativnih odluka o tome kako na najbolji način osigurati usklađenost proizvoda koji sadržava jedan ili više UI sustava sa svim primjenjivim zahtjevima zakonodavstva Unije o usklađivanju. UI sustavi utvrđeni kao visokorizični trebali bi biti ograničeni samo na one koji imaju znatan štetan učinak na zdravlje, sigurnost i temeljna prava osoba u Uniji i takvim bi se ograničenjem trebalo svesti na najmanju moguću mjeru bilo kakvo potencijalno ograničenje u pogledu međunarodne trgovine.

- (47) UI sustavi mogli bi nepovoljno utjecati na zdravlje i sigurnost osoba, osobito ako ti sustavi funkcioniraju kao sigurnosne komponente proizvoda. U skladu s ciljevima zakonodavstva Unije o usklađivanju, kako bi se olakšalo slobodno kretanje proizvoda na unutarnjem tržištu i kako bi se zajamčilo da na tržište dolaze samo sigurni i sukladni proizvodi, važno je da se propisno spriječe i ublaže mogući sigurnosni rizici koje proizvod u cijelosti može predstavljati zbog svojih digitalnih komponenti, uključujući UI sustave. Na primjer, sve autonomniji roboti, bilo u kontekstu proizvodnje ili osobne skrbi i njege, trebali bi moći funkcionirati na siguran način i obavljati svoje zadaće u složenim okruženjima. Slično tome, u zdravstvenom sektoru u kojem su rizici za život i zdravlje osobito visoki, sve sofisticiraniji dijagnostički sustavi i sustavi koji pomažu ljudima u donošenju odluka trebali bi biti pouzdani i točni.
- (48) Razmjer nepovoljnih učinaka UI sustava na temeljna prava zaštićena Poveljom posebno je važan pri klasificiranju UI sustava kao visokorizičnog. Ta prava uključuju pravo na ljudsko dostojanstvo, poštovanje privatnog i obiteljskog života, zaštitu osobnih podataka, slobodu izražavanja i informiranja, slobodu okupljanja i udruživanja, pravo na nediskriminaciju, pravo na obrazovanje, zaštitu potrošača, prava radnika, prava osoba s invaliditetom, rodnu ravnopravnost, prava intelektualnog vlasništva, pravo na djelotvoran pravni lijek i na pošteno suđenje, pravo na obranu i pretpostavku nedužnosti te pravo na dobru upravu. Povrh tih prava, važno je naglasiti činjenicu da djeca imaju posebna prava sadržana u članku 24. Povelje i u Konvenciji Ujedinjenih naroda o pravima djeteta, podrobnije razrađena u Općoj napomeni br. 25 Odbora UN-a o pravima djece u pogledu digitalnog okruženja, kojima se zahtijeva da se vodi računa o njihovoj ranjivosti te da se osiguraju zaštita i skrb potrebni za njihovu dobrobit. Pri procjeni težine štete koju pojedini UI sustav može prouzročiti, među ostalim i u pogledu zdravlja i sigurnosti osoba, trebalo bi uzeti u obzir i temeljno pravo na visoku razinu zaštite okoliša koje je utvrđeno u Povelji i provodi se u politikama Unije.
- (49) Kad je riječ o visokorizičnim UI sustavima koji su sigurnosne komponente proizvoda ili sustava odnosno koji su sami proizvodi ili sustavi obuhvaćeni područjem primjene Uredbe (EZ) br. 300/2008 Europskog parlamenta i Vijeća ⁽²⁴⁾, Uredbe (EU) br. 167/2013 Europskog parlamenta i Vijeća ⁽²⁵⁾, Uredbe (EU) br. 168/2013 Europskog parlamenta i Vijeća ⁽²⁶⁾, Direktive 2014/90/EU Europskog parlamenta i Vijeća ⁽²⁷⁾, Direktive (EU) 2016/797 Europskog parlamenta i Vijeća ⁽²⁸⁾, Uredbe (EU) 2018/858 Europskog parlamenta i Vijeća ⁽²⁹⁾, Uredbe (EU)

⁽²⁴⁾ Uredba (EZ) br. 300/2008 Europskog parlamenta i Vijeća od 11. ožujka 2008. o zajedničkim pravilima u području zaštite civilnog zračnog prometa i stavljanju izvan snage Uredbe (EZ) br. 2320/2002 (SL L 97, 9.4.2008., str. 72.).

⁽²⁵⁾ Uredba (EU) br. 167/2013 Europskog parlamenta i Vijeća od 5. veljače 2013. o homologaciji i nadzoru tržišta traktora za poljoprivredu i šumarstvo (SL L 60, 2.3.2013., str. 1.).

⁽²⁶⁾ Uredba (EU) br. 168/2013 Europskog parlamenta i Vijeća od 15. siječnja 2013. o homologaciji i nadzoru tržišta vozila na dva ili tri kotača i četverokotaka (SL L 60, 2.3.2013., str. 52.).

⁽²⁷⁾ Direktiva 2014/90/EU Europskog parlamenta i Vijeća od 23. srpnja 2014. o pomorskoj opremi i stavljanju izvan snage Direktive Vijeća 96/98/EZ (SL L 257, 28.8.2014., str. 146.).

⁽²⁸⁾ Direktiva (EU) 2016/797 Europskog parlamenta i Vijeća od 11. svibnja 2016. o interoperabilnosti željezničkog sustava u Europskoj uniji (SL L 138, 26.5.2016., str. 44.).

⁽²⁹⁾ Uredba (EU) 2018/858 Europskog parlamenta i Vijeća od 30. svibnja 2018. o homologaciji i nadzoru tržišta motornih vozila i njihovih prikolica te sustava, sastavnih dijelova i zasebnih tehničkih jedinica namijenjenih za takva vozila, o izmjeni uredaba (EZ) br. 715/2007 i (EZ) br. 595/2009 te o stavljanju izvan snage Direktive 2007/46/EZ (SL L 151, 14.6.2018., str. 1.).

2018/1139 Europskog parlamenta i Vijeća⁽³⁰⁾ i Uredbe (EU) 2019/2144 Europskog parlamenta i Vijeća⁽³¹⁾, primjereno je te akte izmijeniti kako bi se osiguralo da Komisija, na temelju tehničkih i regulatornih posebnosti svakog sektora te bez uplitanja u postojeće mehanizme upravljanja, ocjenjivanja sukladnosti i izvršavanja te rad tijela koja su u njima utvrđena, pri donošenju svih relevantnih delegiranih akata ili provedbenih akata na temelju tih akata uzima u obzir obvezne zahtjeve za visokorizične UI sustave utvrđene u ovoj Uredbi.

- (50) Kad je riječ o UI sustavima koji su sigurnosne komponente proizvoda ili koji su sami proizvodi, a obuhvaćeni su područjem primjene određenog zakonodavstva Unije o usklađivanju navedenog u prilogu ovoj Uredbi, primjereno ih je klasificirati kao visokorizične na temelju ove Uredbe ako je dotični proizvod predmet postupka ocjenjivanja sukladnosti koji provodi tijelo za ocjenjivanje sukladnosti kao treća strana na temelju relevantnog zakonodavstva Unije o usklađivanju. Takvi su proizvodi osobito strojevi, igračke, dizala, oprema i zaštitni sustavi namijenjeni za korištenje u potencijalno eksplozivnim atmosferama, radijska oprema, tlačna oprema, oprema za rekreacijska plovila, žičare, aparati na plinovita goriva, medicinski proizvodi i *in vitro* dijagnostički medicinski proizvodi, automobili i zrakoplovi.
- (51) Klasifikacija UI sustava kao visokorizičnog na temelju ove Uredbe ne bi nužno trebala značiti da se proizvod čija je sigurnosna komponenta UI sustav ili da se sâm UI sustav kao proizvod smatra „visokorizičnim” na temelju kriterija utvrđenih u relevantnom zakonodavstvu Unije o usklađivanju koje se primjenjuje na taj proizvod. To se osobito odnosi na uredbe (EU) 2017/745 i (EU) 2017/746 ako je predviđeno da treća strana provodi ocjenjivanje sukladnosti za srednjorizične i visokorizične proizvode.
- (52) Kad je riječ o samostalnim UI sustavima, odnosno visokorizičnim UI sustavima koji nisu sigurnosne komponente proizvoda ili koji su sami proizvodi, primjereno ih je klasificirati kao visokorizične ako, s obzirom na njihovu namjenu, kod njih postoji visok rizik od štete za zdravlje i sigurnost ili temeljna prava osoba, uzimajući u obzir i težinu moguće štete i njezinu vjerojatnost nastanka, te ako se upotrebljavaju u nekoliko posebnih unaprijed definiranih područja navedenih u ovoj Uredbi. Utvrđivanje tih sustava temelji se na istoj metodologiji i kriterijima predviđenima i za sve buduće izmjene popisa visokorizičnih UI sustava koje bi Komisija trebala biti ovlaštena donijeti delegiranim aktima kako bi se uzeo u obzir brz tempo tehnološkog razvoja i moguće promjene u korištenju UI sustava.
- (53) Važno je pojasniti i da mogu postojati posebni slučajevi u kojima UI sustavi na koje se upućuje u unaprijed definiranim područjima navedenima u ovoj Uredbi ne dovode do znatnog rizika od štete za pravne interese zaštićene na temelju tih područja jer bitno ne utječu na donošenje odluka ili ne štete znatno tim interesima. Za potrebe ove Uredbe UI sustav koji bitno ne utječe na ishod donošenja odluka trebalo bi razumjeti kao UI sustav koji ne utječe na sadržaj, a time ni na ishod donošenja odluka, bilo da je odluke donose ljudi ili da je donošenje odluka automatizirano. UI sustav koji bitno ne utječe na ishod donošenja odluka mogao bi uključivati situacije u kojima je ispunjen jedan od sljedećih uvjeta ili više njih. Prvi takav uvjet trebao bi biti da je UI sustav namijenjen obavljanju uske postupovne zadaće, kao što je UI sustav koji pretvara nestrukturirane podatke u strukturirane podatke, UI sustav koji dolazne dokumente klasificira u kategorije ili UI sustav koji se upotrebljava za otkrivanje duplikata među velikim brojem primjena. Te su zadaće toliko uske i ograničene da predstavljaju samo ograničene rizike koji se ne povećavaju korištenjem UI sustava u kontekstu koji je naveden kao visokorizična upotreba u prilogu ovoj Uredbi. Drugi uvjet trebao bi biti da je zadaća koju obavlja UI sustav namijenjena poboljšanju rezultata prethodno završene

⁽³⁰⁾ Uredba (EU) 2018/1139 Europskog parlamenta i Vijeća od 4. srpnja 2018. o zajedničkim pravilima u području civilnog zrakoplovstva i osnivanju Agencije Europske unije za sigurnost zračnog prometa i izmjeni uredbi (EZ) br. 2111/2005, (EZ) br. 1008/2008, (EU) br. 996/2010, (EU) br. 376/2014 i direktiva 2014/30/EU i 2014/53/EU Europskog parlamenta i Vijeća te stavljanju izvan snage uredbi (EZ) br. 552/2004 i (EZ) br. 216/2008 Europskog parlamenta i Vijeća i Uredbe Vijeća (EEZ) br. 3922/91 (SL L 212, 22.8.2018., str. 1.).

⁽³¹⁾ Uredba (EU) 2019/2144 Europskog parlamenta i Vijeća od 27. studenoga 2019. o zahtjevima za homologaciju tipa za motorna vozila i njihove prikolicke te za sustave, sastavne dijelove i zasebne tehničke jedinice namijenjene za takva vozila, u pogledu njihove opće sigurnosti te zaštite osoba u vozilima i nezaštićenih sudionika u cestovnom prometu, o izmjeni Uredbe (EU) 2018/858 Europskog parlamenta i Vijeća i stavljanju izvan snage uredbi (EZ) br. 78/2009, (EZ) br. 79/2009 i (EZ) br. 661/2009 Europskog parlamenta i Vijeća i uredbi Komisije (EZ) br. 631/2009, (EU) br. 406/2010, (EU) br. 672/2010, (EU) br. 1003/2010, (EU) br. 1005/2010, (EU) br. 1008/2010, (EU) br. 1009/2010, (EU) br. 19/2011, (EU) br. 109/2011, (EU) br. 458/2011, (EU) br. 65/2012, (EU) br. 130/2012, (EU) br. 347/2012, (EU) br. 351/2012, (EU) br. 1230/2012 i (EU) 2015/166 (SL L 325, 16.12.2019., str. 1.).

ljudske aktivnosti koja može biti relevantna za potrebe visokorizičnih upotreba navedenih u prilogu ovog Uredbi. S obzirom na te značajke UI sustav samo je dodatak ljudskoj aktivnosti uz posljedično smanjeni rizik. Na primjer, taj bi se uvjet primjenjivao na UI sustave namijenjene poboljšanju jezika koji se upotrebljava u prethodno izrađenim dokumentima, primjerice u vezi s profesionalnim tonom, akademskim stilom jezika ili usklađivanjem teksta s određenim porukama robne marke. Treći uvjet trebao bi biti da je namjena UI sustava otkrivanje obrazaca donošenja odluka ili odstupanja od prethodnih obrazaca donošenja odluka. Rizik bi se smanjio jer korištenje UI sustava slijedi nakon prethodno dovršene ljudske procjene, koju ono ne namjerava zamijeniti niti utjecati na nju bez odgovarajućeg preispitivanja koje provodi čovjek. Takvi UI sustavi obuhvaćaju, na primjer, sustave koji se na temelju određenog obrasca nastavnikova ocjenjivanja mogu upotrebljavati za *ex post* provjeru toga je li nastavnik možda odstupio od svojeg obrasca ocjenjivanja kako bi se upozorilo na moguće nedosljednosti ili nepravilnosti. Četvrti uvjet trebao bi biti da je UI sustav namijenjen obavljanju zadaće koja je samo pripremna za procjenu relevantnu za svrhe UI sustava navedenih u prilogu ovoj Uredbi, čime se mogući učinak izlaznih vrijednosti sustava čini vrlo niskim u smislu predstavljanja rizika za procjenu koja treba uslijediti. Taj uvjet obuhvaća, među ostalim, pametna rješenja za postupanje s datotekama, koja uključuju različite funkcije poput indeksiranja, pretraživanja, obrade teksta i govora ili povezivanja podataka s drugim izvorima podataka, ili UI sustave koji se upotrebljavaju za prevođenje početnih dokumenata. U svakom slučaju, za UI sustave koji se upotrebljavaju u slučajevima visokih rizika koji su navedeni u prilogu ovoj Uredbi trebalo bi smatrati da predstavljaju znatne rizike od štete za zdravlje, sigurnost ili temeljna prava fizičkih osoba ako UI sustav podrazumijeva izradu profila u smislu članka 4. točke 4. Uredbe (EU) 2016/679 ili članka 3. točke 4. Direktive (EU) 2016/680 ili članka 3. točke 5. Uredbe (EU) 2018/1725. Kako bi se osigurala sljedivost i transparentnost, dobavljač koji na temelju prethodno navedenih uvjeta smatra da UI sustav nije visokorizičan trebao bi sastaviti dokumentaciju o ocjenjivanju prije nego što taj sustav bude stavljen na tržište ili u upotrebu i trebao bi tu dokumentaciju na zahtjev dostaviti nacionalnim nadležnim tijelima. Taj dobavljač trebao bi biti obavezan registrirati UI sustav u bazi podataka EU-a uspostavljenoj na temelju ove Uredbe. Kako bi se pružilo dodatno usmjeravanje za praktičnu provedbu uvjeta na temelju kojih UI sustavi navedeni u prilogu ovoj Uredbi iznimno nisu visokorizični, Komisija bi nakon savjetovanja s Vijećem za umjetnu inteligenciju trebala pružiti smjernice u kojima se precizira ta praktična provedba, dopunjene sveobuhvatnim popisom praktičnih primjera slučajeva upotrebe UI sustava koji su visokorizični i primjera upotrebe UI sustava koji nisu visokorizični.

- (54) Budući da biometrijski podaci čine posebnu kategoriju osobnih podataka, nekoliko kritičnih slučajeva korištenja biometrijskih sustava primjereno je klasificirati visokorizičnima, u mjeri u kojoj je njihovo korištenje dopušteno na temelju relevantnog prava Unije i nacionalnog prava. Tehničke netočnosti UI sustava namijenjenih daljinskoj biometrijskoj identifikaciji fizičkih osoba mogu rezultirati pristranim rezultatima i imati diskriminacijske učinke. Rizik od takvih pristranih rezultata i diskriminacijskih učinaka osobito je relevantna s obzirom na dob, etničku pripadnost, rasu, spol ili invaliditet. Stoga bi sustave za daljinsku biometrijsku identifikaciju trebalo klasificirati kao visokorizične s obzirom na rizike koje predstavljaju. Takva klasifikacija isključuje UI sustave namijenjene za biometrijsku provjeru, uključujući autentifikaciju, čija je jedina svrha potvrditi da je određena fizička osoba doista osoba kojom se predstavlja i potvrditi identitet fizičke osobe isključivo u svrhu pristupa usluzi, otključavanja uređaja ili sigurnog pristupa prostorijama. Osim toga, UI sustave namijenjene za biometrijsku kategorizaciju u skladu s osjetljivim atributima ili značajkama zaštićenima na temelju članka 9. stavka 1. Uredbe (EU) 2016/679 na osnovi biometrijskih podataka, u mjeri u kojoj nisu zabranjeni na temelju ove Uredbe, i sustave za prepoznavanje emocija koji nisu zabranjeni na temelju ove Uredbe trebalo bi klasificirati kao visokorizične. Biometrijski sustavi namijenjeni isključivo za omogućavanje kibernetičke sigurnosti i mjera zaštite osobnih podataka ne bi se trebali smatrati visokorizičnim UI sustavima.
- (55) Kad je riječ o upravljanju kritičnom infrastrukturom i njezinu radu, primjereno je kao visokorizične klasificirati one UI sustave koji su namijenjeni upotrebi kao sigurnosne komponente u upravljanju kritičnom digitalnom infrastrukturom navedenom u točki 8. Priloga Direktivi (EU) 2022/2557 i radu takve infrastrukture, u cestovnom prometu te u opskrbi vodom, plinom, grijanjem i električnom energijom jer bi njihov kvar ili neispravnost mogli ugroziti život i zdravlje osoba u velikim razmjerima te znatno poremetiti uobičajeno odvijanje društvenih i gospodarskih aktivnosti. Sigurnosne komponente kritične infrastrukture, uključujući kritičnu digitalnu infrastrukturu, sustavi su koji se upotrebljavaju za izravnu zaštitu fizičkog integriteta kritične infrastrukture ili zdravlja i sigurnosti osoba i imovine, ali koji nisu potrebni za funkcioniranje sustava. Kvar ili neispravnost takvih

komponenti može izravno dovesti do rizika za fizički integritet kritične infrastrukture, a time i do rizika za zdravlje i sigurnost osoba i imovine. Komponente namijenjene korištenju isključivo u svrhe kibernetičke sigurnosti ne bi trebalo smatrati sigurnosnim komponentama. Primjeri sigurnosnih komponenti takve kritične infrastrukture mogu uključivati sustave za praćenje tlaka vode ili sustave za kontrolu protupožarnog alarma u centrima za računalstvo u oblaku.

- (56) Uvođenje UI sustavâ u obrazovanje važno je kako bi se promicalo visokokvalitetno digitalno obrazovanje i osposobljavanje te kako bi se svim učenicima i nastavnicima omogućilo da steknu i dijele potrebne digitalne vještine i kompetencije, uključujući medijsku pismenost i kritičko razmišljanje, kako bi aktivno sudjelovali u gospodarstvu, društvu i demokratskim procesima. Međutim, UI sustave koji se upotrebljavaju u obrazovanju ili strukovnom osposobljavanju, osobito za odlučivanje o pristupu ili upisu, za razvrstavanje osoba u stanove ili programe za obrazovanje i strukovno osposobljavanje na svim razinama, za evaluaciju ishoda učenja osoba, za procjenu odgovarajuće razine obrazovanja pojedinca i bitan utjecaj na razinu obrazovanja i osposobljavanja koju će pojedinci steći ili kojoj će moći pristupiti odnosno za praćenje i otkrivanje zabranjenog ponašanja učenika tijekom testiranja trebalo bi klasificirati kao visokorizične UI sustavi jer mogu odrediti obrazovni i profesionalni tijek života osobe i stoga mogu utjecati na njezinu mogućnost da osigura sredstva za život. Ako se dizajniraju i upotrebljavaju na nepravilan način, takvi sustavi mogu biti osobito intruzivni i kršiti pravo na obrazovanje i osposobljavanje i pravo na nediskriminaciju te perpetuirati povijesne obrasce diskriminacije, primjerice protiv žena, određenih dobnih skupina, osoba s invaliditetom odnosno osoba određenog rasnog ili etničkog podrijetla ili seksualne orijentacije.
- (57) UI sustavi koji se upotrebljavaju za zapošljavanje, kadrovsko upravljanje i pristup samozapošljavanju, osobito za zapošljavanje i odabir osoba, za donošenje odluka koje utječu na uvjete radnog odnosa, promaknuće ili otkazivanje radnih ugovornih odnosa, za dodjelu zadataka na osnovi individualnog ponašanja, osobnih obilježja ili značajki i za praćenje ili evaluaciju osoba u radnim ugovornim odnosima također bi trebali biti klasificirani kao visokorizični jer bi ti sustavi mogli znatno utjecati na buduće izgleda za razvoj karijere, sredstva za život tih osoba i radnička prava. Relevantni radni ugovorni odnosi trebali bi na smislen način uključivati zaposlenike i osobe koji pružaju usluge putem platformi kako je navedeno u programu rada Komisije za 2021. U cijelom procesu zapošljavanja i pri evaluaciji, promaknuću ili zadržavanju osoba u radnim ugovornim odnosima takvi sustavi mogu perpetuirati povijesne obrasce diskriminacije, primjerice protiv žena, određenih dobnih skupina, osoba s invaliditetom odnosno osoba određenog rasnog ili etničkog podrijetla ili seksualne orijentacije. UI sustavi koji se upotrebljavaju za praćenje učinkovitosti i ponašanja takvih osoba mogu ujedno narušavati njihova temeljna prava na zaštitu osobnih podataka i privatnost.
- (58) Još jedno područje u kojem UI sustavima treba posvetiti posebnu pozornost jest dostupnost i uživanje određenih osnovnih privatnih i javnih usluga i naknada potrebnih za potpuno sudjelovanje u društvu ili poboljšanje životnog standarda osoba. Osobito, fizičke osobe koje podnose zahtjev za osnovne naknade i usluge javne pomoći od tijela javne vlasti ili ih od njih primaju, odnosno zdravstvene usluge, naknade socijalne sigurnosti, socijalne usluge kojima se pruža zaštita u slučajevima kao što su majčinstvo, bolest, nesreće na radu, uzdržavanost ili starost i gubitak zaposlenja te socijalna i stambena pomoć, obično ovise o tim naknadama i uslugama te su u ranjivom položaju u odnosu na nadležna tijela. Ako se UI sustavi upotrebljavaju za određivanje toga trebaju li tijela takve naknade i usluge dodijeliti, uskratiti, smanjiti, ukinuti ili tražiti njihov povrat, uključujući određivanje toga imaju li korisnici legitimno pravo na takve naknade ili usluge, ti sustavi mogu znatno utjecati na sredstva za život tih osoba i kršiti njihova temeljna prava, kao što je pravo na socijalnu zaštitu, nediskriminaciju, ljudsko dostojanstvo ili djelotvorno pravno sredstvo, te bi ih stoga trebalo klasificirati kao visokorizične. Međutim, ova Uredba ne bi trebala otežavati razvoj i primjenu inovativnih pristupa u javnoj upravi, koja bi imala koristi od šire upotrebe usklađenih i sigurnih UI sustava, pod uvjetom da ti sustavi ne podrazumijevaju velik rizik za pravne i fizičke osobe. Usto, UI sustave koji se upotrebljavaju za evaluaciju kreditnog rejtinga ili kreditne sposobnosti fizičkih osoba trebalo bi klasificirati kao visokorizične jer određuju pristup tih osoba financijskim resursima ili osnovnim uslugama kao što su stanovanje, električna energija i telekomunikacijske usluge. UI sustavi koji se upotrebljavaju u tu svrhu mogu dovesti do diskriminacije osoba ili skupina te perpetuirati povijesne obrasce diskriminacije, primjerice na temelju rasnog ili etničkog podrijetla, roda, invaliditeta, dobi ili seksualne orijentacije, ili mogu stvoriti nove vrste diskriminacijskih učinaka. Međutim, UI sustavi predviđeni pravom Unije u svrhu otkrivanja prijevара u ponudi financijskih usluga i u bonitetne svrhe za izračun kapitalnih zahtjeva kreditnih institucija i društava za osiguranje ne bi se trebali smatrati visokorizičnima na temelju ove Uredbe. Nadalje, UI sustavi namijenjeni procjeni rizika i određivanju cijena u odnosu

na fizičke osobe za zdravstveno i životno osiguranje mogu znatno utjecati i na sredstva za život tih osoba, a ako nisu propisno dizajnirani, razvijeni i korišteni, mogu kršiti njihova temeljna prava i dovesti do ozbiljnih posljedica za život i zdravlje ljudi, uključujući financijsku isključenost i diskriminaciju. Na kraju, UI sustavi koji se upotrebljavaju za evaluaciju i klasifikaciju hitnih poziva fizičkih osoba ili za dispečiranje ili određivanje prioriteta pri dispečiranju hitnih službi, uključujući policiju, vatrogasce i medicinsku pomoć, kao i sustavi za trijažu pacijenata pri pružanju hitne skrbi, isto bi se trebali smatrati visokorizičnima jer donose odluke u situacijama koje su kritične za život i zdravlje osoba te za njihovu imovinu.

- (59) S obzirom na njihovu ulogu i odgovornost, postupcima tijela kaznenog progona koji uključuju određene oblike korištenja UI sustava svojstvena je znatna neravnoteža moći i mogu dovesti do nadzora, uhićenja ili oduzimanja slobode fizičkih osoba, kao i do drugih nepovoljnih učinaka na temeljna prava zajamčena Poveljom. Posebice, ako UI sustav nije treniran s pomoću visokokvalitetnih podataka, ne ispunjava odgovarajuće zahtjeve u pogledu svoje učinkovitosti, točnosti ili otpornosti ili nije pravilno dizajniran i testiran prije stavljanja na tržište ili u upotrebu, može izdvajati ljude na diskriminatoran ili na drugačije netočan ili nepravedan način. Nadalje, ostvarivanje važnih postupovnih temeljnih prava, kao što su pravo na djelotvorno pravno sredstvo i na pošteno suđenje te pravo na obranu i pretpostavku nedužnosti, moglo bi biti otežano, osobito ako takvi UI sustavi nisu dovoljno transparentni, objašnjivi i dokumentirani. Stoga je primjereno, u mjeri u kojoj je njihovo korištenje dopušteno na temelju relevantnog prava Unije i nacionalnog prava, klasificirati kao visokorizične one UI sustave koji su namijenjeni korištenju u kontekstu kaznenog progona ako su točnost, pouzdanost i transparentnost osobito važne kako bi se izbjegli nepovoljni utjecaji, zadržalo povjerenje javnosti te osigurala odgovornost i djelotvorna pravna zaštita. S obzirom na prirodu tih aktivnosti i s njima povezane rizike, ti visokorizični UI sustavi trebali bi osobito uključivati UI sustave namijenjene za korištenje od strane tijela kaznenog progona ili u njihovo ime ili za korištenje od strane institucija, tijela, ureda ili agencija Unije radi potpore tijelima kaznenog progona za procjenu rizika fizičke osobe da postane žrtva kaznenih djela, kao poligrafi i slični alati, za evaluaciju pouzdanosti dokaza tijekom istrage ili progona kaznenih djela i, u mjeri u kojoj to nije zabranjeno na temelju ove Uredbe, za procjenu rizika da fizička osoba počinu ili ponovno počinu kazneno djelo ne isključivo na osnovi izrade profila fizičkih osoba ili procjene osobina i značajki ili prethodnog kriminalnog ponašanja fizičkih osoba ili skupina, za izradu profila tijekom otkrivanja, istrage ili progona kaznenih djela. UI sustave posebno namijenjene za upravne postupke poreznih i carinskih tijela i financijsko-obavještajnih jedinica koje provode administrativne zadaće analize informacija na temelju prava Unije o sprečavanju pranja novca ne bi trebalo klasificirati kao visokorizične UI sustave koje tijela kaznenog progona upotrebljavaju u svrhu sprečavanja, otkrivanja, istrage i progona kaznenih djela. Tijela kaznenog progona ni druga relevantna tijela ne bi smjela koristiti UI alate tako da postanu čimbenik nejednakosti ili isključenosti. Ne bi se trebao zanemariti utjecaj korištenja UI alata na prava osumnjičenika na obranu, osobito s obzirom na poteškoću u dobivanju smislenih informacija o funkcioniranju tih sustava i posljedičnu poteškoću u osporavanju njihovih rezultata na sudu, osobito za fizičke osobe pod istragom.
- (60) UI sustavi koji se upotrebljavaju u području migracija, azila i upravljanja nadzorom državne granice utječu na osobe koje su često u osobito ranjivu položaju i koje ovise o ishodu postupaka nadležnih tijela javne vlasti. Točnost, nediskriminacija i transparentnost UI sustava koji se upotrebljavaju u tim kontekstima stoga su posebno važne kako bi se zajamčilo poštovanje temeljnih prava zahvaćenih osoba, osobito njihovih prava na slobodno kretanje, nediskriminaciju, zaštitu privatnog života i osobnih podataka, međunarodnu zaštitu i dobru upravu. Stoga je primjereno klasificirati kao visokorizične, u mjeri u kojoj je njihovo korištenje dopušteno na temelju relevantnog prava Unije i nacionalnog prava, UI sustave namijenjene za korištenje od strane nadležnih tijela javne vlasti ili institucija, tijela, ureda ili agencija Unije ili u njihovo ime, a koji su zaduženi za zadaće u području migracija, azila i upravljanja nadzorom državne granice, kao poligrafe i slične alate, za procjenu određenih rizika koje predstavljaju fizičke osobe koje ulaze na državno područje države članice ili podnose zahtjev za vizu ili azil, za pomoć nadležnim tijelima javne vlasti u razmatranju, uključujući povezanu procjenu pouzdanosti dokaza, zahtjeva za azil, viza i boravišnih dozvola te povezanih pritužbi u pogledu cilja utvrđivanja prihvatljivosti fizičkih osoba koje podnose zahtjev za određeni status, u svrhu otkrivanja, priznavanja ili identifikacije fizičkih osoba u kontekstu migracija, azila i upravljanja nadzorom državne granice, uz iznimku provjere putnih isprava. UI sustavi koji se upotrebljavaju u području migracija, azila i upravljanja nadzorom državne granice obuhvaćeni ovom Uredbom trebali bi biti u skladu s relevantnim postupovnim zahtjevima utvrđenima Uredbom (EZ) 810/2009 Europskog parlamenta i Vijeća ⁽³²⁾, Direktivom 2013/32/EU Europskog parlamenta i Vijeća ⁽³³⁾ i drugim relevantnim pravom Unije. Države

⁽³²⁾ Uredba (EZ) br. 810/2009 Europskog parlamenta i Vijeća od 13. srpnja 2009. o uspostavi Zakonika Zajednice o vizama (Zakonik o vizama) (SL L 243, 15.9.2009., str. 1.).

⁽³³⁾ Direktiva 2013/32/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o zajedničkim postupcima za priznavanje i oduzimanje međunarodne zaštite (SL L 180, 29.6.2013., str. 60.).

članice odnosno institucije, tijela, uredi ili agencije Unije ni u kojem slučaju ne bi smjeli koristiti UI sustave u području migracija, azila i upravljanja nadzorom državne granice kao sredstvo za zaobilazanje svojih međunarodnih obveza na temelju Konvencije UN-a o statusu izbjeglica potpisane u Ženevi 28. srpnja 1951., kako je izmijenjena Protokolom od 31. siječnja 1967. Njima se ne bi trebalo ni na koji način kršiti načelo zabrane prisilnog udaljenja ili vraćanja niti uskraćivati sigurne i djelotvorne zakonite načine za dolazak na područje Unije, uključujući pravo na međunarodnu zaštitu.

- (61) Određene UI sustave namijenjene sudovanju i demokratskim procesima trebalo bi klasificirati kao visokorizične s obzirom na njihov potencijalno velik utjecaj na demokraciju, vladavinu prava, osobne slobode te pravo na djelotvoran pravno sredstvo i na pošteno suđenje. Točnije, radi odgovora na rizike od mogućih pristranosti, pogrešaka i netransparentnosti, primjereno je klasificirati kao visokorizične one UI sustave koji su namijenjeni korištenju od strane pravosudnog tijela ili u njegovo ime za pomoć pravosudnim tijelima u istraživanju i tumačenju činjenica i prava te primjeni prava na konkretan skup činjenica. UI sustavi namijenjeni korištenju od strane tijela za alternativno rješavanje sporova u te svrhe također bi se trebali smatrati visokorizičnima ako ishodi postupka alternativnog rješavanja sporova proizvode pravne učinke za stranke. Alati umjetne inteligencije mogu biti potpora ovlasti sudaca za donošenje odluka ili neovisnosti sudstva, ali ih ne bi smjeli zamijeniti: konačno donošenje odluka mora i dalje biti aktivnost koju obavljaju ljudi. Klasifikacija UI sustava kao visokorizičnih ne bi se trebala odnositi na UI sustave namijenjene isključivo pomoćnim administrativnim aktivnostima koje ne utječu na stvarno sudovanje u pojedinačnim slučajevima, kao što su anonimizacija ili pseudonimizacija sudskih odluka, dokumenata ili podataka, komunikacija među osobljem ili administrativne zadaće.
- (62) Ne dovodeći u pitanja pravila predviđena u Uredbi (EU) 2024/900. Europskog parlamenta i Vijeća ⁽³⁴⁾, te kako bi se uklonili rizici od neopravdanog vanjskog uplitanja u pravo glasa utvrđeno u članku 39. Povelje i od nerazmjernih učinaka na demokraciju i vladavinu prava, UI sustave namijenjene za korištenje kako bi se utjecalo na ishod izbora ili referenduma ili na ponašanje fizičkih osoba tijekom glasovanja na izborima ili referendumima trebalo bi klasificirati kao visokorizične UI sustave, uz iznimku UI sustava čijim izlaznim vrijednostima fizičke osobe nisu izravno izložene, kao što su alati koji se upotrebljavaju za organizaciju, optimizaciju i strukturiranje političkih kampanja s administrativnog i logističkog stajališta.
- (63) Činjenicu da je pojedini UI sustav klasificiran kao visokorizičan na temelju ove Uredbe ne bi trebalo tumačiti kao da je korištenje tog sustava zakonito na temelju drugih pravnih akata Unije ili nacionalnog prava usklađenog s pravom Unije, primjerice prava o zaštiti osobnih podataka, o korištenju poligrafa i sličnih alata ili drugih sustava kojima se utvrđuje emocionalno stanje fizičkih osoba. Svako takvo korištenje trebalo bi se i dalje ostvarivati samo u skladu s primjenjivim zahtjevima koji proizlaze iz Povelje te primjenjivih akata sekundarnog prava Unije i nacionalnog prava. Ovu Uredbu ne bi trebalo tumačiti kao pružanje pravne osnove za obradu osobnih podataka, uključujući, ako je to relevantno, posebne kategorije osobnih podataka, osim ako je u ovoj Uredbi izričito predviđeno drugačije.
- (64) Kako bi se smanjili rizici visokorizičnih UI sustava koji su stavljeni na tržište ili u upotrebu i kako bi se osigurala visoka razina pouzdanosti, na visokorizične UI sustave trebali bi se primjenjivati određeni obvezni zahtjevi, uzimajući u obzir namjenu i kontekst korištenja UI sustava i u skladu sa sustavom upravljanja rizikom koji treba uspostaviti dobavljač. Mjerama koje dobavljači donose radi usklađivanja s obveznim zahtjevima ove Uredbe trebalo bi uzeti u obzir općepriznata najnovija dostignuća u području umjetne inteligencije i te bi mjere trebale biti razmjerne i djelotvorne za postizanje ciljeva ove Uredbe. Na temelju novog zakonodavnog okvira, kako je pojašnjeno u obavijesti Komisije pod nazivom „Plavi vodič” o provedbi pravila EU-a o proizvodima 2022., opće je pravilo da se više od jednog pravnog akta zakonodavstva Unije o usklađivanju može primjenjivati na jedan proizvod jer se stavljanje na raspolaganje ili u upotrebu može provesti samo ako je proizvod u skladu sa svim primjenjivim zakonodavstvom Unije o usklađivanju. Opasnosti UI sustava obuhvaćene zahtjevima ove Uredbe odnose se na različite aspekte od onih u postojećem zakonodavstvu Unije o usklađivanju te bi se stoga zahtjevima ove Uredbe dopunio postojeći skup zakonodavstva Unije o usklađivanju. Na primjer, strojevi ili medicinski proizvodi u koje je ugrađen UI sustav mogli bi predstavljati rizike koji nisu obuhvaćeni osnovnim zdravstvenim i sigurnosnim

⁽³⁴⁾ Uredba (EU) 2024/900 Europskog parlamenta i Vijeća od 13. ožujka 2024. o transparentnosti i ciljanju u političkom oglašavanju (SL L, 2024/900, 20.3.2024., ELI: <http://data.europa.eu/eli/reg/2024/900/oj>).

zahtjevima utvrđenima u relevantnom zakonodavstvu Unije o usklađivanju jer se to sektorsko pravo ne bavi rizicima specifičnima za UI sustave. Zbog toga je potrebna istovremena i komplementarna primjena raznih zakonodavnih akata. Kako bi se osigurala dosljednost i izbjeglo nepotrebno administrativno opterećenje i nepotrebni troškovi, dobavljači proizvoda koji sadržava jedan ili više visokorizičnih UI sustava, na koje se primjenjuju zahtjevi iz ove Uredbe i zahtjevi iz zakonodavstva Unije o usklađivanju na temelju novog zakonodavnog okvira i navedeni u prilogu ovoj Uredbi, trebali bi biti fleksibilni u pogledu operativnih odluka o tome kako na najbolji način osigurati usklađenost proizvoda koji sadržava jedan ili više UI sustava sa svim primjenjivim zahtjevima zakonodavstva Unije o usklađivanju. Ta bi fleksibilnost mogla značiti, na primjer, odluku dobavljača da dio potrebnih postupaka testiranja i izvješćivanja, informacija i dokumentacije koji se zahtijevaju na temelju ove Uredbe integrira u već postojeću dokumentaciju i postupke koji se zahtijevaju na temelju postojećeg zakonodavstva Unije o usklađivanju koje se temelji na novom zakonodavnom okviru i koje je navedeno u prilogu ovoj Uredbi. To ni na koji način ne bi trebalo umanjiti obvezu dobavljača da poštuje sve primjenjive zahtjeve.

- (65) Sustav upravljanja rizikom trebao bi se sastojati od kontinuiranog iterativnog procesa koji se planira i izvodi tijekom cijelog životnog ciklusa visokorizičnog UI sustava. Taj bi proces trebao biti usmjeren na utvrđivanje i ublažavanje relevantnih rizika UI sustava za zdravlje, sigurnost i temeljna prava. Sustav upravljanja rizikom trebalo bi redovito preispitivati i ažurirati kako bi se osigurala njegova kontinuirana djelotvornost, kao i obrazlaganje i dokumentiranje svih važnih donesenih odluka i poduzetih mjera koje podliježu ovoj Uredbi. Tim bi procesom trebalo osigurati da dobavljač utvrdi rizike ili nepovoljne učinke i provede mjere za ublažavanje poznatih i razumno predvidljivih rizika UI sustava za zdravlje, sigurnost i temeljna prava s obzirom na njihovu namjenu i razumno predvidljivu pogrešnu upotrebu, uključujući moguće rizike koji proizlaze iz interakcije između UI sustava i okružja u kojem djeluje. Sustav upravljanja rizikom trebao bi primjenjivati najprikladnije mjere upravljanja rizikom s obzirom na najnovija dostignuća u području umjetne inteligencije. Pri utvrđivanju najprikladnijih mjera upravljanja rizikom dobavljač bi trebao dokumentirati i objasniti donesene odluke te, prema potrebi, uključiti stručnjake i vanjske dionike. Pri utvrđivanju razumno predvidljive pogrešne upotrebe visokorizičnih UI sustava dobavljač bi trebao obuhvatiti korištenja UI sustava za koja se, iako nisu izravno obuhvaćena namjenom i navedena u uputama za korištenje, ipak može razumno pretpostaviti da će proizaći iz lako predvidljivog ljudskog ponašanja u kontekstu specifičnih značajki i korištenja određenog UI sustava. Sve poznate i predvidljive okolnosti povezane s korištenjem visokorizičnog UI sustava u skladu s njegovom namjenom ili u uvjetima razumno predvidljive pogrešne upotrebe, koja može prouzročiti rizike za zdravlje i sigurnost ili temeljna prava, trebale bi biti navedene u uputama za korištenje koje pruža dobavljač. Time treba osigurati da ih je subjekt koji uvodi sustav svjestan i da ih uzme u obzir pri korištenju visokorizičnog UI sustava. Utvrđivanje i provedba mjera za ublažavanje rizika od predvidljive pogrešne upotrebe na temelju ove Uredbe ne bi trebali iziskivati posebno dodatno osposobljavanje za visokorizični UI sustav od strane dobavljača kako bi ih se riješila razumno predvidljiva pogrešna upotreba. Međutim, dobavljače se potiče da razmotre takve dodatne mjere osposobljavanja kako bi se ublažile razumno predvidljive pogrešne upotrebe ako je to potrebno i primjereno.
- (66) Zahtjevi bi se trebali primjenjivati na visokorizične UI sustave u pogledu upravljanja rizikom, kvalitete i relevantnosti korištenih skupova podataka, tehničke dokumentacije i vođenja evidencije, transparentnosti i pružanja informacija subjektima koji uvode sustav, ljudskog nadzora te otpornosti, točnosti i kibernetičke sigurnosti. Ti su zahtjevi potrebni kako bi se djelotvorno ublažili rizici za zdravlje, sigurnost i temeljna prava. S obzirom na to da druge mjere kojima se manje ograničava trgovina nisu u razumnoj mjeri dostupne ti zahtjevi nisu neopravdana ograničenja u području trgovine.
- (67) Visokokvalitetni podaci i pristup njima imaju ključnu ulogu u pružanju strukture i osiguravanju učinkovitosti mnogih UI sustava, posebno kad se upotrebljavaju tehnike s treniranjem modela, s ciljem da visokorizični UI sustav funkcionira kako je predviđeno i sigurno te da ne postane izvor diskriminacije koja je zabranjena pravom Unije. Visokokvalitetni skupovi podataka za treniranje, validaciju i testiranje zahtijevaju provedbu odgovarajućih praksi upravljanja i rukovanja podacima. Skupovi podataka za treniranje, validaciju i testiranje, uključujući oznake, trebali bi biti relevantni, dovoljno reprezentativni i u najvećoj mogućoj mjeri biti bez pogrešaka te potpuni s obzirom na namjenu sustava. Kako bi se olakšala usklađenost s pravom Unije o zaštiti podataka, kao što je Uredba (EU) 2016/679, prakse upravljanja i rukovanja podacima trebale bi u slučaju osobnih podataka uključivati transparentnost u vezi s izvornom svrhom prikupljanja podataka. Skupovi podataka trebali bi imati i odgovarajuća statistička obilježja, među ostalim i u pogledu osoba ili skupina osoba u vezi s kojima se visokorizični UI sustav namjerava koristiti, pri čemu se posebna pažnja posvećuje ublažavanju mogućih pristranosti u skupovima podataka, koje bi mogle utjecati na zdravlje i sigurnost osoba, negativno utjecati na temeljna prava ili dovesti do diskriminacije zabranjene pravom Unije, osobito ako izlazne vrijednosti utječu na ulazne vrijednosti za buduće operacije (povratne

veze). Pristranosti mogu primjerice biti inherentne temeljnim skupovima podataka, osobito kad se upotrebljavaju povijesni podaci, ili se mogu generirati kad se sustavi implementiraju u stvarnom svijetu. Na rezultate koje pružaju UI sustavi mogle bi utjecati takve inherentne pristranosti koje imaju tendenciju postupnog povećanja, čime se perpetuira i pojačava postojeća diskriminacija, posebno za osobe koje pripadaju određenim skupinama ranjivih osoba, uključujući rasne ili etničke skupine. Zahtjev da skupovi podataka u najvećoj mogućoj mjeri budu potpuni i bez pogrešaka ne bi trebao utjecati na primjenu tehnika za zaštitu privatnosti u kontekstu razvoja i testiranja UI sustavâ. U skupovima podataka osobito se u obzir uzimaju, u mjeri u kojoj to iziskuje njihova namjena, obilježja, značajke ili elementi specifični za zemljopisno, kontekstualno, bihevioralno ili funkcionalno okruženje u kojem se UI sustav namjerava upotrebljavati. Zahtjevi povezani s upravljanjem podacima mogu se ispuniti angažiranjem trećih strana koje nude certificirane usluge usklađivanja, uključujući provjeru upravljanja podacima, cjelovitosti skupa podataka te prakse treniranja, validacije i testiranja podataka, u mjeri u kojoj je osigurana usklađenost sa zahtjevima u pogledu podataka iz ove Uredbe.

- (68) Kad je riječ o razvoju i procjeni visokorizičnih UI sustava, određeni akteri, kao što su dobavljači, prijavljena tijela i drugi relevantni subjekti, na primjer europski centri za digitalne inovacije, centri za testiranje i eksperimentiranje te istraživači, trebali bi imati pristup visokokvalitetnim skupovima podataka unutar područja aktivnosti tih aktera povezanih s ovom Uredbom. Zajednički europski podatkovni prostori koje je uspostavila Komisija te olakšavanje razmjene podataka među poduzećima i s državnim upravama u javnom interesu bit će ključni za osiguravanje pouzdanog, odgovornog i nediskriminirajućeg pristupa visokokvalitetnim podacima za treniranje, validaciju i testiranje UI sustavâ. Na primjer, u području zdravstva zajednički europski prostor za zdravstvene podatke olakšat će nediskriminirajući pristup zdravstvenim podacima i treniranje algoritama umjetne inteligencije s pomoću tih skupova podataka tako da se očuvaju privatnost, sigurnost, pravovremenost, transparentnost i pouzdanost uz odgovarajuće institucijsko upravljanje. Relevantna nadležna tijela, uključujući sektorska tijela, koja pružaju ili olakšavaju pristup podacima, mogu olakšati i pružanje visokokvalitetnih podataka za treniranje, validaciju i testiranje UI sustavâ.
- (69) Pravo na privatnost i zaštitu osobnih podataka mora biti zajamčeno tijekom cijelog životnog ciklusa UI sustava. U tom su pogledu načela smanjenja količine podataka te tehničke i integrirane zaštite podataka, kako su utvrđena u pravu Unije o zaštiti podataka, primjenjiva tijekom obrade osobnih podataka. Mjere koje dobavljači poduzimaju kako bi osigurali usklađenost s tim načelima mogu uključivati ne samo anonimizaciju i kriptiranje, nego i upotrebu tehnologije kojom se omogućuje dovođenje algoritama u podatke i treniranje UI sustavâ bez prijenosa između strana ili kopiranja samih neobrađenih ili strukturiranih podataka, ne dovodeći u pitanje zahtjeve u pogledu upravljanja podacima predviđene u ovoj Uredbi.
- (70) Kako bi se prava drugih osoba zaštitila od diskriminacije koja bi mogla proizaći iz pristranosti UI sustavâ, dobavljači bi iznimno trebali, u mjeri u kojoj je to nužno u svrhu otkrivanja i ispravljanja pristranosti u vezi s visokorizičnim UI sustavima, podložno odgovarajućim zaštitnim mjerama za temeljna prava i slobode fizičkih osoba i nakon primjene svih primjenjivih uvjeta utvrđenih na temelju ove Uredbe, dodatno uz uvjete utvrđene u uredbama (EU) 2016/679 i (EU) 2018/1725 te Direktivi (EU) 2016/680, moći obrađivati i posebne kategorije osobnih podataka kao pitanje od znatnog javnog interesa u smislu članka 9. stavka 2. točke (g) Uredbe (EU) 2016/679 i članka 10. stavka 2. točke (g) Uredbe (EU) 2018/1725.
- (71) Postojanje razumljivih informacija o načinu na koji su visokorizični UI sustavi razvijeni i načinu njihova rada tijekom cijelog njihova životnog ciklusa ključno je za omogućivanje sljedivosti tih sustava, provjeru usklađenosti sa zahtjevima ove Uredbe te praćenje njihova rada i praćenje nakon stavljanja na tržište. Za to je potrebno vođenje evidencije i dostupnost tehničke dokumentacije koja sadržava informacije potrebne za procjenu usklađenosti UI sustava s relevantnim zahtjevima i olakšavanje praćenja nakon stavljanja na tržište. Takve informacije trebale bi uključivati opće značajke, sposobnosti i ograničenja sustava, algoritme, podatke, postupke treniranja, testiranja i validacije koji su primijenjeni, kao i dokumentaciju o relevantnom sustavu upravljanja rizikom te bi trebale biti sastavljene u obliku koji je jasan i razumljiv. Tehnička dokumentacija trebala bi se ažurirati na odgovarajući način tijekom cijelog životnog ciklusa UI sustava. Nadalje, kod visokorizičnih UI sustava trebalo bi biti tehnički omogućeno automatsko bilježenje događaja putem vođenja evidencije tijekom cijelog životnog ciklusa sustava.

- (72) Kako bi se pristupilo rješavanju problema povezanih s netransparentnošću i složenosti određenih UI sustava i pomoglo subjektima koji uvode UI sustav da ispune svoje obveze na temelju ove Uredbe, za visokorizične UI sustave trebalo bi zahtijevati transparentnost prije njihova stavljanja na tržište ili u upotrebu. Visokorizični UI sustavi trebali bi biti dizajnirani tako da subjekti koji ih uvode mogu razumjeti kako UI sustav funkcionira, evaluirati njegovu funkcionalnost te razumjeti njegove prednosti i ograničenja. Visokorizični UI sustavi trebali bi biti popraćeni odgovarajućim informacijama u obliku uputa za korištenje. Takve informacije trebale bi uključivati značajke, sposobnosti i ograničenja rada UI sustava. Oni bi obuhvaćali informacije o mogućim poznatim i predvidljivim okolnostima povezanim s korištenjem visokorizičnog UI sustava, uključujući djelovanje subjekta koji uvodi sustav koje može utjecati na ponašanje i učinkovitost sustava, u okviru kojeg UI sustav može prouzročiti rizike za zdravlje, sigurnost i temeljna prava, o promjenama koje je dobavljač unaprijed odredio i ocijenio u pogledu sukladnosti te o relevantnim mjerama ljudskog nadzora, uključujući mjere kojima se subjektima koji uvode sustav olakšava tumačenje izlaznih vrijednosti UI sustava. Transparentnost, uključujući popratne upute za korištenje, trebala bi pomoći subjektima koji uvode sustav pri njegovu korištenju i poduprijeti njihovo informirano donošenje odluka. Subjekti koji uvode sustav trebali bi, među ostalim, biti u boljoj poziciji da pravilno odaberu sustav koji namjeravaju upotrebljavati s obzirom na obveze koje se na njih primjenjuju, biti informirani o namjeravanim i isključenim upotrebama te pravilno i primjereno upotrebljavati UI sustav. Kako bi se poboljšale čitljivost i pristupačnost informacija sadržanih u uputama za korištenje, trebalo bi, prema potrebi, u njih uključiti ilustrativne primjere, na primjer o ograničenjima te o namjeravanim i isključenim upotrebama UI sustava. Dobavljači bi trebali osigurati da sva dokumentacija, uključujući upute za korištenje, sadržava smislene, sveobuhvatne, pristupačne i razumljive informacije, uzimajući u obzir potrebe i predvidljivo znanje ciljanih subjekata koji uvode sustav. Upute za korištenje trebale bi biti dostupne na jeziku koji bez poteškoća razumiju ciljni subjekti koji uvode sustav, a određuje ga dotična država članica.
- (73) Visokorizične UI sustave trebalo bi dizajnirati i razvijati tako da fizičke osobe mogu nadzirati njihovo funkcioniranje, osigurati da se upotrebljavaju kako je predviđeno i da se njihovi učinci rješavaju tijekom životnog ciklusa sustava. U tom bi cilju dobavljač sustava prije njegova stavljanja na tržište ili u upotrebu trebao utvrditi odgovarajuće mjere ljudskog nadzora. Prema potrebi takvim bi mjerama osobito trebalo osigurati da su u sustav ugrađena operativna ograničenja koja sam sustav ne može promijeniti i da on reagira na ljudske operatore te da fizičke osobe zadužene za ljudski nadzor imaju potrebne kompetencije, osposobljavanje i ovlasti za obavljanje te zadaće. Također je neophodno, prema potrebi, osigurati da visokorizični UI sustavi uključuju mehanizme za usmjeravanje i informiranje fizičke osobe zadužene za ljudski nadzor kako bi donijela informirane odluke o tome treba li, kada i kako intervenirati da bi se izbjegle negativne posljedice ili rizici odnosno sustav zaustavio ako ne funkcionira kako je predviđeno. S obzirom na znatne posljedice za osobe ako u određenim sustavima za biometrijsku identifikaciju dođe do netočnih rezultata, primjereno je za te sustave predvidjeti zahtjev u pogledu pojačanog ljudskog nadzora tako da subjekt koji uvodi sustav ne može poduzeti nikakve radnje ili odluke na temelju identifikacije proizišle iz sustava ako identifikaciju nisu zasebno provjerile i potvrdile najmanje dvije fizičke osobe. Te osobe mogle bi biti iz jednog ili više subjekata i mogle bi uključivati osobu koja upravlja sustavom ili ga upotrebljava. Taj zahtjev ne bi trebao predstavljati nepotrebno opterećenje ili uzrokovati kašnjenja i moglo bi biti dovoljno da se zasebne provjere koje provode različite osobe automatski bilježe u evidenciji koju generira sustav. S obzirom na posebnosti područja kaznenog progona, migracija, nadzora državne granice i azila, taj se zahtjev ne bi trebao primjenjivati ako se u skladu s pravom Unije ili nacionalnim pravom smatra da je primjena tog zahtjeva nerazmjerna.
- (74) Visokorizični UI sustavi trebali bi imati ujednačen učinak tijekom cijelog životnog ciklusa te posjedovati odgovarajuću razinu točnosti, otpornosti i kibernetičke sigurnosti s obzirom na njihovu namjenu i u skladu s općepriznatim najnovijim dostignućima. Komisija i relevantne organizacije i dionici potiču se da uzmu u obzir ublažavanje rizika i negativnih učinaka UI sustava. Očekivana razina parametara učinkovitosti trebala bi se navesti u popratnim uputama za korištenje. Dobavljači se pozivaju da te informacije dostave subjektima koji uvode sustav na jasan i lako razumljiv način, bez nespornosti ili obmanjujućih izjava. Pravom Unije o zakonskom mjeriteljstvu, uključujući direktive 2014/31/EU ⁽³⁵⁾ i 2014/32/EU ⁽³⁶⁾ Europskog parlamenta i Vijeća, nastoji se osigurati točnost mjerenja te doprinijeti transparentnosti i pravednosti poslovnih transakcija. U tom kontekstu, u suradnji s relevantnim dionicima i organizacijama, kao što su tijela za mjeriteljstvo i utvrđivanje referentnih vrijednosti, Komisija bi prema potrebi trebala poticati razvoj referentnih vrijednosti i metodologija mjerenja za UI sustave. Komisija bi pritom trebala uzeti u obzir međunarodne partnere koji rade na mjeriteljstvu i relevantnim mjernim pokazateljima povezanim s umjetnom inteligencijom te surađivati s njima.

⁽³⁵⁾ Direktiva 2014/31/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o usklađivanju zakonodavstava država članica u odnosu na stavljanje na raspolaganje neautomatskih vaga na tržište (SL L 96, 29.3.2014., str. 107.).

⁽³⁶⁾ Direktiva 2014/32/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o usklađivanju zakonodavstava država članica u odnosu na stavljanje na raspolaganje mjernih instrumenata na tržištu (SL L 96, 29.3.2014., str. 149.).

- (75) Tehnička otpornost ključan je zahtjev za visokorizične UI sustave. Trebali bi biti otporni na štetno ili na drugi način nepoželjno ponašanje koje bi moglo proizaći iz ograničenjâ unutar sustava ili okruţja u kojem sustavi rade (npr. pogreške, kvarovi, nedosljednosti, neočekivane situacije). Stoga bi trebalo poduzeti tehničke i organizacijske mjere kako bi se osigurala otpornost visokorizičnih UI sustava, na primjer dizajniranjem i razvojem odgovarajućih tehničkih rješenja za sprečavanje ili što veće smanjenje štetnog ili na drugi način nepoţelnog ponašanja. Ta tehnička rješenja mogu obuhvaćati, na primjer, mehanizme koji omogućuju sustavu da sigurno prekine svoj rad (sigurnosni planovi) u slučaju određenih anomalija ili ako se rad odvija izvan određenih unaprijed utvrđenih granica. Nepostojanje zaštite od tih rizika moglo bi imati posljedice za sigurnost ili negativno utjecati na temeljna prava, primjerice zbog pogrešnih odluka ili krivih ili pristranih izlaznih vrijednosti koje generira UI sustav.
- (76) Kibernetička sigurnost ključna je za otpornost UI sustavâ na pokušaje zlonamjernih trećih strana da iskoriste slabe točke tih sustava kako bi im izmijenili način korištenja, ponašanje, učinkovitost ili ugrozili njihova sigurnosna svojstva. U kibernetičkim napadima na UI sustave moguće je iskoristiti resurse specifične za umjetnu inteligenciju, kao što su skupovi podataka za treniranje (npr. trovanje podataka) ili istrenirani modeli (npr. neprijateljski napadi ili utvrđivanje pripadnosti) ili iskoristiti slabe točke digitalnih resursa UI sustava odnosno osnovne IKT infrastrukture. Kako bi se osigurala razina kibernetičke sigurnosti primjerena rizicima, dobavljači visokorizičnih UI sustava trebali bi stoga poduzeti odgovarajuće mjere, kao što su sigurnosne kontrole, prema potrebi uzimajući u obzir i osnovnu IKT infrastrukturu.
- (77) Ne dovodeći u pitanje zahtjeve koji se odnose na otpornost i točnost utvrđene u ovoj Uredbi, visokorizični UI sustavi obuhvaćeni područjem primjene uredbe Europskog parlamenta i Vijeća o horizontalnim kibernetičkosigurnosnim zahtjevima za proizvode s digitalnim elementima u skladu s tom uredbom mogu dokazati sukladnost s kibernetičkosigurnosnim zahtjevima ove Uredbe ispunjavanjem osnovnih kibernetičkosigurnosnih zahtjeva iz te uredbe. Ako visokorizični UI sustavi ispunjavaju osnovne zahtjeve iz uredbe Europskog parlamenta i Vijeća o horizontalnim kibernetičkosigurnosnim zahtjevima za proizvode s digitalnim elementima trebalo bi ih smatrati usklađenima s kibernetičkosigurnosnim zahtjevima utvrđenima u ovoj Uredbi u mjeri u kojoj je ispunjavanje tih zahtjeva dokazano u EU izjavi o sukladnosti izdanoj na temelju te uredbe ili u dijelovima te izjave. U tom cilju, tijekom procjene kibernetičkosigurnosnih rizika povezanih s proizvodima s digitalnim elementima koji su klasificirani kao visokorizični UI sustav u skladu s ovom Uredbom, koja se provodi na temelju uredbe Europskog parlamenta i Vijeća o horizontalnim kibernetičkosigurnosnim zahtjevima za proizvode s digitalnim elementima, trebalo bi uzeti u obzir rizike za kibernetičku otpornost UI sustava kad se radi o pokušajima neovlaštenih trećih strana da promijene njegovo korištenje, ponašanje ili učinkovitost, uključujući ranjivosti specifične za umjetnu inteligenciju kao što su trovanje podacima ili neprijateljski napadi, kao i, kada je to relevantno, rizike za temeljna prava kako je propisano ovom Uredbom.
- (78) Postupak ocjenjivanja sukladnosti predviđen ovom Uredbom trebao bi se primjenjivati u odnosu na osnovne kibernetičkosigurnosne zahtjeve za proizvod s digitalnim elementima obuhvaćen uredbom Europskog parlamenta i Vijeća o horizontalnim kibernetičkosigurnosnim zahtjevima za proizvode s digitalnim elementima koji je klasificiran kao visokorizični UI sustav na temelju ove Uredbe. Međutim, to pravilo ne bi trebalo rezultirati smanjenjem potrebne razine jamstva za kritične proizvode s digitalnim elementima obuhvaćene uredbom Europskog parlamenta i Vijeća o horizontalnim kibernetičkosigurnosnim zahtjevima za proizvode s digitalnim elementima. Stoga, odstupajući od tog pravila, visokorizični UI sustavi koji su obuhvaćeni područjem primjene ove Uredbe i ujedno su klasificirani kao vaţni i kritični proizvodi s digitalnim elementima na temelju uredbe Europskog parlamenta i Vijeća o horizontalnim kibernetičkosigurnosnim zahtjevima za proizvode s digitalnim elementima te na koje se primjenjuje postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole utvrđene u prilogu ovoj Uredbi podlijeţu odredbama o ocjenjivanju sukladnosti iz uredbe Europskog parlamenta i Vijeća o horizontalnim kibernetičkosigurnosnim zahtjevima za proizvode s digitalnim elementima u mjeri u kojoj se to odnosi na osnovne kibernetičkosigurnosne zahtjeve iz te uredbe. U tom bi se slučaju na sve ostale aspekte obuhvaćene ovom Uredbom trebale primjenjivati odgovarajuće odredbe o ocjenjivanju sukladnosti na temelju unutarnje kontrole utvrđene u prilogu ovoj Uredbi. Na osnovi znanja i stručnosti ENISA-e u području kibernetičkosigurnosne politike i zadaća dodijeljenih ENISA-i na temelju Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća⁽³⁷⁾, Komisija bi trebala surađivati s ENISA-om u pitanjima povezanim s kibernetičkom sigurnošću UI sustavâ.

⁽³⁷⁾ Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15.).

- (79) Primjereno je da određena fizička ili pravna osoba, koja je definirana kao dobavljač, preuzme odgovornost za stavljanje visokorizičnog UI sustava na tržište ili u upotrebu, bez obzira na to je li ta fizička ili pravna osoba ista osoba koja je dizajnirala ili razvila sustav.
- (80) Kao potpisnice Konvencije Ujedinjenih naroda o pravima osoba s invaliditetom, Unija i države članice imaju pravnu obvezu štititi osobe s invaliditetom od diskriminacije i promicati njihovu ravnopravnost, osigurati da osobe s invaliditetom imaju pristup informacijskim i komunikacijskim tehnologijama i sustavima na ravnopravnoj osnovi te zajamčiti poštovanje privatnosti osoba s invaliditetom. S obzirom na sve veću važnost i upotrebu UI sustava, primjenom univerzalnih načela dizajna na sve nove tehnologije i usluge trebao bi se osigurati potpun i ravnopravan pristup za sve osobe na koje bi tehnologije umjetne inteligencije mogle utjecati ili koje te tehnologije upotrebljavaju, uključujući osobe s invaliditetom, na način kojim se u cijelosti poštuju njihovo inherentno dostojanstvo i raznolikost. Stoga je ključno da dobavljači osiguraju potpunu usklađenost sa zahtjevima u pogledu pristupačnosti, uključujući Direktivu (EU) 2016/2102 Europskog parlamenta i Vijeća ⁽³⁸⁾ i Direktivu (EU) 2019/882. Dobavljači bi trebali osigurati integriranu usklađenost s tim zahtjevima. Stoga bi potrebne mjere trebalo što je više moguće uključiti u dizajn visokorizičnog UI sustava.
- (81) Dobavljač bi trebao uspostaviti pouzdan sustav upravljanja kvalitetom, osigurati realizaciju postupka ocjenjivanja sukladnosti koji se zahtijeva, sastaviti relevantnu dokumentaciju i uspostaviti pouzdan sustav praćenja nakon stavljanja na tržište. Dobavljači visokorizičnih UI sustava koji podliježu obvezama u pogledu sustava upravljanja kvalitetom u skladu s relevantnim sektorskim pravom Unije trebali bi imati mogućnost uključiti elemente sustava upravljanja kvalitetom predviđenog u ovoj Uredbi u postojeći sustav upravljanja kvalitetom predviđen u tom drugom sektorskom pravu Unije. Komplementarnost ove Uredbe i postojećeg sektorskog prava Unije trebala bi se uzeti u obzir i u budućim aktivnostima normizacije ili smjernicama koje donosi Komisija. Tijela javne vlasti koja stavljaju visokorizične UI sustave u upotrebu za vlastite potrebe mogu donijeti i provoditi pravila za sustav upravljanja kvalitetom u okviru sustava upravljanja kvalitetom donesenog na nacionalnoj ili regionalnoj razini, prema potrebi, uzimajući u obzir posebnosti sektora te nadležnosti i organizaciju dotičnog tijela javne vlasti.
- (82) Kako bi se omogućilo izvršavanje ove Uredbe i osigurali jednaki uvjeti za operatere te uzimajući u obzir različite oblike stavljanja digitalnih proizvoda na raspolaganje, važno je osigurati da osoba s poslovnim nastanom u Uniji u svim okolnostima može nadležnim tijelima pružiti sve potrebne informacije o usklađenosti pojedinog UI sustava. Stoga bi dobavljači s poslovnim nastanom u trećim zemljama trebali pisanim ovlaštenjem imenovati ovlaštenog zastupnika s poslovnim nastanom u Uniji prije stavljanja svojih UI sustava na raspolaganje u Uniji. Taj ovlaštenik ima ključnu ulogu u osiguravanju usklađenosti visokorizičnih UI sustava koje ti dobavljači koji nemaju poslovni nastan u Uniji stavljaju na tržište ili u upotrebu u Uniji i služi kao njihova osoba za kontakt s poslovnim nastanom u Uniji.
- (83) S obzirom na prirodu i složenost lanca vrijednosti za UI sustave te u skladu s načelima novog zakonodavnog okvira, ključno je osigurati pravnu sigurnost i olakšati usklađenost s ovom Uredbom. Stoga je potrebno pojasniti ulogu i posebne obveze relevantnih operatera duž tog lanca vrijednosti, kao što su uvoznici i distributeri koji mogu doprinijeti razvoju UI sustava. U određenim situacijama ti bi operateri mogli istodobno djelovati u više uloga i stoga bi trebali kumulativno ispunjavati sve relevantne obveze povezane s tim ulogama. Na primjer, operater bi mogao istodobno djelovati kao distributer i uvoznik.
- (84) Kako bi se zajamčila pravna sigurnost, potrebno je pojasniti da bi se pod određenim posebnim uvjetima svaki dobavljač, uvoznik, subjekt koji uvodi sustav ili treća strana trebali smatrati dobavljačem visokorizičnog UI sustava i stoga preuzeti sve relevantne obveze. To bi bio slučaj ako ta strana stavi svoje ime ili žig na visokorizični UI sustav koji je već stavljen na tržište ili u upotrebu, ne dovodeći u pitanje ugovorne aranžmane u kojima je utvrđena drukčija raspodjela obveza. To bi bio slučaj i ako ta strana bitno izmijeni visokorizični UI sustav koji je već stavljen na tržište ili u upotrebu na način da on i dalje bude visokorizičan u skladu s ovom Uredbom, ili ako izmijeni namjenu UI sustava, uključujući UI sustav opće namjene, koji nije bio klasificiran kao visokorizičan i već je stavljen na tržište ili u upotrebu, na način da UI sustav postane visokorizičan u skladu s ovom Uredbom. Te bi se odredbe trebale primjenjivati ne dovodeći u pitanje detaljnije odredbe utvrđene u određenom zakonodavstvu Unije o usklađivanju na temelju novog zakonodavnog okvira, zajedno s kojima bi se ova Uredba trebala primjenjivati. Na primjer, članak 16.

⁽³⁸⁾ Direktiva (EU) 2016/2102 Europskog parlamenta i Vijeća od 26. listopada 2016. o pristupačnosti internetskih stranica i mobilnih aplikacija tijela javnog sektora (SL L 327, 2.12.2016., str. 1.).

stavak 2. Uredbe (EU) 2017/745, u kojem se navodi da određene promjene ne bi trebalo smatrati izmjenama proizvoda koje mogu utjecati na njegovu usklađenost s primjenjivim zahtjevima, trebao bi se i dalje primjenjivati na visokorizične UI sustave koji su medicinski proizvodi u smislu te uredbe.

- (85) UI sustavi opće namjene mogu se upotrebljavati samostalno kao visokorizični UI sustavi ili mogu biti komponente drugih visokorizičnih UI sustava. Stoga, zbog njihove specifične prirode i radi jamčenja pravedne podjele odgovornosti diljem lanca vrijednosti umjetne inteligencije, neovisno o tome mogu li ih drugi dobavljači upotrebljavati samostalno kao visokorizične UI sustave ili kao komponente visokorizičnih UI sustava i ako na temelju ove Uredbe nije drugačije predviđeno, dobavljači takvih sustava trebali bi blisko surađivati s dobavljačima relevantnih visokorizičnih UI sustava kako bi im se omogućilo ispunjavanje relevantnih obveza na temelju ove Uredbe i s nadležnim tijelima osnovanima na temelju ove Uredbe.
- (86) Ako se u skladu s uvjetima utvrđenima u ovoj Uredbi dobavljač koji je prvotno stavio UI sustav na tržište ili u upotrebu više ne smatra dobavljačem za potrebe ove Uredbe i ako taj dobavljač nije izričito isključio pretvaranje UI sustava u visokorizični UI sustav, bivši dobavljač ipak bi trebao blisko surađivati i staviti na raspolaganje potrebne informacije te pružiti razumno očekivani tehnički pristup i drugu pomoć koji su potrebni za ispunjavanje obveza utvrđenih u ovoj Uredbi, posebno u pogledu usklađenosti s ocjenjivanjem sukladnosti visokorizičnih UI sustava.
- (87) Usto, ako se visokorizični UI sustav koji je sigurnosna komponenta proizvoda obuhvaćenog zakonodavstvom Unije o usklađivanju na temelju novog zakonodavnog okvira ne stavlja na tržište ili u upotrebu neovisno o proizvodu, proizvođač proizvoda definiran u tom zakonodavstvu trebao bi ispunjavati obveze dobavljača utvrđene u ovoj Uredbi, a osobito osigurati da UI sustav ugrađen u konačni proizvod ispunjava zahtjeve iz ove Uredbe.
- (88) U vrijednosnom lancu umjetne inteligencije često više strana dobavlja UI sustave, alate i usluge, ali i komponente ili procese koje dobavljač potom ugrađuje u UI sustav s različitim ciljevima, među ostalim radi treniranja modela, ponovnog treniranja modela, testiranja i evaluacije modela, integracije u softver ili drugih aspekata razvoja modela. Te strane imaju važnu ulogu u lancu vrijednosti prema dobavljaču visokorizičnog UI sustava u koji su integrirani njihovi UI sustavi, alati, usluge, komponente ili procesi te bi tom dobavljaču u pisanom obliku trebale pružiti potrebne informacije, mogućnosti, tehnički pristup i drugu pomoć na temelju općepriznatih najnovijih dostignuća kako bi dobavljač mogao u potpunosti ispuniti obveze utvrđene u ovoj Uredbi, a da se pritom ne dovedu u pitanje njihova prava intelektualnog vlasništva ili poslovne tajne.
- (89) Treće strane koje javnosti na raspolaganje stavljaju UI alate, usluge, procese ili komponente koji nisu UI modeli opće namjene ne bi trebale biti obvezne ispunjavati zahtjeve u vezi s odgovornošću duž lanca vrijednosti umjetne inteligencije, posebno prema dobavljaču koji ih je koristio ili integrirao, ako su ti UI alati, usluge, procesi ili komponente dostupni na temelju besplatne licencije za softver otvorenog koda. Razvojne programere besplatnih UI alata, usluga, procesa otvorenog koda ili komponenti koji nisu UI modeli opće namjene trebalo bi poticati da primjenjuju široko prihvaćene prakse dokumentiranja, kao što su kartice modela i podatkovne kartice kako bi se ubrzala razmjena informacija duž vrijednosnog lanca umjetne inteligencije i omogućilo promicanje pouzdanih UI sustava u Uniji.
- (90) Komisija bi mogla razviti i preporučiti dobrovoljne modele ugovornih uvjeta između dobavljača visokorizičnih UI sustava i trećih strana koji isporučuju alate, usluge, komponente ili procese koji se upotrebljavaju u visokorizičnim UI sustavima ili su u njih integrirani kako bi se olakšala suradnja duž lanca vrijednosti. Pri izradi dobrovoljnih modela ugovornih uvjeta Komisija bi trebala uzeti u obzir i moguće ugovorne zahtjeve primjenjive u određenim sektorima ili poslovnim modelima.
- (91) S obzirom na prirodu UI sustava i rizike za sigurnost i temeljna prava koji se potencijalno mogu povezati s njihovim korištenjem, među ostalim u pogledu potrebe da se osigura propisno praćenje učinkovitosti UI sustava u stvarnim uvjetima, primjereno je utvrditi posebne odgovornosti za subjekte koji ih uvode. Subjekti koji uvode UI sustave osobito bi trebali poduzeti primjerene tehničke i organizacijske mjere kako bi osigurali da upotrebljavaju visokorizične UI sustave u skladu s uputama za korištenje te bi, prema potrebi, trebalo predvidjeti određene druge obveze u pogledu praćenja funkcioniranja UI sustava i vođenja evidencije. Nadalje, subjekti koji uvode sustav trebali bi osigurati da osobe kojima je povjerena provedba uputa za korištenje i ljudskog nadzora kako je utvrđeno u ovoj Uredbi imaju potrebne kompetencije, osobito odgovarajuću razinu pismenosti, osposobljavanja i ovlasti u području

umjetne inteligencije, za pravilno obavljanje tih zadaća. Tim se obvezama ne bi trebale dovoditi u pitanje druge obveze subjekata koji uvode UI sustave u pogledu visokorizičnih UI sustava na temelju prava Unije ili nacionalnog prava.

- (92) Ovom se Uredbom ne dovode u pitanje obveze poslodavaca da obavijeste radnike ili njihove predstavnike ili da se savjetuju s njima na temelju prava i prakse Unije ili nacionalnog prava i prakse, uključujući Direktivu 2002/14/EZ Europskog parlamenta i Vijeća ⁽³⁹⁾, o odlukama o stavljanju u upotrebu ili korištenju UI sustava. I dalje je potrebno osigurati obavješćivanje radnika i njihovih predstavnika o planiranom uvođenju visokorizičnih UI sustava na radnom mjestu ako nisu ispunjeni uvjeti za te obveze obavješćivanja ili obavješćivanja i savjetovanja iz drugih pravnih instrumenata. Nadalje, takvo pravo na obavješćivanje sporedno je i potrebno u odnosu na cilj zaštite temeljnih prava na kojem se temelji ova Uredba. Stoga bi u ovoj Uredbi trebalo utvrditi obvezu obavješćivanja u tu svrhu, a da se pritom ne utječe na postojeća prava radnika.
- (93) Iako rizici povezani s UI sustavima mogu proizlaziti iz načina na koji su ti sustavi dizajnirani, mogu biti uzrokovani i načinom na koji se oni koriste. Subjekti koji uvode visokorizične UI sustave stoga imaju ključnu ulogu u osiguravanju zaštite temeljnih prava, čime se dopunjuju obveze dobavljača pri razvoju UI sustava. Subjekti koji uvode UI sustave u najboljem su položaju da razumiju kako će se visokorizični UI sustav konkretno koristiti te stoga mogu utvrditi potencijalne znatne rizike koji nisu predviđeni u fazi razvoja, zahvaljujući preciznijem poznavanju konteksta korištenja te osoba ili skupina osoba koje bi vjerojatno bile zahvaćene, uključujući skupine ranjivih osoba. Subjekti koji uvode visokorizične UI sustave navedene u prilogu ovoj Uredbi također imaju ključnu ulogu u informiranju fizičkih osoba i trebali bi, kada donose odluke ili pomažu u donošenju odluka povezanih s fizičkim osobama, ako je primjenjivo, obavijestiti fizičke osobe da podliježu korištenju visokorizičnog UI sustava. Te informacije trebale bi obuhvaćati namjenu sustava i vrstu odluka koje donosi. Subjekt koji uvodi sustav trebao bi obavijestiti fizičke osobe i o njihovu pravu na objašnjenje predviđenom na temelju ove Uredbe. Kad je riječ o visokorizičnim UI sustavima koji se upotrebljavaju u svrhu kaznenog progona, tu bi obvezu trebalo provesti u skladu s člankom 13. Direktive (EU) 2016/680.
- (94) Svaka obrada biometrijskih podataka povezana s korištenjem UI sustava za biometrijsku identifikaciju u svrhu kaznenog progona mora biti u skladu s člankom 10. Direktive (EU) 2016/680, kojim se takva obrada dopušta samo ako je to nužno, podložno odgovarajućim zaštitnim mjerama u pogledu prava i sloboda ispitanika i ako je to dopušteno pravom Unije ili pravom države članice. Pri takvom korištenju, ako je odobreno, moraju se poštovati i načela utvrđena u članku 4. stavku 1. Direktive (EU) 2016/680, uključujući zakonitost, pravednost i transparentnost, ograničenje svrhe, točnost i ograničenje pohrane.
- (95) Ne dovodeći u pitanje primjenjivo pravo Unije, osobito Uredbu (EU) 2016/679 i Direktivu (EU) 2016/680, uzimajući u obzir intruzivnu prirodu sustava za naknadnu daljinsku biometrijsku identifikaciju, korištenje sustava za naknadnu daljinsku biometrijsku identifikaciju trebalo bi podlijezati zaštitnim mjerama. Sustavi za naknadnu daljinsku biometrijsku identifikaciju uvijek bi se trebali upotrebljavati na način koji je proporcionalan, legitiman i nužan te stoga ciljan u smislu pojedinaca koje treba identificirati, lokacije i vremenskog opsega te se temeljiti na zatvorenom skupu podataka sa zakonito pribavljenog videozapisa. U svakom slučaju, sustavi za naknadnu daljinsku biometrijsku identifikaciju ne bi se trebali upotrebljavati u okviru kaznenog progona kako bi doveli do neselektivnog nadzora. Uvjeti za naknadnu daljinsku biometrijsku identifikaciju ni u kojem slučaju ne bi trebali biti osnova za zaobilazanje uvjeta zabrane i strogih iznimaka za daljinsku biometrijsku identifikaciju u stvarnom vremenu.
- (96) Kako bi se učinkovito osigurala zaštita temeljnih prava, subjekti koji uvode visokorizične UI sustave koji su javnopravna tijela ili privatni subjekti koji pružaju javne usluge i subjekti koji uvode određene visokorizične UI sustave navedene u prilogu ovoj Uredbi, kao što su bankarski ili osiguravateljski subjekti, trebali bi prije stavljanja tih sustava u upotrebu provesti procjenu učinka na temeljna prava. Usluge važne za pojedince koje su javne prirode mogu pružati i privatni subjekti. Privatni subjekti koji pružaju takve javne usluge povezani su sa zadaćama od javnog interesa, primjerice u područjima obrazovanja, zdravstvene skrbi, socijalnih usluga, stanovanja i sudovanja. Cilj je procjene učinka na temeljna prava da subjekt koji uvodi sustav utvrdi specifične rizike za prava pojedinaca ili skupina pojedinaca na koje bi mogao utjecati te utvrdi mjere koje se moraju poduzeti u slučaju materijalizacije tih rizika. Procjenu učinka trebala bi provesti prije uvođenja visokorizičnog UI sustava te bi je trebalo ažurirati ako

⁽³⁹⁾ Direktiva 2002/14/EZ Europskog parlamenta i Vijeća od 11. ožujka 2002. o uspostavljanju općeg okvira za obavješćivanje i savjetovanje s radnicima u Europskoj zajednici (SL L 80, 23.3.2002., str. 29.).

subjekt koji uvodi sustav smatra da se promijenio bilo koji od relevantnih čimbenika. U procjeni učinka trebalo bi utvrditi relevantne procese subjekta koji uvodi sustav u kojima će se visokorizični UI sustav upotrebljavati u skladu sa svojom namjenom te bi ona trebala uključivati opis razdoblja i učestalosti upotrebe sustava, kao i posebnih kategorija fizičkih osoba i skupina na koje će vjerojatno utjecati u specifičnom kontekstu upotrebe. Procjena bi trebala uključivati i utvrđivanje specifičnih rizika od štete koja bi mogla utjecati na temeljna prava tih osoba ili skupina. Pri provedbi te procjene subjekt koji uvodi UI sustav trebao bi uzeti u obzir informacije relevantne za pravilnu procjenu učinka, uključujući, ali ne ograničavajući se na informacije koje je dobavljač visokorizičnog UI sustava naveo u uputama za korištenje. S obzirom na utvrđene rizike, subjekti koji uvode sustav trebali bi utvrditi mjere koje treba poduzeti u slučaju materijalizacije tih rizika, uključujući na primjer aranžmane upravljanja u tom specifičnom kontekstu upotrebe, kao što su aranžmani za ljudski nadzor u skladu s uputama za korištenje ili postupci rješavanja pritužbi i pravne zaštite, jer bi oni mogli biti ključni za ublažavanje rizika za temeljna prava u konkretnim slučajevima korištenja. Nakon provedbe te procjene učinka subjekt koji uvodi sustav trebao bi obavijestiti relevantno tijelo za nadzor tržišta. Prema potrebi, za prikupljanje relevantnih informacija potrebnih za procjenu učinka subjekti koji uvode visokorizični UI sustav, posebno kada se UI sustavi upotrebljavaju u javnom sektoru, mogli bi u provedbu takvih procjena učinka i osmišljavanje mjera koje se moraju poduzeti u slučaju materijalizacije rizika uključiti relevantne dionike, među kojima su predstavnici skupina osoba na koje će UI sustav vjerojatno utjecati, neovisni stručnjaci i organizacije civilnog društva. Europski ured za umjetnu inteligenciju (Ured za umjetnu inteligenciju) trebao bi izraditi predložak upitnika kako bi se olakšala usklađenost i smanjilo administrativno opterećenje za subjekte koji uvode UI sustav.

- (97) Pojam UI modela opće namjene trebao bi biti jasno definiran i odvojen od pojma UI sustava kako bi se omogućila pravna sigurnost. Definicija bi se trebala temeljiti na ključnim funkcionalnim značajkama UI modela opće namjene, posebno općenitosti i sposobnosti kompetentnog obavljanja širokog raspona različitih zadaća. Ti se modeli obično treniraju s pomoću velikih količina podataka putem različitih metoda, kao što su samostalno nadzirano, nenadzirano ili podržano učenje. UI modeli opće namjene mogu se staviti na tržište na različite načine, među ostalim putem programskih knjižnica, aplikacijskih programskih sučelja, izravnim preuzimanjem ili kao fizička kopija. Ti se modeli mogu dodatno izmijeniti ili prilagoditi novim modelima. Iako su UI modeli ključne komponente UI sustava, oni sami po sebi nisu UI sustavi. UI modeli zahtijevaju dodavanje dodatnih komponenti kao što je korisničko sučelje, kako bi postali UI sustavi. UI modeli obično su integrirani u UI sustave i čine njihov sastavni dio. Ovom se Uredbom utvrđuju posebna pravila za UI modele opće namjene i UI modele opće namjene koji predstavljaju systemske rizike, koja bi se trebala primjenjivati i kada su ti modeli integrirani u UI sustav ili su njegov dio. Trebalo bi podrazumijevati da bi se obveze dobavljača UI modela opće namjene trebale primjenjivati nakon što se ti modeli stave na tržište. Ako dobavljač UI modela opće namjene integrira vlastiti model u vlastiti UI sustav koji je stavljen na raspolaganje na tržištu ili u upotrebu, trebalo bi smatrati da je taj model stavljen na tržište te bi se stoga obveze iz ove Uredbe koje se odnose na modele trebale nastaviti primjenjivati uz one za UI sustave. Obveze utvrđene za modele ni u kojem slučaju ne bi se trebale primjenjivati kada se vlastiti model upotrebljava za isključivo unutarnje procese koji nisu ključni za pružanje proizvoda ili usluge trećim stranama i kada to ne utječe na prava fizičkih osoba. S obzirom na njihove potencijalne znatno negativne učinke, UI modeli opće namjene sa sistemskim rizikom uvijek bi trebali podlijegati relevantnim obvezama na temelju ove Uredbe. Definicija ne bi trebala obuhvaćati UI modele koji se upotrebljavaju prije njihova stavljanja na tržište isključivo u svrhu istraživanja, razvoja i izrade prototipa. Time se ne dovodi u pitanje obveza usklađivanja s ovom Uredbom kada se, nakon takvih aktivnosti, model stavi na tržište.
- (98) Budući da bi se općenitost modela, među ostalim, mogla utvrditi i s pomoću niza parametara, trebalo bi smatrati da modeli s najmanje milijardu parametara i trenirani s pomoću velike količine podataka uz primjenu samostalnog nadzora u širokim razmjerima pokazuju znatnu razinu općenitosti i kompetentno obavljaju širok raspon različitih zadaća.
- (99) Veliki generativni UI modeli tipičan su primjer UI modela opće namjene s obzirom na to da omogućuju fleksibilnu proizvodnju sadržaja, primjerice u obliku teksta, audiozapisa, slika ili videozapisa, koji mogu lako obavljati širok raspon različitih zadaća.
- (100) Ako je UI model opće namjene integriran u UI sustav ili je njegov sastavni dio, taj bi se sustav trebao smatrati UI sustavom opće namjene ako zbog te integracije taj sustav može služiti različitim namjenama. UI sustav opće namjene može se upotrebljavati izravno ili može biti integriran u druge UI sustave.

- (101) Dobavljači UI modela opće namjene imaju posebnu ulogu i odgovornost duž vrijednosnog lanca umjetne inteligencije jer modeli koje pružaju mogu biti osnova za niz sustava niže u lancu, koje često pružaju dobavljači niže u lancu koji zahtijevaju dobro razumijevanje modela i njihovih sposobnosti kako bi omogućili integraciju takvih modela u svoje proizvode i ispunili svoje obveze na temelju ove Uredbe ili drugih uredaba. Stoga bi trebalo utvrditi razmjerne mjere transparentnosti, uključujući sastavljanje i ažuriranje dokumentacije te pružanje informacija o UI modelu opće namjene za dobavljače niže u lancu. Dobavljač UI modela opće namjene trebao bi pripremiti i ažurirati tehničku dokumentaciju kako bi je na zahtjev stavio na raspolaganje Uredu za umjetnu inteligenciju i nacionalnim nadležnim tijelima. Minimalni skup elemenata koje treba uključiti u takvu dokumentaciju trebalo bi utvrditi u specifičnim prilogima ovoj Uredbi. Komisiju bi trebalo ovlastiti da izmijeni te priloge delegiranim aktima s obzirom na tehnološki razvoj.
- (102) Softver i podaci, uključujući modele, koji se objavljuju na temelju besplatne licencije za softver otvorenog koda koja omogućuje njihovo otvoreno dijeljenje i zbog koje im korisnici mogu slobodno pristupiti, upotrebljavati ih, mijenjati i redistribuirati njih ili njihove izmijenjene verzije, mogu doprinijeti istraživanju i inovacijama na tržištu i pružiti znatne prilike za rast gospodarstva Unije. Trebalo bi razmotriti UI modele opće namjene objavljene na temelju besplatnih licencija za softver otvorenog koda kako bi se osigurala visoka razina transparentnosti i otvorenosti ako su njihovi parametri, uključujući težinske faktore, informacije o arhitekturi modela i informacije o upotrebi modela javno dostupni. Licenciju bi trebalo smatrati besplatnom licencijom za softver otvorenog koda i kada omogućuje korisnicima da pokrenu, kopiraju, distribuiraju, proučavaju, mijenjaju i poboljšavaju softver i podatke, uključujući modele, pod uvjetom da je priznat izvorni pružatelj modela i da se poštuju identični ili usporedivi uvjeti distribucije.
- (103) Besplatne UI komponente otvorenog koda obuhvaćaju softver i podatke, uključujući modele i UI modele opće namjene, alate, usluge ili procese UI sustava. Besplatne UI komponente otvorenog koda mogu se pružati različitim kanalima, uključujući njihov razvoj u otvorenim repozitorijima. Za potrebe ove Uredbe na UI komponente koje se pružaju uz naplatu ili se na drugi način monetiziraju, među ostalim i pružanjem tehničke podrške ili drugih usluga povezanih s UI komponentom, među ostalim i putem softverske platforme, ili upotrebom osobnih podataka u svrhe koje nisu isključivo povećanje sigurnosti, kompatibilnosti ili interoperabilnosti softvera, uz iznimku transakcija među mikropoduzećima, ne bi se trebale primjenjivati iznimke za besplatne UI komponente otvorenog koda. Činjenica da se UI komponente stavljaju na raspolaganje putem otvorenih repozitorija ne bi sama po sebi trebala predstavljati monetizaciju.
- (104) Dobavljači UI modela opće namjene koji se objavljuju na temelju besplatne licencije otvorenog koda i čiji su parametri, uključujući težinske faktore, informacije o arhitekturi modela i informacije o upotrebi modela, javno dostupni trebali bi podliježati iznimkama u pogledu zahtjeva povezanih s transparentnošću nametnutih za UI modele opće namjene, osim ako se može smatrati da predstavljaju sistemski rizik, pri čemu se okolnost da je model transparentan i popraćen licencijom otvorenog koda ne bi trebala smatrati dovoljnim razlogom za isključenje ispunjavanja obveza iz ove Uredbe. U svakom slučaju, s obzirom na to da se objavom UI modela opće namjene na temelju besplatne licencije otvorenog koda nužno ne otkrivaju bitne informacije o skupu podataka koji se upotrebljava za treniranje ili doradu modela i o tome kako je time osigurana usklađenost s pravom o autorskom pravu, iznimka od ispunjavanja zahtjeva povezanih s transparentnošću predviđena za UI modele opće namjene ne bi se trebala odnositi na obvezu izrade sažetka o sadržaju koji se upotrebljava za treniranje modela i na obvezu uspostave politike usklađivanja s pravom Unije o autorskom pravu, posebno radi utvrđivanja i poštovanja pridržaja prava u skladu s člankom 4. stavkom 3. Direktive (EU) 2019/790 Europskog parlamenta i Vijeća ⁽⁴⁰⁾.
- (105) UI modeli opće namjene, osobito veliki generativni UI modeli koji mogu generirati tekst, slike i druge sadržaje, pružaju jedinstvene mogućnosti za inovacije, ali i izazove za umjetnike, autore i druge kreatore te za način na koji se njihov kreativni sadržaj stvara, distribuira, upotrebljava i konzumira. Za razvoj i treniranje takvih modela potreban je pristup velikim količinama teksta, slika, videozapisa i drugih podataka. Tehnike rudarenja teksta i podataka mogu se u tom kontekstu u velikoj mjeri upotrebljavati za pronalaženje i analizu takvog sadržaja, koji može biti zaštićen autorskim pravom i povezanih pravima. Za svako korištenje sadržaja zaštićenog autorskim pravom potrebno je odobrenje nositelja prava nad tim sadržajem, osim ako se primjenjuju relevantne iznimke i ograničenja autorskog prava. Direktivom (EU) 2019/790 uvedene su iznimke i ograničenja kojima se omogućuje reproduciranje i izvlačenje djela ili drugih sadržaja u svrhu rudarenja teksta i podataka, pod određenim uvjetima. Na temelju tih pravila nositelji

⁽⁴⁰⁾ Direktiva (EU) 2019/790 Europskog parlamenta i Vijeća od 17. travnja 2019. o autorskom i srodnim pravima na jedinstvenom digitalnom tržištu i izmjeni direktiva 96/9/EZ i 2001/29/EZ (SL L 130, 17.5.2019., str. 92.).

prava mogu odlučiti pridržati svoja prava nad svojim djelima ili drugim sadržajima kako bi spriječili rudarenje teksta i podataka, osim ako se rudarenje teksta i podataka provodi za potrebe znanstvenog istraživanja. Ako je nositelj prava izričito pridržao prava na izuzeće na primjeren način, dobavljači UI modela opće namjene moraju od njega dobiti odobrenje ako žele provoditi rudarenje teksta i podataka nad takvim djelima.

- (106) Dobavljači koji stavljaju UI modele opće namjene na tržište Unije trebali bi osigurati usklađenost s relevantnim obvezama iz ove Uredbe. U tu bi svrhu dobavljači UI modela opće namjene trebali uspostaviti politiku usklađivanja s pravom Unije o autorskom pravu i povezanim pravima, posebno radi utvrđivanja i poštovanja pridržaja prava koji su izrazili nositelji prava u skladu s člankom 4. stavkom 3. Direktive (EU) 2019/790. Svaki dobavljač koji na tržište Unije stavlja UI model opće namjene trebao bi ispunjavati tu obvezu, bez obzira na jurisdikciju u kojoj se odvijaju radnje povezane s autorskim pravima na kojima se temelji treniranje tih UI modela opće namjene. To je potrebno kako bi se osigurali jednaki uvjeti među dobavljačima UI modela opće namjene prema kojima nijedan dobavljač ne bi trebao moći steći konkurentsku prednost na tržištu Unije primjenom nižih standarda autorskih prava od onih koji su predviđeni u Uniji.
- (107) Kako bi se povećala transparentnost podataka koji se upotrebljavaju u prethodnom treniranju i treniranju UI modela opće namjene, uključujući tekst i podatke zaštićene autorskim pravom, primjereno je da dobavljači takvih modela sastave i objave dovoljno detaljan sažetak sadržaja koji se upotrebljava za treniranje UI modela opće namjene. Uzimajući u obzir potrebu za zaštitom poslovnih tajni i povjerljivih poslovnih informacija, taj bi sažetak trebao biti općenito sveobuhvatan u svojem opsegu, a ne tehnički detaljan, kako bi se strankama s legitimnim interesima, uključujući nositelje autorskih prava, olakšalo ostvarivanje i izvršavanje njihovih prava na temelju prava Unije, na primjer navođenjem glavnih zbirki ili skupova podataka koji su upotrijebljeni pri treniranju modela, kao što su velike privatne ili javne baze podataka ili arhive podataka, te pružanjem opisnog objašnjenja o drugim korištenim izvorima podataka. Primjereno je da Ured za umjetnu inteligenciju dostavi predložak sažetka, koji bi trebao biti jednostavan, djelotvoran i omogućiti dobavljaču da dostavi traženi sažetak u opisnom obliku.
- (108) Kad je riječ o obvezama nametnutima dobavljačima UI modela opće namjene da uspostave politiku usklađivanja s pravom Unije o autorskom pravu i objave sažetak sadržaja koji se upotrebljava za treniranje, Ured za umjetnu inteligenciju trebao bi pratiti je li dobavljač ispunio te obveze bez provjere ili pojedinačnog ocjenjivanja podataka korištenih za treniranje u pogledu usklađenosti s autorskim pravom. Ova Uredba ne utječe na izvršavanje pravila o autorskom pravu kako su predviđena pravom Unije.
- (109) Usklađenost s obvezama koje se primjenjuju na dobavljače UI modela opće namjene trebala bi biti razmjerna i primjerena vrsti dobavljača modela, isključujući potrebu za usklađenosti za osobe koje razvijaju ili upotrebljavaju modele u neprofesionalne ili znanstveno-istraživačke svrhe, no koje bi ipak trebalo poticati da dobrovoljno ispune te zahtjeve. Ne dovodeći u pitanje pravo Unije o autorskom pravu, pri ispunjavanju tih obveza trebalo bi uzeti u obzir veličinu dobavljača i omogućiti pojednostavnjene načine usklađivanja za MSP-ove, uključujući *start-up* poduzeća, koji ne bi trebali predstavljati pretjerani trošak niti obeshrabrivati korištenje takvih modela. U slučaju izmjene ili dorade modela, obveze dobavljača UI modela opće namjene trebale bi biti ograničene na tu izmjenu ili doradu, na primjer dopunjavanjem već postojeće tehničke dokumentacije informacijama o izmjenama, uključujući nove izvore podataka za treniranje, kako bi se ispunile obveze u pogledu vrijednosnog lanca predviđene u ovoj Uredbi.
- (110) UI modeli opće namjene mogli bi predstavljati sistemske rizike koji uključuju, ali nisu ograničeni na, sve stvarne ili razumno predvidljive negativne učinke povezane s velikim nesrećama, poremećajima u kritičnim sektorima i ozbiljnim posljedicama za javno zdravlje i sigurnost; sve stvarne ili razumno predvidljive negativne učinke na demokratske procese, javnu i gospodarsku sigurnost; širenje nezakonitog, lažnog ili diskriminirajućeg sadržaja. Trebalo bi razumjeti da se sistemski rizici povećavaju s kapacitetom i dosegom modela, da se mogu pojaviti tijekom cijelog životnog ciklusa modela i da na njih utječu uvjeti pogrešne upotrebe, pouzdanost modela, pravednost modela i sigurnost modela, razinu autonomije modela, njegov pristup alatima, novi ili kombinirani modaliteti, strategije objave i distribucije, potencijal za uklanjanje zaštitnih mehanizama i drugi čimbenici. Konkretno, u međunarodnim pristupima dosad je utvrđeno da je potrebno posvetiti pozornost rizicima od moguće namjerne pogrešne upotrebe ili nenamjernih problemima u kontroli koji se odnose na usklađivanje s ljudskom namjerom; kemijskim, biološkim, radiološkim i nuklearnim rizicima, kao što su načini na koje se mogu smanjiti prepreke za pristup, uključujući za

razvoj oružja, nabavu njihova dizajna ili njihovu upotrebu; ofenzivnim kibernetičkim sposobnostima, kao što su načini omogućavanja otkrivanja, iskorištavanja ili operativne upotrebe slabih točaka; učincima interakcije i upotrebe alata, uključujući, na primjer, sposobnost kontrole fizičkih sustava i ometanja kritične infrastrukture; rizicima povezanim s modelima koji izrađuju svoje kopije ili se „samorepliciraju” ili treniraju druge modele; načinima na koje modeli mogu dovesti do štetne pristranosti i diskriminacije uz rizike za pojedince, zajednice ili društva; olakšavanju širenja dezinformacija ili ugrožavanju privatnosti prijetnjama demokratskim vrijednostima i ljudskim pravima; riziku od toga da bi određeni događaj mogao dovesti do lančane reakcije sa znatnim negativnim učincima koji bi mogli utjecati na cijeli grad, cijelu aktivnost u nekoj domeni ili cijelu zajednicu.

- (111) Primjereno je uspostaviti metodologiju za klasifikaciju UI modela opće namjene kao UI modela opće namjene sa sistemskim rizicima. Budući da sistemski rizici proizlaze iz posebno visokih sposobnosti, trebalo bi smatrati da UI model opće namjene predstavlja sistemske rizike ako ima sposobnosti visokog učinka, koje se ocjenjuje na temelju odgovarajućih tehničkih alata i metodologija, ili ako zbog svojeg dosega znatno utječe na unutarnje tržište. Sposobnosti visokog učinka kod UI modela opće namjene znači sposobnosti koje odgovaraju sposobnostima zabilježenima kod najnaprednijih UI modela opće namjene ili ih nadilaze. Cijeli raspon sposobnosti modela mogao bi se bolje razumjeti nakon njegova stavljanja na tržište ili pri interakciji dobavljača s modelom. U skladu s najnovijim dostignućima u trenutku stupanja na snagu ove Uredbe, kumulativna količina računanja korištena za treniranje UI modela opće namjene iskazana brojem matematičkih operacija nad brojevima s pomičnim zarezom jedna je od relevantnih približnih vrijednosti za sposobnosti modela. Kumulativna količina računanja korištena za treniranje uključuje računanje korišteno u svim aktivnostima i metode namijenjene poboljšanju sposobnosti modela prije uvođenja, kao što su prethodno treniranje, generiranje sintetičkih podataka i dorada. Stoga bi trebalo utvrditi početni prag za matematičke operacije nad brojevima s pomičnim zarezom, koji, ako ga UI model opće namjene dosegne, dovodi do pretpostavke da je riječ o UI modelu opće namjene sa sistemskim rizicima. Taj bi prag trebalo s vremenom prilagoditi kako bi odražavao tehnološke i industrijske promjene, kao što su algoritamska poboljšanja ili povećana učinkovitost hardvera, te bi ga trebalo dopuniti referentnim vrijednostima i pokazateljima sposobnosti modela. U tu bi svrhu Ured za umjetnu inteligenciju trebao surađivati sa znanstvenom zajednicom, strukom, civilnim društvom i drugim stručnjacima. Pragovi, kao i alati i referentne vrijednosti za procjenu sposobnosti visokog učinka, trebali bi u velikoj mjeri predvidjeti općenitost, sposobnosti i povezani sistemski rizik UI modela opće namjene te bi se njima moglo uzeti u obzir način na koji će se model staviti na tržište ili broj korisnika na koji bi mogao utjecati. Kako bi se taj sustav dopunio, Komisija bi trebala moći donijeti pojedinačne odluke kojima se UI model opće namjene određuje kao UI model opće namjene sa sistemskim rizikom ako se utvrdi da takav model ima sposobnosti ili učinak jednakovrijedan onima koji su obuhvaćeni utvrđenim pragom. Ta bi se odluka trebala donijeti na temelju opće procjene kriterija za određivanje UI modela opće namjene sa sistemskim rizikom navedenih u prilogu ovoj Uredbi, kao što su kvaliteta ili veličina skupa podataka za treniranje, broj poslovnih i krajnjih korisnika, njihovi ulazni i izlazni modaliteti, razina autonomije i skalabilnosti ili alati kojima ima pristup. Na obrazloženi zahtjev dobavljača čiji je model određen kao UI model opće namjene sa sistemskim rizikom Komisija bi takav zahtjev trebala uzeti u obzir i može odlučiti ponovno ocijeniti može li se i dalje smatrati da UI model opće namjene predstavlja sistemske rizike.
- (112) Također je potrebno pojasniti proceduru za klasifikaciju UI modela opće namjene kao UI modela opće namjene sa sistemskim rizicima. Za UI model opće namjene koji je dosegao primjenjivi prag za sposobnosti visokog učinka trebalo bi se pretpostaviti da je riječ o UI modelu opće namjene sa sistemskim rizikom. Dobavljač bi trebao obavijestiti Ured za umjetnu inteligenciju najkasnije dva tjedna nakon što su zahtjevi ispunjeni ili nakon što postane poznato da će UI model opće namjene ispunjavati zahtjeve koji dovode do te pretpostavke. To je posebno važno u odnosu na prag matematičkih operacija nad brojevima s pomičnim zarezom jer je za treniranje UI modela opće namjene potrebno znatno planiranje koje uključuje prethodnu dodjelu računalnih resursa te stoga dobavljači UI modela opće namjene mogu znati bi li njihov model dosegnuo prag prije završetka postupka treniranja. U kontekstu te obavijesti dobavljač bi trebao moći dokazati da, zbog posebnih značajki UI modela opće namjene, taj model iznimno ne predstavlja sistemske rizike te da ga stoga ne bi trebalo klasificirati kao UI model opće namjene sa sistemskim rizicima. Te su informacije vrijedne Uredu za umjetnu inteligenciju kako bi predvidio stavljanje na tržište

UI modela opće namjene sa sistemskim rizicima, a dobavljači mogu rano početi surađivati s Uredom za umjetnu inteligenciju. Te su informacije posebno važne u pogledu UI modela opće namjene koji se planiraju objaviti kao otvoreni kod, s obzirom na to da bi nakon objave modela otvorenog koda moglo biti teže provesti potrebne mjere za osiguravanje usklađenosti s obvezama iz ove Uredbe.

- (113) Ako Komisija sazna da UI model opće namjene ispunjava zahtjeve da ga se klasificira kao UI model opće namjene sa sistemskim rizikom, a prethodno nije bio poznat ili o njemu relevantni dobavljač nije obavijestio Komisiju, Komisija bi trebala biti ovlaštena odrediti ga kao takvoga. Sustav kvalificiranih upozorenja trebao bi osigurati da znanstveno povjerenstvo obavijesti Ured za umjetnu inteligenciju o UI modelima opće namjene koje bi potencijalno trebalo klasificirati kao UI modele opće namjene sa sistemskim rizikom, kao i o aktivnostima praćenja Ureda za umjetnu inteligenciju.
- (114) Dobavljači UI modela opće namjene koji predstavljaju sistemske rizike trebali bi, uz obveze predviđene za dobavljače UI modela opće namjene, podlijeći obvezama usmjerenima na utvrđivanje i ublažavanje tih rizika i osiguravanje odgovarajuće razine kibernetičkosigurnosne zaštite, bez obzira na to pružaju li se kao samostalni model ili su ugrađeni u UI sustav ili proizvod. Kako bi se postigli ti ciljevi, ovom bi se Uredbom od dobavljača trebalo zahtijevati da provedu potrebne evaluacije modela, posebno prije njihova prvog stavljanja na tržište, uključujući provođenje i dokumentiranje neprijateljskog testiranja modela, također, prema potrebi, unutarnjim testiranjem ili neovisnim vanjskim testiranjem. Osim toga, dobavljači UI modela opće namjene sa sistemskim rizicima trebali bi kontinuirano procjenjivati i ublažavati sistemske rizike, među ostalim i, primjerice, uspostavom politika upravljanja rizikom, kao što su postupci odgovornosti i upravljanja, provedbom praćenja nakon stavljanja na tržište, poduzimanjem odgovarajućih mjera tijekom cijelog životnog ciklusa modela i suradnjom s relevantnim akterima duž lanca vrijednosti umjetne inteligencije.
- (115) Dobavljači UI modela opće namjene sa sistemskim rizicima trebali bi procijeniti i ublažiti moguće sistemske rizike. Ako, unatoč nastojanjima da se utvrde i spriječe rizici povezani s UI modelom opće namjene koji bi mogao predstavljati sistemske rizike, razvoj ili korištenje modela uzrokuju ozbiljan incident, dobavljač UI modela opće namjene trebao bi bez nepotrebne odgode pratiti incident i izvješćivati Komisiju i nacionalna nadležna tijela o svim relevantnim informacijama i mogućim korektivnim mjerama. Nadalje, dobavljači bi trebali osigurati odgovarajuću razinu kibernetičkosigurnosne zaštite modela i njegove fizičke infrastrukture, prema potrebi, tijekom cijelog životnog ciklusa modela. Kibernetičkosigurnosnom zaštitom koja je povezana sa sistemskim rizicima povezanim sa zlonamjernom upotrebom ili napadima trebalo bi na odgovarajući način uzeti u obzir slučajno curenje iz modela, neovlaštena objavljivanja, zaoblazanje sigurnosnih mjera i obranu od kibernetičkih napada, neovlaštenog pristupa ili krađe modela. Ta bi se zaštita mogla olakšati osiguravanjem težinskih faktora modela, algoritama, poslužitelja i skupova podataka, primjerice mjerama operativne sigurnosti za informacijsku sigurnost, posebnim kibernetičko-sigurnosnim politikama, odgovarajućim tehničkim i utvrđenim rješenjima te kontrolama kibernetičkog i fizičkog pristupa, koji su primjereni relevantnim okolnostima i uključenim rizicima.
- (116) Ured za umjetnu inteligenciju trebao bi poticati i olakšati izradu, preispitivanje i prilagodbu kodeksa prakse, uzimajući u obzir međunarodne pristupe. Svi dobavljači UI modela opće namjene mogli bi biti pozvani na sudjelovanje. Kako bi se osiguralo da se kodeksima prakse odražavaju najnovija dostignuća i na odgovarajući način uzimaju u obzir različite perspektive, Ured za umjetnu inteligenciju trebao bi surađivati s relevantnim nacionalnim nadležnim tijelima te bi se, prema potrebi, mogao savjetovati s organizacijama civilnog društva i drugim relevantnim dionicima i stručnjacima, uključujući znanstveno povjerenstvo, radi izrade takvih kodeksa. Kodeksi prakse trebali bi obuhvaćati obveze dobavljača UI modela opće namjene i UI modela opće namjene koji predstavljaju sistemske rizike. Osim toga, kad je riječ o sistemskim rizicima, kodeksi prakse trebali bi pomoći u uspostavi taksonomije vrste i prirode sistemskih rizika na razini Unije, uključujući njihove izvore. Kodeksi prakse trebali bi biti usmjereni i na posebne mjere procjene i ublažavanja rizika.
- (117) Kodeksi prakse trebali bi biti središnji alat za pravilno ispunjavanje obveza predviđenih na temelju ove Uredbe za dobavljače UI modela opće namjene. Dobavljači bi se trebali moći osloniti na kodekse prakse kako bi dokazali ispunjavanje obveza. Komisija provedbenim aktima može odlučiti odobriti kodeks prakse i učiniti ga općenito valjanim u Uniji ili, alternativno, utvrditi zajednička pravila za provedbu relevantnih obveza ako do početka primjene ove Uredbe kodeks prakse ne može biti dovršen ili ga Ured za umjetnu inteligenciju ne smatra adekvatnim. Nakon što se usklađena norma objavi i Ured za umjetnu inteligenciju ocijeni je prikladnom za obuhvaćanje

relevantnih obveza, ispunjavanje europske usklađene norme dobavljačima bi trebalo omogućiti pretpostavku sukladnosti. Nadalje, dobavljači UI modela opće namjene trebali bi moći dokazati ispunjavanje obveza s pomoću alternativnih odgovarajućih sredstava ako kodeksi prakse ili usklađene norme nisu dostupni ili ako odluče da se neće oslanjati na njih.

- (118) Ovom se Uredbom reguliraju UI sustavi i modeli uvođenjem određenih zahtjeva i obveza za relevantne aktere na tržištu koji ih stavljaju na tržište ili u upotrebu ili ih upotrebljavaju u Uniji, čime se dopunjuju obveze pružatelja usluga posredovanja koji takve sustave ili modele ugrađuju u svoje usluge regulirane Uredbom (EU) 2022/2065. U mjeri u kojoj su takvi sustavi ili modeli ugrađeni u određene vrlo velike internetske platforme ili vrlo velike internetske tražilice, na njih se primjenjuje okvir za upravljanje rizicima predviđen u Uredbi (EU) 2022/2065. Stoga bi trebalo pretpostaviti da su odgovarajuće obveze iz ove Uredbe ispunjene, osim ako se u takvim modelima pojave znatni sistemski rizici koji nisu obuhvaćeni Uredbom (EU) 2022/2065. Unutar tog okvira pružatelji vrlo velikih internetskih platformi i vrlo velikih internetskih tražilica obvezni su procijeniti potencijalne sistemske rizike koji proizlaze iz dizajna, funkcioniranja i korištenja njihovih usluga, uključujući način na koji dizajn algoritamskih sustava koji se upotrebljavaju u usluzi može doprinijeti takvim rizicima, kao i sistemske rizike koji proizlaze iz mogućih pogrešnih upotreba. Ti su pružatelji također obvezni poduzeti odgovarajuće mjere za ublažavanje rizika za temeljna prava.
- (119) S obzirom na brz tempo inovacija i tehnološki razvoj digitalnih usluga u području primjene različitih instrumenata prava Unije, posebno imajući na umu upotrebu i percepciju njihovih primatelja, UI sustavi koji podliježu ovoj Uredbi mogu se pružati kao usluge posredovanja ili njihovi dijelovi u smislu Uredbe (EU) 2022/2065, koje bi trebalo tumačiti na tehnološki neutralan način. Na primjer, UI sustavi mogu se upotrebljavati za pružanje internetskih tražilica, posebno u mjeri u kojoj UI sustav, kao što je internetski chatbot, u načelu pretražuje sve internetske stranice, zatim uključuje rezultate u svoje postojeće znanje i upotrebljava nadopunjeno znanje kako bi generirao jedan izlazni rezultat koji objedinjuje različite izvore informacija.
- (120) Nadalje, obveze propisane u ovoj Uredbi za dobavljače i za subjekte koji uvođe određene UI sustave kako bi se omogućilo prepoznavanje i otkrivanje umjetno stvorenih ili manipuliranih izlaznih rezultata tih sustava posebno su relevantne za olakšavanje djelotvorne provedbe Uredbe (EU) 2022/2065. To se posebno odnosi na obveze pružatelja vrlo velikih internetskih platformi ili vrlo velikih internetskih tražilica da utvrde i ublaže sistemske rizike koji mogu proizaći iz širenja umjetno stvorenog ili manipuliranog sadržaja, posebno rizik od stvarnih ili predvidljivih negativnih učinaka na demokratske procese, građanski diskurs i izborne procese, među ostalim dezinformiranjem.
- (121) Normizacija bi trebala imati ključnu ulogu u pružanju tehničkih rješenja dobavljačima kako bi se osigurala usklađenost s ovom Uredbom, u skladu s najnovijim dostignućima, kako bi se promicale inovacije te konkurentnost i rast na jedinstvenom tržištu. Poštovanje usklađenih normi kako su definirane u članku 2. točki 1. podtočki (c) Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća ⁽⁴¹⁾, za koje se obično očekuje da odražavaju najnovija dostignuća, trebalo bi biti sredstvo kojim će dobavljači dokazivati sukladnost sa zahtjevima ove Uredbe. Stoga bi u skladu s člancima 5. i 6. Uredbe (EU) br. 1025/2012 trebalo poticati uravnoteženu zastupljenost interesa koja uključuje sve relevantne dionike u razvoju normi, posebno MSP-ove, organizacije potrošača te dionike u području okoliša i socijalne dionike. Kako bi se olakšala sukladnost, Komisija bi trebala izdati zahtjeve za normizaciju bez nepotrebne odgode. Pri izradi zahtjeva za normizaciju Komisija bi se trebala savjetovati sa savjetodavnim forumom i Vijećem za umjetnu inteligenciju kako bi obuhvatila relevantno stručno znanje. Međutim, u nedostatku relevantnih upućivanja na usklađene norme, Komisija bi trebala moći provedbenim aktima i nakon savjetovanja sa savjetodavnim forumom utvrditi zajedničke specifikacije za određene zahtjeve na temelju ove Uredbe. Zajednička specifikacija trebala bi biti iznimno zamjensko rješenje kako bi se dobavljaču olakšalo ispunjavanje zahtjeva iz ove Uredbe kada nijedna europska organizacija za normizaciju nije prihvatila zahtjev za normizaciju ili kada se relevantnim usklađenim normama u nedovoljnoj mjeri rješavaju problemi u području temeljnih prava ili kada

⁽⁴¹⁾ Uredba (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća (SL L 316, 14.11.2012., str. 12.).

usklađene norme nisu u skladu sa zahtjevom ili kada dođe do kašnjenja u donošenju odgovarajuće usklađene norme. Ako je takvo kašnjenje u donošenju usklađene norme posljedica tehničke složenosti te norme, Komisija bi to trebala razmotriti prije razmatranja utvrđivanja zajedničkih specifikacija. Pri izradi zajedničkih specifikacija Komisiju se potiče na suradnju s međunarodnim partnerima i međunarodnim tijelima za normizaciju.

- (122) Ne dovodeći u pitanje upotrebu usklađenih normi i zajedničkih specifikacija, primjereno je da se za dobavljače visokorizičnog UI sustava koji je treniran i testiran na podacima koji odražavaju specifično zemljopisno, bihevioralno, kontekstualno ili funkcionalno okruženje u kojem se UI sustav namjerava upotrebljavati smatra da su sukladni s relevantnom mjerom predviđenom u zahtjevu u pogledu upravljanja podacima utvrđenom u ovoj Uredbi. Ne dovodeći u pitanje zahtjeve koji se odnose na otpornost i točnost utvrđene u ovoj Uredbi, u skladu s člankom 54. stavkom 3. Uredbe (EU) 2019/881, za visokorizične UI sustave koji su certificirani ili za koje je izdana izjava o sukladnosti u okviru programa kibernetičke sigurnosti na temelju te uredbe i na koje su objavljena upućivanja u *Službenom listu Europske unije* trebalo bi pretpostaviti da ispunjavaju kibernetičkosigurnosne zahtjeve iz ove Uredbe u mjeri u kojoj certifikat o kibernetičkoj sigurnosti ili izjava o sukladnosti ili njihovi dijelovi obuhvaćaju kibernetičkosigurnosne zahtjeve iz ove Uredbe. Time se i dalje ne dovodi u pitanje dobrovoljna priroda tog programa kibernetičke sigurnosti.
- (123) Kako bi se osigurala visoka razina pouzdanosti visokorizičnih UI sustava, ti bi sustavi trebali podlijegati ocjenjivanju sukladnosti prije njihova stavljanja na tržište ili u upotrebu.
- (124) Kako bi se opterećenje za operatore svelo na najmanju moguću mjeru i izbjeglo moguće udvostručavanje, za visokorizične UI sustave povezane s proizvodima koji su obuhvaćeni postojećim zakonodavstvom Unije o usklađivanju na temelju novog zakonodavnog okvira, usklađenost tih UI sustava sa zahtjevima ove Uredbe trebala bi se ocjenjivati u okviru ocjenjivanja sukladnosti koje je već predviđeno u tom pravu. Primjenjivost zahtjeva ove Uredbe stoga ne bi trebala utjecati na specifičnu logiku, metodologiju ili opću strukturu ocjenjivanja sukladnosti na temelju relevantnog zakonodavstva Unije o usklađivanju.
- (125) S obzirom na složenost visokorizičnih UI sustava i s njima povezane rizike, važno je razviti odgovarajući sustav postupka ocjenjivanja sukladnosti visokorizičnih UI sustava koji uključuje prijavljena tijela, tzv. ocjenjivanje sukladnosti koje provodi treća strana. Međutim, s obzirom na trenutačno iskustvo profesionalnih certifikatora proizvoda prije stavljanja na tržište u području sigurnosti proizvoda i različitu prirodu uključenih rizika, primjereno je, barem u početnoj fazi primjene ove Uredbe, ograničiti područje primjene ocjenjivanja sukladnosti visokorizičnih UI sustava koje provodi treća strana, osim za one sustave koji su povezani s proizvodima. Stoga bi ocjenjivanje sukladnosti takvih sustava u pravilu trebao provoditi dobavljač na vlastitu odgovornost, uz jedinu iznimku UI sustava namijenjenih za biometriju.
- (126) Za ocjenjivanje sukladnosti koje provodi treća strana kada je to potrebno, nacionalna nadležna tijela trebala bi na temelju ove Uredbe prijavljivati prijavljena tijela, pod uvjetom da ispunjavaju niz zahtjeva, ponajprije u pogledu neovisnosti, kompetentnosti, nepostojanja sukoba interesa i odgovarajućih kibernetičkosigurnosnih zahtjeva. Nacionalna nadležna tijela trebala bi Komisiji i drugim državama članicama slati obavijesti o prijavljivanju tih tijela pomoću alata za elektroničko prijavljivanje koji je razvila i kojim upravlja Komisija u skladu s člankom R23. Priloga I. Odluci br. 768/2008/EZ.
- (127) U skladu s obvezama Unije na temelju Sporazuma Svjetske trgovinske organizacije o tehničkim preprekama u trgovini primjereno je olakšati uzajamno prihvaćanje rezultata ocjenjivanja sukladnosti koje su proizvela nadležna tijela za ocjenjivanje sukladnosti, bez obzira na to na kojem području imaju poslovni nastan, pod uvjetom da ta tijela za ocjenjivanje sukladnosti osnovana na temelju prava treće zemlje ispunjavaju primjenjive zahtjeve ove Uredbe i da je Unija sklopila odgovarajući sporazum. U tom kontekstu Komisija bi trebala aktivno istražiti moguće međunarodne instrumente u tu svrhu, a posebno nastojati sklopiti sporazume o uzajamnom priznavanju s trećim zemljama.
- (128) U skladu sa zajednički utvrđenim pojmom znatne izmjene za proizvode regulirane zakonodavstvom Unije o usklađivanju primjereno je da se svaki put kad dođe do promjene koja može utjecati na usklađenost visokorizičnog UI sustava s ovom Uredbom (npr. promjena operativnog sustava ili softverske arhitekture) ili kad se promijeni namjena sustava, taj UI sustav smatra novim UI sustavom koji bi trebao proći novo ocjenjivanje sukladnosti. Međutim, promjene algoritma i učinkovitosti UI sustava koji nakon stavljanja na tržište ili u upotrebu nastavljaju „učiti”, odnosno automatski prilagođavati način izvršavanja funkcija, ne bi trebale predstavljati znatnu izmjenu, pod uvjetom da je te promjene unaprijed odredio dobavljač i da su ocijenjene u trenutku ocjenjivanja sukladnosti.

- (129) Visokorizični UI sustavi trebali bi nositi oznaku CE koja upućuje na njihovu sukladnost s ovom Uredbom kako bi se mogli slobodno kretati na unutarnjem tržištu. Kad je riječ o visokorizičnim UI sustavima ugrađenima u proizvod, fizička oznaka CE trebala bi biti pričvršćena na njih te se može dopuniti digitalnom oznakom CE. Za visokorizične UI sustave koji se pružaju samo digitalno trebalo bi upotrebljavati digitalnu oznaku CE. Države članice ne bi trebale stvarati neopravdane zapreke stavljanju na tržište ili u upotrebu visokorizičnih UI sustava koji ispunjavaju zahtjeve utvrđene u ovoj Uredbi i nose oznaku CE.
- (130) Po određenim uvjetima brza dostupnost inovativnih tehnologija može biti ključna za zdravlje i sigurnost osoba, zaštitu okoliša i klimatske promjene te za društvo u cjelini. Stoga je primjereno da bi zbog iznimnih razloga povezanih s javnom sigurnošću ili zaštitom života i zdravlja fizičkih osoba, zaštitom okoliša i ključne industrijske i infrastrukturne imovine, tijela za nadzor tržišta mogla odobriti stavljanje na tržište ili u upotrebu UI sustava za koje nije proveden postupak ocjenjivanja sukladnosti. U propisno opravdanim situacijama, kako je predviđeno u ovoj Uredbi, tijela kaznenog progona ili tijela civilne zaštite mogu staviti u upotrebu određeni visokorizični UI sustav bez odobrenja tijela za nadzor tržišta, pod uvjetom da se takvo odobrenje zatraži tijekom ili nakon korištenja bez nepotrebne odgode.
- (131) Kako bi se olakšao rad Komisije i država članica u području umjetne inteligencije i povećala transparentnost prema javnosti, od dobavljača visokorizičnih UI sustava koji nisu povezani s proizvodima obuhvaćenima područjem primjene relevantnog postojećeg zakonodavstva Unije o usklađivanju, kao i dobavljača koji smatraju da pojedini UI sustav naveden u primjerima visokorizične upotrebe iz priloga ovoj Uredbi nije visokorizičan na temelju odstupanja, trebalo bi zahtijevati da sebe i informacije o svojem UI sustavu registriraju u bazi podataka EU-a, koju će uspostaviti i kojom će upravljati Komisija. Prije upotrebi UI sustava navedenog u primjerima visokorizične upotrebe iz priloga ovoj Uredbi subjekti koji uvode visokorizične UI sustave koji su tijela javne vlasti, javne agencije ili javna tijela trebali bi se registrirati u takvoj bazi podataka i odabrati sustav koji namjeravaju upotrebljavati. Ostali subjekti koji uvode sustav trebali bi imati pravo to učiniti dobrovoljno. Taj dio baze podataka EU-a trebao bi biti javno dostupan, besplatno, a informacije bi trebale biti lako dostupne, razumljive i strojno čitljive. Baza podataka EU-a trebala bi biti prilagođena korisnicima, na primjer pružanjem funkcija pretraživanja, među ostalim s pomoću ključnih riječi, čime bi se široj javnosti omogućio pronalazak relevantnih informacija koje treba dostaviti nakon registracije visokorizičnih UI sustava i relevantnih informacija o slučaju upotrebe visokorizičnih UI sustava navedenih u prilogu ovoj Uredbi, kojima visokorizični UI sustavi odgovaraju. Svaka bitna izmjena visokorizičnih UI sustava također bi se trebala registrirati u bazi podataka EU-a. Kad je riječ o visokorizičnim UI sustavima u područjima kaznenog progona ili migracija, azila i upravljanja nadzorom državne granice, obveze registracije trebale bi se ispuniti u sigurnom dijelu baze podataka EU-a koji nije javan. Pristup sigurnom dijelu koji nije javan trebao bi biti strogo ograničen na Komisiju i tijela za nadzor tržišta na čiju se državu odnosi taj dio baze podataka. Visokorizične UI sustave u području kritične infrastrukture trebalo bi registrirati samo na nacionalnoj razini. Komisija bi trebala biti voditelj obrade baze podataka EU-a, u skladu s Uredbom (EU) 2018/1725. Kako bi baza podataka EU-a bila posve funkcionalna od puštanja u rad, postupak njezina uspostavljanja trebao bi uključivati razvoj funkcionalnih specifikacija, što je zadaća Komisije, te neovisno revizorsko izvješće. Komisija bi pri obavljanju svojih zadaća voditelja obrade podataka u bazi podataka EU-a trebala uzeti u obzir rizike povezane s kibernetičkom sigurnosti. Kako bi se maksimalno povećale dostupnost i upotreba baze podataka EU-a u javnosti, baza podataka EU-a, uključujući podatke koji su u njoj dostupni, trebala bi ispunjavati zahtjeve iz Direktive (EU) 2019/882.
- (132) Kod određenih UI sustava namijenjenih interakciji s fizičkim osobama ili generiranju sadržaja mogu postojati posebni rizici u pogledu lažnog predstavljanja ili obmanjivanja, bez obzira na to smatraju li se visokorizičnima. Korištenje tih sustava stoga bi u određenim okolnostima trebalo podlijevati posebnim obvezama u pogledu transparentnosti, ne dovodeći u pitanje zahtjeve i obveze za visokorizične UI sustave, i ciljanim iznimkama kako bi se uzela u obzir posebna potreba kaznenog progona. Osobito bi fizičke osobe trebalo obavijestiti o tome da su u interakciji s UI sustavom, osim ako je to očito sa stajališta razmjerno dobro informirane, pronicljive i oprezne fizičke osobe, uzimajući u obzir okolnosti i kontekst upotrebe. Pri provedbi te obveze trebalo bi uzeti u obzir karakteristike fizičkih osoba koje pripadaju skupinama ranjivih osoba zbog svoje dobi ili invaliditeta u mjeri u kojoj je UI sustav namijenjen i interakciji s tim skupinama. Nadalje, fizičke osobe trebalo bi obavijestiti kada su izložene UI sustavima koji obradom njihovih biometrijskih podataka mogu identificirati emocije, izvoditi zaključke o njihovim emocijama ili namjerama ili te osobe razvrstati u određene kategorije. Te se određene kategorije mogu odnositi na aspekte kao što su spol, dob, boja kose, boja očiju, tetovaže, osobna obilježja, etničko podrijetlo, osobne preferencije i interesi. Takve informacije i obavijesti trebale bi se davati u oblicima koji su pristupačni osobama s invaliditetom.

- (133) Različiti UI sustavi mogu generirati velike količine sintetičkog sadržaja koji ljudima postaje sve teže razlikovati od autentičnog sadržaja koji je stvorio čovjek. Široka dostupnost i sve veće sposobnosti tih sustava znatno utječu na integritet informacijskog ekosustava i povjerenje u njega, pri čemu dovode do novih rizika od široko rasprostranjenih dezinformacija i manipulacije, prijevara, lažnog predstavljanja i obmanjivanja potrošača. S obzirom na te učinke, brz tehnološki razvoj i potrebu za novim metodama i tehnikama za praćenje podrijetla informacija, primjereno je od dobavljača tih sustava zahtijevati da ugrade tehnička rješenja koja omogućuju označavanje u strojno čitljivom formatu i prepoznavanje toga da je izlazni rezultat generirao ili je njime manipulirao UI sustav, a ne čovjek. Takve tehnike i metode trebale bi biti dovoljno pouzdane, interoperabilne, učinkovite i pouzdane u mjeri u kojoj je to tehnički izvedivo, uzimajući u obzir raspoložive tehnike ili kombinaciju takvih tehnika, kao što su vođeni žigovi, identifikacija metapodataka, kriptografske metode za dokazivanje podrijetla i autentičnosti sadržaja, metode evidentiranja, otisci prstiju ili druge tehnike, ovisno o slučaju. Pri provedbi te obveze dobavljači bi trebali uzeti u obzir i posebnosti i ograničenja različitih vrsta sadržaja te relevantna tehnološka i tržišna kretanja u tom području, kako se odražavaju u općepriznatim najnovijim dostignućima. Takve tehnike i metode mogu se primijeniti na razini UI sustava ili na razini UI modela, uključujući UI modele opće namjene koji generiraju sadržaj, čime se dobavljaču UI sustava niže u lancu olakšava ispunjavanje te obveze. Kako bi i dalje bila razmjerna, primjereno je predvidjeti da ta obveza označavanja ne bi trebala obuhvaćati UI sustave koji prvenstveno imaju pomoćnu funkciju za standardno uređivanje ili UI sustave koji bitno ne mijenjaju ulazne podatke koje pruža subjekt koji uvodi sustav ili njihovu semantiku.
- (134) Uz tehnička rješenja koja primjenjuju dobavljači sustava, subjekti koji uvode UI sustav, koji upotrebljavaju UI sustav za generiranje slikovnog sadržaja, audiosadržaja ili videosadržaja u kojem postoji znatna sličnost s postojećim osobama, predmetima, mjestima, subjektima ili događajima i koji bi se nekome lažno činio vjerodostojnim ili istinitim (uvjerljiv krivotvoreni sadržaj, eng. *deep fakes*) te za manipuliranje takvim sadržajem, također bi trebali jasno istaknuti da je sadržaj umjetno stvoren ili da je njime manipulirano označavanjem izlaznih rezultata umjetne inteligencije i navođenjem njegova umjetnog podrijetla. Usklađenost s tom obvezom transparentnosti ne bi se trebala tumačiti niti kao da upućuje na to da se korištenjem UI sustava ili njegovih izlaznih rezultata ugrožava pravo na slobodu izražavanja i pravo na slobodu umjetnosti i znanosti koja su zajamčena Poveljom, posebno ako je sadržaj očito dio kreativnog, satiričkog, umjetničkog, fiktivnog ili analognog djela ili programa, podložno odgovarajućim zaštitnim mjerama za prava i slobode trećih strana. U tim je slučajevima obveza transparentnosti za uvjerljiv krivotvoreni sadržaj utvrđena u ovoj Uredbi ograničena na otkrivanje postojanja takvog generiranog ili manipuliranog sadržaja na odgovarajući način kojim se ne ometa prikazivanje djela ili uživanje u njemu, uključujući njegovo uobičajeno iskorištavanje i upotrebu, uz istodobno održavanje korisnosti i kvalitete djela. Osim toga, primjereno je predvidjeti sličnu obvezu otkrivanja u odnosu na tekst stvoren ili manipuliran umjetnom inteligencijom u mjeri u kojoj se objavljuje u svrhu informiranja javnosti o pitanjima od javnog interesa, osim ako je sadržaj stvoren umjetnom inteligencijom prošao proces preispitivanja koje provodi čovjek ili uredničku kontrolu i ako fizička ili pravna osoba snosi uredničku odgovornost za objavu sadržaja.
- (135) Ne dovodeći u pitanje obveznu prirodu i potpunu primjenjivost obveza u pogledu transparentnosti, Komisija može poticati i olakšavati izradu kodeksa prakse na razini Unije kako bi se olakšala djelotvorna provedba obveza u pogledu otkrivanja i označavanja umjetno stvorenog ili manipuliranog sadržaja, među ostalim i kako bi se poduprla praktična rješenja za osiguravanje dostupnosti, prema potrebi, mehanizama za otkrivanje i olakšavanje suradnje s drugim akterima duž vrijednosnog lanca, širenje sadržaja ili provjera njegove autentičnosti i podrijetla kako bi se javnosti omogućilo djelotvorno prepoznavanje sadržaja stvorenog umjetnom inteligencijom.
- (136) Obveze propisane u ovoj Uredbi za dobavljače i za subjekte koji uvode određene UI sustave kako bi se omogućilo prepoznavanje i otkrivanje umjetno stvorenih ili manipuliranih izlaznih rezultata tih sustava posebno su relevantne za olakšavanje djelotvorne provedbe Uredbe (EU) 2022/2065. To se osobito odnosi na obveze pružatelja vrlo velikih internetskih platformi ili vrlo velikih internetskih tražilica da utvrde i ublaže sistemske rizike koji mogu proizaći iz širenja umjetno stvorenog ili manipuliranog sadržaja, posebno rizik od stvarnih ili predvidljivih negativnih učinaka na demokratske procese, građanski diskurs i izborne procese, među ostalim dezinformiranjem. Zahtjevom u pogledu označavanja sadržaja koji generiraju UI sustavi na temelju ove Uredbe ne dovodi se u pitanje obveza iz članka 16. stavka 6. Uredbe (EU) 2022/2065 prema kojoj pružatelji usluga smještaja informacija na poslužitelju moraju obrađivati prijave nezakonitog sadržaja zaprimljene na temelju članka 16. stavka 1. te uredbe i on ne bi trebao utjecati na procjenu i odluku o nezakonitosti određenog sadržaja. Ta bi se ocjena trebala provesti isključivo s obzirom na pravila kojima se uređuje zakonitost sadržaja.

- (137) Sukladnost s obvezama u pogledu transparentnosti za UI sustave obuhvaćene ovom Uredbom ne bi se trebala tumačiti kao da upućuje na to da je upotreba UI sustava ili njegovih izlaznih rezultata zakonita na temelju ove Uredbe ili drugog prava Unije i prava država članica i njome se ne bi trebale dovoditi u pitanje druge obveze u pogledu transparentnosti za subjekte koji uvode UI sustave koje su utvrđene u pravu Unije ili u nacionalnom pravu.
- (138) Umjetna inteligencija skup je tehnologija koje se vrlo brzo razvijaju, što zahtijeva regulatorni nadzor i siguran i kontroliran prostor za eksperimentiranje, pri čemu se osigurava da se inovacije razvijaju na odgovoran način te da se integriraju odgovarajuće zaštitne mjere i mjere za ublažavanje rizika. Kako bi se osigurao pravni okvir kojim se promiču inovacije te koji je spreman za buduće promjene i otporan na poremećaje, države članice trebale bi zajamčiti da njihova nacionalna nadležna tijela uspostave barem jedno regulatorno izolirano okruženje za umjetnu inteligenciju na nacionalnoj razini radi lakšeg razvoja i testiranja inovativnih UI sustava pod strogim regulatornim nadzorom prije stavljanja tih sustava na tržište ili u upotrebu. Države članice mogle bi ispuniti tu obvezu i sudjelovanjem u već postojećim regulatornim izoliranim okruženjima ili zajedničkom uspostavom izoliranog okruženja s jednim ili više nadležnih tijela država članica, u mjeri u kojoj se tim sudjelovanjem osigurava jednaka razina nacionalne pokrivenosti za države članice sudionice. Regulatorna izolirana okruženja za umjetnu inteligenciju mogla bi se uspostaviti u fizičkom, digitalnom ili hibridnom obliku te mogu uključivati fizičke i digitalne proizvode. Tijela nadležna za uspostavu regulatornih izoliranih okruženja za umjetnu inteligenciju trebala bi osigurati i da regulatorna izolirana okruženja imaju odgovarajuće resurse za njihovo funkcioniranje, uključujući financijske i ljudske resurse.
- (139) Ciljevi regulatornih izoliranih okruženja za umjetnu inteligenciju trebali bi biti poticanje inovacija u području umjetne inteligencije uspostavom kontroliranog okruženja za eksperimentiranje i testiranje u fazi razvoja i prije stavljanja na tržište kako bi se osigurala usklađenost inovativnih UI sustava s ovom Uredbom i drugim relevantnim pravom Unije i nacionalnim pravom. Nadalje, regulatornim izoliranim okruženjima za umjetnu inteligenciju trebalo bi nastojati povećati pravnu sigurnost za inovatore, poboljšati nadzor koji provode nadležna tijela i njihovo razumijevanje mogućnosti, novih rizika i učinaka upotrebe umjetne inteligencije, olakšati regulatorno učenje za nadležna tijela i poduzeća, među ostalim radi budućih prilagodbi pravnog okvira, poduprijeti suradnju i razmjenu primjera najbolje prakse s tijelima uključenima u regulatorno izolirano okruženje za umjetnu inteligenciju te ubrzati pristup tržištima, među ostalim uklanjanjem zapreka za MSP-ove, uključujući *start-up* poduzeća. Regulatorna izolirana okruženja za umjetnu inteligenciju trebala bi biti široko dostupna u cijeloj Uniji, a posebnu pozornost trebalo bi posvetiti njihovoj pristupačnosti za MSP-ove, uključujući *start-up* poduzeća. Sudjelovanje u regulatornom izoliranom okruženju za umjetnu inteligenciju trebalo bi biti usmjereno na pitanja koja uzrokuju pravnu nesigurnost za dobavljače i potencijalne dobavljače u pogledu inovacija, eksperimentiranja s umjetnom inteligencijom u Uniji i doprinosa regulatornom učenju utemeljenom na dokazima. Nadzor UI sustava u regulatornom izoliranom okruženju za umjetnu inteligenciju stoga bi trebao obuhvaćati njihov razvoj, treniranje, testiranje i validaciju prije stavljanja tih sustava na tržište ili u upotrebu, kao i pojam i pojavu znatne izmjene koja bi mogla zahtijevati novi postupak ocjenjivanja sukladnosti. Ako se tijekom razvoja i testiranja takvih UI sustava uoče znatni rizici, ti bi se rizici trebali smanjiti na primjeren način, a ako to nije moguće, treba se prekinuti postupak razvoja i testiranja sve dok se oni ne smanje. Nacionalna nadležna tijela koja uspostavljaju regulatorna izolirana okruženja za umjetnu inteligenciju trebala bi prema potrebi surađivati s drugim relevantnim tijelima, među ostalim s tijelima koja nadziru zaštitu temeljnih prava, i mogla bi omogućiti sudjelovanje drugih aktera iz ekosustava umjetne inteligencije, kao što su nacionalne ili europske organizacije za normizaciju, prijavljena tijela, objekti za testiranje i eksperimentiranje, laboratoriji za istraživanje i eksperimentiranje, europski centri za digitalne inovacije i relevantne organizacije dionika i organizacije civilnog društva. Radi ujednačene provedbe u cijeloj Uniji i ekonomije razmjera, primjereno je uspostaviti zajednička pravila za primjenu regulatornih izoliranih okruženja za umjetnu inteligenciju i okvir za suradnju relevantnih tijela uključenih u nadzor izoliranih okruženja. Regulatornim izoliranim okruženjima za umjetnu inteligenciju uspostavljenima na temelju ove Uredbe ne bi se trebalo dovoditi u pitanje drugo pravo kojim se omogućuje uspostava drugih izoliranih okruženja u cilju osiguravanja usklađenosti s pravom koje nije ova Uredba. Relevantna nadležna tijela zadužena za ta druga regulatorna izolirana okruženja trebala bi prema potrebi razmotriti prednosti upotrebe tih izoliranih okruženja i za potrebe osiguravanja usklađenosti UI sustava s ovom Uredbom. Slijedom dogovora između nacionalnih nadležnih tijela i sudionika u regulatornom izoliranom okruženju za umjetnu inteligenciju testiranje u stvarnim uvjetima može se također provoditi i nadzirati u okviru regulatornog izoliranog okruženja za umjetnu inteligenciju.
- (140) Ovom bi se Uredbom dobavljačima i potencijalnim dobavljačima u regulatornom izoliranom okruženju za umjetnu inteligenciju trebala osigurati pravna osnova za upotrebu osobnih podataka prikupljenih u druge svrhe za razvoj određenih UI sustava u javnom interesu u regulatornom izoliranom okruženju za umjetnu inteligenciju, samo pod određenim uvjetima, u skladu s člankom 6. stavkom 4. i člankom 9. stavkom 2. točkom (g) Uredbe (EU) 2016/679 i člancima 5., 6. i 10. Uredbe (EU) 2018/1725 te ne dovodeći u pitanje članak 4. stavak 2. i članak 10. Direktive (EU) 2016/680. I dalje se primjenjuju sve ostale obveze voditelja obrade podataka i prava ispitanika na temelju uredbi (EU) 2016/679 i (EU) 2018/1725 te Direktive (EU) 2016/680. Ovom Uredbom osobito se ne bi trebala osigurati pravna osnova u smislu članka 22. stavka 2. točke (b) Uredbe (EU) 2016/679 i članka 24. stavka 2. točke (b) Uredbe (EU) 2018/1725. Dobavljači i potencijalni dobavljači u regulatornom izoliranom okruženju za umjetnu inteligenciju

trebali bi osigurati odgovarajuće zaštitne mjere i surađivati s nadležnim tijelima, među ostalim tako da slijede njihove smjernice i postupaju žurno i u dobroj vjeri kako bi se na primjeren način ublažili svi utvrđeni znatni rizici za sigurnost, zdravlje i temeljna prava koji mogu nastati tijekom razvoja, testiranja i eksperimentiranja u tom izoliranom okruženju.

- (141) Kako bi se ubrzao proces razvoja i stavljanja na tržište visokorizičnih UI sustava navedenih u prilogu ovoj Uredbi, važno je da se dobavljači ili potencijalni dobavljači takvih sustava mogu služiti posebnim režimom za testiranje tih sustava u stvarnim uvjetima, bez sudjelovanja u regulatornom izoliranom okruženju za umjetnu inteligenciju. Međutim, u takvim slučajevima, uzimajući u obzir moguće posljedice takvog testiranja na pojedince, trebalo bi osigurati da se ovom Uredbom uvedu odgovarajuća i dostatna jamstva i uvjeti za dobavljače ili potencijalne dobavljače. Takva bi jamstva među ostalim trebala uključivati traženje informiranog pristanka fizičke osobe za sudjelovanje u testiranju u stvarnim uvjetima, uz iznimku tijela kaznenog progona ako bi traženje informiranog pristanka spriječilo testiranje UI sustava. Pristanak ispitanika za sudjelovanje u takvom testiranju na temelju ove Uredbe razlikuje se od privole ispitanika za obradu njihovih osobnih podataka na temelju relevantnog zakonodavstva o zaštiti podataka i njime se privola za obradu osobnih podataka ne dovodi u pitanje. Također je važno smanjiti rizike i omogućiti nadzor od strane nadležnih tijela te stoga zahtijevati od potencijalnih dobavljača da imaju plan testiranja u stvarnim uvjetima koji se podnosi nadležnom tijelu za nadzor tržišta, da registriiraju testiranje u posebnim odjeljcima u bazi podataka EU-a podložno određenim ograničenim iznimkama, da utvrde ograničenja u pogledu razdoblja u kojem se testiranje može provesti i da zahtijevaju dodatne zaštitne mjere za osobe koje pripadaju određenim skupinama ranjivih osoba, kao i pisani sporazum kojim se utvrđuju uloge i odgovornosti potencijalnih dobavljača i subjekata koji uvode sustav te djelotvoran nadzor koji provodi nadležno osoblje uključeno u testiranje u stvarnim uvjetima. Nadalje, primjereno je predvidjeti dodatne zaštitne mjere kako bi se osiguralo da se predviđanja, preporuke ili odluke UI sustava mogu djelotvorno poništiti i zanemariti te da se osobni podaci zaštite i brišu ako ispitanici povuku svoj pristanak za sudjelovanje u testiranju, ne dovodeći u pitanje prava koja imaju kao ispitanici u skladu s pravom Unije o zaštiti podataka. Kad je riječ o prijenosu podataka, također je primjereno predvidjeti da bi se podaci prikupljeni i obrađeni u svrhu testiranja u stvarnim uvjetima trebali prenositi trećim zemljama samo ako se provode odgovarajuće i primjenjive zaštitne mjere na temelju prava Unije, posebno u skladu s osnovama za prijenos osobnih podataka na temelju prava Unije o zaštiti podataka, dok su za neosobne podatke uspostavljene odgovarajuće zaštitne mjere u skladu s pravom Unije, kao što su uredbe (EU) 2022/868⁽⁴²⁾ i (EU) 2023/2854⁽⁴³⁾ Europskog parlamenta i Vijeća.

- (142) Kako bi se osiguralo da umjetna inteligencija dovede do društveno i okolišno korisnih ishoda, države članice potiču se da podupiru i promiču istraživanje i razvoj UI rješenja kojima se podupiru ishodi korisni za društvo i okoliš, kao što su rješenja koja se temelje na umjetnoj inteligenciji za povećanje pristupačnosti za osobe s invaliditetom, uklanjanje socioekonomskih nejednakosti ili postizanje okolišnih ciljeva dodjelom dostatnih sredstava, uključujući javno financiranje i financiranje sredstvima Unije, te, prema potrebi i pod uvjetom da su ispunjeni kriteriji prihvatljivosti i odabira, posebno uzimajući u obzir projekte kojima se nastoje ostvariti takvi ciljevi. Takvi bi se projekti trebali temeljiti na načelu interdisciplinarnе suradnje među razvojnim programerima umjetne inteligencije, stručnjacima za nejednakost i nediskriminaciju, pristupačnost te potrošačka, okolišna i digitalna prava te akademskom zajednicom.

- (143) Kako bi se promicale i štitile inovacije, posebno je važno uzeti u obzir interese MSP-ova, među ostalima i *start-up* poduzeća, koji su dobavljači UI sustava ili subjekti koji ih uvode. U tom cilju bi države članice trebale osmisliti inicijative usmjerene na te operatore, među ostalim u pogledu podizanja svijesti i informiranja. Države članice trebale bi MSP-ovima, među ostalim i *start-up* poduzećima, koji imaju registrirano sjedište ili podružnicu u Uniji, osiguravati prioritetni pristup regulatornim izoliranim okruženjima za umjetnu inteligenciju, pod uvjetom da ispunjavaju uvjete prihvatljivosti i kriterije za odabir te da drugim dobavljačima i potencijalnim dobavljačima ne onemogućuju pristup izoliranim okruženjima pod uvjetom da su ispunjeni isti uvjeti i kriteriji. Države članice trebale bi se koristiti postojećim kanalima i, prema potrebi, uspostaviti nove namjenske kanale za komunikaciju s MSP-ovima, među ostalim i *start-up* poduzećima, subjektima koji uvode sustav, drugim inovatorima i, prema potrebi, lokalnim tijelima javne vlasti, radi podupiranja MSP-ova tijekom cijelog njihova razvoja pružanjem smjernica i odgovaranjem na upite o provedbi ove Uredbe. Prema potrebi, ti kanali trebali bi međusobno surađivati kako bi se stvorila sinergija i osigurala homogenost smjernica za MSP-ove, uključujući *start-up* poduzeća, i subjekte koji uvode sustav. Osim toga, države članice trebale bi olakšavati sudjelovanje MSP-ova i drugih relevantnih dionika u procesima razvoja

⁽⁴²⁾ Uredba (EU) 2022/868 Europskog parlamenta i Vijeća od 30. svibnja 2022. o europskom upravljanju podacima i izmjeni Uredbe (EU) 2018/1724 (Akt o upravljanju podacima) (SL L 152, 3.6.2022., str. 1.).

⁽⁴³⁾ Uredba (EU) 2023/2854 Europskog parlamenta i Vijeća od 13. prosinca 2023. o usklađenim pravilima za pravedan pristup podacima i njihovu uporabu i o izmjeni Uredbe (EU) 2017/2394 i Direktive (EU) 2020/1828 (Akt o podacima) (SL L, 2023/2854, 22.12.2023., ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).

normizacije. Usto, prijavljena tijela trebala bi uzeti u obzir posebne interese i potrebe dobavljača koji su MSP-ova, među ostalima i onih koji su *start-up* poduzeća, kad određuju naknade za ocjenjivanje sukladnosti. Komisija bi s pomoću transparentnog savjetovanja trebala redovito ocjenjivati troškove certifikacije i usklađivanja za MSP-ove, među ostalima i za *start-up* poduzeća, te surađivati s državama članicama u cilju smanjenja takvih troškova. Na primjer, dobavljači i drugi operateri, posebno oni manji, mogu imati znatne troškove prijevoda obvezne dokumentacije i komunikacije s tijelima. Države članice trebale bi možda osigurati da jedan od jezika koji odrede i prihvaćaju za relevantnu dokumentaciju dobavljača i komunikaciju s operaterima bude jedan od jezika koji u velikoj mjeri razumije najveći mogući broj prekograničnih subjekata koji uvode sustav. Kako bi se odgovorilo na posebne potrebe MSP-ova, uključujući *start-up* poduzeća, Komisija bi na zahtjev Vijeća za umjetnu inteligenciju trebala osigurati standardizirane predloške za područja obuhvaćena ovom Uredbom. Osim toga, Komisija bi trebala dopuniti napore država članica osiguravanjem jedinstvene informacijske platforme koja pruža informacije o ovoj Uredbi jednostavne za upotrebu za sve dobavljače i subjekte koji uvode sustav, organiziranjem odgovarajućih komunikacijskih kampanja za podizanje svijesti o obvezama koje proizlaze iz ove Uredbe te evaluacijom i promicanjem konvergencije primjera najbolje prakse u postupcima javne nabave u vezi s UI sustavima. Srednja poduzeća koja su do nedavno ispunjavala uvjete za mala poduzeća u smislu Priloga Preporuci Komisije 2003/361/EZ⁽⁴⁴⁾ trebala bi imati pristup tim mjerama potpore jer tim novim srednjim poduzećima ponekad možda nedostaju pravni resursi i osposobljavanje potrebni za osiguravanje pravilnog razumijevanja i usklađenosti s ovom Uredbom.

- (144) Kako bi se promicale i zaštitile inovacije, ostvarivanju ciljeva ove Uredbe trebalo bi, prema potrebi, doprinositi putem platforme za umjetnu inteligenciju na zahtjev i svih relevantnih programa i projekata za financiranje sredstvima Unije, poput programa Digitalna Europa i Obzor Europa, koje provode Komisija i države članice na razini Unije ili nacionalnoj razini.
- (145) Kako bi se rizici za provedbu koji proizlaze iz nedostatka znanja i iskustva na tržištu sveli na najmanju moguću mjeru i kako bi se dobavljačima, posebno MSP-ovima, uključujući *start-up* poduzeća, i prijavljenim tijelima olakšalo ispunjavanje obveza iz ove Uredbe, provedbi ove Uredbe trebalo bi doprinositi putem platforme za umjetnu inteligenciju na zahtjev, europskih centara za digitalne inovacije te centara za testiranje i eksperimentiranje koje uspostavljaju Komisija i države članice na razini Unije ili nacionalnoj razini. U okviru svoje misije i područja nadležnosti, platforma za umjetnu inteligenciju na zahtjev, europski centri za digitalne inovacije te centri za testiranje i eksperimentiranje mogu posebno pružati tehničku i znanstvenu potporu dobavljačima i prijavljenim tijelima.
- (146) Nadalje, s obzirom na vrlo malenu veličinu pojedinih operatera i kako bi se osigurala proporcionalnost u pogledu troškova inovacija, primjereno je omogućiti mikropoduzećima da ispune jednu od najskupljih obveza, a to je uspostava sustava upravljanja kvalitetom, na pojednostavljen način, čime bi se smanjili administrativno opterećenje i troškovi za ta poduzeća, a bez utjecaja na razinu zaštite i potrebu za usklađivanjem sa zahtjevima za visokorizične UI sustave. Komisija bi trebala izraditi smjernice za određivanje elemenata sustava upravljanja kvalitetom koje mikropoduzeća moraju ispuniti na taj pojednostavljen način.
- (147) Primjereno je da Komisija olakša, u mjeri u kojoj je to moguće, pristup centrima za testiranje i eksperimentiranje tijelima, skupinama ili laboratorijima uspostavljenima ili akreditiranim na temelju bilo kojeg dijela zakonodavstva Unije o usklađivanju, a koji obavljaju zadaće u kontekstu postupaka ocjenjivanja sukladnosti proizvoda ili uređaja obuhvaćenih tim zakonodavstvom Unije o usklađivanju. To se posebno odnosi na stručne skupine, stručne laboratorije i referentne laboratorije u području medicinskih proizvoda na temelju uredaba (EU) 2017/745 i (EU) 2017/746.
- (148) Ovom bi se Uredbom trebao uspostaviti okvir upravljanja koji omogućuje i koordinaciju primjene ove Uredbe na nacionalnoj razini i potporu primjeni ove Uredbe na nacionalnoj razini, kao i izgradnju kapaciteta na razini Unije i integraciju dionika u području umjetne inteligencije. Za djelotvornu provedbu i izvršavanje ove Uredbe potreban je okvir upravljanja koji omogućuje koordinaciju i prikupljanje središnjeg stručnog znanja na razini Unije. Ured za umjetnu inteligenciju osnovan je Odlukom Komisije⁽⁴⁵⁾, a njegova je zadaća razvoj stručnog znanja i sposobnosti Unije u području umjetne inteligencije te doprinos provedbi prava Unije o umjetnoj inteligenciji. Države članice trebale bi olakšati zadaće Ureda za umjetnu inteligenciju kako bi se podržao razvoj stručnog znanja i sposobnosti Unije na razini Unije te ojačalo funkcioniranje jedinstvenog digitalnog tržišta. Nadalje, trebalo bi osnovati Vijeće za umjetnu inteligenciju koje se sastoji od predstavnika država članica, znanstveno povjerenstvo za integraciju znanstvene zajednice i savjetodavni forum za doprinos dionika provedbi ove Uredbe, na razini Unije i na nacionalnoj

⁽⁴⁴⁾ Preporuka Komisije od 6. svibnja 2003. o definiciji mikro, malih i srednjih poduzeća (SL L 124, 20.5.2003., str. 36.).

⁽⁴⁵⁾ Odluka Komisije od 24. siječnja 2024. o osnivanju Europskog ureda za umjetnu inteligenciju C(2024) 390.

razini. Razvoj stručnog znanja i sposobnosti Unije trebao bi uključivati i iskorištavanje postojećih resursa i stručnog znanja, posebno putem sinergije sa strukturama uspostavljenima u kontekstu provedbe drugog prava i sinergije s povezanim inicijativama na razini Unije, kao što su Zajedničko poduzeće EuroHPC i objekti za testiranje i eksperimentiranje umjetne inteligencije u okviru programa Digitalna Europa.

- (149) Kako bi se olakšala nesmetana, djelotvorna i usklađena provedba ove Uredbe, trebalo bi osnovati Vijeće za umjetnu inteligenciju. U Vijeću za umjetnu inteligenciju trebali bi se odražavati različiti interesi ekosustava umjetne inteligencije, a trebao bi biti sastavljen od predstavnika država članica. Vijeće za umjetnu inteligenciju trebalo bi biti odgovorno za niz savjetodavnih zadaća, uključujući davanje mišljenja, preporuka i savjeta ili doprinošenje smjernicama o pitanjima povezanim s provedbom ove Uredbe, među ostalim pitanjima izvršenja, tehničkim specifikacijama ili postojećim normama povezanim sa zahtjevima ove Uredbe, te za davanje savjeta Komisiji i državama članicama te njihovim nacionalnim nadležnim tijelima u vezi sa specifičnim pitanjima povezanim s umjetnom inteligencijom. Kako bi se državama članicama pružila određena fleksibilnost u vezi s imenovanjem njihovih predstavnika u Vijeće za umjetnu inteligenciju, ti predstavnici mogu biti sve osobe koje pripadaju javnim subjektima i koje bi trebale imati odgovarajuće nadležnosti i ovlasti za olakšavanje koordinacije na nacionalnoj razini i doprinošenje ostvarivanju zadaća Vijeća za umjetnu inteligenciju. Vijeće za umjetnu inteligenciju trebalo bi osnovati dvije stalne podskupine kako bi osigurao platformu za suradnju i razmjenu između tijela za nadzor tržišta i tijela koja provode prijavljivanje o pitanjima koja se odnose na nadzor tržišta odnosno na prijavljena tijela. Stalna podskupina za nadzor tržišta trebala bi djelovati kao skupina za administrativnu suradnju (ADCO) za ovu Uredbu u smislu članka 30. Uredbe (EU) 2019/1020. U skladu s člankom 33. te uredbe Komisija bi trebala podupirati aktivnosti stalne podskupine za nadzor tržišta provođenjem evaluacija ili studija tržišta, osobito u cilju utvrđivanja aspekata ove Uredbe koji zahtijevaju posebnu i hitnu koordinaciju među tijelima za nadzor tržišta. Vijeće za umjetnu inteligenciju prema potrebi može osnovati druge stalne ili privremene podskupine za razmatranje specifičnih pitanja. Vijeće za umjetnu inteligenciju također bi prema potrebi trebalo surađivati s relevantnim tijelima Unije, stručnim skupinama i mrežama koje djeluju u kontekstu relevantnog prava Unije, uključujući posebno one koje djeluju na temelju relevantnog prava Unije o podacima, digitalnim proizvodima i uslugama.
- (150) Kako bi se osiguralo sudjelovanje dionika u provedbi i primjeni ove Uredbe, trebalo bi uspostaviti savjetodavni forum radi savjetovanja Vijeća za umjetnu inteligenciju i Komisije i pružanja tehničkog stručnog znanja Vijeću za umjetnu inteligenciju i Komisiji. Kako bi se osigurala raznolika i uravnotežena zastupljenost dionika s komercijalnim i nekomercijalnim interesima te, unutar kategorije komercijalnih interesa, u pogledu MSP-ova i drugih poduzeća, savjetodavni forum trebao bi obuhvaćati, među ostalim, industriju, *start-up* poduzeća, MSP-ove, akademsku zajednicu, civilno društvo, uključujući socijalne partnere, kao i Agenciju za temeljna prava, ENISA-u, Europski odbor za normizaciju (CEN), Europski odbor za elektrotehničku normizaciju (CENELEC) i Europski institut za telekomunikacijske norme (ETSI).
- (151) Kako bi se poduprli provedba i izvršavanje ove Uredbe, osobito aktivnosti praćenja koje provodi Ured za umjetnu inteligenciju u pogledu UI modelâ opće namjene, trebalo bi osnovati znanstveno povjerenstvo neovisnih stručnjaka. Neovisni stručnjaci koji čine znanstveno povjerenstvo trebali bi se birati na temelju najnovijeg znanstvenog ili tehničkog stručnog znanja u području umjetne inteligencije te bi trebali obavljati svoje zadaće nepristrano i objektivno te osigurati povjerljivost informacija i podataka dobivenih pri obavljanju svojih zadaća i aktivnosti. Kako bi se omogućilo jačanje nacionalnih kapaciteta potrebnih za djelotvorno izvršavanje ove Uredbe, države članice trebale bi za svoje aktivnosti izvršavanja moći zatražiti potporu skupine stručnjaka koji čine znanstveno povjerenstvo.
- (152) Kako bi se poduprlo odgovarajuće izvršavanje u vezi s UI sustavima i ojačali kapaciteti država članica, trebalo bi uspostaviti potporne strukture Unije za testiranje umjetne inteligencije i staviti ih na raspolaganje državama članicama.
- (153) Države članice imaju ključnu ulogu u primjeni i izvršavanju ove Uredbe. Svaka bi država članica stoga trebala imenovati barem jedno tijelo koje provodi prijavljivanje i barem jedno tijelo za nadzor tržišta kao nacionalna nadležna tijela za potrebe nadziranja primjene i provedbe ove Uredbe. Države članice mogu odlučiti imenovati bilo koju vrstu javnog subjekta za obavljanje zadaća nacionalnih nadležnih tijela u smislu ove Uredbe, u skladu sa svojim posebnim nacionalnim organizacijskim karakteristikama i potrebama. Kako bi se povećala učinkovitost organizacije u državama članicama i uspostavila jedinstvena kontaktna točka za javne i druge partnere na razini država članica i na razini Unije, svaka bi država članica trebala imenovati tijelo za nadzor tržišta koje će djelovati kao jedinstvena kontaktna točka.

- (154) Ta nacionalna nadležna tijela trebala bi izvršavati svoje ovlasti neovisno, objektivno i nepristrano kako bi zaštitila načela objektivnosti svojih aktivnosti i zadaća te osigurala primjenu i provedbu ove Uredbe. Članovi tih tijela trebali bi se suzdržati od svakog djelovanja koje nije u skladu s njihovim dužnostima te bi trebali podlijeđati pravilima o povjerljivosti na temelju ove Uredbe.
- (155) Kako bi se osiguralo da dobavljači visokorizičnih UI sustava mogu uzeti u obzir iskustvo stečeno korištenjem visokorizičnih UI sustava za poboljšanje svojih sustava te za proces dizajniranja i razvoja ili da mogu pravodobno poduzeti korektivne mjere, svi bi dobavljači trebali uspostaviti sustav praćenja nakon stavljanja na tržište. Ako je to relevantno, praćenje nakon stavljanja na tržište trebalo bi obuhvaćati analizu interakcije s drugim UI sustavima, uključujući druge uređaje i softver. Praćenje nakon stavljanja na tržište ne bi trebalo obuhvaćati osjetljive operativne podatke subjekata koji uvode sustav koji su tijela kaznenog progona. Taj je sustav ključan i za učinkovitije i pravodobnije poduzimanje mjera povezanih s mogućim rizicima od UI sustava koji „uče” i nakon što su stavljeni na tržište ili u upotrebu. U tom bi kontekstu od dobavljača trebalo također zahtijevati da uspostave sustav za prijavljivanje relevantnim tijelima svih ozbiljnih incidenata koji su posljedica korištenja njihovih UI sustava, odnosno incidenta ili neispravnosti koji dovode do smrti ili teške štete za zdravlje, ozbiljnih i nepovratnih poremećaja u upravljanju kritičnom infrastrukturom i njezinu radu, povreda obveza na temelju prava Unije namijenjenih zaštiti temeljnih prava ili teške štete za imovinu ili okoliš.
- (156) Kako bi se osiguralo odgovarajuće i djelotvorno izvršavanje zahtjeva i obveza utvrđenih u ovoj Uredbi, koja je zakonodavstvo Unije o usklađivanju, u cijelosti bi se trebao primjenjivati sustav nadzora tržišta i sukladnosti proizvoda uspostavljen Uredbom (EU) 2019/1020. Tijela za nadzor tržišta imenovana na temelju ove Uredbe trebala bi imati sve ovlasti izvršavanja utvrđene u ovoj Uredbi i u Uredbi (EU) 2019/1020 i svoje bi ovlasti i dužnosti trebala izvršavati neovisno, objektivno i nepristrano. Iako većina UI sustava ne podliježe posebnim zahtjevima i obvezama na temelju ove Uredbe, tijela za nadzor tržišta mogu poduzeti mjere u vezi sa svim UI sustavima kada oni predstavljaju rizik u skladu s ovom Uredbom. Zbog specifične prirode institucija, agencija i tijela Unije obuhvaćenih područjem primjene ove Uredbe primjereno je za njih imenovati Europskog nadzornika za zaštitu podataka tijelom nadležnim za nadzor tržišta. Time se ne bi trebalo dovoditi u pitanje imenovanje nacionalnih nadležnih tijela koje provode države članice. Aktivnosti nadzora tržišta ne bi trebale utjecati na sposobnost nadziranih subjekata da neovisno obavljaju svoje zadaće kada se takva neovisnost zahtijeva pravom Unije.
- (157) Ovom se Uredbom ne dovode u pitanje nadležnosti, zadaće, ovlasti i neovisnost relevantnih nacionalnih tijela javne vlasti ili javnih tijela koja nadziru primjenu prava Unije o zaštiti temeljnih prava, uključujući tijela za ravnopravnost i tijela za zaštitu podataka. Ako je to potrebno za njihov mandat, ta nacionalna tijela javne vlasti ili javna tijela trebala bi također imati pristup svojoj dokumentaciji izrađenoj na temelju ove Uredbe. Trebalo bi utvrditi poseban zaštitni postupak kako bi se osiguralo adekvatno i pravodobno izvršavanje u pogledu UI sustava koji predstavljaju rizik za zdravlje, sigurnost i temeljna prava. Postupak za takve UI sustave koji predstavljaju rizik trebao bi se primjenjivati na visokorizične UI sustave koji predstavljaju rizik, zabranjene sustave koji su stavljeni na tržište, stavljeni u upotrebu ili se upotrebljavaju protivno odredbama o zabranjenim praksama iz ove Uredbe i na UI sustave koji su stavljeni na raspolaganje protivno odredbama o zahtjevima u pogledu transparentnosti iz ove Uredbe i koji predstavljaju rizik.
- (158) Pravo Unije o financijskim uslugama uključuje pravila i zahtjeve o unutarnjem upravljanju i upravljanju rizikom koji se primjenjuju na regulirane financijske institucije pri pružanju tih usluga, među ostalim kad upotrebljavaju UI sustave. Kako bi se osigurala dosljedna primjena i izvršavanje obveza iz ove Uredbe te relevantnih pravila i zahtjeva iz pravnih akata Unije o financijskim uslugama, nadležna tijela odgovorna za nadzor i izvršavanje tih pravnih akata, posebno nadležna tijela kako su definirana u Uredbi (EU) br. 575/2013 Europskog parlamenta i Vijeća ⁽⁴⁶⁾ i direktivama 2008/48/EZ ⁽⁴⁷⁾, 2009/138/EZ ⁽⁴⁸⁾, 2013/36/EU ⁽⁴⁹⁾, 2014/17/EU ⁽⁵⁰⁾ i (EU) 2016/97 ⁽⁵¹⁾ Europskog

⁽⁴⁶⁾ Uredba (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni Uredbe (EU) br. 648/2012 (SL L 176, 27.6.2013., str. 1.).

⁽⁴⁷⁾ Direktiva 2008/48/EZ Europskog parlamenta i Vijeća od 23. travnja 2008. o ugovorima o potrošačkim kreditima i stavljanju izvan snage Direktive Vijeća 87/102/EEZ (SL L 133, 22.5.2008., str. 66.).

⁽⁴⁸⁾ Direktiva 2009/138/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja (Solventnost II) (SL L 335, 17.12.2009., str. 1.).

⁽⁴⁹⁾ Direktiva 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama i investicijskim društvima, izmjeni Direktive 2002/87/EZ te stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ (SL L 176, 27.6.2013., str. 338.).

⁽⁵⁰⁾ Direktiva 2014/17/EU Europskog parlamenta i Vijeća od 4. veljače 2014. o ugovorima o potrošačkim kreditima koji se odnose na stambene nekretnine i o izmjeni direktiva 2008/48/EZ i 2013/36/EU i Uredbe (EU) br. 1093/2010 (SL L 60, 28.2.2014., str. 34.).

⁽⁵¹⁾ Direktiva (EU) 2016/97 Europskog parlamenta i Vijeća od 20. siječnja 2016. o distribuciji osiguranja (SL L 26, 2.2.2016., str. 19.).

parlamenta i Vijeća, trebala bi biti imenovana, u okviru vlastitih nadležnosti, nadležnim tijelima za potrebe nadziranja provedbe ove Uredbe, među ostalim i za aktivnosti nadzora tržišta, kad je riječ o UI sustavima koje pružaju ili upotrebljavaju financijske institucije koje su regulirane i pod nadzorom, osim ako države članice odluče za obavljanje tih zadaća nadzora tržišta imenovati drugo tijelo. Ta bi nadležna tijela trebala imati sve ovlasti na temelju ove Uredbe i Uredbe (EU) 2019/1020 za izvršavanje zahtjeva i obveza iz ove Uredbe, uključujući ovlasti za provođenje *ex post* aktivnosti nadzora tržišta koje se prema potrebi mogu integrirati u njihove postojeće nadzorne mehanizme i postupke na temelju relevantnog prava Unije o financijskim uslugama. Primjereno je predvidjeti da bi, kada djeluju kao tijela za nadzor tržišta na temelju ove Uredbe, nacionalna tijela odgovorna za nadziranje kreditnih institucija reguliranih Direktivom 2013/36/EU, koja sudjeluju u jedinstvenom nadzornom mehanizmu uspostavljenom Uredbom Vijeća (EU) br. 1024/2013 ⁽⁵²⁾, trebala bez odgode izvijestiti Europsku središnju banku o svim informacijama utvrđenima tijekom njihovih aktivnosti nadzora tržišta koje bi mogle biti od interesa za zadaće bonitetnog nadzora Europske središnje banke navedene u toj uredbi. Kako bi se dodatno poboljšala usklađenost između ove Uredbe i pravila koja se primjenjuju na kreditne institucije regulirane Direktivom 2013/36/EU, također je primjereno integrirati neke od postupovnih obveza dobavljača povezanih s upravljanjem rizikom, praćenjem nakon stavljanja na tržište i vođenjem dokumentacije u postojeće obveze i postupke na temelju Direktive 2013/36/EU. Kako bi se izbjegla preklapanja, trebalo bi predvidjeti i ograničena odstupanja u pogledu sustava dobavljača za upravljanje kvalitetom i obveze praćenja za subjekte koji uvode visokorizične UI sustave u mjeri u kojoj se primjenjuju na kreditne institucije regulirane Direktivom 2013/36/EU. Isti bi se režim trebao primjenjivati na društva za osiguranje i reosiguranje i osigurateljne holdinge na temelju Direktive 2009/138/EZ i posrednike u osiguranju na temelju Direktive (EU) 2016/97 te na druge vrste financijskih institucija koje podliježu zahtjevima u pogledu unutarnjeg upravljanja, aranžmana ili postupaka uspostavljenih na temelju relevantnog prava Unije o financijskim uslugama kako bi se osigurala dosljednost i jednako postupanje u financijskom sektoru.

(159) Svako tijelo za nadzor tržišta za visokorizične UI sustave u području biometrije, kako je navedeno u prilogu ovoj Uredbi, u mjeri u kojoj se ti sustavi upotrebljavaju u svrhu kaznenog progona, migracija, azila i upravljanja nadzorom državne granice ili za sudovanje i demokratske procese, trebalo bi imati djelotvorne istražne i korektivne ovlasti, uključujući barem ovlast za dobivanje pristupa svim osobnim podacima koji se obrađuju i svim informacijama potrebnima za obavljanje svojih zadaća. Tijela za nadzor tržišta trebala bi moći izvršavati svoje ovlasti potpuno neovisno. Bilo kakvim ograničenjima njihova pristupa osjetljivim operativnim podacima na temelju ove Uredbe ne bi se trebale dovoditi u pitanje ovlasti koje su im dodijeljene Direktivom (EU) 2016/680. Nijedno isključenje otkrivanja podataka nacionalnim tijelima za zaštitu podataka na temelju ove Uredbe ne bi trebalo utjecati na aktualne ili buduće ovlasti tih tijela izvan područja primjene ove Uredbe.

(160) Tijela za nadzor tržišta i Komisija trebali bi moći predložiti zajedničke aktivnosti, uključujući zajedničke istrage, koje trebaju provoditi tijela za nadzor tržišta ili tijela za nadzor tržišta zajedno s Komisijom, a čiji je cilj promicanje sukladnosti, utvrđivanje nesukladnosti, podizanje svijesti i pružanje smjernica u vezi s ovom Uredbom u pogledu specifičnih kategorija visokorizičnih UI sustava za koje je utvrđeno da predstavljaju ozbiljan rizik u dvjema ili više država članica. Zajedničke aktivnosti u cilju promicanja sukladnosti trebale bi se provoditi u skladu s člankom 9. Uredbe (EU) 2019/1020. Ured za umjetnu inteligenciju trebao bi pružati koordinacijsku potporu za zajedničke istrage.

(161) Potrebno je pojasniti odgovornosti i nadležnosti na razini Unije i na nacionalnoj razini u pogledu UI sustava koji se temelje na UI modelima opće namjene. Kako bi se izbjeglo preklapanje nadležnosti, ako se UI sustav temelji na UI modelu opće namjene, a model i sustav osigurava isti dobavljač, nadzor bi se trebao provoditi na razini Unije putem

⁽⁵²⁾ Uredba Vijeća (EU) br. 1024/2013 od 15. listopada 2013. o dodjeli određenih zadaća Europskoj središnjoj banci u vezi s politikama bonitetnog nadzora kreditnih institucija (SL L 287, 29.10.2013., str. 63.).

Ureda za umjetnu inteligenciju, koji bi u tu svrhu trebao imati ovlasti tijela za nadzor tržišta u smislu Uredbe (EU) 2019/1020. U svim ostalim slučajevima nacionalna tijela za nadzor tržišta i dalje su odgovorna za nadzor UI sustava. Međutim, kad je riječ o UI sustavima opće namjene koje subjekti koji uvode UI sustav mogu izravno upotrebljavati u barem jednu svrhu koja je klasificirana kao visokorizična, tijela za nadzor tržišta trebala bi surađivati s Uredom za umjetnu inteligenciju na provedbi evaluacija usklađenosti te o tome obavijestiti Vijeće za umjetnu inteligenciju i druga tijela za nadzor tržišta. Nadalje, tijela za nadzor tržišta trebala bi moći zatražiti pomoć od Ureda za umjetnu inteligenciju ako tijelo za nadzor tržišta ne može zaključiti istragu visokorizičnog UI sustava zbog toga što ne može pristupiti određenim informacijama povezanim s UI modelom opće namjene na kojem je izgrađen visokorizični UI sustav. U takvim bi se slučajevima postupak u pogledu uzajamne pomoći u prekograničnim slučajevima iz poglavlja VI. Uredbe (EU) 2019/1020 trebao primjenjivati *mutatis mutandis*.

- (162) Kako bi se na razini Unije na najbolji način iskoristilo centralizirano stručno znanje i sinergija Unije, ovlasti nadzora i izvršavanja obveza dobavljača UI modela opće namjene trebale bi biti u nadležnosti Komisije. Ured za umjetnu inteligenciju trebao bi moći provoditi sve potrebne mjere za praćenje djelotvorne provedbe ove Uredbe u pogledu UI modela opće namjene. Trebao bi moći istražiti moguće povrede pravila o dobavljačima UI modela opće namjene na vlastitu inicijativu, na temelju rezultata svojih aktivnosti praćenja ili na zahtjev tijela za nadzor tržišta u skladu s uvjetima utvrđenima u ovoj Uredbi. Kako bi se poduprlo djelotvorno praćenje koje provodi Ured za umjetnu inteligenciju, trebalo bi predvidjeti mogućnost da dobavljači niže u lancu podnose pritužbe o mogućim povredama pravila o dobavljačima UI modela i sustava opće namjene.
- (163) Kako bi se dopunili sustavi upravljanja za UI modele opće namjene, znanstveno povjerenstvo trebalo bi podupirati aktivnosti praćenja koje provodi Ured za umjetnu inteligenciju i može, u određenim slučajevima, Uredu za umjetnu inteligenciju dostaviti kvalificirana upozorenja kojima se pokreću daljnje mjere, kao što su istrage. To bi trebao biti slučaj kada znanstveno povjerenstvo ima razloga sumnjati da UI model opće namjene predstavlja konkretan i utvrdiv rizik na razini Unije. Nadalje, to bi trebao biti slučaj kada znanstveno povjerenstvo ima razloga sumnjati da UI model opće namjene ispunjava kriterije koji bi doveli do toga da ga se klasificira kao UI model opće namjene sa sistemskim rizikom. Kako bi znanstveno povjerenstvo dobilo informacije potrebne za obavljanje tih zadaća, trebao bi postojati mehanizam kojim ono može zatražiti od Komisije da od dobavljača zatraži dokumentaciju ili informacije.
- (164) Ured za umjetnu inteligenciju trebao bi moći poduzeti potrebne mjere za praćenje djelotvorne provedbe i ispunjavanja obveza dobavljača UI modela opće namjene koje su utvrđene u ovoj Uredbi. Ured za umjetnu inteligenciju trebao bi moći istražiti moguće povrede u skladu s ovlastima predviđenima u ovoj Uredbi, među ostalim traženjem dokumentacije i informacija, provođenjem evaluacija i zahtijevanjem od dobavljača UI modela opće namjene da provede mjere. Kako bi se iskoristilo neovisno stručno znanje, pri provedbi evaluacija Ured za umjetnu inteligenciju trebao bi moći uključiti neovisne stručnjake da provedu evaluacije u njegovo ime. Usklađenost s obvezama trebala bi biti izvršiva, među ostalim, s pomoću zahtjeva za poduzimanje odgovarajućih mjera, među ostalim i mjera za ublažavanje rizika u slučaju utvrđenih sistemskih rizika, kao i ograničavanja stavljanja na raspolaganje na tržištu, povlačenja ili opoziva modela. Kao zaštitna mjera, ako je to potrebno izvan okvira postupovnih prava predviđenih u ovoj Uredbi, dobavljači UI modela opće namjene trebali bi imati postupovna prava predviđena u članku 18. Uredbe (EU) 2019/1020, koji bi se trebao primjenjivati *mutatis mutandis*, ne dovodeći u pitanje specifičnija postupovna prava predviđena ovom Uredbom.
- (165) Razvoj UI sustava koji nisu visokorizični u skladu sa zahtjevima ove Uredbe može dovesti do šire primjene etične i pouzdane umjetne inteligencije u Uniji. Dobavljači UI sustava koji nisu visokorizični trebalo bi poticati na izradu kodeksa ponašanja, uključujući povezane mehanizme upravljanja, namijenjenih poticanju dobrovoljne primjene nekih ili svih obveznih zahtjeva koji se primjenjuju na visokorizične UI sustave, prilagođenih namjeni sustava i manjem riziku te uzimajući u obzir dostupna tehnička rješenja i najbolje industrijske prakse kao što su kartice modela i podatkovne kartice. Dobavljači i, prema potrebi, subjekte koji uvode sve UI sustave, bez obzira na to jesu li visokorizični, i UI modele trebalo bi također poticati da dobrovoljno primjenjuju dodatne zahtjeve koji se odnose, na primjer, na elemente Etičkih smjernica Unije za pouzdanu umjetnu inteligenciju, okolišnu održivost, mjere

pismenosti u području umjetne inteligencije, uključiv i raznolik dizajn i razvoj UI sustava, uključujući usmjeravanje pozornosti na ranjive osobe i pristupačnost za osobe s invaliditetom, sudjelovanje dionika uz uključenost, prema potrebi, relevantnih dionika kao što su poduzeća i organizacije civilnog društva, akademska zajednica, istraživačke organizacije, sindikati i organizacije za zaštitu potrošača u dizajnu i razvoju UI sustava te raznolikost razvojnih timova, uključujući ravnotežu spolova. Kako bi se osigurala djelotvornost dobrovoljnih kodeksa ponašanja, oni bi se trebali temeljiti na jasnim ciljevima i ključnim pokazateljima uspješnosti za mjerenje ostvarenja tih ciljeva. Trebalo bi ih također razvijati na uključiv način, prema potrebi, uz sudjelovanje relevantnih dionika kao što su poduzeća i organizacije civilnog društva, akademska zajednica, istraživačke organizacije, sindikati i organizacije za zaštitu potrošača. Komisija može osmisliti inicijative, među ostalim na sektorskoj razini, za olakšavanje smanjivanja tehničkih zapreka prekograničnoj razmjeni podataka u svrhu razvoja umjetne inteligencije, među ostalim i u području infrastrukture za pristup podacima te semantičke i tehničke interoperabilnosti različitih vrsta podataka.

- (166) Važno je da UI sustavi povezani s proizvodima koji nisu visokorizični u skladu s ovom Uredbom te stoga ne moraju ispunjavati zahtjeve utvrđene za visokorizične UI sustave ipak budu sigurni kad se stavljaju na tržište ili u upotrebu. Kako bi se doprinijelo tom cilju, Uredba (EU) 2023/988 Europskog parlamenta i Vijeća ⁽⁵³⁾ primjenjivala bi se kao sigurnosni mehanizam.
- (167) Kako bi se osigurala pouzdana i konstruktivna suradnja nadležnih tijela na razini Unije i na nacionalnoj razini, sve strane uključene u primjenu ove Uredbe trebale bi poštovati povjerljivost informacija i podataka prikupljenih pri obavljanju svojih zadaća, u skladu s pravom Unije ili nacionalnim pravom. Svoje zadaće i aktivnosti trebale bi obavljati tako da osobito štite prava intelektualnog vlasništva, povjerljive poslovne informacije i poslovne tajne, djelotvornu provedbu ove Uredbe, javne i nacionalne sigurnosne interese, integritet kaznenih i upravnih postupaka te integritet klasificiranih podataka.
- (168) Usklađenost s ovom Uredbom trebala bi biti izvršiva izricanjem sankcija i drugih mjera izvršavanja. Države članice trebale bi poduzeti sve mjere potrebne za osiguravanje provedbe odredaba ove Uredbe, među ostalim utvrđivanjem učinkovitih, proporcionalnih i odvraćajućih sankcija za povrede tih odredaba, i za poštovanje načela *ne bis in idem*. Kako bi se postrožile i uskladile upravne sankcije za povrede ove Uredbe, trebalo bi utvrditi gornje granice za određivanje upravnih novčanih kazni za određene specifične povrede. Pri procjeni iznosa novčanih kazni države članice trebale bi u svakom pojedinačnom slučaju uzeti u obzir sve relevantne okolnosti specifične situacije, posebno uzimajući u obzir prirodu, težinu i trajanje povrede i njezine posljedice te veličinu dobavljača, posebno ako je dobavljač MSP, uključujući *start-up* poduzeće. Europski nadzornik za zaštitu podataka trebao bi imati ovlast izreći novčane kazne institucijama, agencijama i tijelima Unije obuhvaćenima područjem primjene ove Uredbe.
- (169) Usklađenost s obvezama dobavljača UI modela opće namjene koje su propisane na temelju ove Uredbe trebala bi biti izvršiva, među ostalim, novčanim kaznama. U tu bi svrhu također trebalo utvrditi odgovarajuće razine novčanih kazni za povrede tih obveza, uključujući nepoštovanje mjera koje je Komisija zatražila u skladu s ovom Uredbom, podložno odgovarajućim rokovima zastare u skladu s načelom proporcionalnosti. Sve odluke koje Komisija donosi na temelju ove Uredbe podliježu postupku preispitivanja pred Sudom Europske unije u skladu s UFEU-om, među ostalim i neograničenoj nadležnosti Suda u pogledu sankcija u skladu s člankom 261. UFEU-a.
- (170) Pravom Unije i nacionalnim pravom već su predviđena djelotvorna pravna sredstva za fizičke i pravne osobe na čija prava i slobode negativno utječe upotreba UI sustava. Ne dovodeći u pitanje ta pravna sredstva, svaka fizička ili pravna osoba koja ima razloga smatrati da je došlo do povrede ove Uredbe trebala bi imati pravo podnijeti pritužbu relevantnom tijelu za nadzor tržišta.
- (171) Zahvaćene osobe trebale bi imati pravo dobiti objašnjenje ako se odluka subjekta koji uvodi sustav uglavnom temelji na izlaznim rezultatima iz određenih visokorizičnih UI sustava obuhvaćenih područjem primjene ove Uredbe i ako ta odluka proizvodi pravne učinke ili na sličan način znatno utječe na te osobe na način za koji smatraju da ima

⁽⁵³⁾ Uredba (EU) 2023/988 Europskog parlamenta i Vijeća od 10. svibnja 2023. o općoj sigurnosti proizvoda, izmjeni Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća i Direktive (EU) 2020/1828 Europskog parlamenta i Vijeća te o stavljanju izvan snage Direktive 2001/95/EZ Europskog parlamenta i Vijeća i Direktive Vijeća 87/357/EEZ (SL L 135, 23.5.2023., str. 1.).

negativan učinak na njihovo zdravlje, sigurnost ili temeljna prava. To bi objašnjenje trebalo biti jasno i smisleno te bi trebalo biti osnova koja omogućuje zahvaćenim osobama da ostvare svoja prava. Pravo na dobivanje objašnjenja ne bi se trebalo primjenjivati na upotrebu UI sustava za koje iznimke ili ograničenja proizlaze iz prava Unije ili nacionalnog prava i trebalo bi se primjenjivati samo u mjeri u kojoj to pravo već nije predviđeno pravom Unije.

- (172) Osobe koje djeluju kao zviždači u vezi s povredama ove Uredbe trebale bi biti zaštićene pravom Unije. Direktiva (EU) 2019/1937 Europskog parlamenta i Vijeća⁽⁵⁴⁾ stoga bi se trebala primjenjivati na prijavljivanje povreda ove Uredbe i na zaštitu osoba koje prijavljuju te povrede.
- (173) Kako bi se osiguralo da se regulatorni okvir može prilagođavati ako je to potrebno, Komisiji bi trebalo delegirati ovlast za donošenje akata u skladu s člankom 290. UFEU-a radi izmjene uvjeta na temelju kojih se UI sustav ne treba smatrati visokorizičnim, popisa visokorizičnih UI sustava, odredaba o tehničkoj dokumentaciji, sadržaja EU izjave o sukladnosti, odredaba o postupcima ocjenjivanja sukladnosti, odredaba kojima se utvrđuju visokorizični UI sustavi na koje bi se trebao primjenjivati postupak ocjenjivanja sukladnosti na temelju ocjene sustava upravljanja kvalitetom i ocjene tehničke dokumentacije, praga, referentnih vrijednosti i pokazatelja, među ostalim dopunjavanjem tih referentnih vrijednosti i pokazatelja, u pravilima za klasifikaciju UI modela opće namjene sa sistemskim rizikom, kriterija za određivanje UI modela opće namjene sa sistemskim rizikom, tehničke dokumentacije za dobavljače UI modela opće namjene i informacija o transparentnosti za dobavljače UI modela opće namjene. Posebno je važno da Komisija tijekom svojeg pripremnog rada provede odgovarajuća savjetovanja, uključujući ona na razini stručnjaka, te da se ta savjetovanja provedu u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.⁽⁵⁵⁾ Osobito, s ciljem osiguravanja ravnopravnog sudjelovanja u pripremi delegiranih akata, Europski parlament i Vijeće primaju sve dokumente istodobno kada i stručnjaci iz država članica te njihovi stručnjaci sustavno imaju pristup sastancima stručnih skupina Komisije koji se odnose na pripremu delegiranih akata.
- (174) S obzirom na brz tehnološki razvoj i tehničko stručno znanje koje je potrebno za djelotvornu primjenu ove Uredbe, Komisija bi trebala evaluirati i preispitati ovu Uredbu do 2. kolovoza 2029. i svake četiri godine nakon toga te o tome izvjestiti Europski parlament i Vijeće. Osim toga, uzimajući u obzir posljedice za područje primjene ove Uredbe, Komisija bi jednom godišnje trebala provesti procjenu potrebe za izmjenom popisa visokorizičnih UI sustava i popisa zabranjenih praksi. Nadalje, do 2. kolovoza 2028. i svake četiri godine nakon toga Komisija bi trebala evaluirati potrebu za izmjenom popisa naslova visokorizičnih područja iz priloga ovoj Uredbi, UI sustava obuhvaćenih obvezama transparentnosti, djelotvornosti sustava nadzora i upravljanja te napretka u razvoju normizacijskih dokumenata o energetski učinkovitom razvoju UI modela opće namjene, uključujući potrebu za daljnjim mjerama ili djelovanjima, te o tome izvjestiti Europski parlament i Vijeće. Naposljetku, do 2. kolovoza 2028. i svake tri godine nakon toga Komisija bi trebala evaluirati učinak i djelotvornost dobrovoljnih kodeksa ponašanja namijenjenih poticanju primjene zahtjeva predviđenih za visokorizične UI sustave u slučaju UI sustava koji nisu visokorizični i eventualno drugih dodatnih zahtjeva za takve UI sustave.
- (175) Radi osiguranja jedinstvenih uvjeta za provedbu ove Uredbe provedbene ovlasti trebalo bi dodijeliti Komisiji. Te bi ovlasti trebalo izvršavati u skladu s Uredbom (EU) br. 182/2011 Europskog parlamenta i Vijeća⁽⁵⁶⁾.
- (176) S obzirom na to da cilj ove Uredbe, to jest poboljšanje funkcioniranja unutarnjeg tržišta i promicanje uvođenja antropocentrične umjetne inteligencije, uz istodobno osiguravanje visoke razine zaštite zdravlja, sigurnosti i temeljnih prava sadržanih u Povelji, uključujući demokraciju, vladavinu prava i zaštitu okoliša od štetnih učinaka UI

⁽⁵⁴⁾ Direktiva (EU) 2019/1937 Europskog parlamenta i Vijeća od 23. listopada 2019. o zaštiti osoba koje prijavljuju povrede prava Unije (SL L 305, 26.11.2019., str. 17.).

⁽⁵⁵⁾ SL L 123, 12.5.2016., str. 1.

⁽⁵⁶⁾ Uredba (EU) br. 182/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o utvrđivanju pravila i općih načela u vezi s mehanizmima nadzora država članica nad izvršavanjem provedbenih ovlasti Komisije (SL L 55, 28.2.2011., str. 13.).

sustavâ u Uniji te podupiranje inovacija, ne mogu dostatno ostvariti države članice, nego se zbog opsega ili učinaka djelovanja on na bolji način može ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti utvrđenim u članku 5. UEU-a. U skladu s načelom proporcionalnosti utvrđenim u tom članku ova Uredba ne prelazi ono što je potrebno za ostvarivanje tog cilja.

- (177) Kako bi se zajamčila pravna sigurnost, osiguralo odgovarajuće razdoblje prilagodbe za operatore i izbjegli poremećaji na tržištu, među ostalim osiguravanjem kontinuiteta korištenja UI sustavâ, primjereno je da se ova Uredba primjenjuje na visokorizične UI sustave koji su stavljeni na tržište ili u upotrebu prije općeg datuma početka njezine primjene samo ako od tog datuma u tim sustavima dođe do znatnih promjena u pogledu njihova dizajna ili namjene. Primjereno je pojasniti da bi u tom pogledu pojam znatne promjene trebalo razumjeti kao sadržajno jednakovrijedan pojmu znatne izmjene, koji se upotrebljava samo u pogledu visokorizičnih UI sustava na temelju ove Uredbe. Iznimno i s obzirom na javnu odgovornost, operateri UI sustava koji su komponente opsežnih informacijskih sustava uspostavljenih pravnim aktima navedenima u prilogu ovoj Uredbi i operateri visokorizičnih UI sustava namijenjenih korištenju od strane tijela javne vlasti trebali bi poduzeti potrebne korake kako bi ispunili zahtjeve iz ove Uredbe do kraja 2030. i do 2. kolovoza 2030.
- (178) Dobavljače visokorizičnih UI sustava potiče se da dobrovoljno počnu ispunjavati relevantne obveze iz ove Uredbe već tijekom prijelaznog razdoblja.
- (179) Ova Uredba trebala bi se primjenjivati od 2. kolovoza 2026. Međutim, uzimajući u obzir neprihvatljiv rizik povezan s korištenjem umjetne inteligencije na određene načine, zabrane kao i opće odredbe ove Uredbe trebale bi se trebale primjenjivati već od 2. veljače 2025. Iako potpuni učinak tih zabrana proizlazi iz uspostave upravljanja i izvršavanja ove Uredbe, predviđanje primjene zabrana važno je kako bi se uzeli u obzir neprihvatljivi rizici i kako bi se utjecalo na druge postupke, primjerice u građanskom pravu. Nadalje, infrastruktura povezana s upravljanjem i sustavom za ocjenjivanje sukladnosti trebala bi biti spremna za upotrebu prije 2. kolovoza 2026., pa bi se stoga odredbe o prijavljenim tijelima i strukturama upravljanja trebale primjenjivati od 2. kolovoza 2025. S obzirom na brz tehnološki napredak i usvajanje UI modelâ opće namjene, obveze dobavljača UI modelâ opće namjene trebale bi se primjenjivati od 2. kolovoza 2025. Kodeksi prakse trebali bi biti spremni do 2. svibnja 2025. kako bi se dobavljačima omogućilo da pravodobno dokažu usklađenost. Ured za umjetnu inteligenciju trebao bi osigurati da pravila i postupci klasifikacije budu ažurirani s obzirom na tehnološki razvoj. Usto, države članice trebale bi utvrditi pravila o sankcijama i obavijestiti Komisiju o tim pravilima, uključujući upravne novčane kazne, te osigurati njihovu pravilnu i djelotvornu provedbu do datuma početka primjene ove Uredbe. Stoga bi se odredbe o sankcijama trebale primjenjivati od 2. kolovoza 2025.
- (180) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka i s Europskim odborom za zaštitu podataka u skladu s člankom 42. stavcima 1. i 2. Uredbe (EU) 2018/1725 te su oni dali zajedničko mišljenje 18. lipnja 2021.,

DONIJELI SU OVU UREDBU:

POGLAVLJE I. OPĆE ODREDBE

Članak 1.

Predmet

1. Svrha je ove Uredbe poboljšati funkcioniranje unutarnjeg tržišta i promicati uvođenje antropocentrične i pouzdane umjetne inteligencije, uz istodobno osiguravanje visoke razine zaštite zdravlja, sigurnosti i temeljnih prava sadržanih u Povelji, uključujući demokraciju, vladavinu prava i zaštitu okoliša, od štetnih učinaka UI sustavâ u Uniji, te podupiranje inovacija.

2. Ovom se Uredbom utvrđuju:

(a) usklađena pravila za stavljanje na tržište, stavljanje u upotrebu i korištenje UI sustava u Uniji;

- (b) zabrane određenih praksi u području umjetne inteligencije;
- (c) posebni zahtjevi za visokorizične UI sustave i obveze za operatere takvih sustava;
- (d) usklađena pravila o transparentnosti za određene UI sustave;
- (e) usklađena pravila za stavljanje na tržište UI modelâ opće namjene;
- (f) pravila o praćenju tržišta, nadzoru tržišta, upravljanju i izvršavanju;
- (g) mjere za potporu inovacijama, posebno usmjerene na MSP-ove, uključujući *start-up* poduzeća.

Članak 2.

Područje primjene

1. Ova Uredba primjenjuje se na:

- (a) dobavljače koji stavljaju na tržište ili u upotrebu UI sustave ili stavljaju na tržište UI modele opće namjene u Uniji, bez obzira na to imaju li ti dobavljači poslovni nastan u Uniji ili u nekoj trećoj zemlji ili nalaze li se u Uniji ili u trećoj zemlji;
- (b) subjekte koji uvode UI sustave, a koji imaju poslovni nastan u Uniji ili se nalaze u Uniji;
- (c) dobavljače UI sustava i subjekte koji uvode UI sustave koji imaju poslovni nastan u trećoj zemlji ili se nalaze u trećoj zemlji ako se izlazni rezultati UI sustava upotrebljavaju u Uniji;
- (d) uvoznike i distributere UI sustavâ;
- (e) proizvođače proizvoda koji stavljaju na tržište ili u upotrebu UI sustav zajedno sa svojim proizvodom i pod vlastitim imenom ili žigom;
- (f) ovlaštene zastupnike dobavljača koji nemaju poslovni nastan u Uniji;
- (g) zahvaćene osobe koje se nalaze u Uniji.

2. Na UI sustave klasificirane kao visokorizične u skladu s člankom 6. stavkom 1. u odnosu na proizvode obuhvaćene zakonodavstvom Unije o usklađivanju navedenim u odjeljku B Priloga I. primjenjuju se samo članak 6. stavak 1., članci od 102. do 109. i članak 112. Članak 57. primjenjuje se samo u mjeri u kojoj su zahtjevi za visokorizične UI sustave iz ove Uredbe uključeni u to zakonodavstvo Unije o usklađivanju.

3. Ova se Uredba ne primjenjuje na područja izvan područja primjene prava Unije i ni u kojem slučaju ne utječe na nadležnosti država članica u pogledu nacionalne sigurnosti, bez obzira na vrstu subjekta kojem su države članice povjerile obavljanje zadaća u vezi s tim nadležnostima.

Ova se Uredba ne primjenjuje na UI sustave ako i u mjeri u kojoj se stavljaju na tržište, u upotrebu ili upotrebljavaju s izmjenama ili bez njih isključivo u vojne svrhe, obrambene svrhe ili u svrhe povezane s nacionalnom sigurnošću, bez obzira na vrstu subjekta koji obavlja te aktivnosti.

Ova se Uredba ne primjenjuje na UI sustave koji se ne stavljaju na tržište ni u upotrebu u Uniji ako se izlazni rezultati upotrebljavaju u Uniji isključivo u vojne svrhe, obrambene svrhe ili u svrhe povezane s nacionalnom sigurnošću, bez obzira na vrstu subjekta koji obavlja te aktivnosti.

4. Ova se Uredba ne primjenjuje na tijela javne vlasti u trećoj zemlji ni na međunarodne organizacije obuhvaćene područjem primjene ove Uredbe na temelju stavka 1. ako ta tijela ili te organizacije upotrebljavaju UI sustave u okviru međunarodne suradnje ili sporazumâ o suradnji u području kaznenog progona i pravosudne suradnje s Unijom ili s jednom ili više država članica, pod uvjetom da takva treća zemlja ili međunarodna organizacija pruža odgovarajuće zaštitne mjere u pogledu zaštite temeljnih prava i sloboda pojedinaca.

5. Ova Uredba ne utječe na primjenu odredaba o odgovornosti pružateljâ usluga posredovanja kako je utvrđeno u poglavlju II. Uredbe (EU) 2022/2065.

6. Ova Uredba ne primjenjuje se na UI sustave ili UI modele, uključujući njihove izlazne rezultate, koji su posebno razvijeni i stavljeni u upotrebu isključivo u svrhu znanstvenih istraživanja i razvoja.
7. Pravo Unije o zaštiti osobnih podataka, privatnosti i povjerljivosti komunikacija primjenjuje se na osobne podatke koji se obrađuju u vezi s pravima i obvezama utvrđenima u ovoj Uredbi. Ova Uredba ne utječe na uredbu (EU) 2016/679 i (EU) 2018/1725 ni na direktive 2002/58/EZ i (EU) 2016/680, ne dovodeći pritom u pitanje članak 10. stavak 5. i članak 59. ove Uredbe.
8. Ova se Uredba ne primjenjuje na aktivnosti istraživanja, testiranja ili razvoja UI sustava ili UI modela prije njihova stavljanja na tržište ili u upotrebu. Takve se aktivnosti provode u skladu s primjenjivim pravom Unije. Testiranje u stvarnim uvjetima nije obuhvaćeno tim isključenjem.
9. Ovom se Uredbom ne dovode u pitanje pravila utvrđena drugim pravnim aktima Unije povezanim sa zaštitom potrošača i sigurnošću proizvoda.
10. Ova se Uredba ne primjenjuje na obveze subjekata koji uvode sustav koji su fizičke osobe koje upotrebljavaju UI sustave isključivo u osobnoj neprofesionalnoj djelatnosti.
11. Ovom se Uredbom Uniju ili države članice ne sprečava da zadrže ili uvedu zakone i druge propise koji su pogodniji za radnike u smislu zaštite njihovih prava u pogledu korištenja UI sustava od strane poslodavaca, ili da potiču ili dopuštaju primjenu kolektivnih ugovora koji su pogodniji za radnike.
12. Ova se Uredba ne primjenjuje na UI sustave koji se objavljuju na temelju besplatnih licencija za softver otvorenog koda, osim ako se stavljaju na tržište ili u upotrebu kao visokorizični UI sustavi ili kao UI sustav obuhvaćen člankom 5. ili člankom 50.

Članak 3.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

1. „UI sustav” znači strojni sustav dizajniran za rad s promjenjivim razinama autonomije i koji nakon uvođenja može pokazati prilagodljivost te koji, za eksplicitne ili implicitne ciljeve, iz ulaznih vrijednosti koje prima, zaključuje kako generirati izlazne vrijednosti kao što su predviđanja, sadržaj, preporuke ili odluke koji mogu utjecati na fizička ili virtualna okruženja;
2. „rizik” znači kombinacija vjerojatnosti nastanka štete i težine te štete;
3. „dobavljač” znači fizička ili pravna osoba, tijelo javne vlasti, javna agencija ili drugo javno tijelo koje razvija UI sustav ili UI model opće namjene ili koji ima razvijen UI sustav ili UI model opće namjene i stavlja ga na tržište ili stavlja UI sustav u upotrebu pod vlastitim imenom ili žigom, uz plaćanje ili besplatno;
4. „subjekt koji uvodi sustav” znači fizička ili pravna osoba, tijelo javne vlasti, javna agencija ili drugo javno tijelo koje upotrebljava UI sustav u okviru svoje nadležnosti, osim ako se UI sustav upotrebljava u osobnoj neprofesionalnoj djelatnosti;
5. „ovlašteni zastupnik” znači fizička ili pravna osoba koja se nalazi u Uniji ili ima poslovni nastan u Uniji, koju je dobavljač UI sustava ili UI modela opće namjene pisanim putem ovlastio da u njegovo ime izvršava i provodi obveze i postupke utvrđene u ovoj Uredbi i koja je takvo ovlaštenje prihvatila;
6. „uvoznik” znači fizička ili pravna osoba koja se nalazi u Uniji ili ima poslovni nastan u Uniji i koja stavlja na tržište UI sustav s imenom ili žigom fizičke ili pravne osobe s poslovnim nastanom u trećoj zemlji;
7. „distributer” znači fizička ili pravna osoba u opskrbnom lancu koja nije dobavljač ni uvoznik i koja stavlja UI sustav na tržište Unije;
8. „operator” znači dobavljač, proizvođač proizvoda, subjekt koji uvodi sustav, ovlašteni zastupnik, uvoznik ili distributer;

9. „stavljanje na tržište” znači prvo stavljanje UI sustava ili UI modela opće namjene na raspolaganje na tržištu Unije;
10. „stavljanje na raspolaganje na tržištu” znači isporuka UI sustava ili UI modela opće namjene za distribuciju ili upotrebu na tržištu Unije u okviru komercijalne djelatnosti, uz plaćanje ili besplatno;
11. „stavljanje u upotrebu” znači isporuka UI sustava za prvu upotrebu u Uniji u skladu s njegovom namjenom izravno subjektu koji uvodi sustav ili za vlastite potrebe;
12. „namjena” znači korištenje za koje je dobavljač namijenio UI sustav, uključujući specifični kontekst i uvjete korištenja, kako je određeno u informacijama koje je dobavljač naveo u uputama za korištenje, promotivnim ili prodajnim materijalima i izjavama te u tehničkoj dokumentaciji;
13. „razumno predvidljiva pogrešna upotreba” znači upotreba UI sustava na način koji nije u skladu s njegovom namjenom, ali može biti posljedica razumno predvidljivog čovjekova ponašanja ili interakcije s drugim sustavima, uključujući druge UI sustave;
14. „sigurnosna komponenta” znači komponenta proizvoda ili UI sustava koja ima sigurnosnu funkciju u tom proizvodu ili UI sustavu ili čiji kvar ili neispravnost ugrožava zdravlje i sigurnost osoba ili imovine;
15. „upute za korištenje” znači informacije kojima dobavljač u prvom redu informira subjekt koji uvodi sustav o namjeni i pravilnom korištenju UI sustava;
16. „opoziv UI sustava” znači svaka mjera čiji je cilj postizanje vraćanja dobavljaču UI sustava stavljenog na raspolaganje subjektima koji uvode sustav ili njegovo izuzimanje iz usluge ili onemogućavanje njegova korištenja;
17. „povlačenje UI sustava” znači svaka mjera čiji je cilj sprečavanje da se UI sustav u opskrbnom lancu stavi na raspolaganje na tržištu;
18. „učinkovitost UI sustava” znači sposobnost UI sustava da ostvari svoju namjenu;
19. „tijelo koje provodi prijavljivanje” znači nacionalno tijelo odgovorno za utvrđivanje i provedbu postupaka potrebnih za ocjenjivanje, imenovanje, obavješćivanje i praćenje tijela za ocjenjivanje sukladnosti;
20. „ocjenjivanje sukladnosti” znači postupak kojim se dokazuje jesu li ispunjeni zahtjevi utvrđeni u poglavlju III. odjeljku 2. koji se odnose na visokorizični UI sustav;
21. „tijelo za ocjenjivanje sukladnosti” znači tijelo koje provodi aktivnosti ocjenjivanja sukladnosti kao treća strana, uključujući testiranje, certifikaciju i inspekciju;
22. „prijavljeno tijelo” znači tijelo za ocjenjivanje sukladnosti prijavljeno u skladu s ovom Uredbom i drugim relevantnim zakonodavstvom Unije o usklađivanju;
23. „bitna izmjena” znači promjena UI sustava nakon njegova stavljanja na tržište ili u upotrebu koja nije predviđena ili planirana u okviru početnog ocjenjivanja sukladnosti koje je proveo dobavljač i koja utječe na usklađenost UI sustava sa zahtjevima utvrđenima u poglavlju III. odjeljku 2. ili koja prouzroči izmjenu namjene prema kojoj je UI sustav bio ocijenjen;
24. „oznaka CE” znači oznaka kojom dobavljač označuje da je UI sustav sukladan sa zahtjevima utvrđenima u poglavlju III. odjeljku 2. i drugim primjenjivim zakonodavstvom Unije o usklađivanju kojim se propisuje stavljanje te oznake;
25. „sustav praćenja nakon stavljanja na tržište” znači sve aktivnosti kojima dobavljači UI sustava prikupljaju i analiziraju iskustva stečena korištenjem UI sustava koje stavlja u na tržište ili u upotrebu kako bi utvrdili postoji li potreba za hitnim poduzimanjem eventualnih nužnih korektivnih ili preventivnih mjera;
26. „tijelo za nadzor tržišta” znači nacionalno tijelo koje provodi aktivnosti i poduzima mjere na temelju Uredbe (EU) 2019/1020;

27. „usklađena norma” znači usklađena norma kako je definirana u članku 2. stavku 1. točki (c) Uredbe (EU) br. 1025/2012;
28. „zajednička specifikacija” znači skup tehničkih specifikacija kako su definirane u članku 2. točki 4. Uredbe (EU) br. 1025/2012, kojim se pružaju sredstva za ispunjavanje određenih zahtjeva utvrđenih ovom Uredbom;
29. „podaci za treniranje” znači podaci koji se upotrebljavaju za treniranje UI sustava prilagođavanjem njegovih poučivih parametara;
30. „podaci za validaciju” znači podaci koji se upotrebljavaju za evaluaciju treniranog UI sustava te za ugađanje njegovih nepoučivih parametara i njegova procesa učenja kako bi se, među ostalim, izbjegla nedovoljna prilagodba ili prekomjerna prilagodba;
31. „skup podataka za validaciju” znači zaseban skup podataka ili fiksni ili varijabilni dio skupa podataka za treniranje;
32. „podaci za testiranje” znači podaci koji se upotrebljavaju za neovisnu evaluaciju UI sustava kako bi se potvrdila očekivana učinkovitost tog sustava prije njegova stavljanja na tržište ili u upotrebu;
33. „ulazni podaci” znači podaci koji su uneseni u UI sustav ili koje je UI sustav izravno stekao, a na temelju kojih sustav stvara izlazni rezultat;
34. „biometrijski podaci” znači osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim, fiziološkim i bihevioralnim obilježjima fizičke osobe, kao što su prikazi lica ili daktiloskopski podaci;
35. „biometrijska identifikacija” znači automatizirano prepoznavanje fizičkih, fizioloških, bihevioralnih ili psiholoških obilježja ljudi u svrhu utvrđivanja identiteta fizičke osobe usporedbom biometrijskih podataka tog pojedinca s biometrijskim podacima pojedinaca pohranjenima u bazi podataka;
36. „biometrijska provjera” znači automatizirana provjera usporedbom dvaju uzoraka, uključujući autentifikaciju, kojom se identitet fizičkih osoba provjerava usporedbom njihovih biometrijskih podataka s prethodno dostavljenim biometrijskim podacima;
37. „posebne kategorije osobnih podataka” znači kategorije osobnih podataka iz članka 9. stavka 1. Uredbe (EU) 2016/679, članka 10. Direktive (EU) 2016/680 i članka 10. stavka 1. Uredbe (EU) 2018/1725;
38. „osjetljivi operativni podaci” znači operativni podaci povezani s aktivnostima sprečavanja, otkrivanja, istrage ili progona kaznenih djela čije bi otkrivanje moglo ugroziti integritet kaznenog postupka;
39. „sustav za prepoznavanje emocija” znači UI sustav namijenjen prepoznavanju emocija ili namjera fizičkih osoba ili izvođenju zaključaka o njihovim emocijama ili namjerama na temelju njihovih biometrijskih podataka;
40. „sustav za biometrijsku kategorizaciju” znači UI sustav namijenjen razvrstavanju fizičkih osoba u određene kategorije na temelju njihovih biometrijskih podataka, osim ako je on pomoćni element druge komercijalne usluge i nužan iz objektivnih tehničkih razloga;
41. „sustav za daljinsku biometrijsku identifikaciju” znači UI sustav namijenjen identifikaciji fizičkih osoba, bez njihova aktivnog sudjelovanja, obično na daljinu usporedbom biometrijskih podataka dotične osobe s biometrijskim podacima iz referentne baze podataka;
42. „sustav za daljinsku biometrijsku identifikaciju u stvarnom vremenu” znači sustav za daljinsku biometrijsku identifikaciju koji bez većeg kašnjenja prikuplja biometrijske podatke, vrši usporedbe i provodi identifikaciju, a obuhvaća ne samo trenutačnu identifikaciju nego i ograničena manja kašnjenja kako bi se izbjeglo zaobilaženje propisa;
43. „sustav za naknadnu daljinsku biometrijsku identifikaciju” znači sustav za daljinsku biometrijsku identifikaciju koji nije sustav za daljinsku biometrijsku identifikaciju u stvarnom vremenu;
44. „javno mjesto” znači svako fizičko mjesto u javnom ili privatnom vlasništvu dostupno neodređenom broju fizičkih osoba, bez obzira na to primjenjuju li se određeni uvjeti za pristup i bez obzira na moguća ograničenja kapaciteta;

45. „tijelo kaznenog progona” znači:

- (a) svako tijelo javne vlasti nadležno za sprečavanje, istragu, otkrivanje ili progon kaznenih djela ili izvršenje kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje; ili
- (b) svako drugo tijelo ili subjekt kojem je pravom države članice povjereno izvršavanje javne vlasti i javnih ovlasti u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršenja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje;

46. „kazneni progon” znači aktivnosti koje provode tijela kaznenog progona ili koje se provode u njihovo ime radi sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršenja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje;

47. „Ured za umjetnu inteligenciju” znači Komisijina funkcija doprinošenja provedbi, praćenju i nadzoru UI sustavâ i UI modelâ opće namjene i upravljanju umjetnom inteligencijom koja je predviđena u Odluci Komisije od 24. siječnja 2024.; upućivanja na Ured za umjetnu inteligenciju u ovoj Uredbi tumače se kao upućivanja na Komisiju;

48. „nacionalno nadležno tijelo” znači tijelo koje provodi prijavljivanje ili tijelo za nadzor tržišta; kad je riječ o UI sustavima koje stavljaju u uporabu ili koriste institucije, agencije, uredi i tijela Unije, upućivanja na nacionalna nadležna tijela ili tijela za nadzor tržišta u ovoj Uredbi smatraju se upućivanjima na Europskog nadzornika za zaštitu podataka;

49. „ozbiljan incident” znači incident ili neispravnost UI sustava koji su izravno ili neizravno doveli do bilo kojeg od sljedećeg:

- (a) smrti osobe ili ozbiljnog narušavanja zdravlja osobe;
- (b) ozbiljnog i nepovratnog poremećaja u upravljanju kritičnom infrastrukturom ili njezinu radu;
- (c) povrede obveza na temelju prava Unije namijenjenih zaštiti temeljnih prava;
- (d) teške štete za imovinu ili okoliš;

50. „osobni podaci” znači osobni podaci kako su definirani u članku 4. točki 1. Uredbe (EU) 2016/679;

51. „neosobni podaci” znači podaci koji nisu osobni podaci kako su definirani u članku 4. točki 1. Uredbe (EU) 2016/679;

52. „izrada profila” znači izrada profila kako je definirana u članku 4. točki 4. Uredbe (EU) 2016/679;

53. „plan testiranja u stvarnim uvjetima” znači dokument u kojem se opisuju ciljevi, metodologija, geografski, populacijski i vremenski opseg, praćenje, organizacija i provedba testiranja u stvarnim uvjetima;

54. „plan izoliranog okruženja” znači dokument koji su usuglasili uključeni dobavljač i nadležno tijelo, a u kojem se opisuju ciljevi, uvjeti, vremenski okvir, metodologija i zahtjevi za aktivnosti koje se provode u izoliranom okruženju;

55. „regulatorno izolirano okruženje za umjetnu inteligenciju” znači kontroliran okvir koji je uspostavilo nadležno tijelo i kojim se dobavljačima ili potencijalnim dobavljačima UI sustavâ nudi mogućnost razvoja, treniranja, validacije i testiranja inovativnog UI sustava, po mogućnosti u stvarnim uvjetima, u skladu s planom izoliranog okruženja, na ograničeno vrijeme i pod regulatornim nadzorom;

56. „pismenost u području umjetne inteligencije” znači vještine, znanje i razumijevanje koji dobavljačima, subjektima koji uvode sustav i zahvaćenim osobama omogućuju, uzimajući u obzir njihova prava i obveze u kontekstu ove Uredbe, da informirano uvode UI sustave, kao i da steknu svijest o mogućnostima i rizicima umjetne inteligencije te šteti koju može izazvati;

57. „testiranje u stvarnim uvjetima” znači privremeno testiranje UI sustava u odnosu na njegovu namjenu u stvarnim uvjetima izvan laboratorija ili u na drugi način simuliranom okruženju radi prikupljanja pouzdanih i čvrstih podataka te ocjenjivanja i provjere sukladnosti UI sustava sa zahtjevima ove Uredbe te se ne smatra stavljanjem UI sustava na tržište ili u upotrebu u smislu ove Uredbe, pod uvjetom da su ispunjeni svi uvjeti utvrđeni u članku 57. ili članku 60.;
58. „ispitanik” za potrebe testiranja u stvarnim uvjetima znači fizička osoba koja sudjeluje u testiranju u stvarnim uvjetima;
59. „informirani pristanak” znači ispitanikov slobodan, specifičan, nedvosmislen i dobrovoljan iskaz spremnosti da sudjeluje u određenom testiranju u stvarnim uvjetima nakon što je obaviješten o svim aspektima testiranja relevantnima za njegovu odluku o sudjelovanju;
60. „uvjerljiv krivotvoreni sadržaj (*deep fake*)” znači slike, audiosadržaj ili videosadržaj koji generira ili kojim manipulira umjetna inteligencija, a koji nalikuju stvarnim osobama, predmetima, mjestima, subjektima ili događajima i koji bi se nekome lažno činio vjerodostojnim ili istinitim;
61. „raširena povreda” znači svaki čin ili propust protivan pravu Unije kojim se štite interesi pojedinaca, a:
- (a) kojim je nanesena ili će vjerojatno biti nanesena šteta kolektivnim interesima pojedinaca koji borave u najmanje dvjema državama članicama koje nisu država članica:
 - i. u kojoj je čin ili propust nastao ili se dogodio;
 - ii. u kojoj se dotični dobavljač ili, ako je primjenjivo, njegov ovlašteni zastupnik nalazi ili ima poslovni nastan; ili
 - iii. u kojoj subjekt koji uvodi sustav ima poslovni nastan ako je povredu počinio taj subjekt;
 - (b) koji je uzrokovao, uzrokuje ili će vjerojatno uzrokovati nanošenje štete kolektivnim interesima pojedinaca i koji ima zajednička obilježja, uključujući istu nezakonitu praksu ili povredu istog interesa, i koji je istodobno počinio isti operater u najmanje trima državama članicama;
62. „kritična infrastruktura” znači kritična infrastruktura kako je definirana u članku 2. točki 4. Direktive (EU) 2022/2557;
63. „UI model opće namjene” znači UI model, uključujući takav UI model treniran s pomoću velike količine podataka uz primjenu samostalnog nadzora u širokim razmjerima, koji ima vrlo općenitu namjenu i može kompetentno obavljati širok raspon različitih zadataka bez obzira na način na koji se model stavlja na tržište i koji se može integrirati u razne sustave ili primjene niže u lancu, osim UI modela koji se upotrebljavaju za aktivnosti istraživanja, razvoja ili izrade prototipova prije njihova stavljanja na tržište;
64. „sposobnosti visokog učinka” znači sposobnosti koje odgovaraju sposobnostima zabilježenima kod najnaprednijih UI modela opće namjene ili ih nadilaze;
65. „sistemski rizik” znači rizik specifičan za sposobnosti visokog učinka UI modela opće namjene, koji ima znatan utjecaj na tržište Unije zbog svojeg dosega ili zbog stvarnih ili razumno predvidljivih negativnih učinaka na javno zdravlje, sigurnost, javnu sigurnost, temeljna prava ili društvo u cjelini, a koji se može proširiti po cijelom vrijednosnom lancu;
66. „UI sustav opće namjene” znači UI sustav koji se temelji na UI modelu opće namjene i koji može služiti različitim namjenama, ili za izravnu upotrebu ili za integraciju u druge UI sustave;
67. „matematička operacija nad brojevima s pomičnim zarezom” znači svaka matematička operacija ili dodjela koja uključuje brojeve s pomičnim zarezom, koji su podskup realnih brojeva koji su na računalima obično predstavljeni kao cijeli broj fiksne preciznosti skaliran cjelobrojnim eksponentom fiksne baze;
68. „dobavljač niže u lancu” znači dobavljač UI sustava, uključujući UI sustav opće namjene, u koji je integriran UI model, bez obzira na to dobavlja li UI model on sâm i je li vertikalno integriran ili ga dobavlja drugi subjekt na temelju ugovornih odnosa.

Članak 4.

Pismenost u području umjetne inteligencije

Dobavljači i subjekti koji uvode UI sustave poduzimaju mjere kako bi na najbolji mogući način osigurali dostatnu razinu pismenosti u području umjetne inteligencije za svoje osoblje i druge osobe uključene u rad i korištenje UI sustava u njihovo ime, uzimajući u obzir njihovo tehničko znanje, iskustvo, obrazovanje i osposobljavanje te kontekst u kojem će se UI sustavi koristiti, kao i osobe ili skupine osoba na kojima se UI sustavi trebaju upotrijebiti.

POGLAVLJE II.

ZABRANJENE PRAKSE U PODRUČJU UMJETNE INTELIGENCIJE

Članak 5.

Zabranjene prakse u području umjetne inteligencije

1. Zabranjuju se sljedeće prakse u području umjetne inteligencije:

- (a) stavljanje na tržište, stavljanje u upotrebu ili korištenje UI sustava u kojem se primjenjuju subliminalne tehnike kojih osoba nije svjesna ili namjerno manipulativne ili obmanjujuće tehnike s ciljem ili s učinkom bitnog iskrivljavanja ponašanja osobe ili skupine osoba tako da se znatno narušava njihova sposobnost da donesu informiranu odluku, zbog čega donose odluku koju inače ne bi donijele, na način kojim se toj osobi, drugoj osobi ili skupini osoba uzrokuje znatna šteta ili se može razumno očekivati da će se prouzročiti takva šteta;
- (b) stavljanje na tržište, stavljanje u upotrebu ili korištenje UI sustava koji iskorištava bilo koju slabost fizičke osobe ili određene skupine osoba zbog njihove dobi, invaliditeta ili specifičnog društvenog ili ekonomskog položaja s ciljem ili s učinkom bitnog iskrivljavanja ponašanja te osobe ili osobe koja pripada toj skupini na način kojim se toj osobi ili nekoj drugoj osobi uzrokuje znatna šteta ili se može razumno očekivati da će se prouzročiti takva šteta;
- (c) stavljanje na tržište, stavljanje u upotrebu ili korištenje UI sustava radi evaluacije ili klasifikacije fizičkih osoba ili skupina osoba tijekom određenog razdoblja na temelju njihova društvenog ponašanja ili poznatih, izvedenih ili predviđenih osobnih obilježja ili obilježja ličnosti, pri čemu njihov društveni rejting uzrokuje barem jedno od sljedećeg:
 - i. štetno ili nepovoljno postupanje prema određenim fizičkim osobama ili skupinama osoba u društvenim kontekstima koji nisu povezani s kontekstima u kojima su podaci izvorno generirani ili prikupljeni;
 - ii. štetno ili nepovoljno postupanje prema određenim fizičkim osobama ili skupinama osoba koje je neopravdano ili nerazmjerno njihovu društvenom ponašanju ili njegovoj ozbiljnosti;
- (d) stavljanje na tržište, stavljanje u upotrebu u tu specifičnu svrhu ili korištenje UI sustava za procjene rizika u pogledu fizičkih osoba kako bi se procijenio ili predvidio rizik da će fizička osoba počiniti kazneno djelo, isključivo na temelju izrade profila fizičke osobe ili procjene njezinih osobina i obilježja ličnosti; ta se zabrana ne primjenjuje na UI sustave koji se upotrebljavaju za potporu ljudskoj procjeni uključenosti osobe u kriminalnu aktivnost, koja se već temelji na objektivnim i provjerljivim činjenicama izravno povezanim s kriminalnom aktivnošću;
- (e) stavljanje na tržište, stavljanje u upotrebu u tu specifičnu svrhu ili korištenje UI sustava koji stvaraju ili proširuju baze podataka za prepoznavanje lica neciljanim prikupljanjem fotografija lica s interneta ili snimki CCTV-a;
- (f) stavljanje na tržište, stavljanje u upotrebu u tu specifičnu svrhu ili korištenje UI sustava za izvođenje zaključaka o emocijama fizičke osobe na radnome mjestu i u obrazovnim ustanovama, osim ako se UI sustav namjerava staviti u upotrebu ili na tržište iz medicinskih ili sigurnosnih razloga;

- (g) stavljanje na tržište, stavljanje u upotrebu u tu specifičnu svrhu ili upotreba sustavâ za biometrijsku kategorizaciju u kojima se fizičke osobe pojedinačno kategoriziraju na temelju njihovih biometrijskih podataka kako bi se zaključilo ili izvelo zaključke o njihovoj rasi, političkim mišljenjima, članstvu u sindikatu, vjerskim ili filozofskim uvjerenjima, spolnom životu ili seksualnoj orijentaciji; ta zabrana ne obuhvaća označivanje ili filtriranje zakonito pribavljenih biometrijskih skupova podataka, kao što su slike, na temelju biometrijskih podataka ili kategorizacije biometrijskih podataka u području kaznenog progona;
- (h) upotreba sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona, osim ako je takva upotreba nužna i u mjeri u kojoj je nužna radi jednog od sljedećih ciljeva:
 - i. ciljane potrage za konkretnim žrtvama otmice, trgovine ljudima ili seksualnog iskorištavanja ljudi, kao i potrage za nestalim osobama;
 - ii. sprečavanja konkretne, znatne i izravne prijetnje životu ili tjelesnoj sigurnosti fizičkih osoba ili stvarne i prisutne ili stvarne i predvidljive prijetnje od terorističkog napada;
 - iii. lociranja ili identifikacije osobe osumnjičene za počinjenje kaznenog djela u svrhu vođenja kaznene istrage ili progona ili izvršenja kaznene sankcije za kaznena djela iz Priloga II. za koja je u dotičnoj državi članici zapriječena kazna zatvora ili oduzimanja slobode u maksimalnom trajanju od najmanje četiri godine.

Prvim podstavkom točkom (h) ne dovodi se u pitanje članak 9. Uredbe (EU) 2016/679 kad je riječ o obradi biometrijskih podataka u svrhe koje nisu kazneni progon.

2. Upotreba sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona radi bilo kojeg od ciljeva iz stavka 1. prvog podstavka točke (h) smije se uvesti u svrhe utvrđene u toj točki samo kako bi se potvrdio identitet konkretno ciljanog pojedinca, pri čemu se uzimaju u obzir sljedeći elementi:

- (a) priroda situacije zbog koje se pojavila mogućnost upotrebe, osobito težina, vjerojatnost i razmjernost štete koja bi nastala da se sustav ne koristi;
- (b) posljedice upotrebe sustava na prava i slobode svih dotičnih osoba, osobito težina, vjerojatnost i razmjernost tih posljedica.

Usto, upotreba sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona radi bilo kojeg od ciljeva iz stavka 1. prvog podstavka točke (h) ovog članka mora biti u skladu s potrebnim i razmjernim zaštitnim mjerama i uvjetima korištenja u skladu s nacionalnim pravom kojim se odobrava njihova upotreba, osobito u pogledu vremenskih i zemljopisnih ograničenja i ograničenja u pogledu osoba. Upotrebu sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima odobrava se samo ako je tijelo kaznenog progona dovršilo procjenu učinka na temeljna prava kako je predviđeno u članku 27. i registriralo sustav u bazi podataka EU-a u skladu s člankom 49. Međutim, u propisno opravdanim hitnim slučajevima takvi se sustavi mogu početi upotrebljavati bez registracije u bazi podataka EU-a, pod uvjetom da se takva registracija dovrši bez nepotrebne odgode.

3. Za potrebe stavka 1. prvog podstavka točke (h) i stavka 2., za svaku upotrebu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona potrebno je prethodno odobrenje pravosuđnog tijela ili neovisnog upravnog tijela čija je odluka obvezujuća iz države članice u kojoj će se sustav upotrebljavati, a koje se izdaje na obrazloženi zahtjev i u skladu s detaljnim pravilima nacionalnog prava iz stavka 5. Međutim, u propisno opravdanim hitnim situacijama takav se sustav može početi upotrebljavati bez odobrenja, pod uvjetom da se takvo odobrenje zatraži bez nepotrebne odgode, a najkasnije u roku od 24 sata. Ako je takvo odobrenje odbijeno, upotreba se smjesta zaustavlja te se svi podaci, kao i rezultati i izlazni podaci te upotrebe odmah odbacuju i brišu.

Nadležno pravosuđno tijelo ili neovisno upravno tijelo čija je odluka obvezujuća izdaje odobrenje samo ako je uvjeren, na temelju objektivnih dokaza ili jasnih informacija koje su mu predložene, da je upotreba dotičnog sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu potrebna za postizanje jednog od ciljeva iz stavka 1. prvog podstavka točke (h) navedenog u zahtjevu i razmjerna tom cilju, a ponajprije ostaje ograničena na ono što je nužno kad je riječ

o razdoblju te zemljopisnom i personalnom području primjene. Pri odlučivanju o zahtjevu to tijelo uzima u obzir elemente iz stavka 2. Odluka koja proizvodi negativan pravni učinak na osobu ne smije se donijeti isključivo na temelju izlaznih podataka sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu.

4. Ne dovodeći u pitanje stavak 3., o svakoj upotrebi sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona obavješćuju se relevantno tijelo za nadzor tržišta i nacionalno tijelo za zaštitu podataka u skladu s nacionalnim pravilima iz stavka 5. Obavijest mora sadržavati barem informacije navedene u stavku 6. i ne smije uključivati osjetljive operativne podatke.

5. Država članica može odlučiti predvidjeti mogućnost potpunog ili djelomičnog odobravanja upotrebe sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona uz ograničenja i pod uvjetima iz stavka 1. prvog podstavka točke (h) te stavaka 2. i 3. Dotična država članica u svojem nacionalnom pravu utvrđuje potrebna podrobna pravila o podnošenju zahtjeva za odobrenja iz stavka 3., o izdavanju, izvršenju i nadzoru tih odobrenja te izvješćivanju u vezi s njima. U tim se pravilima također određuje za koje se ciljeve iz stavka 1. prvog podstavka točke (h), među ostalim i za koja kaznena djela iz njegove točke (h) podtočke iii., nadležnim tijelima može odobriti upotreba tih sustava u svrhu kaznenog progona. Države članice priopćuju Komisiji ta pravila najkasnije 30 dana nakon njihova donošenja. Države članice mogu, u skladu s pravom Unije, uvesti restriktivnije propise o upotrebi sustava za daljinsku biometrijsku identifikaciju.

6. Nacionalna tijela za nadzor tržišta i nacionalna tijela za zaštitu podataka država članica koja su obaviještena o upotrebi sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona na temelju stavka 4. podnose Komisiji godišnja izvješća o takvoj upotrebi. U tu svrhu Komisija državama članicama i nacionalnim tijelima za nadzor tržišta i zaštitu podataka dostavlja predložak, uključujući informacije o broju odluka koje su nadležna pravosudna tijela ili neovisno upravno tijelo čija je odluka obvezujuća donijeli na temelju zahtjeva za izdavanje odobrenja u skladu sa stavkom 3. i njihov rezultat.

7. Komisija objavljuje godišnja izvješća o upotrebi sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona na temelju agregiranih podataka u državama članicama i godišnjih izvješća iz stavka 6. Ta godišnja izvješća ne smiju uključivati osjetljive operativne podatke o povezanim aktivnostima kaznenog progona.

8. Ovaj članak ne utječe na zabrane koje se primjenjuju ako se praksom u području umjetne inteligencije krši drugo pravo Unije.

POGLAVLJE III.

VISOKORIZIČNI UI SUSTAVI

ODJELJAK 1.

Klasifikacija UI sustava kao visokorizičnih

Članak 6.

Pravila o klasifikaciji UI sustava kao visokorizičnih

1. Bez obzira na to stavlja li se UI sustav na tržište ili u upotrebu neovisno o proizvodima iz točaka (a) i (b) taj se UI sustav smatra visokorizičnim ako su ispunjena oba sljedeća uvjeta:

- (a) UI sustav namijenjen je za korištenje kao sigurnosna komponenta proizvoda ili je UI sustav sam po sebi proizvod koji je obuhvaćen zakonodavstvom Unije o usklađivanju navedenim u Prilogu I;
- (b) za proizvod čija je sigurnosna komponenta na temelju točke (a) UI sustav ili UI sustav koji je sam po sebi proizvod zahtijeva se ocjenjivanje sukladnosti koje provodi treća strana radi stavljanja na tržište ili stavljanja u upotrebu tog proizvoda na temelju zakonodavstva Unije o usklađivanju navedenog u Prilogu I.

2. Uz visokorizične UI sustave iz stavka 1., u visokorizične sustave ubrajaju se UI sustavi iz Priloga III.

3. Odstupajući od stavka 2., UI sustav iz Priloga III. ne smatra se visokorizičnim ako ne predstavlja znatan rizik od štete za zdravlje, sigurnost ili temeljna prava fizičkih osoba, među ostalim ako bitno ne utječe na ishod donošenja odluka.

Prvi podstavak primjenjuje se ako je ispunjen bilo koji od sljedećih uvjeta:

- (a) UI sustav namijenjen je obavljanju uske postupovne zadaće;
- (b) UI sustav namijenjen je poboljšanju rezultata prethodno dovršene ljudske aktivnosti;
- (c) UI sustav namijenjen je otkrivanju obrazaca donošenja odluka ili odstupanja od ranijih obrazaca donošenja odluka i ne bi trebao zamijeniti prethodno dovršenu ljudsku procjenu niti na nju utjecati, bez odgovarajućeg preispitivanja koje provodi čovjek; ili
- (d) UI sustav namijenjen je obavljanju pripremne zadaće za ocjenjivanje relevantno za slučajeve upotrebe navedene u Prilogu III.

Ne dovodeći u pitanje prvi podstavak, UI sustav iz Priloga III. uvijek se smatra visokorizičnim ako taj UI sustav izrađuje profile fizičkih osoba.

4. Dobavljač koji smatra da UI sustav iz Priloga III. nije visokorizičan dokumentira svoje ocjenjivanje prije stavljanja tog sustava na tržište ili u upotrebu. Takav dobavljač podliježe obvezi registracije utvrđenoj u članku 49. stavku 2. Na zahtjev nacionalnih nadležnih tijela dobavljač dostavlja dokumentaciju o ocjenjivanju.

5. Komisija, nakon savjetovanja s Europskim vijećem za umjetnu inteligenciju („Vijeće za umjetnu inteligenciju”), a najkasnije 2. veljače 2026., izdaje smjernice u kojima se utvrđuje praktična provedba ovog članka u skladu s člankom 96. zajedno sa sveobuhvatnim popisom praktičnih slučajeva upotrebe UI sustava koji su visokorizični i koji nisu visokorizični.

6. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene stavka 3. drugog podstavka ovog članka dodavanjem novih uvjeta uvjetima koji su utvrđeni u stavku 3. drugom podstavku ovog članka ili mijenjanjem tih uvjeta ako postoje konkretni i pouzdani dokazi o postojanju UI sustava koji su obuhvaćeni područjem primjene Priloga III., ali ne predstavljaju znatan rizik od štete za zdravlje, sigurnost ili temeljna prava fizičkih osoba.

7. Komisija donosi delegirane akte u skladu s člankom 97. radi izmjene stavka 3. drugog podstavka ovog članka brisanjem bilo kojeg od uvjeta utvrđenih u stavku 3. drugom podstavku ovog članka ako postoje konkretni i pouzdani dokazi da je to potrebno radi održavanja razine zaštite zdravlja, sigurnosti i temeljnih prava koja je predviđena ovom Uredbom.

8. Nijednom izmjenom uvjeta utvrđenih u stavku 3. drugom podstavku donesenom u skladu sa stavcima 6. i 7. ovog članka ne smije se smanjiti ukupna razina zaštite zdravlja, sigurnosti i temeljnih prava koja je predviđena ovom Uredbom te se njome mora osigurati usklađenost s delegiranim aktima donesenima na temelju članka 7. stavka 1. i uzeti u obzir tržišni i tehnološki razvoj.

Članak 7.

Izmjene Priloga III.

1. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene Priloga III. dodavanjem ili prilagodbom slučajeva upotrebe visokorizičnih UI sustava ako su ispunjena oba sljedeća uvjeta:

- (a) UI sustavi namijenjeni su za korištenje u bilo kojem od područja iz Priloga III.;
- (b) UI sustavi predstavljaju rizik od štete za zdravlje i sigurnost ili rizik od nepovoljnog utjecaja na temeljna prava, a taj je rizik jednakovrijedan riziku ili veći od rizika od štete ili nepovoljnog utjecaja koji predstavljaju visokorizični UI sustavi već navedeni u Prilogu III.

2. Pri procjeni uvjeta iz stavka 1. točke (b) Komisija uzima u obzir sljedeće kriterije:
- (a) namjenu UI sustava;
 - (b) stupanj u kojem se UI sustav upotrebljava ili će se vjerojatno upotrebljavati;
 - (c) prirodu i količinu podataka koje obrađuje i upotrebljava UI sustav, a posebice obrađuju li se posebne kategorije osobnih podataka;
 - (d) stupanj u kojem UI sustav djeluje autonomno i mogućnost da čovjek nadjača odluku ili preporuke koje bi mogle prouzročiti štetu;
 - (e) stupanj u kojem je upotreba UI sustava već prouzročila štetu za zdravlje ili sigurnost ili imala nepovoljan utjecaj na temeljna prava ili izazvala ozbiljnu zabrinutost da bi mogla prouzročiti takvu štetu ili nepovoljan utjecaj, kako je, primjerice, potvrđeno u izvješćima ili dokumentiranim navodima koji su podneseni nacionalnim nadležnim tijelima ili u drugim izvješćima, ovisno o slučaju;
 - (f) potencijalne razmjere takve štete ili takvog nepovoljnog utjecaja, osobito u smislu intenziteta i mogućnosti da pogodi više osoba ili da nerazmjerno pogodi određenu skupinu osoba;
 - (g) stupanj u kojem potencijalno oštećene osobe ili osobe izložene nepovoljnom utjecaju ovise o ishodu upotrebe UI sustava, osobito ako taj ishod nije razumno moguće ne prihvatiti zbog praktičnih ili pravnih razloga;
 - (h) stupanj u kojem postoji neravnoteža moći ili su potencijalno oštećene osobe ili osobe izložene nepovoljnom utjecaju u ranjivu položaju u odnosu na subjekt koji uvodi UI sustav, osobito zbog statusa, autoriteta, znanja, ekonomskih ili socijalnih okolnosti ili dobi;
 - (i) stupanj u kojem je ishod nastao upotrebom UI sustava lako ispravljiv ili poništiv, uzimajući u obzir tehnička rješenja dostupna za njegovo ispravljanje ili poništenje, pri čemu se smatra da ishodi koji nepovoljno utječu na zdravlje, sigurnost ili temeljna prava nisu lako ispravljivi ili poništivi;
 - (j) razmjer i vjerojatnost koristi od uvođenja UI sustava za pojedince, skupine ili društvo u cjelini, uključujući moguća poboljšanja sigurnosti proizvoda;
 - (k) stupanj u kojem se postojećim pravom Unije predviđaju:
 - i. djelotvorne mjere pravne zaštite od rizika koji predstavlja UI sustav, uz iznimku zahtjeva za naknadu štete;
 - ii. djelotvorne mjere za sprečavanje ili što veće smanjenje tih rizika.
3. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene popisa iz Priloga III. uklanjanjem visokorizičnih UI sustava ako su ispunjena oba sljedeća uvjeta:
- (a) dotični visokorizični UI sustav više ne predstavlja znatan rizik za temeljna prava, zdravlje ili sigurnost, uzimajući u obzir kriterije navedene u stavku 2.;
 - (b) brisanjem se ne smanjuje ukupna razina zaštite zdravlja, sigurnosti i temeljnih prava na temelju prava Unije.

ODJELJAK 2.

Zahtjevi za visokorizične UI sustave

Članak 8.

Ispunjavanje zahtjeva

1. Visokorizični UI sustavi mora ispunjavati zahtjeve utvrđene u ovom odjeljku, uzimajući u obzir njihovu namjenu i općepriznata najnovija dostignuća u području umjetne inteligencije i tehnologija povezanih s umjetnom inteligencijom. Pri osiguravanju ispunjavanja tih zahtjeva u obzir se uzima sustav upravljanja rizikom iz članka 9.

2. Ako proizvod sadržava UI sustav na koji se primjenjuju zahtjevi ove Uredbe i zahtjevi zakonodavstva Unije o usklađivanju iz odjeljka A Priloga I., dobavljači su odgovorni za osiguravanje potpune usklađenosti njihova proizvoda sa svim primjenjivim zahtjevima na temelju primjenjivog zakonodavstva Unije o usklađivanju. Pri osiguravanju usklađenosti visokorizičnih UI sustava iz stavka 1. sa zahtjevima utvrđenima u ovom odjeljku te kako bi se osigurala dosljednost, izbjeglo udvostručavanje i na najmanju moguću mjeru svela dodatna opterećenja, dobavljači imaju mogućnost da potrebne postupke testiranja i izvješćivanja, informacije i dokumentaciju koje pružaju u vezi sa svojim proizvodom prema potrebi integriraju u dokumentaciju i postupke koji već postoje i koji se zahtijevaju na temelju zakonodavstva Unije o usklađivanju navedenog u odjeljku A Priloga I.

Članak 9.

Sustav upravljanja rizikom

1. Za visokorizične UI sustave uspostavlja se, primjenjuje i održava sustav upravljanja rizikom te se o njemu vodi dokumentacija.

2. Sustav upravljanja rizikom shvaća se kao kontinuiran iterativan proces koji se planira i izvodi tijekom cijelog životnog ciklusa visokorizičnog UI sustava i koji je potrebno redovito i sustavno preispitivati i ažurirati. Obuhvaća sljedeće korake:

- (a) utvrđivanje i analizu poznatih i razumno predvidljivih rizika koje visokorizični UI sustav može predstavljati za zdravlje, sigurnost ili temeljna prava kada se visokorizični UI sustav koristi u skladu sa svojom namjenom;
- (b) procjenjivanje i evaluaciju rizika koji mogu nastati pri korištenju visokorizičnog UI sustava u skladu s njegovom namjenom i u uvjetima razumno predvidljive pogrešne upotrebe;
- (c) evaluaciju drugih potencijalnih rizika na temelju analize podataka prikupljenih sustavom praćenja nakon stavljanja na tržište iz članka 72.;
- (d) donošenje odgovarajućih i ciljanih mjera upravljanja rizikom osmišljenih za uklanjanje rizika utvrđenih na temelju točke (a).

3. Rizici iz ovog članka odnose se samo na one rizike koji se mogu razumno ublažiti ili ukloniti razvijanjem ili dizajnom visokorizičnog UI sustava ili pružanjem adekvatnih tehničkih informacija.

4. U mjerama upravljanja rizikom iz stavka 2. točke (d) na odgovarajući način uzimaju se u obzir učinci i moguća interakcija koji proizlaze iz kombinirane primjene zahtjeva utvrđenih u ovom odjeljku, u cilju djelotvornijeg svođenja rizika na najmanju moguću mjeru i istodobnog postizanja odgovarajuće ravnoteže u provedbi mjera za ispunjavanje tih zahtjeva.

5. Mjere upravljanja rizikom iz stavka 2. točke (d) takve su da su relevantni preostali rizik povezan sa svakom pojedinom opasnošću kao i cjelokupni preostali rizik visokorizičnih UI sustava procijenjeni prihvatljivima.

Pri utvrđivanju najprikladnijih mjera upravljanja rizikom osigurava se sljedeće:

- (a) uklanjanje ili smanjenje rizika utvrđenih i evaluiranih na temelju stavka 2. u mjeri u kojoj je to tehnički izvedivo putem adekvatnog dizajna i razvoja visokorizičnog UI sustava;
- (b) prema potrebi, provedba adekvatnih mjera za ublažavanje i kontrolu rizika koji se ne mogu ukloniti;
- (c) pružanje informacija koje se zahtijevaju u skladu s člankom 13. i, prema potrebi, osposobljavanja za subjekte koji uvode sustav.

U cilju uklanjanja ili smanjenja rizika povezanih s korištenjem visokorizičnog UI sustava u obzir se na odgovarajući način uzimaju tehničko znanje, iskustvo, obrazovanje i osposobljavanje koje treba očekivati od subjekta koji uvodi sustav te pretpostavljeni kontekst u kojem se sustav namjerava koristiti.

6. Visokorizični UI sustavi testiraju se kako bi se utvrdile najprikladnije i ciljane mjere upravljanja rizikom. Testiranjem se osigurava da visokorizični UI sustavi postojano rade u skladu sa svojom namjenom i da ispunjavaju zahtjeve utvrđene u ovom odjeljku.
7. Postupci testiranja mogu uključivati testiranje u stvarnim uvjetima u skladu s člankom 60.
8. Visokorizični UI sustavi testiraju se prema potrebi u bilo kojem trenutku razvojnog procesa, a u svakom slučaju prije stavljanja na tržište ili u upotrebu. Testiranje se provodi u odnosu na prethodno definirane parametre i probabilističke pragove koji su primjereni za namjenu visokorizičnog UI sustava.
9. Pri provedbi sustava upravljanja rizikom predviđenog u stavcima od 1. do 7. dobavljači razmatraju je li vjerojatno da će, s obzirom na njegovu namjenu, visokorizični UI sustav imati nepovoljan utjecaj na osobe mlađe od 18 godina i, prema potrebi, na druge skupine ranjivih osoba.
10. Kad je riječ o dobavljačima visokorizičnih UI sustava na koje se primjenjuju zahtjevi u pogledu unutarnjih procesa upravljanja rizikom na temelju drugih relevantnih odredaba prava Unije, aspekti iz stavaka od 1. do 9. mogu biti dio postupaka upravljanja rizikom uspostavljenih na temelju tog prava ili se kombinirati s tim postupcima.

Članak 10.

Podaci i upravljanje podacima

1. Visokorizični UI sustavi koji upotrebljavaju tehnike s treniranjem UI modelâ s pomoću podataka moraju se razvijati na temelju skupova podataka za treniranje, validaciju i testiranje koji ispunjavaju kriterije kvalitete iz stavaka od 2. do 5. kad god se takvi skupovi podataka upotrebljavaju.
2. Na skupove podataka za treniranje, validaciju i testiranje primjenjuju se prakse upravljanja i rukovanja podacima prikladne za namjenu visokorizičnog UI sustava. Te se prakse ponajprije odnose na:
 - (a) relevantne odluke o dizajnu;
 - (b) procese prikupljanja podataka i podrijetlo podataka te, u slučaju osobnih podataka, izvornu svrhu prikupljanja podataka;
 - (c) relevantne postupke obrade za pripremu podataka, kao što su obilježavanje, označivanje, čišćenje, ažuriranje, obogaćivanje i agregiranje;
 - (d) formuliranje pretpostavki, osobito s obzirom na informacije koje bi podaci trebali mjeriti i predstavljati;
 - (e) procjenu raspoloživosti, količine i prikladnosti potrebnih skupova podataka;
 - (f) ispitivanje s obzirom na moguće pristranosti koje bi mogle utjecati na zdravlje i sigurnost osoba, imati negativan utjecaj na temeljna prava ili dovesti do diskriminacije zabranjene pravom Unije, posebno ako izlazni podaci utječu na ulazne podatke za buduće operacije;
 - (g) odgovarajuće mjere za otkrivanje, sprečavanje i ublažavanje mogućih pristranosti utvrđenih u skladu s točkom (f);
 - (h) utvrđivanje relevantnih nedostataka u podacima ili drugih nedostataka koji onemogućuju usklađivanje s ovom Uredbom te načina na koji se ti nedostaci mogu ukloniti.
3. Skupovi podataka za treniranje, validaciju i testiranje moraju biti relevantni, dovoljno reprezentativni te, u najvećoj mogućoj mjeri, bez pogrešaka i potpuni s obzirom na namjenu. Moraju imati odgovarajuća statistička obilježja, među ostalim u odnosu na osobe ili skupine osoba u pogledu kojih se visokorizični UI sustav namjerava koristiti, ako je primjenjivo. Te se karakteristike skupova podataka mogu postići na razini pojedinačnih skupova podataka ili na razini kombinacije skupova podataka.
4. U skupovima podataka moraju se uzeti u obzir, u mjeri u kojoj to iziskuje namjena, karakteristike ili elementi specifični za zemljopisno, kontekstualno, bihevioralno ili radno okruženje u kojem se visokorizični UI sustav namjerava koristiti.

5. U mjeri u kojoj je to nužno u svrhu osiguravanja otkrivanja i ispravljanja pristranosti u vezi s visokorizičnim UI sustavima u skladu sa stavkom 2. točkama (f) i (g) ovog članka, dobavljači takvih sustava mogu iznimno obrađivati posebne kategorije osobnih podataka, podložno odgovarajućim zaštitnim mjerama za temeljna prava i slobode fizičkih osoba. Kako bi se takva obrada provela, uz odredbe utvrđene u uredbama (EU) 2016/679 i (EU) 2018/1725 te Direktivi (EU) 2016/680 moraju se ispuniti svi sljedeći uvjeti:

- (a) otkrivanje i ispravljanje pristranosti ne može se djelotvorno postići obradom drugih podataka, uključujući sintetičke ili anonimizirane podatke;
- (b) posebne kategorije osobnih podataka podliježu tehničkim ograničenjima u pogledu ponovne upotrebe osobnih podataka i najsuvremenijim mjerama sigurnosti i zaštite privatnosti, uključujući pseudonimizaciju;
- (c) posebne kategorije osobnih podataka podliježu mjerama kojima se osigurava da su obrađeni osobni podaci osigurani i zaštićeni, podložno odgovarajućim zaštitnim mjerama, uključujući stroge kontrole i dokumentaciju pristupa, kako bi se izbjegla pogrešna upotreba i osiguralo da pristup tim osobnim podacima imaju samo ovlaštene osobe i uz odgovarajuće obveze u pogledu povjerljivosti;
- (d) posebne kategorije osobnih podataka ne smiju se prenositi, prosljeđivati niti im druge strane smiju na neki drugi način pristupiti;
- (e) posebne kategorije osobnih podataka brišu se nakon ispravljanja pristranosti ili završetka razdoblja čuvanja osobnih podataka, ovisno o tome što nastupi ranije;
- (f) evidencija aktivnosti obrade na temelju uredbi (EU) 2016/679 i (EU) 2018/1725 te Direktive (EU) 2016/680 sadržava razloge zbog kojih je obrada posebnih kategorija osobnih podataka bila nužna za otkrivanje i ispravljanje pristranosti te zbog kojih se taj cilj nije mogao postići obradom drugih podataka.

6. Kad je riječ o razvoju visokorizičnih UI sustava u kojima se ne upotrebljavaju tehnike koje uključuju treniranje UI modelâ, stavci od 2. do 5. primjenjuju se samo na skupove podataka za testiranje.

Članak 11.

Tehnička dokumentacija

1. Tehnička dokumentacija visokorizičnog UI sustava sastavlja se prije njegova stavljanja na tržište ili u upotrebu te se ažurira.

Tehnička dokumentacija sastavlja se tako da se njome dokaže da visokorizični UI sustav ispunjava zahtjeve utvrđene u ovom odjeljku te da se nacionalnim nadležnim tijelima i prijavljenim tijelima na jasan i sveobuhvatan način pruže informacije potrebne za ocjenjivanje usklađenosti UI sustava s tim zahtjevima. Tehnička dokumentacija sadržava barem elemente utvrđene u Prilogu IV. MSP-ovi, uključujući *start-up* poduzeća, mogu elemente tehničke dokumentacije iz Priloga IV. dostaviti na pojednostavnjen način. U tom cilju Komisija utvrđuje pojednostavnjeni obrazac za tehničku dokumentaciju namijenjen potrebama malih poduzeća i mikropoduzeća. Ako MSP, uključujući *start-up* poduzeće, odluči na pojednostavnjen način dostaviti informacije koje se zahtijevaju u Prilogu IV., koristi se obrascem na koji se upućuje u ovom stavku. Prijavljena tijela prihvaćaju taj obrazac u svrhu ocjenjivanja sukladnosti.

2. Ako se na tržište ili u upotrebu stavlja visokorizični UI sustav povezan s proizvodom koji je obuhvaćen zakonodavstvom Unije o usklađivanju navedenim u odjeljku A Priloga I., sastavlja se jedinstvena tehnička dokumentacija koja sadržava sve informacije utvrđene u stavku 1., kao i informacije koje se zahtijevaju tim pravnim aktima.

3. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene, prema potrebi, Priloga IV. kako bi se osiguralo da, s obzirom na tehnički napredak, tehnička dokumentacija sadržava sve informacije potrebne za ocjenjivanje usklađenosti sustava sa zahtjevima utvrđenima u ovom odjeljku.

Članak 12.

Čuvanje evidencije

1. Kod visokorizičnih UI sustava mora biti tehnički omogućeno automatsko evidentiranje događaja („evidencija”) tijekom cijelog životnog ciklusa sustava.
2. Kako bi se osigurala određena razina sljedivosti funkcioniranja visokorizičnog UI sustava koja je u skladu s namjenom sustava, funkcije evidentiranja događaja omogućuju evidentiranje događaja relevantnih za:
 - (a) utvrđivanje situacija koje mogu dovesti do toga da visokorizični UI sustav predstavlja rizik u smislu članka 79. stavka 1. ili do znatne izmjene;
 - (b) olakšavanje praćenja nakon stavljanja na tržište iz članka 72.; i
 - (c) praćenje rada visokorizičnih UI sustava iz članka 26. stavka 5.
3. Kad je riječ o visokorizičnim UI sustavima iz točke 1. podtočke (a) Priloga III., funkcijama evidentiranja evidentira se najmanje:
 - (a) razdoblje svake upotrebe sustava (datum i vrijeme početka te datum i vrijeme završetka svake upotrebe);
 - (b) referentna baza podataka s kojom je sustav usporedio ulazne podatke;
 - (c) ulazni podaci za koje je pretragom utvrđena podudarnost;
 - (d) identitet fizičkih osoba iz članka 14. stavka 5. koje su sudjelovale u provjeri rezultata.

Članak 13.

Transparentnost i pružanje informacija subjektima koji uvode sustav

1. Visokorizični UI sustavi dizajniraju se i razvijaju na takav način da se osigura da je njihov rad dovoljno transparentan kako bi se subjektima koji uvode sustav omogućilo da tumače izlazne podatke sustava i primjereno ih upotrebljavaju. Osiguravaju se odgovarajuća vrsta i stupanj transparentnosti kako bi se ispunile relevantne obveze dobavljača i subjekta koji uvodi sustav utvrđene u odjeljku 3.
2. Visokorizičnim UI sustavima prilažu se upute za korištenje u odgovarajućem digitalnom ili drugom formatu sa sažetom, potpunom, točnim i jasnim informacijama koje su subjektima koji uvode sustav relevantne, pristupačne i razumljive.
3. Upute za korištenje sadržavaju barem sljedeće informacije:
 - (a) identitet i kontaktne podatke dobavljača i, ako je primjenjivo, njegova ovlaštenog zastupnika;
 - (b) karakteristike, sposobnosti i ograničenja učinkovitosti visokorizičnog UI sustava, uključujući:
 - i. njegovu namjenu;
 - ii. razinu točnosti, uključujući njezine parametre, te razinu otpornosti i kibernetičke sigurnosti iz članka 15. u odnosu na koju je visokorizični UI sustav testiran i validiran i koja se može očekivati, te sve poznate i predvidljive okolnosti koje mogu utjecati na tu očekivanu razinu točnosti, otpornosti i kibernetičke sigurnosti;
 - iii. sve poznate ili predvidljive okolnosti povezane s korištenjem visokorizičnog UI sustava u skladu s njegovom namjenom ili u uvjetima razumno predvidljive pogrešne upotrebe koje mogu prouzročiti rizike za zdravlje i sigurnost ili temeljna prava iz članka 9. stavka 2.;
 - iv. ako je primjenjivo, tehničke sposobnosti i karakteristike visokorizičnog UI sustava za pružanje informacija koje su relevantne za objašnjenje njegovih izlaznih podataka;

- v. prema potrebi, učinkovitost sustava u odnosu na konkretne osobe ili skupine osoba na kojima se sustav namjerava koristiti;
 - vi. prema potrebi, specifikacije ulaznih podataka ili sve ostale relevantne informacije o korištenim skupovima podataka za treniranje, validaciju i testiranje, uzimajući u obzir namjenu visokorizičnog UI sustava;
 - vii. ako je primjenjivo, informacije koje subjektima koji uvode sustav omogućuju tumačenje izlaznih podataka visokorizičnog UI sustava i njihovu prikladnu upotrebu;
- (c) eventualne promjene visokorizičnog UI sustava i njegove učinkovitosti koje je dobavljač unaprijed odredio u trenutku početnog ocjenjivanja sukladnosti;
 - (d) mjere ljudskog nadzora iz članka 14., uključujući tehničke mjere uvedene kako bi se subjektima koji uvode sustav olakšalo tumačenje izlaznih podataka visokorizičnih UI sustava;
 - (e) potrebne računalne i hardverske resurse, očekivani životni ciklus visokorizičnog UI sustava i sve potrebne mjere održavanja i brige, uključujući njihovu učestalost, kako bi se osiguralo pravilno funkcioniranje tog UI sustava, što se odnosi i na softverska ažuriranja;
 - (f) prema potrebi, opis mehanizama uključenih u visokorizični UI sustav koji omogućuje subjektima koji uvode sustav da pravilno prikupljaju, pohranjuju i tumače evidenciju u skladu s člankom 12.

Članak 14.

Ljudski nadzor

1. Visokorizični UI sustavi dizajniraju se i razvijaju na takav način, među ostalim s odgovarajućim alatima sučelja čovjek-stroj, da ih fizičke osobe mogu djelotvorno nadzirati tijekom njihove upotrebe.
2. Cilj je ljudskog nadzora spriječiti ili što više smanjiti rizike za zdravlje, sigurnost ili temeljna prava koji se mogu pojaviti tijekom upotrebe visokorizičnog UI sustava u skladu s njegovom namjenom ili u uvjetima razumno predvidljive pogrešne upotrebe, osobito ako takvi rizici i dalje postoje unatoč primjeni drugih zahtjeva utvrđenih u ovom odjeljku.
3. Mjere nadzora razmjerne su rizicima, razini autonomije i kontekstu korištenja visokorizičnog UI sustava, a osiguravaju se barem jednom od sljedećih vrsta mjera:
 - (a) mjerama koje dobavljač utvrđuje i ugrađuje, ako je to tehnički izvedivo, u visokorizični UI sustav prije njegova stavljanja na tržište ili u upotrebu;
 - (b) mjerama koje dobavljač utvrđuje prije stavljanja visokorizičnog UI sustava na tržište ili u upotrebu, a koje su primjerene da ih provodi subjekt koji uvodi sustav.
4. Za potrebe provedbe stavaka 1., 2. i 3. visokorizični UI sustav isporučuje se subjektu koji uvodi sustav na takav način da fizičke osobe kojima je povjeren ljudski nadzor mogu, ako je to potrebno i razmjerno:
 - (a) pravilno razumjeti relevantne kapacitete i ograničenja visokorizičnog UI sustava i biti sposobne na odgovarajući način pratiti njegov rad, među ostalim radi otkrivanja i uklanjanja nepravilnosti, disfunkcija i neočekivanih rezultata;
 - (b) biti na oprezu u pogledu moguće tendencije automatskog ili pretjeranog oslanjanja na izlazne podatke visokorizičnog UI sustava („automatizacijska pristranost”), osobito kad je riječ o visokorizičnim UI sustavima koji se upotrebljavaju za davanje informacija ili preporuka na temelju kojih odluke donose fizičke osobe;
 - (c) točno protumačiti izlazne podatke visokorizičnog UI sustava, uzimajući u obzir, primjerice, dostupne alate i metode za tumačenje;

- (d) u određenoj situaciji odustati od upotrebe visokorizičnog UI sustava ili na neki drugi način zanemariti, nadjačati ili poništiti izlazni podatak visokorizičnog UI sustava;
- (e) intervenirati u rad visokorizičnog UI sustava ili prekinuti rad sustava pritiskom gumba za zaustavljanje ili sličnim postupkom koji omogućuje sigurno zaustavljanje sustava.

5. Kad je riječ o visokorizičnim UI sustavima iz točke 1. podtočke (a) Priloga III., mjerama iz stavka 3. ovog članka mora se usto osigurati da subjekt koji uvodi sustav ne poduzima nikakve radnje ili odluke na temelju identifikacije proizišle iz sustava ako identifikaciju nisu zasebno provjerile i potvrdile barem dvije fizičke osobe koje imaju potrebne kompetencije, osposobljenost i ovlasti.

Zahtjev da najmanje dvije fizičke osobe moraju provesti zasebnu provjeru ne primjenjuje se na visokorizične UI sustave koji se upotrebljavaju u svrhu kaznenog progona, migracija, nadzora državne granice ili azila ako se u pravu Unije ili nacionalnom pravu primjena tog zahtjeva smatra nerazmjernom.

Članak 15.

Točnost, otpornost i kibernetička sigurnost

1. Visokorizični UI sustavi dizajniraju se i razvijaju tako da postignu odgovarajuću razinu točnosti, otpornosti i kibernetičke sigurnosti te da im je u tim aspektima radni učinak tijekom cijelog životnog ciklusa konstantan.

2. Kako bi se uvažili tehnički aspekti načina mjerenja odgovarajućih razina točnosti i otpornosti iz stavka 1. i ostali relevantni parametri učinkovitosti, Komisija u suradnji s relevantnim dionicima i organizacijama, kao što su tijela za mjeriteljstvo i utvrđivanje referentnih vrijednosti, prema potrebi potiče razvoj referentnih vrijednosti i metodologija mjerenja.

3. Razine točnosti i relevantni parametri točnosti visokorizičnih UI sustava navode se u popratnim uputama za korištenje.

4. Visokorizični UI sustavi moraju biti otporni što je više moguće na greške, kvarove ili nedosljednosti koji se mogu dogoditi unutar sustava ili okruženja u kojem sustav radi, osobito zbog njihove interakcije s fizičkim osobama ili drugim sustavima. U tom se pogledu moraju poduzimati tehničke i organizacijske mjere.

Otpornost visokorizičnih UI sustava može se postići tehničkom redundancijom, što može uključivati pričuvene planove ili sigurnosne planove.

Visokorizični UI sustavi koji nastavljaju učiti nakon stavljanja na tržište ili u upotrebu razvijaju se na takav način da se otkloni ili na najmanju moguću mjeru svede rizik od potencijalno pristranih izlaznih podataka koji utječu na ulazne podatke u budućim operacijama („povratne veze”) te da se osigura da se na takve eventualne povratne veze na odgovarajući način reagira primjerenim mjerama ublažavanja.

5. Visokorizični UI sustavi moraju biti otporni na pokušaje neovlaštenih trećih strana da im izmijene upotrebu, izlazne podatke ili učinkovitost iskorištavanjem slabih točaka sustava.

Tehnička rješenja za osiguravanje kibernetičke sigurnosti visokorizičnih UI sustava moraju biti primjerena relevantnim okolnostima i rizicima.

Tehnička rješenja za prevladavanje specifičnih slabih točaka umjetne inteligencije obuhvaćaju, prema potrebi, mjere za sprečavanje, otkrivanje, odgovor, rješavanje i kontrolu u vezi s napadima čiji je cilj manipuliranje skupom podataka za treniranje („trovanje podataka”) ili prethodno treniranim komponentama koje se upotrebljavaju u treniranju („trovanje modela”), ulaznim podacima osmišljenima kako bi UI model načinio pogrešku („neprijateljski primjeri”) ili „zaobilazanje modela”), napadima na povjerljivost ili nedostacima modela.

ODJELJAK 3.

Obveze dobavljača visokorizičnih UI sustava i subjekata koji ih uvode te drugih strana

Članak 16.

Obveze dobavljača visokorizičnih UI sustava

Dobavljači visokorizičnih UI sustava:

- (a) osiguravaju da njihovi visokorizični UI sustavi ispunjavaju zahtjeve utvrđene u odjeljku 2.;
- (b) na visokorizičnom UI sustavu ili, ako to nije moguće, na njegovoj ambalaži ili u njegovoj popratnoj dokumentaciji, ovisno o slučaju, navode svoje ime, registrirano trgovačko ime ili registrirani žig te adresu za kontakt;
- (c) imaju uspostavljen sustav upravljanja kvalitetom koji je u skladu s člankom 17.;
- (d) vode dokumentaciju iz članka 18.;
- (e) čuvaju evidenciju koju automatski generiraju njihovi visokorizični UI sustavi dok su pod njihovom kontrolom, kako je navedeno u članku 19.;
- (f) osiguravaju da visokorizični UI sustav prije stavljanja na tržište ili u upotrebu prođe relevantni postupak ocjenjivanja sukladnosti iz članka 43.;
- (g) sastavljaju EU izjavu o sukladnosti u skladu s člankom 47.;
- (h) stavljaju oznaku CE na visokorizični UI sustav ili, ako to nije moguće, na njegovu ambalažu ili u njegovu popratnu dokumentaciju kako bi se označila sukladnost s ovom Uredbom, u skladu s člankom 48.;
- (i) ispunjavaju obveze registracije iz članka 49. stavka 1.;
- (j) poduzimaju potrebne korektivne mjere i pružaju informacije u skladu s člankom 20.;
- (k) na obrazloženi zahtjev nacionalnog nadležnog tijela dokazuju sukladnost visokorizičnog UI sustava sa zahtjevima utvrđenima u odjeljku 2.;
- (l) osiguravaju da visokorizični UI sustav ispunjava zahtjeve u pogledu pristupačnosti u skladu s direktivama (EU) 2016/2102 i (EU) 2019/882.

Članak 17.

Sustav upravljanja kvalitetom

1. Dobavljači visokorizičnih UI sustava uspostavljaju sustav upravljanja kvalitetom kojim se osigurava usklađenost s ovom Uredbom. O tom se sustavu na sustavan i uredan način sastavlja dokumentacija u obliku pisanih politika, postupaka i uputa, a obuhvaća barem sljedeće aspekte:

- (a) strategiju za usklađenost s propisima, uključujući usklađenost s postupcima ocjenjivanja sukladnosti i postupcima za upravljanje izmjenama visokorizičnog UI sustava;
- (b) tehnike, postupke i sustavne aktivnosti koji se moraju provoditi u dizajnu te kontroli i provjeri dizajna visokorizičnog UI sustava;
- (c) tehnike, postupke i sustavne aktivnosti koji se moraju provoditi u razvoju te kontroli kvalitete i osiguravanju kvalitete visokorizičnog UI sustava;
- (d) postupke ispitivanja, testiranja i validacije koji se moraju provoditi prije, tijekom i poslije razvoja visokorizičnog UI sustava te učestalost kojom se moraju provoditi;

- (e) tehničke specifikacije, uključujući norme, koje se moraju primjenjivati i, ako relevantne usklađene norme nisu u cijelosti primijenjene ili ne obuhvaćaju sve relevantne zahtjeve utvrđene u odjeljku 2., sredstva koja se moraju upotrijebiti kako bi se osigurala usklađenost visokorizičnog UI sustava s tim zahtjevima;
 - (f) sustave i postupke za upravljanje podacima, uključujući pribavljanje podataka, prikupljanje podataka, analizu podataka, označivanje podataka, pohranu podataka, filtriranje podataka, rudarenje podataka, agregiranje podataka, zadržavanje podataka i sve druge operacije s podacima koje se obavljaju prije stavljanja visokorizičnih UI sustava na tržište ili u upotrebu i u svrhu tog stavljanja;
 - (g) sustav upravljanja rizikom iz članka 9.;
 - (h) uspostavu, primjenu i održavanje sustava praćenja nakon stavljanja na tržište u skladu s člankom 72.;
 - (i) postupke povezane s prijavljivanjem ozbiljnog incidenta u skladu s člankom 73.;
 - (j) postupke komunikacije s nacionalnim nadležnim tijelima, drugim relevantnim tijelima, uključujući tijela za pružanje ili olakšavanje pristupa podacima, prijavljenim tijelima, drugim operaterima, klijentima ili drugim zainteresiranim stranama;
 - (k) sustave i postupke za čuvanje evidencije o svojoj relevantnoj dokumentaciji i svim relevantnim informacijama;
 - (l) upravljanje resursima, uključujući mjere koje se odnose na sigurnost opskrbe;
 - (m) okvir za odgovornost kojim se utvrđuju odgovornosti uprave i drugog osoblja za sve aspekte navedene u ovom stavku.
2. Aspekti iz stavka 1. provode se razmjerno veličini dobavljačeve organizacije. Dobavljači u svakom slučaju moraju poštovati stupanj strogosti i razinu zaštite koji su potrebni kako bi se osigurala usklađenost njihovih UI sustava s ovom Uredbom.
3. Dobavljači visokorizičnih UI sustava koji podliježu obvezama u pogledu sustavâ upravljanja kvalitetom ili jednakovrijedne funkcije na temelju relevantnog sektorskog prava Unije mogu uključiti aspekte navedene u stavku 1. u sustave upravljanja kvalitetom u skladu s tim pravom.
4. Kad je riječ o dobavljačima koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu njihova unutarnjeg upravljanja, njihovih aranžmana ili njihovih procesa na temelju prava Unije o financijskim uslugama, obveza uspostave sustava upravljanja kvalitetom, uz iznimku stavka 1. točaka (g), (h) i (i) ovog članka, smatra se ispunjenom ako se poštuju pravila o unutarnjem upravljanju, aranžmanima ili procesima u skladu s relevantnim pravom Unije o financijskim uslugama. U tom se cilju u obzir uzimaju sve usklađene norme iz članka 40.

Članak 18.

Čuvanje dokumentacije

1. Tijekom razdoblja od deset godina nakon što je visokorizični UI sustav umjetne inteligencije stavljen na tržište ili u upotrebu dobavljač nacionalnim nadležnim tijelima na raspolaganju drži:
- (a) tehničku dokumentaciju iz članka 11.;
 - (b) dokumentaciju o sustavu upravljanja kvalitetom iz članka 17.;
 - (c) dokumentaciju o promjenama koje su odobrila prijavljena tijela, ako je primjenjivo;
 - (d) odluke i druge dokumente koje su izdala prijavljena tijela, ako je primjenjivo;
 - (e) EU izjavu o sukladnosti iz članka 47.

2. Svaka država članica određuje uvjete pod kojima dokumentacija iz stavka 1. ostaje na raspolaganju nacionalnim nadležnim tijelima tijekom razdoblja navedenog u tom stavku u slučaju da dobavljač ili njegov ovlašten zastupnik s poslovnim nastanom na njezinu državnom području proglasi stečaj ili prestane s radom prije kraja tog razdoblja.

3. Dobavljači koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu njihova unutarnjeg upravljanja, njihovih aranžmana ili njihovih procesa na temelju prava Unije o financijskim uslugama čuvaju tehničku dokumentaciju u sklopu dokumentacije koja se čuva na temelju relevantnog prava Unije o financijskim uslugama.

Članak 19.

Automatski generirana evidencija

1. Dobavljači visokorizičnih UI sustava čuvaju evidenciju iz članka 12. stavka 1. koju automatski generiraju njihovi visokorizični UI sustavi u mjeri u kojoj je takva evidencija pod njihovom kontrolom. Ne dovodeći u pitanje primjenjivo pravo Unije ili nacionalno pravo, evidencija se čuva u razdoblju koje je primjereno namjeni visokorizičnog UI sustava, a najmanje šest mjeseci, osim ako je drukčije predviđeno u primjenjivom pravu Unije ili nacionalnom pravu, a posebno u pravu Unije o zaštiti osobnih podataka.

2. Dobavljači koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu njihova unutarnjeg upravljanja, njihovih aranžmana ili njihovih procesa na temelju prava Unije o financijskim uslugama čuvaju evidenciju koju automatski generiraju njihovi visokorizični UI sustavi u sklopu dokumentacije koja se čuva na temelju relevantnog prava o financijskim uslugama.

Članak 20.

Korektivne mjere i obveza obavješćivanja

1. Dobavljači visokorizičnih UI sustava koji smatraju ili imaju razloga smatrati da visokorizični UI sustav koji su stavili na tržište ili u upotrebu nije sukladan s ovom Uredbom odmah poduzimaju potrebne korektivne mjere kako bi, prema potrebi, postigli sukladnost tog sustava s ovom Uredbom, povukli ga, onesposobili ili ga opozvali. O dotičnom visokorizičnom UI sustavu na odgovarajući obavješćuju distributere i, ako je primjenjivo, subjekte koji uvode sustav, ovlaštenog zastupnika i uvoznike.

2. Ako visokorizični UI sustav predstavlja rizik u smislu članka 79. stavka 1. i dobavljač sustava sazna za taj rizik, on odmah istražuje uzroke, ako je primjenjivo u suradnji sa subjektom koji uvodi sustav i koji je to prijavio, te obavješćuje tijela za nadzor tržišta koja su nadležna za dotični visokorizični UI i, ako je primjenjivo, prijavljeno tijelo koje je izdalo potvrdu za taj visokorizični UI sustav u skladu s člankom 44., osobito o prirodi neusklađenosti i relevantnim korektivnim mjerama koje su eventualno već poduzete.

Članak 21.

Suradnja s nadležnim tijelima

1. Dobavljači visokorizičnih UI sustava nadležnom tijelu na njegov obrazloženi zahtjev dostavljaju sve informacije i dokumentaciju koji su potrebni za dokazivanje sukladnosti visokorizičnog UI sustava sa zahtjevima utvrđenima u odjeljku 2. na jednom od službenih jezika institucija Unije koji je navela dotična država članica i koji to tijelo može bez poteškoća razumjeti.

2. Na obrazloženi zahtjev nadležnog tijela dobavljači nadležnom tijelu koje je podnijelo zahtjev, ako je primjenjivo, također daju pristup automatski generiranoj evidenciji visokorizičnog UI sustava iz članka 12. stavka 1. u mjeri u kojoj je takva evidencija pod njihovom kontrolom.

3. Sa svim informacijama koje nadležno tijelo pribavi na temelju ovog članka postupa se u skladu s obvezama u pogledu povjerljivosti utvrđenima u članku 78.

Članak 22.

Ovlašteni zastupnici dobavljača visokorizičnih UI sustava

1. Prije stavljanja svojih visokorizičnih UI sustava na tržište Unije dobavljači s poslovnim nastanom u trećim zemljama pisanim ovlaštenjem imenuju ovlaštenog zastupnika s poslovnim nastanom u Uniji.
2. Dobavljač omogućuje svojem ovlaštenom zastupniku da obavlja zadaće navedene u ovlaštenju koje je dobio od dobavljača.
3. Ovlašteni zastupnik obavlja zadaće navedene u ovlaštenju koje je dobio od dobavljača. On na zahtjev dostavlja primjerak ovlaštenja tijelima za nadzor tržišta na jednom od službenih jezika institucije Unije koji je navelo nadležno tijelo. Za potrebe ove Uredbe ovlaštenjem se ovlaštenom zastupniku daje ovlast da obavlja sljedeće zadaće:
 - (a) provjerava jesu li sastavljene EU izjava o sukladnosti iz članka 47. i tehnička dokumentacija iz članka 11. i je li dobavljač proveo odgovarajući postupak ocjenjivanja sukladnosti;
 - (b) nadležnim tijelima te nacionalnim tijelima iz članka 74. stavka 10., tijekom razdoblja od deset godina nakon što je visokorizični UI sustav stavljen na tržište ili u upotrebu, drži na raspolaganju kontaktne podatke dobavljača koji je imenovao ovlaštenog zastupnika, primjerak EU izjave o sukladnosti iz članka 47., tehničku dokumentaciju i, ako je primjenjivo, potvrdu koju je izdalo prijavljeno tijelo;
 - (c) nadležnom tijelu na obrazloženi zahtjev dostavlja sve informacije i dokumentaciju, uključujući one iz točke (b) ovog podstavka, koji su potrebni za dokazivanje sukladnosti visokorizičnog UI sustava sa zahtjevima utvrđenima u odjeljku 2., što uključuje pristup evidenciji iz članka 12. stavka 1. koju automatski generira visokorizični UI sustav u mjeri u kojoj je takva evidencija pod kontrolom dobavljača;
 - (d) na obrazloženi zahtjev surađuje s nadležnim tijelima u svim aktivnostima koje ta tijela poduzimaju u vezi s visokorizičnim UI sustavom, posebno kako bi se smanjili i ublažili rizici koje predstavlja visokorizični UI sustav;
 - (e) ako je primjenjivo, ispunjava obveze registracije iz članka 49. stavka 1. ili, ako registraciju provodi sam dobavljač, osigurava točnost informacija iz točke 3. odjeljka A Priloga VIII.

Ovlaštenjem se ovlaštenom zastupniku daje ovlast da mu se, uz dobavljača ili umjesto dobavljaču, obraćaju nadležna tijela u vezi sa svim pitanjima povezanim s osiguravanjem usklađenosti s ovom Uredbom.

4. Ovlašteni zastupnik ukida ovlaštenje ako smatra ili ima razloga smatrati da dobavljač postupi protivno svojim obvezama na temelju ove Uredbe. U tom slučaju ovlašteni zastupnik o ukidanju ovlaštenja i razlozima za ukidanje odmah obavješćuje relevantno tijelo za nadzor tržišta i, ako je primjenjivo, relevantno prijavljeno tijelo.

Članak 23.

Obveze uvoznika

1. Prije stavljanja visokorizičnog UI sustava na tržište uvoznici osiguravaju da je sustav sukladan s ovom Uredbom tako da provjere je li:
 - (a) dobavljač visokorizičnog UI sustava proveo relevantni postupak ocjenjivanja sukladnosti iz članka 43.;
 - (b) dobavljač sastavio tehničku dokumentaciju u skladu s člankom 11. i Prilogom IV.;
 - (c) sustav označen oznakom CE te jesu li mu priložene EU izjava o sukladnosti iz članka 47. i upute za korištenje;
 - (d) dobavljač imenovao ovlaštenog zastupnika u skladu s člankom 22. stavkom 1.

2. Ako uvoznik ima dovoljno razloga smatrati da visokorizični UI sustav nije sukladan s ovom Uredbom, da je krivotvoren ili da mu je priložena krivotvorena dokumentacija, ne stavlja taj sustav na tržište dok on ne postane sukladan s ovom Uredbom. Ako visokorizični UI sustav predstavlja rizik u smislu članka 79. stavka 1., uvoznik o tome obavješćuje dobavljača sustava, ovlaštene zastupnike i tijela za nadzor tržišta.
3. Uvoznici navode svoje ime, registrirano trgovačko ime ili registrirani žig i adresu za kontakt na visokorizičnom UI sustavu i na njegovoj ambalaži ili u njegovoj popratnoj dokumentaciji, ako je primjenjivo.
4. Dok je visokorizični UI sustav pod njihovom odgovornošću uvoznici osiguravaju da uvjeti skladištenja ili prijevoza, ako je primjenjivo, ne ugrožavaju njegovu usklađenost sa zahtjevima utvrđenima u odjeljku 2.
5. Uvoznici tijekom razdoblja od deset godina nakon što je visokorizični UI sustav stavljen na tržište ili u upotrebu čuvaju primjerak potvrde koju je izdalo prijavljeno tijelo, ako je primjenjivo, uputa za korištenje i EU izjave o sukladnosti iz članka 47.
6. Uvoznici relevantnim nadležnim tijelima na obrazloženi zahtjev dostavljaju sve informacije i dokumentaciju, uključujući informacije i dokumentaciju navedene u stavku 5., koji su potrebni za dokazivanje sukladnosti visokorizičnog UI sustava sa zahtjevima utvrđenima u odjeljku 2. na jeziku koji ta tijela mogu bez poteškoća razumjeti. U tu svrhu također osiguravaju da se tim tijelima na raspolaganje može staviti tehnička dokumentacija.
7. Uvoznici surađuju s relevantnim nadležnim tijelima u svim mjerama koje ta tijela poduzimaju u vezi s visokorizičnim UI sustavom koji uvoznici stavljaju na tržište, posebno kako bi se smanjili i ublažili rizici koje on predstavlja.

Članak 24.

Obveze distributerâ

1. Prije stavljanja visokorizičnog UI sustava na raspolaganje na tržištu distributeri provjeravaju ima li on potrebnu oznaku CE, jesu li mu priloženi primjerak EU izjave o sukladnosti iz članka 47. i upute za korištenje te jesu li dobavljač i uvoznik tog sustava, ovisno o slučaju, ispunili svoje obveze utvrđene u članku 16. točkama (b) i (c) i članku 23. stavku 3.
2. Ako distributer na temelju informacija kojima raspolaže smatra ili ima razloga smatrati da visokorizični UI sustav nije sukladan sa zahtjevima utvrđenima u odjeljku 2., ne stavlja visokorizični UI sustav na tržište dok sustav ne postane sukladan s tim zahtjevima. Osim toga, ako visokorizični UI sustav predstavlja rizik u smislu članka 79. stavka 1., distributer o tome obavješćuje dobavljača ili uvoznika tog sustava, ovisno o slučaju.
3. Dok je visokorizični UI sustav pod njihovom odgovornošću, distributeri osiguravaju da uvjeti skladištenja ili prijevoza, ako je primjenjivo, ne ugrožavaju njegovu usklađenost sa zahtjevima utvrđenima u odjeljku 2.
4. Ako distributer na temelju informacija kojima raspolaže smatra ili ima razloga smatrati da visokorizični UI sustav koji je stavio na raspolaganje na tržištu nije sukladan sa zahtjevima utvrđenima u odjeljku 2., poduzima korektivne mjere potrebne kako bi postigao sukladnost dotičnog sustava s tim zahtjevima, povukao ga ili opozvao ili, osigurava da te korektivne mjere poduzme, prema potrebi, dobavljač, uvoznik ili drugi relevantni operater. Ako visokorizični UI sustav predstavlja rizik u smislu članka 79. stavka 1., distributer o tome odmah obavješćuje dobavljača ili uvoznika sustava i tijela nadležna za dotični visokorizični UI sustav, navodeći pojedinosti, osobito o neusklađenosti i poduzetim korektivnim mjerama.
5. Distributeri visokorizičnog UI sustava relevantnom nadležnom tijelu na obrazloženi zahtjev tog tijela dostavljaju sve informacije i dokumentaciju o svim njihovim mjerama na temelju stavaka od 1. do 4. koje su potrebne za dokazivanje sukladnosti tog sustava sa zahtjevima utvrđenima u odjeljku 2.
6. Distributeri surađuju s relevantnim nadležnim tijelima u svim mjerama koje ta tijela poduzimaju u vezi s visokorizičnim UI sustavom koji su distributeri stavili na raspolaganje na tržištu, posebno kako bi se smanjili ili ublažili rizici koje on predstavlja.

Članak 25.

Odgovornosti duž vrijednosnog lanca umjetne inteligencije

1. Svi distributeri, uvoznici, subjekti koji uvode sustav ili ostale treće strane smatraju se dobavljačima visokorizičnog UI sustava za potrebe ove Uredbe i podliježu obvezama dobavljača iz članka 16. u bilo kojoj od sljedećih okolnosti:

- (a) ako stave svoje ime ili žig na visokorizični UI sustav koji je već stavljen na tržište ili u upotrebu, ne dovodeći u pitanje ugovorne aranžmane u kojima je utvrđena drukčija raspodjela obveza;
- (b) ako znatno izmijene visokorizični UI sustav koji je već stavljen na tržište ili u upotrebu i to na takav način da i dalje ostane visokorizični UI sustav na temelju članka 6.;
- (c) ako izmijene namjenu UI sustava, uključujući UI sustav opće namjene, koji nije klasificiran kao visokorizičan i već je stavljen na tržište ili u upotrebu i to na takav način da dotični UI sustav postane visokorizični UI sustav u skladu s člankom 6.;

2. Ako nastupe okolnosti iz stavka 1., dobavljač koji je prvobitno stavio UI sustav na tržište ili u upotrebu više se ne smatra dobavljačem tog konkretnog UI sustava za potrebe ove Uredbe. Taj početni dobavljač blisko surađuje s novim dobavljačima te stavlja na raspolaganje potrebne informacije i pruža razumno očekivani tehnički pristup i drugu pomoć koji su potrebni za ispunjavanje obveza utvrđenih u ovoj Uredbi, posebno u pogledu poštovanja ocjenjivanja sukladnosti visokorizičnih UI sustava. Ovaj se stavak ne primjenjuje u slučajevima u kojima je početni dobavljač jasno naveo da se njegov UI sustav ne smije promijeniti u visokorizični UI sustav i stoga nije obuhvaćen obvezom predaje dokumentacije.

3. Kad je riječ o visokorizičnim UI sustavima koji su sigurnosna komponenta proizvoda obuhvaćenih zakonodavstvom Unije o usklađivanju navedenim u odjeljku A Priloga I., proizvođač proizvoda smatra se dobavljačem visokorizičnog UI sustava i podliježe obvezama iz članka 16. u bilo kojoj od sljedećih okolnosti:

- (a) visokorizični UI sustav stavljen je na tržište zajedno s dotičnim proizvodom pod imenom ili žigom proizvođača proizvoda;
- (b) visokorizični UI sustav stavljen je u upotrebu pod imenom ili žigom proizvođača proizvoda nakon što je proizvod stavljen na tržište.

4. Dobavljač visokorizičnog UI sustava i treća strana koja isporučuje UI sustav, alate, usluge, komponente ili procese koji se upotrebljavaju u visokorizičnom UI sustavu ili su u njega integrirani, pisanim dogovorom utvrđuju informacije, mogućnosti, tehnički pristup i drugu pomoć na temelju općepriznatih najnovijih dostignuća koji su potrebni kako bi dobavljač visokorizičnog UI sustava mogao u potpunosti ispuniti obveze utvrđene u ovoj Uredbi. Ovaj se stavak ne primjenjuje na treće strane koje stavljaju na raspolaganje javnosti alate, usluge, procese ili komponente, osim UI modela opće namjene, na temelju besplatne licencije za softver otvorenog koda.

Ured za umjetnu inteligenciju može razviti i preporučiti dobrovoljne modele uvjeta za ugovore između dobavljača visokorizičnih UI sustava i trećih strana koji isporučuju alate, usluge, komponente ili procese koji se upotrebljavaju u visokorizičnim UI sustavima ili su u njih integrirani. Pri izradi tih dobrovoljnih modela uvjeta Ured za umjetnu inteligenciju uzima u obzir moguće ugovorne zahtjeve primjenjive u određenim sektorima ili poslovnim slučajevima. Dobrovoljni modeli uvjeta objavljuju se i besplatno su dostupni u lako upotrebljivom elektroničkom obliku.

5. Stavcima 2. i 3. ne dovodi se u pitanje potreba za poštovanjem i zaštitom prava intelektualnog vlasništva, povjerljivih poslovnih informacija i poslovnih tajni u skladu s pravom Unije i nacionalnim pravom.

Članak 26.

Obveze subjekata koji uvode visokorizične UI sustave

1. Subjekti koji uvode visokorizične UI sustave poduzimaju odgovarajuće tehničke i organizacijske mjere kako bi osigurali da upotrebljavaju takve sustave u skladu s uputama za korištenje priloženima sustavima na temelju stavaka 3. i 6.

2. Subjekti koji uvode sustav dodjeljuju zadaću ljudskog nadzora fizičkim osobama koje imaju potrebne kompetencije, osposobljenost i ovlasti, te im pružaju potrebnu potporu.

3. Obvezama utvrđenima u stavcima 1. i 2. ne dovode se u pitanje druge obveze subjekta koji uvodi sustav na temelju prava Unije ili nacionalnog prava ni sloboda subjekta koji uvodi sustav da organizira svoje resurse i aktivnosti u svrhu provedbe mjera ljudskog nadzora koje je naveo dobavljač.

4. Ne dovodeći u pitanje stavke 1. i 2., subjekt koji uvodi sustav osigurava, u mjeri u kojoj ima kontrolu nad ulaznim podacima, da su ulazni podaci relevantni i dovoljno reprezentativni s obzirom na namjenu visokorizičnog UI sustava.

5. Subjekti koji uvode sustav prate rad visokorizičnog UI sustava u skladu s uputama za korištenje i prema potrebi obavješćuju dobavljače u skladu s člankom 72. Ako subjekti koji uvode sustav imaju razloga smatrati da korištenje visokorizičnog UI sustava u skladu s uputama može dovesti do toga da UI sustav predstavlja rizik u smislu članka 79. stavka 1., o tome bez nepotrebne odgode obavješćuju dobavljača ili distributera i relevantno tijelo za nadzor tržišta te suspendiraju korištenje tog sustava. Ako subjekti koji uvode sustav utvrde ozbiljan incident, o tom incidentu odmah obavješćuju prvo dobavljača, a zatim uvoznika ili distributera i relevantna tijela za nadzor tržišta. Ako subjekt koji uvodi sustav ne može stupiti u kontakt s dobavljačem, članak 73. primjenjuje se *mutatis mutandis*. Ova obveza ne obuhvaća osjetljive operativne podatke subjekata koji uvode UI sustave koji su tijela kaznenog progona.

Kad je riječ o subjektima koji uvode sustav, a koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu njihova unutarnjeg upravljanja, njihovih aranžmana ili njihovih postupaka na temelju prava Unije o financijskim uslugama, obveza praćenja utvrđena u prvom podstavku smatra se ispunjenom ako se poštuju pravila o aranžmanima, procesima i mehanizmima unutarnjeg upravljanja na temelju relevantnog prava o financijskim uslugama.

6. Subjekti koji uvode visokorizične UI sustave čuvaju evidenciju koju automatski generira taj visokorizični UI sustav u mjeri u kojoj je takva evidencija pod njihovom kontrolom, tijekom razdoblja koje je primjereno namjeni visokorizičnog UI sustava, a najmanje šest mjeseci, osim ako je drukčije predviđeno u primjenjivom pravu Unije ili nacionalnom pravu, a posebno u pravu Unije o zaštiti osobnih podataka.

Subjekti koji uvode sustav, a koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu njihova unutarnjeg upravljanja, njihovih aranžmana ili njihovih procesa na temelju prava Unije o financijskim uslugama čuvaju evidenciju u sklopu dokumentacije koja se čuva na temelju relevantnog prava Unije o financijskim uslugama.

7. Prije stavljanja u upotrebu ili korištenja visokorizičnog UI sustava na radnom mjestu subjekti koji uvode visokorizični UI sustav, a koji su poslodavci, obavješćuju predstavnike radnika i radnike na koje se to odnosi da će podlijeći upotrebi visokorizičnog UI sustava. Te se informacije pružaju, ako je primjenjivo, u skladu s pravilima i postupcima utvrđenima u pravu Unije i nacionalnom pravu te praksom o informiranju radnika i njihovih predstavnika.

8. Subjekti koji uvode visokorizične UI sustave koji su javna tijela ili institucije, tijela, uredi ili agencije Unije moraju ispunjavati obveze registracije iz članka 49. Ako takvi subjekti koji uvode sustav utvrde da visokorizični UI sustav koji namjeravaju upotrebljavati nije registriran u bazi podataka EU-a iz članka 71., taj sustav ne upotrebljavaju i o tome obavješćuju dobavljača ili distributera.

9. Ako je primjenjivo, subjekti koji uvode visokorizične UI sustave služe se informacijama iz članka 13. ove Uredbe da bi ispunili svoju obvezu provedbe procjene učinka na zaštitu podataka iz članka 35. Uredbe (EU) 2016/679 ili članka 27. Direktive (EU) 2016/680.

10. Ne dovodeći u pitanje Direktivu (EU) 2016/680, u okviru istrage radi ciljane potrage za osobom osumnjičenom ili osuđenom za počinjenje kaznenog djela, subjekt koji uvodi visokorizični UI sustav za naknadnu daljinsku biometrijsku identifikaciju od pravosudnog ili upravnog tijela čija je odluka obavezujuća i podliježe sudskom preispitivanju traži, *ex ante* ili bez nepotrebne odgode, a najkasnije u roku od 48 sati odobrenje za upotrebu tog sustava osim ako se on upotrebljava za početnu identifikaciju potencijalnog osumnjičenika na temelju objektivnih i provjerljivih činjenica izravno povezanih s kaznenim djelom. Svaka upotreba mora biti ograničena na ono što je nužno za istragu određenog kaznenog djela.

Ako je odobrenje zatraženo na temelju prvog podstavka odbijeno, upotreba sustava za naknadnu daljinsku biometrijsku identifikaciju povezanog s tim zatraženim odobrenjem smjesta se zaustavlja te se brišu osobni podaci povezani s upotrebom visokorizičnog UI sustava za koji je zatraženo odobrenje.

Takav visokorizični UI sustav za naknadnu daljinsku biometrijsku identifikaciju ni u kojem se slučaju ne smije upotrebljavati u svrhu kaznenog progona na neciljani način, bez ikakve poveznice s kaznenim djelom, kaznenim postupkom, stvarnom i prisutnom ili stvarnom i predvidljivom prijetnjom kaznenog djela ili potragom za određenom nestalom osobom. Mora se osigurati da tijela kaznenog progona ne mogu donositi odluke koje proizvode negativan pravni učinak na osobu isključivo na temelju izlaznih podataka takvih sustava za naknadnu daljinsku biometrijsku identifikaciju.

Ovim se stavkom ne dovode u pitanje članak 9. Uredbe (EU) 2016/679 i članak 10. Direktive (EU) 2016/680 kad je riječ o obradi biometrijskih podataka.

Neovisno o namjeni ili subjektu koji uvodi sustav, svaka upotreba takvih visokorizičnih UI sustava dokumentira se u relevantnom policijskom spisu i na zahtjev se stavlja na raspolaganje relevantnom tijelu za nadzor tržišta i nacionalnom tijelu za zaštitu podataka, isključujući otkrivanje osjetljivih operativnih podataka povezanih s kaznenim progonom. Ovim se podstavkom ne dovode u pitanje ovlasti dodijeljene nadzornim tijelima Direktivom (EU) 2016/680.

Subjekti koji uvode sustav podnose godišnja izvješća relevantnim tijelima za nadzor tržišta i nacionalnim tijelima za zaštitu podataka o svojoj upotrebi sustava za naknadnu daljinsku biometrijsku identifikaciju, isključujući otkrivanje osjetljivih operativnih podataka povezanih s kaznenim progonom. Izvješća mogu biti skupna kako bi obuhvatila više od jednog uvođenja.

Države članice mogu, u skladu s pravom Unije, uvesti restriktivnije propise o upotrebi sustava za naknadnu daljinsku biometrijsku identifikaciju.

11. Ne dovodeći u pitanje članak 50. ove Uredbe, subjekti koji uvode visokorizične UI sustave iz Priloga III. koji donose odluke ili pomažu u donošenju odluka povezanih s fizičkim osobama obavješćuju fizičke osobe o tome da podliježu upotrebi visokorizičnog UI sustava. Na visokorizične UI sustave koji se upotrebljavaju u svrhu kaznenog progona primjenjuje se članak 13. Direktive (EU) 2016/680.

12. Subjekti koji uvode sustav surađuju s relevantnim nadležnim tijelima u svim mjerama koje ta tijela poduzimaju u vezi s visokorizičnim UI sustavom radi provedbe ove Uredbe.

Članak 27.

Procjena učinka visokorizičnih UI sustava na temeljna prava

1. Prije uvođenja visokorizičnog UI sustava iz članka 6. stavka 2., uz iznimku visokorizičnih UI sustava namijenjenih za upotrebu u području navedenom u točki 2. Priloga III., subjekti koji uvode sustav koji su javnopravna tijela ili su privatni subjekti koji pružaju javne usluge i subjekti koji uvode visokorizične UI sustave iz točke 5. podtočaka (b) i (c) Priloga III. provode procjenu učinka koji upotreba takvog sustava može imati na temeljna prava. U tu svrhu subjekti koji uvode sustav provode procjenu koja sadržava:

- (a) opis procesa subjekta koji uvodi sustav u kojima će se visokorizični UI sustav upotrebljavati u skladu sa svojom namjenom;
- (b) opis razdoblja i učestalosti namjeravane upotrebe svakog visokorizičnog UI sustava;
- (c) kategorije fizičkih osoba i skupina na koje će vjerojatno utjecati upotreba sustava u konkretnom kontekstu;
- (d) specifične rizike od štete koji će vjerojatno utjecati na kategorije fizičkih osoba ili skupine osoba identificirane u skladu s točkom (c) ovog stavka, uzimajući u obzir informacije koje je dostavio dobavljač u skladu s člankom 13.;
- (e) opis provedbe mjera ljudskog nadzora u skladu s uputama za korištenje;
- (f) mjere koje se moraju poduzeti u slučaju materijalizacije tih rizika, uključujući aranžmane za unutarnje upravljanje i mehanizme za podnošenje pritužbi.

2. Obveza utvrđene u stavku 1. primjenjuje se na prvu upotrebu visokorizičnog UI sustava. Subjekt koji uvodi sustav može se u sličnim slučajevima osloniti na prethodno provedene procjene učinka na temeljna prava ili postojeću procjenu učinka koju je proveo dobavljač. Ako tijekom upotrebe visokorizičnog UI sustava subjekt koji uvodi sustav smatra da se neki od elemenata iz stavka 1. promijenio ili da nije ažuriran, subjekt koji uvodi sustav poduzima potrebne korake za ažuriranje informacija.
3. Nakon provedbe procjene iz stavka 1. ovog članka subjekt koji uvodi sustav obavješćuje tijelo za nadzor tržišta o njezinim rezultatima, podnošenjem ispunjenog predloška iz stavka 5. ovog članka u okviru obavijesti. U slučaju iz članka 46. stavka 1. subjekti koji uvode sustav mogu biti izuzeti od te obveze obavješćivanja.
4. Ako je bilo koja od obveza utvrđenih u ovom članku već ispunjena procjenom učinka na zaštitu podataka provedenom na temelju članka 35. Uredbe (EU) 2016/679 ili članka 27. Direktive (EU) 2016/680, procjena učinka na temeljna prava iz stavka 1. ovog članka dopunjuje tu procjenu učinka na zaštitu podataka.
5. Ured za umjetnu inteligenciju izrađuje predložak upitnika, među ostalim s pomoću automatiziranog alata, kako bi se subjektima koji uvode sustav olakšalo da na pojednostavljen način ispune svoje obveze iz ovog članka.

ODJELJAK 4.

Tijela koja provode prijavljivanje i prijavljena tijela

Članak 28.

Tijela koja provode prijavljivanje

1. Svaka država članica imenuje ili osniva barem jedno tijelo koje provodi prijavljivanje, koje je odgovorno za utvrđivanje i provedbu postupaka potrebnih za ocjenjivanje, imenovanje, prijavljivanje i praćenje tijela za ocjenjivanje sukladnosti. Te postupke u suradnji razvijaju tijela koja provode prijavljivanje iz svih država članica.
2. Države članice mogu odlučiti da ocjenjivanje i praćenje iz stavka 1. provodi nacionalno akreditacijsko tijelo u smislu Uredbe (EZ) br. 765/2008 i u skladu s tom uredbom.
3. Tijela koja provode prijavljivanje osnivaju se, organiziraju i rade na takav način da ne dolazi do sukoba interesa s tijelima za ocjenjivanje sukladnosti te da su zajamčene objektivnost i nepristranost njihovih aktivnosti.
4. Tijela koja provode prijavljivanje organizirana su na takav način da odluke povezane s prijavljivanjem tijela za ocjenjivanje sukladnosti donose nadležne osobe različite od osoba koje su provele ocjenjivanje tih tijela.
5. Tijela koja provode prijavljivanje ne smiju nuditi obavljanje aktivnosti niti smiju obavljati aktivnosti koje obavljaju tijela za ocjenjivanje sukladnosti, kao ni usluge savjetovanja na tržišnoj ili konkurentskoj osnovi.
6. Tijela koja provode prijavljivanje u skladu s člankom 78. štite povjerljivost informacija koje su pribavila.
7. Tijela koja provode prijavljivanje moraju imati adekvatan broj članova stručnog osoblja za propisno obavljanje svojih zadaća. Stručno osoblje mora imati, ako je primjenjivo, potrebno stručno znanje za svoju funkciju u područjima kao što su informacijske tehnologije, umjetna inteligencija i pravo, uključujući nadzor temeljnih prava.

Članak 29.

Zahtjev tijela za ocjenjivanje sukladnosti za prijavljivanje

1. Tijela za ocjenjivanje sukladnosti podnose zahtjev za prijavljivanje tijelu koje provodi prijavljivanje u državi članici u kojoj imaju poslovni nastan.

2. Zahtjevu za prijavljivanje prilaže se opis aktivnosti ocjenjivanja sukladnosti, jednog ili više modula za ocjenjivanje sukladnosti i vrsta UI sustava za koje tijelo za ocjenjivanje sukladnosti tvrdi da je nadležno te potvrda o akreditaciji, ako postoji, koju je izdalo nacionalno akreditacijsko tijelo i kojom se potvrđuje da tijelo za ocjenjivanje sukladnosti ispunjava zahtjeve utvrđene u članku 31.

Dodaju se svi valjani dokumenti koji se odnose na postojeća imenovanja, na temelju drugog zakonodavstva Unije o usklađivanju, prijavljenog tijela koje podnosi zahtjev.

3. Ako dotično tijelo za ocjenjivanje sukladnosti ne može predložiti potvrdu o akreditaciji, tijelu koje provodi prijavljivanje dostavlja sve dokumente potrebne za provjeru, priznavanje i redovito praćenje njegova ispunjavanja zahtjeva utvrđenih u članku 31.

4. Kad je riječ o prijavljenim tijelima koja su imenovana na temelju drugog zakonodavstva Unije o usklađivanju, svi dokumenti i potvrde povezani s tim imenovanjima mogu se, prema potrebi, upotrijebiti u postupku njihova imenovanja na temelju ove Uredbe. Prijavljeno tijelo ažurira dokumentaciju iz stavaka 2. i 3. ovog članka u slučaju bilo kakvih relevantnih promjena kako bi tijelu odgovornom za prijavljena tijela omogućilo da prati i provjerava kontinuirano ispunjavanje svih zahtjeva utvrđenih u članku 31.

Članak 30.

Postupak prijavljivanja

1. Tijela koja provode prijavljivanje mogu prijaviti samo tijela za ocjenjivanje sukladnosti koja ispunjavaju zahtjeve utvrđene u članku 31.

2. Tijela koja provode prijavljivanje pomoću alata za elektroničko prijavljivanje koji je razvila i kojim upravlja Komisija dostavljaju prijavu Komisiji i drugim državama članicama o svakom tijelu za ocjenjivanje sukladnosti iz stavka 1.

3. Prijavljivanje iz stavka 2. ovog članka obuhvaća sve pojedinosti o aktivnostima ocjenjivanja sukladnosti, jednom ili više modula za ocjenjivanje sukladnosti, vrstama dotičnih UI sustava te relevantnu potvrdu o stručnosti. Ako se prijavljivanje ne temelji na potvrdi o akreditaciji iz članka 29. stavka 2., tijelo koje provodi prijavljivanje dostavlja Komisiji i drugim državama članicama pisane dokaze kojima se potvrđuju stručnost tijela za ocjenjivanje sukladnosti i aranžmani koji su uspostavljeni kako bi se osiguralo da će se to tijelo redovito pratiti i da će nastaviti ispunjavati zahtjeve utvrđene u članku 31.

4. Dotično tijelo za ocjenjivanje sukladnosti može obavljati aktivnosti prijavljenog tijela samo ako Komisija ili druge države članice ne podnesu prigovor u roku od dva tjedna od prijavljivanja koje je izvršilo tijelo koje provodi prijavljivanje ako prijava uključuje potvrdu o akreditaciji iz članka 29. stavka 2. odnosno u roku od dva mjeseca od prijavljivanja koje je izvršilo tijelo koje provodi prijavljivanje ako prijava uključuje pisane dokaze iz članka 29. stavka 3.

5. Ako se podnesu prigovori, Komisija bez odgode započinje savjetovanja s relevantnim državama članicama i tijelom za ocjenjivanje sukladnosti. S obzirom na savjetovanja Komisija odlučuje je li odobrenje opravdano. Komisija svoju odluku upućuje dotičnoj državi članici i relevantnom tijelu za ocjenjivanje sukladnosti.

Članak 31.

Zahtjevi koji se odnose na prijavljena tijela

1. Prijavljeno tijelo osniva se na temelju nacionalnog prava države članice i ima pravnu osobnost.

2. Prijavljena tijela moraju ispunjavati organizacijske zahtjeve i zahtjeve koji se odnose na upravljanje kvalitetom, resurse i procese koji su potrebni za obavljanje njihovih zadaća, kao i odgovarajuće zahtjeve u pogledu kibernetičke sigurnosti.

3. Organizacijskom strukturom, podjelom odgovornosti, linijama izvješćivanja i radom prijavljenih tijela osigurava se povjerenje u njihovu učinkovitost i u rezultate aktivnosti ocjenjivanja sukladnosti koje ona provode.

4. Prijavljena tijela moraju biti neovisna o dobavljaču visokorizičnog UI sustava u vezi s kojim provode aktivnosti ocjenjivanja sukladnosti. Prijavljena tijela ujedno moraju biti neovisna o svim ostalim operaterima koji imaju gospodarski interes u visokorizičnim UI sustavima koji se ocjenjuju, kao i o svim konkurentima dobavljača. Time se ne sprečava upotreba ocijenjenih visokorizičnih UI sustava koji su potrebni za rad tijela za ocjenjivanje sukladnosti ni upotreba takvih visokorizičnih UI sustava za osobne potrebe.
5. Tijelo koje ocjenjuje sukladnost, njegovo najviše rukovodstvo i osoblje odgovorno za provedbu zadaća ocjenjivanja sukladnosti ne smiju biti izravno uključeni u dizajn, razvoj, stavljanje na tržište ili upotrebu visokorizičnih UI sustava niti smiju zastupati strane uključene u te aktivnosti. Oni ne smiju sudjelovati u aktivnostima koje bi mogle dovesti u pitanje njihovu neovisnost prosudbe ili njihov integritet u vezi s aktivnostima ocjenjivanja sukladnosti za koje su prijavljeni. To se osobito odnosi na usluge savjetovanja.
6. Prijavljena tijela organizirana su i rade na način kojim se jamče neovisnost, objektivnost i nepristranost njihovih aktivnosti. Prijavljena tijela dokumentiraju i primjenjuju strukturu i postupke za očuvanje nepristranosti te za promicanje i primjenu načela nepristranosti u cijeloj svojoj organizaciji, među svojim osobljem i u svojim aktivnostima ocjenjivanja.
7. Prijavljena tijela moraju imati uspostavljene dokumentirane postupke kojima se osigurava da njihovo osoblje, odbori, podružnice, podugovaratelji i sva povezana tijela ili osoblje vanjskih tijela u skladu s člankom 78. poštuju povjerljivost informacija koje prime tijekom obavljanja aktivnosti ocjenjivanja sukladnosti, osim ako se otkrivanje tih informacija zahtijeva zakonom. Osoblje prijavljenih tijela obvezno je čuvati profesionalnu tajnu u pogledu svih informacija koje pribavi tijekom obavljanja svojih zadaća na temelju ove Uredbe, osim u odnosu na tijela koja provode prijavljivanje u državi članici u kojoj prijavljena tijela obavljaju svoje aktivnosti.
8. Prijavljena tijela moraju imati uspostavljene postupke za obavljanje aktivnosti kojima se propisno uzimaju u obzir veličina dobavljača, sektor u kojem on posluje, njegova struktura i stupanj složenosti dotičnog UI sustava.
9. Prijavljena tijela sklapaju odgovarajuće osiguranje od odgovornosti za svoje aktivnosti ocjenjivanja sukladnosti, osim ako u skladu s nacionalnim pravom odgovornost preuzima država članica u kojoj imaju poslovni nastan ili je ta država članica sama izravno odgovorna za ocjenjivanje sukladnosti.
10. Prijavljena tijela moraju biti sposobna provoditi sve svoje zadaće na temelju ove Uredbe s najvećom razinom profesionalnog integriteta i potrebnim kompetencijama u određenom području, bez obzira na to provode li te zadaće sama prijavljena tijela ili se one provode u njihovo ime i pod njihovom odgovornošću.
11. Prijavljena tijela moraju imati dostatne unutarnje kompetencije da bi mogla djelotvorno evaluirati zadaće koje u njihovo ime obavljaju vanjske strane. Prijavljeno tijelo mora kontinuirano imati dovoljan broj članova administrativnog, tehničkog, pravnog i znanstvenog osoblja koji posjeduju iskustvo i znanje u vezi s relevantnim vrstama UI sustava, podacima i obradom podataka te u vezi sa zahtjevima utvrđenima u odjeljku 2.
12. Prijavljena tijela sudjeluju u koordinacijskim aktivnostima iz članka 38. Osim toga, izravno sudjeluju ili imaju predstavnika u europskim organizacijama za normizaciju, ili osiguravaju da su upoznata s relevantnim normama i prate razvoj zbivanja.

Članak 32.

Pretpostavka sukladnosti sa zahtjevima koji se odnose na prijavljena tijela

Ako tijelo za ocjenjivanje sukladnosti dokaže svoju sukladnost s kriterijima utvrđenima u relevantnim usklađenim normama ili njihovim dijelovima, na koje su upućivanja objavljena u *Službenom listu Europske unije*, pretpostavlja se da ispunjava zahtjeve utvrđene u članku 31. u mjeri u kojoj primjenjive usklađene norme obuhvaćaju te zahtjeve.

Članak 33.**Podružnice prijavljenih tijela i podugovaranje**

1. Ako prijavljeno tijelo određene zadaće povezane s ocjenjivanjem sukladnosti povjeri podugovarateljima ili ih prenese podružnici, ono osigurava da podugovaratelj ili podružnica ispunjava zahtjeve utvrđene u članku 31. te o tome obavješćuje tijelo koje provodi prijavljivanje.
2. Prijavljena tijela preuzimaju punu odgovornost za svoje zadaće koje obavljaju podugovaratelji ili podružnice.
3. Aktivnosti se samo uz suglasnost dobavljača smiju povjeriti podugovaratelju odnosno smije ih provoditi podružnica. Prijavljena tijela objavljuju popis svojih podružnica.
4. Relevantni dokumenti koji se odnose na ocjenjivanje kvalifikacija podugovaratelja ili podružnica i rada koji su oni obavili na temelju ove Uredbe stavljaju se na raspolaganje tijelu koje provodi prijavljivanje tijekom razdoblja od pet godina od datuma okončanja podugovaranja.

Članak 34.**Operativne obveze prijavljenih tijela**

1. Prijavljena tijela provjeravaju sukladnost visokorizičnih UI sustava u skladu s postupcima ocjenjivanja sukladnosti utvrđenima u članku 43.
2. Prijavljena tijela pri obavljanju svojih aktivnosti izbjegavaju nepotrebno opterećenje za dobavljače i uzimaju u obzir veličinu dobavljača, sektor u kojem posluje, njegovu strukturu i stupanj složenosti dotičnog visokorizičnog UI sustava, posebno kako bi se na najmanju moguću mjeru sveli administrativno opterećenje i troškovi usklađivanja za mikropoduzeća i mala poduzeća u smislu Preporuke 2003/361/EZ. Prijavljeno tijelo ipak poštuje stupanj strogosti i razinu zaštite koji su potrebni kako bi visokorizični UI sustav ispunjavao zahtjeve ove Uredbe.
3. Prijavljena tijela tijelu koje provodi prijavljivanje iz članka 28. stavljaju na raspolaganje i na zahtjev dostavljaju svu relevantnu dokumentaciju, uključujući dokumentaciju dobavljača, kako bi to tijelo moglo provoditi svoje aktivnosti ocjenjivanja, imenovanja, prijavljivanja i praćenja te kako bi se olakšalo ocjenjivanje opisano u ovom odjeljku.

Članak 35.**Identifikacijski brojevi i popisi prijavljenih tijela**

1. Komisija svakom prijavljenom tijelu dodjeljuje jedinstveni identifikacijski broj, čak i ako je tijelo prijavljeno na temelju više od jednog akta Unije.
2. Komisija objavljuje popis tijela prijavljenih na temelju ove Uredbe, uključujući njihove identifikacijske brojeve i aktivnosti za koje su prijavljena. Komisija osigurava ažuriranje tog popisa.

Članak 36.**Promjene u vezi s prijavama**

1. Tijelo koje provodi prijavljivanje obavješćuje Komisiju i druge države članice o svim relevantnim promjenama u vezi s prijavom prijavljenog tijela pomoću alata za elektroničko prijavljivanje iz članka 30. stavka 2.
2. Postupci utvrđeni u člancima 29. i 30. primjenjuju se na proširenja opsega prijave.

Na promjene u vezi s prijavom, uz iznimku proširenja njezina opsega, primjenjuju se postupci utvrđeni u stavcima od 3. do 9.

3. Ako prijavljeno tijelo odluči prestati obavljati aktivnosti ocjenjivanja sukladnosti, o tome obavješćuje tijelo koje provodi prijavljivanje i dotične dobavljače u najkraćem mogućem roku, a u slučaju planiranog prestanka obavljanja aktivnosti barem godinu dana prije prestanka obavljanja svojih aktivnosti. Potvrde prijavljenog tijela mogu ostati valjane tijekom razdoblja od devet mjeseci nakon prestanka obavljanja aktivnosti prijavljenog tijela pod uvjetom da je neko drugo prijavljeno tijelo u pisanom obliku potvrdilo da će preuzeti odgovornost za visokorizične UI sustave na koje se te potvrde odnose. Potonje prijavljeno tijelo provodi cjelovito ocjenjivanje dotičnih visokorizičnih UI sustava do kraja tog devetomjesečnog razdoblja prije nego što izda nove potvrde za te sustave. Ako je prijavljeno tijelo prestalo obavljati svoje aktivnosti, tijelo koje provodi prijavljivanje povlači imenovanje.

4. Ako tijelo koje provodi prijavljivanje ima dovoljno razloga smatrati da određeno prijavljeno tijelo više ne ispunjava zahtjeve utvrđene u članku 31. ili da ne ispunjava svoje obveze, tijelo koje provodi prijavljivanje bez odgode i uz najveću moguću pozornost istražuje to pitanje. U tom kontekstu tijelo koje provodi prijavljivanje obavješćuje dotično prijavljeno tijelo o podnesenim prigovorima i daje mu mogućnost da se izjasni. Ako tijelo koje provodi prijavljivanje zaključi da prijavljeno tijelo više ne ispunjava zahtjeve utvrđene u članku 31. ili da ne ispunjava svoje obveze, ono prema potrebi ograničava, suspendira ili povlači imenovanje, ovisno o težini neispunjavanja tih zahtjeva ili obveza. Tijelo koje provodi prijavljivanje o tome odmah obavješćuje Komisiju i druge države članice.

5. Ako je imenovanje prijavljenog tijela suspendirano, ograničeno ili djelomično ili potpuno povučeno, to tijelo o tome obavješćuje dotične dobavljače u roku od deset dana.

6. U slučaju ograničenja, suspendije ili povlačenja imenovanja, tijelo koje provodi prijavljivanje poduzima odgovarajuće mjere kako bi osiguralo da se spisi dotičnog prijavljenog tijela sačuvaju te da se stave na raspolaganje tijelima koja provode prijavljivanje u drugim državama članicama i tijelima za nadzor tržišta na njihov zahtjev.

7. U slučaju ograničenja, suspendije ili povlačenja imenovanja, tijelo koje provodi prijavljivanje:

- (a) ocjenjuje učinak koji to ima na potvrde koje je izdalo prijavljeno tijelo;
 - (b) Komisiji i drugim državama članicama podnosi izvješće o svojim nalazima u roku od tri mjeseca nakon što ih je obavijestilo o promjenama u vezi s imenovanjem;
 - (c) od prijavljenog tijela zahtijeva da u razumnom roku koji odredi tijelo koje provodi prijavljivanje suspendira ili povuče sve nepropisno izdane potvrde kako bi se osigurala kontinuirana sukladnost visokorizičnih UI sustava na tržištu;
 - (d) obavješćuje Komisiju i države članice o potvrdama za koje je zatražilo suspendiju ili povlačenje;
 - (e) nacionalnim nadležnim tijelima države članice u kojoj dobavljač ima registrirano mjesto poslovanja dostavlja sve relevantne informacije o potvrdama za koje je zatražilo suspendiju ili povlačenje; to tijelo prema potrebi poduzima odgovarajuće mjere kako bi se izbjegao potencijalni rizik za zdravlje, sigurnost ili temeljna prava.
8. Osim ako su potvrde nepropisno izdane i ako je imenovanje suspendirano ili ograničeno, potvrde ostaju valjane u jednoj od sljedećih okolnosti:
- (a) tijelo koje provodi prijavljivanje potvrdilo je, u roku od mjesec dana od suspendije ili ograničenja, da potvrde na koje se odnosi suspendija ili ograničenje ne predstavljaju rizik za zdravlje, sigurnost ili temeljna prava te je navelo vremenski raspored za mjere s pomoću kojih bi se suspendija ili ograničenje mogli ispraviti; ili
 - (b) tijelo koje provodi prijavljivanje potvrdilo je da se tijekom razdoblja suspendije ili ograničenja neće izdavati, mijenjati ili ponovno izdavati potvrde na koje se odnosi suspendija te navodi je li prijavljeno tijelo sposobno nastaviti pratiti već izdane potvrde i odgovarati za njih tijekom razdoblja suspendije ili ograničenja. U slučaju da tijelo koje provodi prijavljivanje utvrdi da prijavljeno tijelo nije sposobno dati podršku za već izdane potvrde, dobavljač sustava na koji se potvrda odnosi u roku od tri mjeseca od suspendije ili ograničenja u pisanom obliku potvrđuje nacionalnim nadležnim tijelima države članice u kojoj ima registrirano mjesto poslovanja da neko drugo kvalificirano prijavljeno tijelo privremeno preuzima funkcije prijavljenog tijela u pogledu praćenja potvrda i odgovaranja za njih tijekom razdoblja suspendije ili ograničenja.

9. Osim ako su potvrde nepropisno izdane i ako je imenovanje povučeno, potvrde ostaju valjane tijekom razdoblja od devet mjeseci u sljedećim okolnostima:

- (a) nacionalno nadležno tijelo države članice u kojoj dobavljač visokorizičnog UI sustava na koji se potvrda odnosi ima registrirano mjesto poslovanja potvrdilo je da dotični visokorizični UI sustavi ne predstavljaju rizik za zdravlje, sigurnost ili temeljna prava; i
- (b) drugo prijavljeno tijelo potvrdilo je u pisanom obliku da će preuzeti izravnu odgovornost za te UI sustave i da će dovršiti njihovo ocjenjivanje u roku od dvanaest mjeseci od povlačenja imenovanja.

U okolnostima iz prvog podstavka nacionalno nadležno tijelo države članice u kojoj dobavljač sustava na koji se potvrda odnosi ima registrirano mjesto poslovanja može produljiti privremenu valjanost potvrda za dodatna razdoblja od tri mjeseca, pri čemu ukupno razdoblje ne smije biti dulje od 12 mjeseci.

Nacionalno nadležno tijelo ili prijavljeno tijelo koje preuzima funkcije prijavljenog tijela na koje se odnosi promjena u vezi s imenovanjem odmah o tome obavješćuje Komisiju, druge države članice i druga prijavljena tijela.

Članak 37.

Osporavanje stručnosti prijavljenih tijela

- 1. Komisija prema potrebi istražuje sve slučajeve u kojima postoje razlozi za sumnju u stručnost prijavljenog tijela ili u to da prijavljeno tijelo kontinuirano ispunjava zahtjeve utvrđene u članku 31. i svoje konkretne odgovornosti.
- 2. Tijelo koje provodi prijavljivanje Komisiji na zahtjev dostavlja sve relevantne informacije koje se odnose na prijavu ili održavanje stručnosti dotičnog prijavljenog tijela.
- 3. Komisija osigurava da se sa svim osjetljivim informacijama pribavljenima tijekom njezinih istraga na temelju ovog članka postupa na povjerljiv način u skladu s člankom 78.
- 4. Ako Komisija utvrdi da prijavljeno tijelo ne ispunjava ili da više ne ispunjava zahtjeve za svoju prijavu, o tome obavješćuje državu članicu koja provodi prijavljivanje i od nje zahtijeva da poduzme potrebne korektivne mjere, uključujući suspenziju ili povlačenje prijave ako je to potrebno. Ako država članica ne provede potrebne korektivne mjere, Komisija može provedbenim aktom suspendirati, ograničiti ili povući imenovanje. Taj provedbeni akt donosi se u skladu s postupkom ispitivanja iz članka 98. stavka 2.

Članak 38.

Koordinacija prijavljenih tijela

- 1. Komisija osigurava da se u vezi s visokorizičnim UI sustavima uspostave i pravilno provode primjerena koordinacija i suradnja prijavljenih tijela koja se bave postupcima ocjenjivanja sukladnosti na temelju ove Uredbe, i to u okviru sektorske skupine prijavljenih tijela.
- 2. Svako tijelo koje provodi prijavljivanje osigurava da tijela koja je prijavilo sudjeluju u radu skupine iz stavka 1., izravno ili preko imenovanih predstavnika.
- 3. Komisija osigurava razmjenu znanja i primjera najbolje prakse među tijelima koja provode prijavljivanje.

Članak 39.

Tijela za ocjenjivanje sukladnosti iz trećih zemalja

Tijela za ocjenjivanje sukladnosti uspostavljena na temelju prava određene treće zemlje s kojom je Unija sklopila sporazum mogu biti ovlaštena za obavljanje aktivnosti prijavljenih tijela na temelju ove Uredbe, pod uvjetom da ispunjavaju zahtjeve utvrđene u članku 31. ili osiguraju jednakovrijednu razinu usklađenosti.

ODJELJAK 5.

Norme, ocjenjivanje sukladnosti, potvrde, registracija

Članak 40.

Usklađene norme i normizacijski dokumenti

1. Za visokorizične UI sustave ili UI modele opće namjene koji su sukladni s usklađenim normama ili dijelovima usklađenih normi na koje su objavljena upućivanja u *Službenom listu Europske unije* u skladu s Uredbom (EU) br. 1025/2012 pretpostavlja se da su sukladni sa zahtjevima utvrđenima u odjeljku 2. ovog poglavlja odnosno, ovisno o slučaju, s obvezama utvrđenima u poglavlju V. odjeljcima 2. i 3. ove Uredbe, u mjeri u kojoj te norme obuhvaćaju te zahtjeve ili obveze.

2. U skladu s člankom 10. Uredbe (EU) br. 1025/2012 Komisija bez nepotrebne odgode upućuje zahtjeve za normizaciju koji obuhvaćaju sve zahtjeve utvrđene u odjeljku 2. ovog poglavlja i, ovisno o slučaju, zahtjeve za normizaciju koji obuhvaćaju obveze utvrđene u poglavlju V. odjeljcima 2. i 3. ove Uredbe. U okviru zahtjeva za normizaciju također se zahtijeva izrada dokumenata u vezi s procesom izvješćivanja i dokumentiranja kako bi se poboljšala resursna učinkovitost UI sustava, primjerice kako bi visokorizični UI sustav smanjio potrošnju energije i drugih resursa tijekom svojeg životnog ciklusa, te u vezi s energetski učinkovitim razvojem UI modela opće namjene. Pri izradi zahtjeva za normizaciju Komisija se savjetuje s Vijećem za umjetnu inteligenciju i relevantnim dionicima, uključujući savjetodavni forum.

Pri upućivanju zahtjeva za normizaciju europskim organizacijama za normizaciju Komisija navodi da norme moraju biti jasne i usklađene, među ostalim i s normama razvijenima u raznim sektorima za proizvode obuhvaćene postojećim zakonodavstvom Unije o usklađivanju navedenim u Prilogu I., i da se njima mora osigurati da visokorizični UI sustavi ili UI modeli opće namjene koji se stavljaju na tržište ili u upotrebu u Uniji ispunjavaju relevantne zahtjeve ili obveze utvrđene u ovoj Uredbi.

Komisija također zahtijeva od europskih organizacija za normizaciju da dostave dokaze o svojim nastojanjima da ispune ciljeve iz prvog i drugog podstavka ovog stavka u skladu s člankom 24. Uredbe (EU) br. 1025/2012.

3. Sudionici u procesu normizacije nastoje promicati ulaganja i inovacije u području umjetne inteligencije, među ostalim povećanjem pravne sigurnosti, kao i konkurentnosti i rasta tržišta Unije, te doprinositi jačanju globalne suradnje u području normizacije, uzimajući u obzir postojeće međunarodne norme u području umjetne inteligencije koje su u skladu s vrijednostima, temeljnim pravima i interesima Unije, i poboljšati višedioničko upravljanje osiguravanjem ujednačene zastupljenosti interesa i djelotvornog sudjelovanja svih relevantnih dionika u skladu s člancima 5., 6. i 7. Uredbe (EU) br. 1025/2012.

Članak 41.

Zajedničke specifikacije

1. Komisija može donositi provedbene akte o utvrđivanju zajedničkih specifikacija za zahtjeve utvrđene u odjeljku 2. ovog poglavlja odnosno, ovisno o slučaju, za obveze utvrđene u odjeljcima 2. i 3. poglavlja V. ako su ispunjeni sljedeći uvjeti:

(a) Komisija je na temelju članka 10. stavka 1. Uredbe (EU) br. 1025/2012 zatražila od jedne ili više europskih organizacija za normizaciju da izrade usklađenu normu za zahtjeve utvrđene u odjeljku 2. ovog poglavlja odnosno, ovisno o slučaju, za obveze utvrđene u odjeljcima 2. i 3. poglavlja V., a:

i. zahtjev nije prihvatila nijedna europska organizacija za normizaciju; ili

ii. usklađene norme koje se odnose na taj zahtjev nisu izrađene u roku utvrđenom u skladu s člankom 10. stavkom 1. Uredbe (EU) br. 1025/2012; ili

iii. relevantnim usklađenim normama nisu dostatno uvažena pitanja temeljnih prava; ili

iv. usklađene norme nisu u skladu sa zahtjevom; i

(b) u *Službenom listu Europske unije* nije objavljeno, u skladu s Uredbom (EU) br. 1025/2012, upućivanje na usklađene norme koje obuhvaćaju zahtjeve utvrđene u odjeljku 2. ovog poglavlja odnosno, ovisno o slučaju, obveze utvrđene u odjeljcima 2. i 3. poglavlja V., niti se očekuje objava takvih upućivanja u razumnom roku.

Pri izradi zajedničkih specifikacija Komisija se savjetuje sa savjetodavnim forumom iz članka 67.

Provedbeni akti iz prvog podstavka ovog stavka donose se u skladu s postupkom ispitivanja iz članka 98. stavka 2.

2. Prije nego što izradi nacrt provedbenog akta Komisija obavješćuje odbor iz članka 22. Uredbe (EU) br. 1025/2012 o tome da smatra da su uvjeti utvrđeni u stavku 1. ovog članka ispunjeni.

3. Za visokorizične UI sustave ili UI modele opće namjene koji su sukladni sa zajedničkim specifikacijama iz stavka 1. ili dijelovima tih specifikacija pretpostavlja se da su sukladni sa zahtjevima utvrđenima u odjeljku 2. ovog poglavlja odnosno, ovisno o slučaju, da su u skladu s obvezama utvrđenima u odjeljcima 2. i 3. poglavlja V., u mjeri u kojoj te zajedničke specifikacije obuhvaćaju te zahtjeve ili te obveze.

4. Ako europska organizacija za normizaciju donese usklađenu normu i Komisiji predloži da se upućivanje na nju objavi u *Službenom listu Europske unije*, Komisija ocjenjuje tu usklađenu normu u skladu s Uredbom (EU) br. 1025/2012. Kad se upućivanje na usklađenu normu objavi u *Službenom listu Europske unije*, Komisija stavlja izvan snage provedbene akte iz stavka 1. ili njihove dijelove koji obuhvaćaju iste zahtjeve utvrđene u odjeljku 2. ovog poglavlja odnosno, ovisno o slučaju, iste obveze utvrđene u odjeljcima 2. i 3. poglavlja V.

5. Ako dobavljači visokorizičnih UI sustava ili UI modela opće namjene ne ispunjavaju zajedničke specifikacije iz stavka 1., moraju propisno obrazložiti da su usvojili tehnička rješenja kojima se ispunjavaju zahtjevi iz odjeljka 2. ovog poglavlja odnosno, ovisno o slučaju, kojima se ispunjavaju obveze utvrđene u odjeljcima 2. i 3. poglavlja V., na razini koja je barem jednakovrijedna tim zajedničkim specifikacijama.

6. Ako država članica smatra da zajednička specifikacija ne ispunjava u potpunosti zahtjeve utvrđene u odjeljku 2. odnosno, ovisno o slučaju, obveze utvrđene u odjeljcima 2. i 3. poglavlja V., ona o tome obavješćuje Komisiju i navodi detaljno objašnjenje. Komisija ocjenjuje te informacije i, prema potrebi, mijenja provedbeni akt kojim se utvrđuje dotična zajednička specifikacija.

Članak 42.

Pretpostavka sukladnosti s određenim zahtjevima

1. Za visokorizične UI sustave koji su trenirani i testirani na podacima koji odražavaju specifično zemljopisno, bihevioralno, kontekstualno ili radno okružje u kojem se namjeravaju koristiti pretpostavlja se da ispunjavaju relevantne zahtjeve utvrđene u članku 10. stavku 4.

2. Za visokorizične UI sustave koji su certificirani ili za koje je izdana izjava o sukladnosti u okviru programa kibernetičke sigurnosti na temelju Uredbe (EU) 2019/881 i na koje su objavljena upućivanja u *Službenom listu Europske unije* pretpostavlja se da ispunjavaju zahtjeve u pogledu kibernetičke sigurnosti iz članka 15. ove Uredbe ako certifikat o kibernetičkoj sigurnosti ili izjava o sukladnosti ili njihovi dijelovi obuhvaćaju te zahtjeve.

Članak 43.

Ocjenjivanje sukladnosti

1. U vezi s visokorizičnim UI sustavima iz točke 1. Priloga III., ako je dobavljač pri dokazivanju usklađenosti visokorizičnog UI sustava sa zahtjevima utvrđenima u odjeljku 2. primijenio usklađene norme iz članka 40. ili, ako je primjenjivo, zajedničke specifikacije iz članka 41., dobavljač bira jedan od sljedećih postupaka ocjenjivanja sukladnosti na temelju:

- (a) unutarnje kontrole iz Priloga VI.; ili
- (b) ocjenjivanja sustava upravljanja kvalitetom i ocjenjivanja tehničke dokumentacije iz Priloga VII., uz sudjelovanje prijavljenog tijela.

Pri dokazivanju usklađenosti visokorizičnog UI sustava sa zahtjevima utvrđenima u odjeljku 2. dobavljač primjenjuje postupak ocjenjivanja sukladnosti iz Priloga VII. ako:

- (a) usklađene norme iz članka 40. ne postoje, a zajedničke specifikacije iz članka 41. nisu dostupne;
- (b) dobavljač nije primijenio usklađenu normu ili je primijenio samo dio usklađene norme;
- (c) zajedničke specifikacije iz točke (a) postoje, ali ih dobavljač nije primijenio;
- (d) jedna ili više usklađenih normi iz točke (a) objavljena je uz ograničenje, i to samo za dio norme koji je ograničen.

Za potrebe postupka ocjenjivanja sukladnosti iz Priloga VII. dobavljač može odabrati bilo koje prijavljeno tijelo. Međutim, ako visokorizični UI sustav u upotrebu namjeravaju staviti tijela kaznenog progona, tijela za imigraciju ili tijela za azil odnosno institucije, tijela, uredi ili agencije Unije, tijelo za nadzor tržišta iz članka 74. stavka 8. ili 9., ovisno o slučaju, djeluje kao prijavljeno tijelo.

2. Za visokorizične UI sustave iz točaka od 2. do 8. Priloga III. dobavljači primjenjuju postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole iz Priloga VI., kojim se ne predviđa sudjelovanje prijavljenog tijela.

3. Za visokorizične UI sustave obuhvaćene zakonodavstvom Unije o usklađivanju navedenim u odjeljku A Priloga I. dobavljač primjenjuje relevantni postupak ocjenjivanja sukladnosti kako se zahtijeva tim pravnim aktima. Na te visokorizične UI sustave primjenjuju se zahtjevi utvrđeni u odjeljku 2. ovog poglavlja i dio su tog ocjenjivanja. Također se primjenjuju točke 4.3., 4.4., 4.5. i točka 4.6. peti odlomak Priloga VII.

Za potrebe tog ocjenjivanja prijavljena tijela koja su prijavljena na temelju tih pravnih akata imaju pravo kontrolirati sukladnost visokorizičnih UI sustava sa zahtjevima utvrđenima u odjeljku 2. pod uvjetom da je u kontekstu postupka prijavljivanja na temelju tih pravnih akata ocijenjeno ispunjavaju li dotična prijavljena tijela zahtjeve utvrđene u članku 31. stavcima 4., 5., 10. i 11.

Ako je pravnim aktom navedenim u odjeljku A Priloga II. proizvođaču proizvoda omogućeno da se izuzme iz ocjenjivanja sukladnosti koje provodi treća strana pod uvjetom da je taj proizvođač primijenio sve usklađene norme koje obuhvaćaju sve relevantne zahtjeve, taj proizvođač tu mogućnost može iskoristiti samo ako je primijenio i usklađene norme ili, ako je primjenjivo, zajedničke specifikacije iz članka 41., koje obuhvaćaju sve zahtjeve utvrđene u odjeljku 2. ovog poglavlja.

4. Za visokorizične UI sustave koji su već bili podvrgnuti postupku ocjenjivanja sukladnosti provodi se novi postupak ocjenjivanja sukladnosti ako dođe do bitnih izmjena, neovisno o tome namjerava li se izmijenjeni sustav dalje distribuirati ili ga nastavlja upotrebljavati isti subjekt koji ga već uvodi.

Za visokorizične UI sustave koji nastavljaju učiti nakon stavljanja na tržište ili u upotrebu, promjene visokorizičnog UI sustava i njegove učinkovitosti koje je dobavljač unaprijed odredio u trenutku početnog ocjenjivanja sukladnosti i koje su obuhvaćene informacijama u tehničkoj dokumentaciji iz točke 2. podtočke (f) Priloga IV. ne čine bitnu izmjenu.

5. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene priloga VI. i VII. njihovim ažuriranjem s obzirom na tehnički napredak.

6. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene stavaka 1. i 2. ovog članka kako bi visokorizične UI sustave iz točaka od 2. do 8. Priloga III. podvrgnula postupku ocjenjivanja sukladnosti iz Priloga VII. ili dijelovima tog postupka. Komisija takve delegirane akte donosi uzimajući u obzir djelotvornost postupka ocjenjivanja sukladnosti na temelju unutarnje kontrole iz Priloga VI. u sprečavanju rizika za zdravlje i sigurnost te zaštitu temeljnih prava koje takvi sustavi predstavljaju ili svođenju takvih rizika na najmanju moguću mjeru, kao i dostupnost adekvatnih kapaciteta i resursa među prijavljenim tijelima.

Članak 44.

Potvrde

1. Potvrde koje izdaju prijavljena tijela u skladu s Prilogom VII. sastavljaju se na jeziku koji relevantna tijela u državi članici u kojoj prijavljeno tijelo ima poslovni nastan mogu bez poteškoća razumjeti.

2. Potvrde vrijede tijekom razdoblja koje je u njima navedeno, a ono ne smije biti dulje od pet godina za UI sustave obuhvaćene Prilogom I. i dulje od četiri godine za UI sustave obuhvaćene Prilogom III. Na zahtjev dobavljača valjanost potvrde može se produljivati za daljnja razdoblja od kojih nijedno ne smije biti dulje od pet godina za UI sustave obuhvaćene Prilogom I. i dulje od četiri godine za UI sustave obuhvaćene Prilogom III., i to na temelju ponovnog ocjenjivanja u skladu s primjenjivim postupcima ocjenjivanja sukladnosti. Svaka dopuna potvrde ostaje valjana pod uvjetom da je valjana potvrda koju dopunjuje.

3. Ako prijavljeno tijelo ustanovi da UI sustav više ne ispunjava zahtjeve utvrđene u odjeljku 2., to prijavljeno tijelo, uzimajući u obzir načelo proporcionalnosti, suspendira ili povlači izdanu potvrdu ili uvodi ograničenja za nju, osim ako se primjerenim korektivnim mjerama koje dobavljač sustava poduzme u primjerenom roku koji je utvrdilo prijavljeno tijelo osigura usklađenost UI sustava s tim zahtjevima. Prijavljeno tijelo daje obrazloženje za svoju odluku.

Protiv odluka prijavljenih tijela, među ostalim protiv odluka o izdanim potvrdama o sukladnosti, mora biti dostupan žalbeni postupak.

Članak 45.

Obveze prijavljenih tijela u pogledu obavješćivanja

1. Prijavljena tijela obavješćuju tijelo koje provodi prijavljivanje o sljedećem:

- (a) potvrdama Unije o ocjenjivanju tehničke dokumentacije, dopunama tih potvrda i odobrenjima sustava upravljanja kvalitetom izdanima u skladu sa zahtjevima iz Priloga VII.;
- (b) odbijanju, ograničenju, suspenziji ili povlačenju potvrde Unije o ocjenjivanju tehničke dokumentacije ili odobrenja sustava upravljanja kvalitetom izdanog u skladu sa zahtjevima iz Priloga VII.;
- (c) svim okolnostima koje utječu na opseg prijavljivanja ili uvjete za prijavljivanje;
- (d) zahtjevima za dostavu informacija koje su primila od tijela za nadzor tržišta u vezi s aktivnostima ocjenjivanja sukladnosti;
- (e) na zahtjev, o aktivnostima ocjenjivanja sukladnosti provedenima u okviru njihove prijave i svim ostalim provedenim aktivnostima, uključujući prekogranične aktivnosti i podugovaranje.

2. Svako prijavljeno tijelo obavješćuje druga prijavljena tijela o sljedećem:

- (a) odobrenjima sustava upravljanja kvalitetom koja je odbilo, suspendiralo ili povuklo i, na zahtjev, odobrenjima sustava upravljanja kvalitetom koja je izdalo;
- (b) potvrdama Unije o ocjenjivanju tehničke dokumentacije ili dopunama tih potvrda koje je odbilo, povuklo, suspendiralo ili na neki drugi način ograničilo te, na zahtjev, potvrdama i/ili njihovim dopunama koje je izdalo.

3. Svako prijavljeno tijelo drugim prijavljenim tijelima koja provode slične aktivnosti ocjenjivanja sukladnosti za iste vrste UI sustava dostavlja relevantne informacije o pitanjima povezanim s negativnim i, na zahtjev, pozitivnim rezultatima ocjenjivanja sukladnosti.
4. Prijavljena tijela u skladu s člankom 78. štite povjerljivost informacija koje su pribavila.

Članak 46.

Odstupanje od postupka ocjenjivanja sukladnosti

1. Odstupajući od članka 43., i na propisno obrazložen zahtjev, svako tijelo za nadzor tržišta može odobriti stavljanje određenih visokorizičnih UI sustava na tržište ili u upotrebu na državnom području dotične države članice zbog iznimnih razloga koji se odnose na javnu sigurnost ili zaštitu života i zdravlja ljudi, zaštitu okoliša ili zaštitu ključne industrijske i infrastrukturne imovine. Trajanje tog odobrenja ograničeno je na razdoblje provedbe potrebnih postupaka ocjenjivanja sukladnosti, uzimajući u obzir iznimne razloge koji opravdavaju odstupanje. Ti se postupci dovršavaju bez nepotrebne odgode.
2. U propisno opravdanoj hitnoj situaciji zbog iznimnih razloga koji se odnose na javnu sigurnost ili u slučaju konkretne, znatne i izravne prijetnje životu ili tjelesnoj sigurnosti fizičkih osoba, tijela kaznenog progona ili tijela civilne zaštite mogu određeni visokorizični UI sustav staviti u upotrebu bez odobrenja iz stavka 1. pod uvjetom da se to odobrenje bez nepotrebne odgode zatraži tijekom ili nakon upotrebe. Ako je odobrenje iz stavka 1. odbijeno, upotreba visokorizičnog UI sustava smjesta se prekida te se odmah odbacuju svi rezultati i izlazni podaci proizašli iz takve upotrebe.
3. Odobrenje iz stavka 1. izdaje se samo ako tijelo za nadzor tržišta zaključi da visokorizični UI sustav ispunjava zahtjeve iz odjeljka 2. Tijelo za nadzor tržišta obavješćuje Komisiju i druge države članice o svim odobrenjima izdanim na temelju stavaka 1 i 2. Ta obveza ne obuhvaća osjetljive operativne podatke u vezi s aktivnostima tijela kaznenog progona.
4. Ako u roku od 15 kalendarskih dana od primitka informacija iz stavka 3. nijedna država članica ni Komisija ne podnese prigovor na odobrenje koje je izdalo tijelo za nadzor tržišta određene države članice u skladu sa stavkom 1., to se odobrenje smatra opravdanim.
5. Ako u roku od 15 kalendarskih dana od primitka obavijesti iz stavka 3. određena država članica podnese prigovor na odobrenje koje je izdalo tijelo za nadzor tržišta druge države članice ili ako Komisija smatra da je to odobrenje u suprotnosti s pravom Unije ili da je zaključak država članica o usklađenosti sustava iz stavka 3. neosnovan, Komisija bez odgode započinje savjetovanje s relevantnom državom članicom. U savjetovanju sudjeluju dotični operateri i omogućuje im se da iznesu svoja stajališta. Komisija ih uzima u obzir i odlučuje je li odobrenje opravdano. Komisija svoju odluku upućuje dotičnim državama članicama i dotičnim operaterima.
6. Ako Komisija odobrenje smatra neopravdanim, tijelo za nadzor tržišta dotične države članice povlači to odobrenje.
7. Kad je riječ o visokorizičnim UI sustavima koji su povezani s proizvodima obuhvaćenima zakonodavstvom Unije o usklađivanju navedenim u odjeljku A Priloga I., primjenjuju se samo odstupanja od ocjenjivanja sukladnosti utvrđena u tom zakonodavstvu Unije o usklađivanju.

Članak 47.

EU izjava o sukladnosti

1. Dobavljač sastavlja pisanu, strojno čitljivu EU izjavu o sukladnosti, potpisanu fizički ili elektronički, za svaki visokorizični UI sustav i drži je na raspolaganju nacionalnim nadležnim tijelima tijekom razdoblja od deset godina nakon stavljanja tog visokorizičnog UI sustava na tržište ili u upotrebu. U EU izjavi o sukladnosti navodi se za koji je visokorizični UI sustav ona sastavljena. Primjerak EU izjave o sukladnosti dostavlja se relevantnim nacionalnim nadležnim tijelima na njihov zahtjev.

2. U EU izjavi o sukladnosti navodi se da dotični visokorizični UI sustav ispunjava zahtjeve utvrđene u odjeljku 2. EU izjava o sukladnosti sadržava informacije utvrđene u Prilogu V. i prevodi se na jezik koji nacionalna nadležna tijela država članica u kojima se visokorizični UI sustav stavlja na tržište ili na raspolaganje mogu bez poteškoća razumjeti.

3. Ako visokorizični UI sustavi podliježu drugom zakonodavstvu Unije o usklađivanju kojim se također zahtijeva EU izjava o sukladnosti, sastavlja se jedinstvena EU izjava o sukladnosti koja se odnosi na svo pravo Unije koje se primjenjuje na dotični visokorizični UI sustav. Ta izjava sadržava sve informacije potrebne za identifikaciju zakonodavstva Unije o usklađivanju na koje se izjava odnosi.

4. Sastavljanjem EU izjave o sukladnosti dobavljač preuzima odgovornost za ispunjavanje zahtjeva utvrđenih u odjeljku 2. Dobavljač prema potrebi ažurira EU izjavu o sukladnosti.

5. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene Priloga V. ažuriranjem sadržaja EU izjave o sukladnosti utvrđene u tom prilogu kako bi se uveli elementi koji postanu potrebni s obzirom na tehnički napredak.

Članak 48.

Oznaka CE

1. Za oznaku CE vrijede opća načela utvrđena u članku 30. Uredbe (EZ) br. 765/2008.

2. Za visokorizične UI sustave koji se pružaju digitalno digitalna oznaka CE upotrebljava se samo ako joj se može lako pristupiti preko sučelja s kojeg se pristupa tom sustavu ili s pomoću lako dostupnog strojno čitljivog koda ili drugih elektroničkih sredstava.

3. Oznaka CE stavlja se na visokorizične UI sustave tako da bude vidljiva, čitka i neizbrisiva. Ako to zbog prirode visokorizičnog UI sustava nije moguće ili nije opravdano, oznaka CE stavlja se na pakiranje ili na popratnu dokumentaciju, ovisno o slučaju.

4. Ako je primjenjivo, uz oznaku CE navodi se identifikacijski broj prijavljenog tijela odgovornog za postupke ocjenjivanja sukladnosti iz članka 43. Identifikacijski broj prijavljenog tijela stavlja samo prijavljeno tijelo ili ga prema njegovim uputama stavlja dobavljač ili dobavljačev ovlašteni zastupnik. Taj identifikacijski broj navodi se i u svim promotivnim materijalima u kojima se navodi da dotični visokorizični UI sustav ispunjava zahtjeve u pogledu oznake CE.

5. Ako visokorizični UI sustavi podliježu drugom pravu Unije kojim se također predviđa stavljanje oznake CE, na oznaci CE navodi se da visokorizični UI sustav ispunjava i zahtjeve iz tog drugog prava.

Članak 49.

Registracija

1. Prije stavljanja na tržište ili u upotrebu visokorizičnog UI sustava iz Priloga III., uz izuzeće visokorizičnih UI sustava iz točke 2. Priloga III., dobavljač ili, ako je primjenjivo, ovlašteni zastupnik registrira sebe i svoj sustav u bazi podataka EU-a iz članka 71.

2. Prije stavljanja na tržište ili u upotrebu UI sustava za koji je dobavljač zaključio da nije visokorizičan u skladu s člankom 6. stavkom 3., taj dobavljač ili, ako je primjenjivo, ovlašteni zastupnik registrira sebe i taj sustav u bazi podataka EU-a iz članka 71.

3. Prije stavljanja u upotrebu ili korištenja visokorizičnog UI sustava iz Priloga III., uz izuzeće visokorizičnih UI sustava iz točke 2. Priloga III., subjekti koji uvode sustav koji su tijela javne vlasti, institucije, tijela uredi ili agencije Unije ili osobe koje djeluju u njihovo ime registriraju se, odabiru sustav i registriraju njegovo korištenje u bazi podataka EU-a iz članka 71.

4. Za visokorizične UI sustave iz točaka 1., 6. i 7. Priloga III., u području kaznenog progona, migracija, azila i upravljanja nadzorom državne granice registracija iz stavaka 1., 2. i 3. ovog članka provodi se u sigurnom dijelu baze podataka EU-a iz članka 71. koji nije javno dostupan, a uključuje samo informacije iz sljedećega, ovisno o slučaju:

(a) odjeljka A točaka od 1. do 10. Priloga VIII., osim točaka 6., 8. i 9.;

(b) odjeljka B točaka od 1. do 5. i točaka 8. i 9. Priloga VIII.;

(c) odjeljka C točaka od 1. do 3. Priloga VIII.;

(d) točaka 1., 2., 3. i 5. Priloga IX.

Samo Komisija i nacionalna tijela iz članka 74. stavka 8. imaju pristup odgovarajućim dijelovima baze podataka EU-a kojima je pristup ograničen, a koji su navedeni u prvom podstavku ovog stavka.

5. Visokorizični UI sustavi iz točke 2. Priloga III. registriraju se na nacionalnoj razini.

POGLAVLJE IV.

OBVEZE U POGLEDU TRANSPARENTNOSTI ZA DOBAVLJAČE ODREĐENIH UI SUSTAVA I SUBJEKTE KOJI IH UVODE

Članak 50.

Obveze u pogledu transparentnosti za dobavljače određenih UI sustava i subjekte koji ih uvode

1. Dobavljači osiguravaju da su UI sustavi koji su namijenjeni izravnoj interakciji s fizičkim osobama dizajnirani i razvijeni na takav način da se dotične fizičke osobe obavješćuje o tome da su u interakciji s UI sustavom, osim ako je to očito sa stajališta razmjerno dobro informirane, pronicljive i oprezne fizičke osobe, uzimajući u obzir okolnosti i kontekst upotrebe. Ta se obveza ne primjenjuje na UI sustave koji su zakonski odobreni za otkrivanje, sprečavanje, istragu ili kazneni progon kaznenih djela, podložno odgovarajućim zaštitnim mjerama za prava i slobode trećih strana, osim ako su ti sustavi dostupni javnosti za prijavu kaznenih djela.

2. Dobavljači UI sustava, uključujući UI sustave opće namjene, koji generiraju sintetički audiosadržaj, slikovni sadržaj, videosadržaj ili tekstovni sadržaj osiguravaju da izlazni rezultati UI sustava budu označeni u strojno čitljivom obliku i da ih se može prepoznati kao umjetno generirane ili manipulirane. Dobavljači osiguravaju da njihova tehnička rješenja budu djelotvorna, interoperabilna, otporna i pouzdana u mjeri u kojoj je to tehnički izvedivo, uzimajući u obzir posebnosti i ograničenja različitih vrsta sadržaja, troškove provedbe i općepriznata najnovija dostignuća, što se može odražavati u relevantnim tehničkim normama. Ta se obveza ne primjenjuje ako UI sustavi obavljaju pomoćnu funkciju za standardno uređivanje ili bitno ne mijenjaju ulazne podatke koje pruža subjekt koji uvodi sustav ili njihovu semantiku, ili ako su zakonski odobreni za otkrivanje, sprečavanje, istragu ili kazneni progon kaznenih djela.

3. Subjekti koji uvode sustav za prepoznavanje emocija ili sustav za biometrijsku kategorizaciju obavješćuju fizičke osobe koje su izložene tom sustavu o njegovu radu, a osobne podatke obrađuju u skladu s uredbama (EU) 2016/679 i (EU) 2018/1725 te Direktivom (EU) 2016/680, ovisno o slučaju. Ta se obveza ne primjenjuje na UI sustave za biometrijsku kategorizaciju i prepoznavanje emocija koji su zakonski odobreni za otkrivanje, sprečavanje ili istragu kaznenih djela, podložno odgovarajućim zaštitnim mjerama za prava i slobode trećih strana i u skladu s pravom Unije.

4. Subjekti koji uvode UI sustav koji generira ili manipulira slikovnim sadržajem, audiosadržajem ili videosadržajem koji čini uvjerljiv krivotvoreni sadržaj (*deep fake*) moraju navesti da je taj sadržaj umjetno generiran ili da je njime manipulirano. Ta se obveza ne primjenjuje ako je korištenje zakonski odobreno za otkrivanje, sprečavanje, istragu ili kazneni progon kaznenih djela. Ako je sadržaj dio očigledno umjetničkog, kreativnog, satiričnog, fiktivnog ili analognog djela ili programa, obveze u pogledu transparentnosti iz ovog stavka ograničene su na otkrivanje postojanja takvog generiranog ili manipuliranog sadržaja na odgovarajući način kojim se ne ometa prikazivanje tog djela ili uživanje u njemu.

Subjekti koji uvode UI sustav koji generira ili manipulira tekstom koji se objavljuje u svrhu informiranja javnosti o pitanjima od javnog interesa moraju navesti da je tekst umjetno generiran ili da je njime manipulirano. Ta se obveza ne primjenjuje ako je korištenje zakonski odobreno za otkrivanje, sprečavanje, istragu ili kazneni progon kaznenih djela ili ako je sadržaj generiran umjetnom inteligencijom prošao proces preispitivanja koje provodi čovjek ili uredničku kontrolu i ako fizička ili pravna osoba snosi uredničku odgovornost za objavu sadržaja.

5. Informacije iz stavaka od 1. do 4. dotičnim se fizičkim osobama pružaju na jasan i raspoznatljiv način najkasnije u trenutku prve interakcije ili prvog izlaganja. Te informacije moraju ispunjavati primjenjive zahtjeve u pogledu pristupačnosti.

6. Stavci od 1. do 4. ne utječu na zahtjeve i obveze iz poglavlja III. i njima se ne dovode u pitanje druge obveze u pogledu transparentnosti utvrđene u pravu Unije ili nacionalnom pravu za subjekte koji uvode UI sustave.

7. Ured za umjetnu inteligenciju potiče i olakšava izradu kodeksa prakse na razini Unije kako bi se olakšala djelotvorna provedba obveza u pogledu otkrivanja i označivanja umjetno generiranog ili manipuliranog sadržaja. Komisija može donositi provedbene akte radi odobravanja tih kodeksa prakse u skladu s postupkom utvrđenim u članku 56. stavku 6. Ako smatra da kodeks nije adekvatan, Komisija može donositi provedbene akte o utvrđivanju zajedničkih pravila za provedbu tih obveza u skladu s postupkom ispitivanja utvrđenim u članku 98. stavku 2.

POGLAVLJE V.

UI MODELI OPĆE NAMJENE

ODJELJAK 1.

Pravila o klasifikaciji

Članak 51.

Klasifikacija UI modela opće namjene kao UI modela opće namjene sa sistemskim rizikom

1. UI model opće namjene klasificira se kao UI model opće namjene sa sistemskim rizikom ako ispunjava bilo koji od sljedećih uvjeta:

- (a) ima sposobnosti visokog učinka evaluirane na temelju odgovarajućih tehničkih alata i metodologija, uključujući pokazatelje i referentne vrijednosti;
- (b) na temelju odluke Komisije, po službenoj dužnosti ili slijedom kvalificiranog upozorenja znanstvenog povjerenstva, ima sposobnosti ili učinak jednakovrijedne onima utvrđenima u točki (a), uzimajući u obzir kriterije utvrđene u Prilogu XIII.

2. Pretpostavlja se da UI model opće namjene ima sposobnosti visokog učinka u skladu sa stavkom 1. točkom (a) ako je kumulativna količina računanja korištena za njegovo treniranje iskazana brojem matematičkih operacija nad brojevima s pomičnim zarezom u sekundi veća od 10^{25} .

3. Komisija donosi delegirane akte u skladu s člankom 97. radi izmjene pragova navedenih u stavcima 1. i 2. ovog članka te, prema potrebi, radi dopune referentnih vrijednosti i pokazatelja s obzirom na tehnološki razvoj, kao što su algoritamska poboljšanja ili povećanje učinkovitosti hardvera, kako bi ti pragovi odražavali najnovija dostignuća.

Članak 52.

Postupak

1. Ako UI model opće namjene ispunjava uvjet iz članka 51. stavka 1. točke (a), dotični dobavljač o tome obavještuje Komisiju bez odgođene, a u svakom slučaju u roku od dva tjedna nakon što je taj zahtjev ispunjen ili nakon što postane poznato da će biti ispunjen. Ta obavijest uključuje informacije potrebne kako bi se dokazalo da je dotični zahtjev ispunjen. Ako Komisija sazna za UI model opće namjene koji predstavlja sistemske rizike, a o kojem nije bila obaviještena, može ga odlučiti odrediti kao model sa sistemskim rizikom.

2. Dobavljač UI modela opće namjene koji ispunjava uvjet iz članka 51. stavka 1. točke (a) može uz svoju obavijest dostaviti dostatno potkrijepljene argumente kako bi dokazao da UI model opće namjene iznimno, iako ispunjava navedeni zahtjev, zbog svojih specifičnih karakteristika ne predstavlja sistemske rizike i da ga stoga ne bi trebalo klasificirati kao UI model opće namjene sa sistemskim rizikom.

3. Ako Komisija zaključi da argumenti dostavljeni na temelju stavka 2. nisu dostatno potkrijepljeni i da dotični dobavljač nije dokazao da UI model opće namjene zbog svojih specifičnih karakteristika ne predstavlja sistemske rizike, ona odbacuje te argumente, a UI model opće namjene smatra se UI modelom opće namjene sa sistemskim rizikom.

4. Komisija može UI model opće namjene odrediti kao model koji predstavlja sistemske rizike na temelju kriterija iz Priloga XIII., po službenoj dužnosti ili slijedom kvalificiranog upozorenja znanstvenog povjerenstva u skladu s člankom 90. stavkom 1. točkom (a).

Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene Priloga XIII. utvrđivanjem i ažuriranjem kriterija utvrđenih u tom prilogu.

5. Na obrazloženi zahtjev dobavljača čiji je model u skladu sa stavkom 4. određen kao UI model opće namjene sa sistemskim rizikom, Komisija takav zahtjev uzima u obzir i može odlučiti ponovno ocijeniti može li se i dalje smatrati da UI model opće namjene predstavlja sistemske rizike na temelju kriterija iz Priloga XIII. Takav zahtjev mora sadržavati objektivne, detaljne i nove razloge koji su se pojavili nakon odluke o određivanju. Dobavljači mogu zatražiti ponovnu ocjenu najranije šest mjeseci nakon odluke o određivanju. Ako Komisija nakon ponovne ocjene odluči zadržati određivanje modela kao UI modela opće namjene sa sistemskim rizikom, dobavljači mogu zatražiti ponovno ocjenjivanje najranije šest mjeseci nakon te odluke.

6. Komisija osigurava objavljivanje popisa UI modelâ opće namjene sa sistemskim rizikom i ažurira ga, ne dovodeći u pitanje potrebu za poštovanjem i zaštitom prava intelektualnog vlasništva i povjerljivih poslovnih informacija ili poslovnih tajni u skladu s pravom Unije i nacionalnim pravom.

ODJELJAK 2.

Obveze dobavljača UI modelâ opće namjene

Članak 53.

Obveze dobavljača UI modelâ opće namjene

1. Dobavljači UI modelâ opće namjene:

(a) izrađuju i ažuriraju tehničku dokumentaciju modela, među ostalim o postupku njegova treniranja i testiranja te rezultatima njegove evaluacije, koja sadržava barem informacije utvrđene u Prilogu XI., kako bi je na zahtjev dostavili Uredu za umjetnu inteligenciju i nacionalnim nadležnim tijelima;

(b) izrađuju, ažuriraju i stavljaju na raspolaganje informacije i dokumentaciju dobavljačima UI sustava koji namjeravaju integrirati UI model opće namjene u svoje UI sustave. Ne dovodeći u pitanje potrebu za poštovanjem i zaštitom prava intelektualnog vlasništva i povjerljivih poslovnih informacija ili poslovnih tajni u skladu s pravom Unije i nacionalnim pravom, te informacije i dokumentacija:

i. omogućuju dobavljačima UI sustava da dobro razumiju sposobnosti i ograničenja UI modela opće namjene i da ispune svoje obveze na temelju ove Uredbe; i

ii. sadržavaju barem elemente utvrđene u Prilogu XII.;

(c) uspostavljaju politiku usklađivanja s pravom Unije o autorskom pravu i povezanim pravima, posebno kako bi utvrdili i poštovali, među ostalim i s pomoću najsuvremenijih tehnologija, pridržaj prava izražen u skladu s člankom 4. stavkom 3. Direktive (EU) 2019/790;

(d) izrađuju i objavljuju dovoljno detaljan sažetak o sadržaju upotrijebljenom za treniranje UI modela opće namjene, prema predlošku Ureda za umjetnu inteligenciju.

2. Obveze utvrđene u stavku 1. točkama (a) i (b) ne primjenjuju se na dobavljače UI modela koji se objavljuju na temelju besplatne licencije za softver otvorenog koda koja omogućuje pristup modelu te njegovu upotrebu, izmjenu i distribuciju i čiji su parametri, uključujući težinske faktore, informacije o arhitekturi modela te informacije o upotrebi modela, javno dostupni. Ta se iznimka ne primjenjuje na UI modele opće namjene sa sistemskim rizikom.
3. Dobavljači UI modela opće namjene prema potrebi surađuju s Komisijom i nacionalnim nadležnim tijelima u izvršavanju njihovih nadležnosti i ovlasti na temelju ove Uredbe.
4. Dobavljači UI modela opće namjene mogu se do objave usklađene norme osloniti na kodekse prakse u smislu članka 56. kako bi dokazali da ispunjavaju obveze utvrđene u stavku 1. ovog članka. Ispunjavanjem europskih usklađenih normi za dobavljače vrijedi pretpostavka sukladnosti u mjeri u kojoj su te obveze obuhvaćene tim normama. Dobavljači UI modela opće namjene koji ne poštuju odobreni kodeks prakse ili ne ispunjavaju europsku usklađenu normu moraju dokazati alternativne adekvatne načine usklađivanja kako bi ih ocijenila Komisija.
5. Kako bi se olakšalo usklađivanje s Prilogom XI., a posebno s njegovom točkom 2. podtočkama (d) i (e), Komisija je ovlaštena z donošenje delegiranih akata u skladu s člankom 97. kako bi detaljno opisala metodologije mjerenja i izračuna u cilju omogućavanja usporedive i provjerljive dokumentacije.
6. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. stavkom 2. radi izmjene priloga XI. i XII. s obzirom na tehnološki razvoj.
7. Sa svim informacijama ili dokumentacijom koji se pribave u skladu s ovim člankom, uključujući poslovne tajne, postupa se u skladu s obvezama u pogledu povjerljivosti utvrđenima u članku 78.

Članak 54.

Ovlašteni zastupnici dobavljača UI modela opće namjene

1. Prije stavljanja UI modela opće namjene na tržište Unije dobavljači s poslovnim nastanom u trećim zemljama pisanim ovlaštenjem imenuju ovlaštenog zastupnika s poslovnim nastanom Uniji.
2. Dobavljač omogućuje svojem ovlaštenom zastupniku da obavlja zadaće navedene u ovlaštenju koje je dobio od dobavljača.
3. Ovlašteni zastupnik obavlja zadaće navedene u ovlaštenju koje je dobio od dobavljača. On dostavlja primjerak ovlaštenja Uredu za umjetnu inteligenciju na njegov zahtjev, na jednom od službenih jezika institucija Unije. Za potrebe ove Uredbe ovlaštenjem se ovlaštenom zastupniku daje ovlast da obavlja sljedeće zadaće:
 - (a) provjerava je li tehnička dokumentacija iz Priloga XI. sastavljena i je li dobavljač ispunio sve obveze iz članka 53. i, ako je primjenjivo, članka 55.;
 - (b) drži primjerak tehničke dokumentacije iz Priloga XI. na raspolaganju Uredu za umjetnu inteligenciju i nacionalnim nadležnim tijelima tijekom razdoblja od deset godina nakon stavljanja UI modela opće namjene na tržište i čuva kontaktne podatke dobavljača koji je imenovao ovlaštenog zastupnika;
 - (c) Uredu za umjetnu inteligenciju na obrazloženi zahtjev dostavlja sve informacije i dokumentaciju, uključujući one iz točke (b), koji su potrebni za dokazivanje ispunjavanja obveza iz ovog poglavlja;
 - (d) na obrazloženi zahtjev surađuje s Uredom za umjetnu inteligenciju i nadležnim tijelima u svim mjerama koje oni poduzimaju u vezi s UI modelom opće namjene, među ostalim onda kada je model integriran u UI sustave koji se stavljaju na tržište ili u upotrebu u Uniji.
4. Ovlaštenjem se ovlaštenog zastupnika ovlašćuje da, uz dobavljača ili umjesto dobavljaču, bude osoba kojoj se obraćaju Ured za umjetnu inteligenciju ili nadležna tijela u vezi sa svim pitanjima povezanim sa osiguravanjem usklađenosti s ovom Uredbom.

5. Ovlašteni zastupnik ukida ovlaštenje ako smatra ili ima razloga smatrati da dobavljač postupa protivno svojim obvezama na temelju ove Uredbe. U tom slučaju ovlašteni zastupnik o ukidanju ovlaštenja i razlozima za ukidanje ujedno odmah obavještuje Ured za umjetnu inteligenciju.

6. Obveza utvrđena u ovom članku ne primjenjuje se na dobavljače UI modela opće namjene koji se objavljuju na temelju besplatne licencije otvorenog koda koja omogućuje pristup modelu te njegovu upotrebu, izmjenu i distribuciju i čiji su parametri, uključujući težinske faktore, informacije o arhitekturi modela te informacije o upotrebi modela, javno dostupni, osim ako UI modeli opće namjene predstavljaju sistemske rizike.

ODJELJAK 3.

Obveze dobavljača UI modelâ opće namjene sa sistemskim rizikom

Članak 55.

Obveze dobavljača UI modelâ opće namjene sa sistemskim rizikom

1. Uz obveze navedene u člancima 53. i 54. dobavljači UI modelâ opće namjene sa sistemskim rizikom:
 - (a) provode evaluaciju modela u skladu sa standardiziranim protokolima i alatima koji odražavaju najnovija dostignuća, uključujući provođenje i dokumentiranje neprijateljskog testiranja modela radi utvrđivanja i smanjivanja sistemskog rizika;
 - (b) procjenjuju i smanjuju moguće sistemske rizike na razini Unije, uključujući njihove izvore, koji mogu proizići iz razvoja, stavljanja na tržište ili korištenja UI modelâ opće namjene sa sistemskim rizikom;
 - (c) prate, dokumentiraju i bez nepotrebne odgode dostavljaju Uredu za umjetnu inteligenciju i, prema potrebi, nacionalnim nadležnim tijelima, relevantne informacije o ozbiljnim incidentima i mogućim korektivnim mjerama za njihovo rješavanje;
 - (d) osiguravaju odgovarajuću razinu kibernetičkosigurnosne zaštite UI modela opće namjene sa sistemskim rizikom i fizičke infrastrukture tog modela.
2. Dobavljači UI modelâ opće namjene sa sistemskim rizikom mogu se do objave usklađene norme osloniti na kodekse prakse u smislu članka 56. kako bi dokazali da ispunjavaju obveze utvrđene u stavku 1. ovog članka. Ispunjavanjem europskih usklađenih normi za dobavljače vrijedi pretpostavka sukladnosti u mjeri u kojoj su te obveze obuhvaćene tim normama. Dobavljači UI modelâ opće namjene sa sistemskim rizikom koji ne poštuju odobreni kodeksa prakse ili ne ispunjavaju europsku usklađenu normu moraju dokazati alternativne adekvatne načine usklađivanja kako bi ih procijenila Komisija.
3. Sa svim informacijama ili dokumentacijom koji se pribave na temelju ovog članka, uključujući poslovne tajne, postupa se u skladu s obvezama u pogledu povjerljivosti utvrđenima u članku 78.

ODJELJAK 4.

Kodeksi prakse

Članak 56.

Kodeksi prakse

1. Ured za umjetnu inteligenciju potiče i olakšava izradu kodeksâ prakse na razini Unije kako bi se doprinijelo pravilnoj primjeni ove Uredbe, uzimajući u obzir međunarodne pristupe.
2. Ured za umjetnu inteligenciju i Vijeće za umjetnu inteligenciju nastoje osigurati da kodeksi prakse obuhvaćaju barem obveze iz članaka 53. i 55., uključujući sljedeća pitanja:

- (a) sredstva kojima se osigurava da se informacije iz članka 53. stavka 1. točaka (a) i (b) ažuriraju s obzirom na tržišni i tehnološki razvoj;
- (b) odgovarajuću razinu detaljnosti sažetka o sadržaju upotrijebljenom za treniranje;
- (c) utvrđivanje vrste i prirode sistemskih rizika na razini Unije, uključujući, prema potrebi, njihove izvore;
- (d) mjere, postupke i modalitete za procjenu sistemskih rizika i upravljanje sistemskim rizicima na razini Unije, uključujući dokumentaciju o njima, koji su razmjerni rizicima i kojima se uzimaju u obzir ozbiljnost i vjerojatnost tih rizika te posebni izazovi uklanjanja tih rizika s obzirom na moguće načine na koje se takvi rizici mogu pojaviti i materijalizirati duž vrijednosnog lanca umjetne inteligencije.

3. Ured za umjetnu inteligenciju može pozvati sve dobavljače UI modelâ opće namjene, kao i relevantna nacionalna nadležna tijela, da sudjeluju u izradi kodeksâ prakse. Taj proces mogu poduprijeti organizacije civilnog društva, industrija, akademska zajednica i drugi relevantni dionici, poput dobavljača niže u lancu opskrbe i neovisnih stručnjaka.

4. Ured za umjetnu inteligenciju i Vijeće za umjetnu inteligenciju nastoje osigurati da se u kodeksima prakse jasno utvrde njihovi specifični ciljevi i da sadržavaju obveze ili mjere, prema potrebi uključujući ključne pokazatelje uspješnosti, za osiguravanje postizanja tih ciljeva, te da se u njima na odgovarajući način uzimaju u obzir potrebe i interesi svih zainteresiranih strana, među ostalim uključenih osoba, na razini Unije.

5. Ured za umjetnu inteligenciju nastoji osigurati da sudionici kodeksâ prakse redovito izvješćuju Ured za umjetnu inteligenciju o provedbi obveza i poduzetim mjerama te njihovim rezultatima, među ostalim u odnosu na ključne pokazatelje uspješnosti, prema potrebi. Ključni pokazatelji uspješnosti i obveze izvješćivanja moraju odražavati razlike u veličini i kapacitetu među različitim sudionicima.

6. Ured za umjetnu inteligenciju i Vijeće za umjetnu inteligenciju redovito prate i ocjenjuju ostvarivanje ciljeva kodeksâ prakse od strane sudionika i njihov doprinos pravilnoj primjeni ove Uredbe. Ured za umjetnu inteligenciju i Vijeće za umjetnu inteligenciju ocjenjuju obuhvaćaju li kodeksi prakse obveze iz članaka 53. i 55., te redovito prate i evaluiraju postizanje njihovih ciljeva. Objavljaju svoju ocjenu adekvatnosti kodeksâ prakse.

Komisija može provedbenim aktom odobriti kodeks prakse i učiniti ga općenito valjanim u Uniji. Taj provedbeni akt donosi se u skladu s postupkom ispitivanja iz članka 98. stavka 2.

7. Ured za umjetnu inteligenciju može pozvati sve dobavljače UI modelâ opće namjene da poštuju kodekse prakse. Za dobavljače UI modela opće namjene koji ne predstavljaju sistemske rizike to poštovanje može se ograničiti na obveze iz članka 53., osim ako izričito izraze interes da se pridruže cijelom kodeksu.

8. Ured za umjetnu inteligenciju prema potrebi također potiče i olakšava preispitivanje i prilagodbu kodeksâ prakse, posebno s obzirom na nove norme. Ured za umjetnu inteligenciju pomaže u ocjenjivanju dostupnih normi.

9. Kodeksi prakse moraju biti spremni najkasnije do 2. svibnja 2025. Ured za umjetnu inteligenciju poduzima potrebne korake, uključujući pozivanje dobavljača u skladu sa stavkom 7.

Ako do 2. kolovoza 2025. kodeks prakse ne može biti dovršen ili ako Ured za umjetnu inteligenciju nakon ocjenjivanja na temelju stavka 6. ovog članka smatra da kodeks prakse nije adekvatan, Komisija može provedbenim aktima propisati zajednička pravila za provedbu obveza iz članaka 53. i 55., među ostalim u pogledu pitanja iz stavka 2. ovog članka. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 98. stavka 2.

POGLAVLJE VI.
MJERE ZA POTPORU INOVACIJAMA

Članak 57.

Regulatorna izolirana okruženja za umjetnu inteligenciju

1. Države članice osiguravaju da njihova nadležna tijela uspostave barem jedno regulatorno izolirano okruženje za umjetnu inteligenciju na nacionalnoj razini, koje mora biti operativno do 2. kolovoza 2026. To izolirano okruženje može se uspostaviti i zajedno s nadležnim tijelima drugih država članica. Komisija može pružiti tehničku potporu, savjete i alate za uspostavu i rad regulatornih izoliranih okruženja za umjetnu inteligenciju.

Obveza iz prvog podstavka može se ispuniti i sudjelovanjem u postojećem izoliranom okruženju ako se tim sudjelovanjem osigurava jednakovrijedna razina nacionalne pokrivenosti za države članice sudionice.

2. Mogu se uspostaviti i dodatna regulatorna izolirana okruženja za umjetnu inteligenciju na regionalnoj ili lokalnoj razini ili se ona mogu uspostaviti zajedno s nadležnim tijelima drugih država članica.

3. Europski nadzornik za zaštitu podataka također može uspostaviti regulatorno izolirano okruženje za umjetnu inteligenciju za institucije, tijela, urede i agencije Unije te može izvršavati uloge i zadaće nacionalnih nadležnih tijela u skladu s ovim poglavljem.

4. Države članice osiguravaju da nadležna tijela iz stavaka 1. i 2. dodijele dostatna sredstva za djelotvorno i pravodobno usklađivanje s ovim člankom. Nacionalna nadležna tijela prema potrebi surađuju s drugim relevantnim tijelima i mogu dopustiti sudjelovanje drugih aktera iz ekosustava umjetne inteligencije. Ovaj članak ne utječe na druga regulatorna izolirana okruženja uspostavljena na temelju prava Unije ili nacionalnog prava. Države članice osiguravaju odgovarajuću razinu suradnje između tijela koja nadziru ta druga izolirana okruženja i nacionalnih nadležnih tijela.

5. Regulatorna izolirana okruženja za umjetnu inteligenciju uspostavljena na temelju stavka 1. pružaju kontrolirano okruženje koje potiče inovacije i olakšava razvoj, treniranje, testiranje i validaciju inovativnih UI sustava tijekom ograničenog razdoblja prije njihova stavljanja na tržište ili u upotrebu u skladu s posebnim planom izoliranog okruženja dogovorenim između dobavljača ili potencijalnih dobavljača i nadležnog tijela. Takva izolirana okruženja mogu uključivati testiranje u stvarnim uvjetima pod nadzorom u izoliranom okruženju.

6. Nadležna tijela prema potrebi pružaju smjernice, nadzor i potporu u regulatornom izoliranom okruženju za umjetnu inteligenciju radi utvrđivanja rizika, posebno za temeljna prava, zdravlje i sigurnost, te radi utvrđivanja testiranja, mjera ublažavanja i njihove djelotvornosti u odnosu na obveze i zahtjeve iz ove Uredbe i, prema potrebi, iz drugog prava Unije i nacionalnog prava čije se ispunjavanje nadzire u izoliranom okruženju.

7. Nadležna tijela dobavljačima i potencijalnim dobavljačima koji sudjeluju u regulatornom izoliranom okruženju za umjetnu inteligenciju pružaju smjernice o regulatornim očekivanjima i načinu ispunjavanja zahtjeva i obveza utvrđenih u ovoj Uredbi.

Na zahtjev dobavljača ili potencijalnog dobavljača UI sustava nadležno tijelo dostavlja pisani dokaz o aktivnostima koje su uspješno provedene u izoliranom okruženju. Nadležno tijelo dostavlja i završno izvješće koje sadržava pojedinosti o aktivnostima provedenima u izoliranom okruženju te povezanim rezultatima i ishodima učenja. Dobavljači mogu takvu dokumentaciju upotrijebiti kako bi dokazali svoju usklađenost s ovom Uredbom putem postupka ocjenjivanja sukladnosti ili relevantnih aktivnosti nadzora tržišta. U tom pogledu tijela za nadzor tržišta i prijavljena tijela pozitivno uzimaju u obzir završna izvješća i pisane dokaze koje je dostavilo nacionalno nadležno tijelo kako bi se u razumnoj mjeri ubrzali postupci ocjenjivanja sukladnosti.

8. Podložno odredbama o povjerljivosti iz članka 78. i uz suglasnost dobavljača ili potencijalnog dobavljača, Komisija i Vijeće za umjetnu inteligenciju ovlašteni su pristupiti završnim izvješćima te ih prema potrebi uzimaju u obzir pri izvršavanju svojih zadaća na temelju ove Uredbe. Ako se i dobavljač odnosno potencijalni dobavljač i nacionalno nadležno tijelo o tome izričito dogovore, završno izvješće može se objaviti na jedinstvenoj informacijskoj platformi iz ovog članka.

9. Svrha uspostave regulatornih izoliranih okruženja za umjetnu inteligenciju doprinošenje je sljedećim ciljevima:

- (a) unapređivanju pravne sigurnosti radi postizanja regulatorne usklađenosti s ovom Uredbom ili, prema potrebi, drugim primjenjivim pravom Unije i nacionalnim pravom;

- (b) podupiranju razmjene primjera najbolje prakse putem suradnje s tijelima uključenima u regulatorno izolirano okruženje za umjetnu inteligenciju;
- (c) poticanju inovacija i konkurentnosti te olakšavanju razvoja ekosustava umjetne inteligencije;
- (d) doprinošenju regulatornom učenju utemeljenom na dokazima;
- (e) olakšavanju i ubrzanju pristupa UI sustava tržištu Unije, posebno ako su njihovi dobavljači MSP-ovi, uključujući *start-up* poduzeća.

10. Nacionalna nadležna tijela osiguravaju da, ako inovativni UI sustavi obuhvaćaju obradu osobnih podataka ili su na neki drugi način obuhvaćeni nadzorom drugih nacionalnih tijela ili nadležnih tijela koja pružaju ili podržavaju pristup podacima, nacionalna tijela za zaštitu podataka i ta druga nacionalna ili nadležna tijela budu uključena u rad regulatornog izoliranog okruženja za umjetnu inteligenciju i uključena u nadzor nad tim aspektima u okviru svojih zadaća i ovlasti.

11. Regulatorna izolirana okruženja za umjetnu inteligenciju ne utječu na nadzorne ili korektivne ovlasti nadležnih tijela koja nadziru izolirana okruženja, među ostalim na regionalnoj ili lokalnoj razini. Ako se tijekom razvoja i testiranja takvih UI sustava uoče znatni rizici za zdravlje, sigurnost i temeljna prava, ti se rizici moraju adekvatno ublažiti. Nacionalna nadležna tijela ovlaštena su privremeno ili trajno suspendirati postupak testiranja ili sudjelovanje u izoliranom okruženju ako rizike nije moguće djelotvorno ublažiti, a o takvoj odluci obavješćuju Ured za umjetnu inteligenciju. Nacionalna nadležna tijela izvršavaju svoje nadzorne ovlasti u granicama relevantnog prava i primjenjuju svoje diskrecijske ovlasti pri provedbi pravnih odredaba u odnosu na određeni projekt u regulatornom izoliranom okruženju za umjetnu inteligenciju, s ciljem podupiranja inovacija u području umjetne inteligencije u Uniji.

12. Dobavljači i potencijalni dobavljači koji sudjeluju u regulatornom izoliranom okruženju za umjetnu inteligenciju i dalje su na temelju primjenjivog prava Unije o odgovornosti i nacionalnog prava o odgovornosti odgovorni za svu štetu nanесenu trećim stranama koja je posljedica eksperimentiranja u izoliranom okruženju. Međutim, ako potencijalni dobavljači poštuju posebni plan i uvjete svojeg sudjelovanja te u dobroj vjeri slijede smjernice nacionalnog nadležnog tijela, tijela ne izriču upravne novčane kazne zbog povrede ove Uredbe. Ako su druga nadležna tijela koja su odgovorna za drugo pravo Unije i nacionalno pravo bila aktivno uključena u nadzor nad UI sustavom u izoliranom okruženju i dala smjernice u pogledu usklađivanja, ne izriču se upravne novčane kazne u vezi s tim pravom.

13. Regulatorna izolirana okruženja za umjetnu inteligenciju dizajniraju se i realiziraju na takav način da se njima, ako je to relevantno, olakšava prekogranična suradnja među nacionalnim nadležnim tijelima.

14. Nacionalna nadležna tijela koordiniraju svoje aktivnosti i surađuju u okviru Vijeća za umjetnu inteligenciju.

15. Nacionalna nadležna tijela obavješćuju Ured za umjetnu inteligenciju i Vijeće za umjetnu inteligenciju o uspostavi izoliranog okruženja i mogu od njih zatražiti potporu i smjernice. Ured za umjetnu inteligenciju objavljuje popis planiranih i postojećih izoliranih okruženja i ažurira ga kako bi se potaknula veća interakcija u regulatornim izoliranim okruženjima za umjetnu inteligenciju i prekogranična suradnja.

16. Nacionalna nadležna tijela podnose godišnja izvješća Uredu za umjetnu inteligenciju i Vijeću za umjetnu inteligenciju, počevši godinu dana nakon uspostave regulatornog izoliranog okruženja za umjetnu inteligenciju i svake godine nakon toga do njegove obustave, te završno izvješće. U tim se izvješćima navode informacije o napretku i rezultatima provedbe tih izoliranih okruženja, uključujući primjere najbolje prakse, incidente, stečena iskustva i preporuke o strukturi tih izoliranih okruženja te, prema potrebi, o primjeni i mogućoj reviziji ove Uredbe, uključujući njezine delegirane akte i provedbene akte, te o primjeni drugog prava Unije koju nadležna tijela nadziru u relevantnom izoliranom okruženju. Nacionalna nadležna tijela ta godišnja izvješća ili njihove sažetke stavljaju na raspolaganje javnosti na internetu. Komisija ta godišnja izvješća prema potrebi uzima u obzir pri izvršavanju svojih zadaća na temelju ove Uredbe.

17. Komisija izrađuje jedinstveno, namjensko sučelje koje sadržava sve relevantne informacije povezane s izoliranim okruženjima za umjetnu inteligenciju kako bi se dionicima omogućilo da ostvare interakciju s regulatornim izoliranim okruženjima za umjetnu inteligenciju, podnesu upite nadležnim tijelima i zatraže neobvezujuće smjernice u vezi sa sukladnošću inovativnih proizvoda, usluga i poslovnih modela u koje su ugrađene tehnologije umjetne inteligencije, u skladu s člankom 62. stavkom 1. točkom (c). Komisija se prema potrebi proaktivno koordinira s nacionalnim nadležnim tijelima.

Članak 58.

Detaljni aranžmani za regulatorna izolirana okruženja za umjetnu inteligenciju i njihovo funkcioniranje

1. Kako bi se u Uniji izbjegla fragmentacija, Komisija donosi provedbene akte o utvrđivanju detaljnih aranžmana za uspostavu, razvoj, provedbu, rad i nadzor regulatornih izoliranih okruženja za umjetnu inteligenciju. Ti provedbeni akti sadržavaju zajednička načela o sljedećim pitanjima:

- (a) kriterijima prihvatljivosti i odabira za sudjelovanje u regulatornom izoliranom okruženju za umjetnu inteligenciju;
- (b) postupcima za primjenu regulatornog izoliranog okruženja za umjetnu inteligenciju, sudjelovanje u njemu, njegovo praćenje, izlazak iz njega i njegovu obustavu, što uključuje plan izoliranog okruženja i završno izvješće;
- (c) uvjetima koji se primjenjuju na sudionike.

Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 98. stavka 2.

2. Provedbenim aktima iz stavka 1. osigurava se sljedeće:

- (a) regulatorna izolirana okruženja za umjetnu inteligenciju otvorena su svim dobavljačima ili potencijalnim dobavljačima UI sustava koji ispunjava kriterije prihvatljivosti i odabira, koji su transparentni i poštjeni, a nacionalna nadležna tijela obavješćuju podnositelje zahtjeva o svojoj odluci u roku od tri mjeseca od podnošenja zahtjeva;
- (b) regulatorna izolirana okruženja za umjetnu inteligenciju omogućuju širok i jednak pristup te drže korak s potražnjom za sudjelovanjem; dobavljači i potencijalni dobavljači također mogu podnijeti zahtjeve u partnerstvu sa subjektima koji uvode sustav i drugim relevantnim trećim stranama;
- (c) detaljnim aranžmanima i uvjetima za regulatorna izolirana okruženja za umjetnu inteligenciju u najvećoj se mogućoj mjeri podupire fleksibilnost nacionalnih nadležnih tijela u uspostavi regulatornih izoliranih okruženja za umjetnu inteligenciju i upravljanju njima;
- (d) pristup regulatornim izoliranim okruženjima za umjetnu inteligenciju besplatan je za MSP-ove, uključujući *start-up* poduzeća, ne dovodeći u pitanje izvanredne troškove čiju naknadu na pravedan i razmjern način mogu zatražiti nacionalna nadležna tijela;
- (e) dobavljačima i potencijalnim dobavljačima olakšavaju, s pomoću ishoda učenja regulatornih izoliranih okruženja za umjetnu inteligenciju, ispunjavanje obveza u pogledu ocjenjivanja sukladnosti na temelju ove Uredbe i dobrovoljnu primjenu kodeksa ponašanja iz članka 95.;
- (f) kako bi se omogućila i olakšala suradnja s javnim sektorom i s privatnim sektorom, regulatorna izolirana okruženja za umjetnu inteligenciju olakšavaju sudjelovanje drugih relevantnih aktera iz ekosustava umjetne inteligencije, kao što su prijavljena tijela i organizacije za normizaciju, MSP-ovi, uključujući *start-up* poduzeća, poduzeća, inovatori, objekti za testiranje i eksperimentiranje, laboratoriji za istraživanja i eksperimentiranje, europski centri za digitalne inovacije, centri izvrsnosti i pojedinačni istraživači;
- (g) postupci, procesi i administrativni uvjeti za podnošenje zahtjeva, odabir, sudjelovanje i izlazak iz regulatornog izoliranog okruženja za umjetnu inteligenciju jednostavni su, lako razumljivi i jasno priopćeni kako bi se olakšalo sudjelovanje MSP-ova, uključujući *start-up* poduzeća, s ograničenim pravnim i administrativnim kapacitetima i pojednostavnjeni su u cijeloj Uniji kako bi se izbjegla rascjepkanost i kako bi se sudjelovanje u regulatornom izoliranom okruženju koje je uspostavila država članica ili Europski nadzornik za zaštitu podataka uzajamno i ujednačeno priznavalo te imalo iste pravne učinke u cijeloj Uniji;
- (h) sudjelovanje u regulatornom izoliranom okruženju za umjetnu inteligenciju ograničeno je na razdoblje koje je primjereno složenosti i opsegu projekta i koje može produljiti nacionalno nadležno tijelo;
- (i) regulatorna izolirana okruženja za umjetnu inteligenciju olakšavaju razvoj alata i infrastrukture za testiranje, utvrđivanje referentnih vrijednosti, ocjenjivanje i objašnjavanje dimenzija UI sustava koje su relevantne za regulatorno učenje, poput točnosti, otpornosti i kibernetičke sigurnosti, kao i mjera za ublažavanje rizika za temeljna prava i društvo u cjelini.

3. Potencijalne dobavljače u regulatornim izoliranim okruženjima za umjetnu inteligenciju, posebno MSP-ove i *start-up* poduzeća, prema potrebi se usmjerava na usluge prije uvođenja, kao što su smjernice o provedbi ove Uredbe, na druge usluge s dodanom vrijednošću, kao što su pomoć u vezi s dokumentima o normizaciji i certifikacijom, na objekte za testiranje i eksperimentiranje, europske centre za digitalne inovacije i centre izvrsnosti.

4. Kada nacionalna nadležna tijela razmatraju izdavanje odobrenja za testiranje u stvarnim uvjetima koje se nadzire u okviru regulatornog izoliranog okruženja za umjetnu inteligenciju koje treba uspostaviti na temelju ovog članka, sa sudionicima izričito dogovaraju uvjete tog testiranja, a posebno odgovarajuće zaštitne mjere u cilju zaštite temeljnih prava, zdravlja i sigurnosti. Prema potrebi surađuju s drugim nacionalnim nadležnim tijelima kako bi se osigurala dosljedna praksa u cijeloj Uniji.

Članak 59.

Daljnja obrada osobnih podataka za razvoj određenih UI sustava u javnom interesu u regulatornom izoliranom okruženju za umjetnu inteligenciju

1. U regulatornom izoliranom okruženju za umjetnu inteligenciju osobni podaci koji su zakonito prikupljeni u druge svrhe mogu se obrađivati samo u svrhu razvoja, treniranja i testiranja određenih UI sustava u izoliranom okruženju ako su ispunjeni svi sljedeći uvjeti:

- (a) UI sustave razvija tijelo javne vlasti ili druga fizička ili pravna osoba u svrhu zaštite znatnog javnog interesa, u jednom ili više sljedećih područja:
 - i. javna sigurnost i javno zdravlje, uključujući otkrivanje, dijagnosticiranje, prevenciju, kontrolu i liječenje bolesti te unapređivanje zdravstvenih sustava;
 - ii. visoka razina zaštite i poboljšanje kvalitete okoliša, zaštita bioraznolikosti, zaštita od onečišćenja, mjere zelene tranzicije, mjere za ublažavanje klimatskih promjena i prilagodbu njima;
 - iii. energetska održivost;
 - iv. sigurnost i otpornost prometnih sustava i mobilnosti, kritične infrastrukture i mreža;
 - v. učinkovitost i kvaliteta javne uprave i javnih usluga;
- (b) podaci koji se obrađuju potrebni su za ispunjavanje jednog ili više zahtjeva iz poglavlja III. odjeljka 2. ako se ti zahtjevi ne mogu djelotvorno ispuniti obradom anonimiziranih, sintetičkih ili drugih neosobnih podataka;
- (c) postoje djelotvorni mehanizmi praćenja kojima se može utvrditi mogu li se tijekom eksperimentiranja u izoliranom okruženju pojaviti veliki rizici za prava i slobode ispitanika, kako je navedeno u članku 35. Uredbe (EU) 2016/679 i u članku 39. Uredbe (EU) 2018/1725, kao i mehanizmi za odgovor kojima se ti rizici mogu brzo ublažiti, a obrada prema potrebi zaustaviti;
- (d) osobni podaci koji se obrađuju u izoliranom okruženju nalaze se u funkcionalno odvojenom, izoliranom i zaštićenom okruženju za obradu podataka pod kontrolom potencijalnog dobavljača i samo ovlaštene osobe imaju pristup tim podacima;
- (e) dobavljači mogu dalje dijeliti izvorno prikupljene podatke samo u skladu s pravom Unije o zaštiti podataka; osobni podaci nastali u izoliranom okruženju ne mogu se dijeliti izvan izoliranog okruženja;
- (f) obrada osobnih podataka u kontekstu izoliranog okruženja ne smije dovesti do mjera ili odluka koje utječu na ispitanike niti smije utjecati na ostvarivanje njihovih prava utvrđenih u pravu Unije o zaštiti osobnih podataka;
- (g) osobni podaci koji se obrađuju u kontekstu izoliranog okruženja zaštićeni su odgovarajućim tehničkim i organizacijskim mjerama i brišu se nakon okončanja sudjelovanja u izoliranom okruženju ili isteka razdoblja čuvanja osobnih podataka;
- (h) evidencija obrade osobnih podataka u kontekstu izoliranog okruženja čuva se za vrijeme sudjelovanja u izoliranom okruženju, osim ako je pravom Unije ili nacionalnim pravom predviđeno drukčije;
- (i) u sklopu tehničke dokumentacije iz Priloga IV. zajedno s rezultatima testiranja čuva se potpun i detaljan opis procesa i obrazloženja treniranja, testiranja i validacije dotičnog UI sustava;

- (j) na internetskim stranicama nadležnih tijela objavljuju se kratak sažetak projekta umjetne inteligencije razvijenog u izoliranom okruženju te njegovi ciljevi i očekivani rezultati; ta obveza ne obuhvaća osjetljive operativne podatke u vezi s aktivnostima tijela kaznenog progona, tijela za nadzor državne granice, tijela za imigraciju ili tijela za azil.
2. U svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršenja kaznenih sankcija, što uključuje zaštitu od prijetnji javnoj sigurnosti i sprečavanje tih prijetnji, pod kontrolom i odgovornošću tijela kaznenog progona, obrada osobnih podataka u regulatornim izoliranim okruženjima za umjetnu inteligenciju temelji se na posebnom pravu Unije ili nacionalnom pravu i podliježe istim kumulativnim uvjetima iz stavka 1.
3. Stavkom 1. ne dovodi se u pitanje pravo Unije ili nacionalno pravo kojim se isključuje obrada osobnih podataka u svrhe koje nisu izričito navedene u tom pravu, kao ni pravo Unije ili nacionalno pravo kojim se utvrđuje osnova za obradu osobnih podataka koja je potrebna u svrhu razvoja, testiranja ili treniranja inovativnih UI sustava ili bilo koja druga pravna osnova, u skladu s pravom Unije o zaštiti osobnih podataka.

Članak 60.

Testiranje visokorizičnih UI sustava u stvarnim uvjetima izvan regulatornih izoliranih okruženja za umjetnu inteligenciju

1. Testiranje visokorizičnih UI sustava u stvarnim uvjetima izvan regulatornih izoliranih okruženja za umjetnu inteligenciju mogu provoditi dobavljači ili potencijalni dobavljači visokorizičnih UI sustava iz Priloga III. u skladu s ovim člankom i planom testiranja u stvarnim uvjetima iz ovog članka, ne dovodeći u pitanje zabrane na temelju članka 5.

Komisija provedbenim aktima utvrđuje pojedinosti plana testiranja u stvarnim uvjetima. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 98. stavka 2.

Ovim se stavkom ne dovodi u pitanje pravo Unije ili nacionalno pravo o testiranju u stvarnim uvjetima visokorizičnih UI sustava povezanih s proizvodima obuhvaćenima zakonodavstvom Unije o usklađivanju navedenim u Prilogu I.

2. Dobavljači ili potencijalni dobavljači mogu u bilo kojem trenutku prije stavljanja UI sustava na tržište ili u upotrebu provesti testiranje visokorizičnih UI sustava iz Priloga III. u stvarnim uvjetima, samostalno ili u partnerstvu s jednim ili više subjekata koji uvode sustav ili potencijalnih subjekata koji uvode sustav.

3. Testiranjem visokorizičnih UI sustava u stvarnim uvjetima na temelju ovog članka ne dovodi se u pitanje etičko preispitivanje koje se zahtijeva pravom Unije ili nacionalnim pravom.

4. Dobavljači ili potencijalni dobavljači testiranje u stvarnim uvjetima mogu provesti samo ako su ispunjeni svi sljedeći uvjeti:

- (a) dobavljač ili potencijalni dobavljač izradio je plan testiranja u stvarnim uvjetima i dostavio ga tijelu za nadzor tržišta u državi članici u kojoj će se provoditi testiranje u stvarnim uvjetima;
- (b) tijelo za nadzor tržišta u državi članici u kojoj će se provoditi testiranje u stvarnim uvjetima odobrilo je testiranje u stvarnim uvjetima i plan testiranja u stvarnim uvjetima; ako tijelo za nadzor tržišta ne odgovori u roku od 30 dana, smatra se da su testiranje u stvarnim uvjetima i plan testiranja u stvarnim uvjetima odobreni; ako nacionalnim pravom nije predviđeno prešutno odobrenje, testiranje u stvarnim uvjetima i dalje podliježe odobrenju;
- (c) dobavljač ili potencijalni dobavljač, uz iznimku dobavljača ili potencijalnih dobavljača visokorizičnih UI sustava iz točaka 1., 6. i 7. Priloga III. u područjima kaznenog progona, migracija, azila i upravljanja nadzorom državne granice i visokorizičnih UI sustava iz točke 2. Priloga III., registrirao je testiranje u stvarnim uvjetima u skladu s člankom 71. stavkom 4. pri čemu je naveo jedinstveni identifikacijski broj na razini Unije i informacije iz Priloga IX.; dobavljač ili potencijalni dobavljač visokorizičnih UI sustava iz točaka 1., 6. i 7. Priloga III. u područjima kaznenog progona, migracija, azila i upravljanja nadzorom državne granice registrirao je testiranje u stvarnim uvjetima u dijelu baze podataka EU-a koji nije javno dostupan u skladu s člankom 49. stavkom 4. točkom (d) pri čemu je naveo jedinstveni identifikacijski broj na razini Unije i informacije sadržane u njemu; dobavljač ili potencijalni dobavljač visokorizičnih UI sustava iz točke 2. Priloga III. registrirao je testiranje u stvarnim uvjetima u skladu s člankom 49. stavkom 5.;

- (d) dobavljač ili potencijalni dobavljač koji provodi testiranje u stvarnim uvjetima ima poslovni nastan u Uniji ili je imenovao pravnog zastupnika s poslovnim nastanom u Uniji;
- (e) podaci koji se prikupljaju i obrađuju u svrhu testiranja u stvarnim uvjetima prenose se trećim zemljama samo pod uvjetom da se provode odgovarajuće i primjenjive zaštitne mjere na temelju prava Unije;
- (f) testiranje u stvarnim uvjetima ne traje dulje nego što je potrebno za postizanje njegovih ciljeva, a u svakom slučaju ne dulje od šest mjeseci, što se može produljiti za dodatno razdoblje od šest mjeseci, pod uvjetom da dobavljač ili potencijalni dobavljač o tome prethodno obavijesti tijelo za nadzor tržišta, čemu prilaže objašnjenje potrebe za takvim produljenjem;
- (g) ispitanici koji sudjeluju u testiranju u stvarnim uvjetima koji zbog svoje dobi ili invaliditeta pripadaju skupinama ranjivih osoba primjereno su zaštićeni;
- (h) ako dobavljač ili potencijalni dobavljač organizira testiranje u stvarnim uvjetima u suradnji s jednim ili više subjekata koji uvođe sustav ili potencijalnih subjekata koji uvođe sustav, korisnici su obaviješteni o svim aspektima testiranja koji su relevantni za njihovu odluku o sudjelovanju i dane su im relevantne upute za korištenje UI sustava iz članka 13.; dobavljač ili potencijalni dobavljač i subjekt koji uvođa sustav ili potencijalni subjekt koji uvođa sustav sklapaju sporazum kojim se utvrđuju njihove uloge i odgovornosti kako bi se osigurala usklađenost s odredbama za testiranje u stvarnim uvjetima na temelju ove Uredbe i na temelju drugog primjenjivog prava Unije i nacionalnog prava;
- (i) ispitanici koji sudjeluju u testiranju u stvarnim uvjetima dali su informirani pristanak u skladu s člankom 61. ili, u slučaju kaznenog progona, ako bi traženje informiranog pristanka spriječilo testiranje UI sustava, samo testiranje i ishod testiranja u stvarnim uvjetima ne smiju imati negativan učinak na ispitanike, a njihovi osobni podaci brišu se nakon provedbe testiranja;
- (j) testiranje u stvarnim uvjetima djelotvorno nadzire dobavljač ili potencijalni dobavljač, kao i subjekti koji uvođe sustav ili potencijalni subjekti koji uvođe sustav, posredstvom osoba koje imaju odgovarajuće kvalifikacije u relevantnom području te koje imaju potrebne kapacitete, osposobljavanje i ovlasti za obavljanje svojih zadaća;
- (k) predviđanja, preporuke ili odluke UI sustava mogu se djelotvorno poništiti i zanemariti.

5. Svi ispitanici koji sudjeluju u testiranju u stvarnim uvjetima ili, ovisno o slučaju, njihov zakonito imenovani zastupnik, mogu se u bilo kojem trenutku povući iz testiranja povlačenjem svojeg informiranog pristanka, a da to za njih nema nikakve negativne posljedice i da pritom ne moraju pružiti nikakvo obrazloženje, te mogu zatražiti da se njihovi osobni podaci odmah i trajno izbrišu. Povlačenje informiranog pristanka ne utječe na već provedene aktivnosti.

6. U skladu s člankom 75. države članice svojim tijelima za nadzor tržišta dodjeljuju ovlasti da od dobavljača i potencijalnih dobavljača zatraže informacije, da provode nenajavljene inspekcije na daljinu ili na licu mjesta i da obavljaju provjere provedbe testiranja u stvarnim uvjetima i povezanih visokorizičnih UI sustava. Tijela za nadzor tržišta koriste te ovlasti kako bi osigurala siguran razvoj testiranja u stvarnim uvjetima.

7. Svaki ozbiljan incident utvrđen tijekom testiranja u stvarnim uvjetima mora se prijaviti nacionalnom tijelu za nadzor tržišta u skladu s člankom 73. Dobavljač ili potencijalni dobavljač odmah donosi mjere ublažavanja ili, ako to nije moguće, suspendira testiranje u stvarnim uvjetima dok se takve mjere ublažavanja ne provedu ili ga u suprotnom slučaju obustavlja. Dobavljač ili potencijalni dobavljač uspostavlja postupak za promptni opoziv UI sustava nakon takve obustave testiranja u stvarnim uvjetima.

8. Dobavljači ili potencijalni dobavljači obavješćuju nacionalno tijelo za nadzor tržišta u državi članici u kojoj se će se provoditi testiranje u stvarnim uvjetima o suspenziji ili obustavi testiranja u stvarnim uvjetima i konačnim ishodima.

9. Dobavljač ili potencijalni dobavljač odgovoran je na temelju primjenjivog prava Unije o odgovornosti i nacionalnog prava o odgovornosti za svu štetu prouzročenu tijekom svojeg testiranja u stvarnim uvjetima.

Članak 61.

Informirani pristanak za sudjelovanje u testiranju u stvarnim uvjetima izvan regulatornih izoliranih okruženja za umjetnu inteligenciju

1. Za potrebe testiranja u stvarnim uvjetima na temelju članka 60. od ispitanika koji sudjeluju u testiranju pribavlja se dobrovoljan informirani pristanak prije njihova sudjelovanja u takvom testiranju, a nakon što su s pomoću jezgrovitih, jasnih, relevantnih i razumljivih informacija propisno obaviješteni o sljedećem:
 - (a) prirodi i ciljevima testiranja u stvarnim uvjetima i mogućim neugodnostima koje mogu biti povezane s njihovim sudjelovanjem;
 - (b) uvjetima pod kojima će se provoditi testiranje u stvarnim uvjetima, uključujući očekivano trajanje sudjelovanja ispitanika;
 - (c) njihovim pravima i jamstvima u pogledu sudjelovanja, osobito o njihovu pravu na odbijanje sudjelovanja u testiranju u stvarnim uvjetima i pravu na povlačenje iz njega u bilo kojem trenutku, a da to za njih nema nikakve negativne posljedice i da pritom ne moraju pružiti nikakvo obrazloženje;
 - (d) aranžmanima za podnošenje zahtjeva za poništenje ili zanemarivanje predviđanja, preporuka ili odluka UI sustava;
 - (e) jedinstvenom identifikacijskom broju na razini Unije za testiranje u stvarnim uvjetima, u skladu s člankom 60. stavkom 4. točkom (c) i kontaktnim podacima dobavljača ili njegova pravnog zastupnika od kojeg se mogu dobiti dodatne informacije.
2. Informirani pristanak mora biti datiran i dokumentiran, a primjerak se daje ispitanicima koji sudjeluju u testiranju ili njihovom pravnom zastupniku.

Članak 62.

Mjere za dobavljače i subjekte koji uvode sustav, posebno MSP-ove, uključujući start-up poduzeća

1. Države članice poduzimaju sljedeće mjere:
 - (a) MSP-ovima, uključujući *start-up* poduzeća, koji u Uniji imaju registrirani ured ili podružnicu, daju prioritetni pristup regulatornim izoliranim okruženjima za umjetnu inteligenciju, u onoj mjeri u kojoj ispunjavaju uvjete prihvatljivosti i kriterije odabira; prioritetni pristup ne sprečava druge MSP-ove, uključujući *start-up* poduzeća, koja nisu ona iz ovog stavka, da pristupe regulatornom izoliranom okruženju za umjetnu inteligenciju, pod uvjetom da i oni ispunjavaju uvjete prihvatljivosti i kriterije odabira;
 - (b) organiziraju specifične aktivnosti podizanja svijesti i osposobljavanja o primjeni ove Uredbe, prilagođene potrebama MSP-ova, uključujući *start-up* poduzeća, subjekata koji uvode sustav te, prema potrebi, lokalnih tijela javne vlasti;
 - (c) koriste postojeće namjenske kanale za komunikaciju i prema potrebi uspostavljaju nove kanale za komunikaciju s MSP-ovima, uključujući *start-up* poduzeća, sa subjektima koji uvode sustav, s drugim inovatorima i, prema potrebi, s lokalnim tijelima javne vlasti, radi pružanja savjeta i odgovaranja na upite u vezi s provedbom ove Uredbe, među ostalim u pogledu sudjelovanja u regulatornim izoliranim okruženjima za umjetnu inteligenciju;
 - (d) olakšavaju sudjelovanje MSP-ova i drugih relevantnih dionika u procesu razvoja normizacije.
2. Pri određivanju naknada za ocjenjivanje sukladnosti na temelju članka 43. uzimaju se u obzir specifični interesi i potrebe dobavljača koji su MSP-ovi, uključujući *start-up* poduzeća, i te se naknade umanjuju razmjerno njihovoj veličini, veličini tržišta i drugim relevantnim pokazateljima.
3. Ured za umjetnu inteligenciju poduzima sljedeće mjere:
 - (a) osigurava standardizirane predloške za područja obuhvaćena ovom Uredbom, kako je navelo Vijeće za umjetnu inteligenciju u svojem zahtjevu;
 - (b) razvija i održava jedinstvenu informacijsku platformu na kojoj se svim operaterima iz cijele Unije pružaju informacije u vezi s ovom Uredbom koje su jednostavne za upotrebu;

- (c) organizira odgovarajuće komunikacijske kampanje za podizanje svijesti o obvezama koje proizlaze iz ove Uredbe;
- (d) evaluiira i promiče konvergenciju primjera najbolje prakse u postupcima javne nabave u vezi s UI sustavima.

Članak 63.

Odstupanja za specifične operatere

1. Mikropoduzeća u smislu Preporuke 2003/361/EZ mogu na pojednostavnjen način ispuniti određene elemente sustava upravljanja kvalitetom koji se zahtijeva člankom 17. ove Uredbe, pod uvjetom da nemaju partnerska poduzeća ili povezana poduzeća u smislu te preporuke. U tu svrhu Komisija izrađuje smjernice o elementima sustava upravljanja kvalitetom koji se mogu ispuniti na pojednostavnjen način s obzirom na potrebe mikropoduzeća, a da se pritom ne utječe na razinu zaštite ili potrebu za ispunjavanjem zahtjeva u vezi s visokorizičnim UI sustavima.
2. Stavak 1. ovog članka ne smije se tumačiti kao izuzimanje tih operatera od ispunjavanja bilo kojih drugih zahtjeva ili obveza utvrđenih u ovoj Uredbi, uključujući one utvrđene u člancima 9., 10., 11., 12., 13., 14., 15., 72. i 73.

POGLAVLJE VII.

UPRAVLJANJE

ODJELJAK 1.

Upravljanje na razini Unije

Članak 64.

Ured za umjetnu inteligenciju

1. Komisija putem Ureda za umjetnu inteligenciju razvija stručno znanje i sposobnosti Unije u području umjetne inteligencije.
2. Države članice olakšavaju provedbu zadaća povjerenih Uredu za umjetnu inteligenciju, kako su odražene u ovoj Uredbi.

Članak 65.

Osnivanje i struktura Europskog vijeća za umjetnu inteligenciju

1. Osniva se Europsko vijeće za umjetnu inteligenciju („Vijeće za umjetnu inteligenciju”).
2. Vijeće za umjetnu inteligenciju sastoji se od jednog predstavnika iz svake države članice. Europski nadzornik za zaštitu podataka sudjeluje u njemu kao promatrač. Ured za umjetnu inteligenciju također prisustvuje sastancima Vijeća za umjetnu inteligenciju, bez sudjelovanja u glasovanju. Ovisno o pojedinačnom slučaju, Vijeće za umjetnu inteligenciju na sastanke može pozvati druga nacionalna tijela ili stručnjake i Unijina tijela ili stručnjake ako su pitanja o kojima se raspravlja relevantna za njih.
3. Svakog predstavnika imenuje njegova država članica na razdoblje od tri godine, koje se može jednom produljiti.
4. Države članice osiguravaju da za njihove predstavnike u Vijeću za umjetnu inteligenciju vrijedi sljedeće:
 - (a) posjeduju relevantne kompetencije i ovlasti u svojoj državi članici kako bi aktivno doprinosili ostvarivanju zadaća Vijeća za umjetnu inteligenciju iz članka 66.;
 - (b) određeni su kao jedinstvena kontaktna točka u odnosu na Vijeće za umjetnu inteligenciju i, prema potrebi, uzimajući u obzir potrebe država članica, kao jedinstvena kontaktna točka za dionike;

(c) ovlašteni su olakšavati dosljednost i koordinaciju među nacionalnim nadležnim tijelima u svojoj državi članici u pogledu provedbe ove Uredbe, među ostalim prikupljanjem relevantnih podataka i informacija u svrhu ispunjavanja svojih zadaća u Vijeću za umjetnu inteligenciju.

5. Imenovani predstavnici država članica donose poslovnik Vijeća za umjetnu inteligenciju dvotrećinskom većinom. Poslovnikom se osobito utvrđuju postupci za postupak odabira, trajanje mandata i specifikacije zadaća predsjednika, detaljni aranžmani za glasovanje te organizacija aktivnosti Vijeća za umjetnu inteligenciju i aktivnosti njegovih podskupina.

6. Vijeće za umjetnu inteligenciju osniva dvije stalne podskupine kako bi osigurao platformu za suradnju i razmjenu među tijelima za nadzor tržišta i tijelima koja provode prijavljivanje o pitanjima koja se odnose na nadzor tržišta odnosno na prijavljena tijela.

Stalna podskupina za nadzor tržišta trebala bi djelovati kao skupina za administrativnu suradnju (skupina za ADCO) za ovu Uredbu u smislu članka 30. Uredbe (EU) 2019/1020.

Vijeće za umjetnu inteligenciju prema potrebi može osnovati druge stalne ili privremene podskupine za razmatranje specifičnih pitanja. U te podskupine ili na posebne sastanke tih podskupina mogu prema potrebi biti pozvani predstavnici savjetodavnog foruma iz članka 67. kao promatrači.

7. Vijeće za umjetnu inteligenciju organizirano je i djeluje tako da čuva objektivnost i nepristranost svojih aktivnosti.

8. Vijećem za umjetnu inteligenciju predsjedja jedan od predstavnika država članica. Ured za umjetnu inteligenciju osigurava tajništvo Vijeća za umjetnu inteligenciju, saziva sastanke na zahtjev predsjednika i priprema dnevni red u skladu sa zadaćama Vijeća za umjetnu inteligenciju na temelju ove Uredbe i njegovim poslovníkom.

Članak 66.

Zadaće Vijeća za umjetnu inteligenciju

Vijeće za umjetnu inteligenciju savjetuje Komisiju i države članice i pomaže im kako bi se olakšala dosljedna i djelotvorna primjena ove Uredbe. U tom cilju Vijeće za umjetnu inteligenciju posebno može:

- (a) doprinositi koordinaciji među nacionalnim nadležnim tijelima odgovornima za primjenu ove Uredbe i, u suradnji s dotičnim tijelima za nadzor tržišta i podložno njihovoj suglasnosti, podupirati zajedničke aktivnosti tijela za nadzor tržišta iz članka 74. stavka 11.;
- (b) prikupljati i razmjenjivati tehničko i regulatorno stručno znanje i primjere najbolje prakse među državama članicama;
- (c) pružati savjete o provedbi ove Uredbe, posebno u pogledu izvršavanja pravila o UI modelima opće namjene;
- (d) doprinositi usklađivanju administrativnih praksi u državama članicama, među ostalim u pogledu odstupanja od postupaka ocjenjivanja sukladnosti iz članka 46., funkcioniranja regulatornih izoliranih okruženja za umjetnu inteligenciju i testiranja u stvarnim uvjetima iz članaka 57., 59. i 60.;
- (e) na zahtjev Komisije ili na vlastitu inicijativu izdavati preporuke i pisana mišljenja o svim relevantnim pitanjima povezanim sa provedbom ove Uredbe i njezinom dosljednom i djelotvornom primjenom, među ostalim:
 - i. o izradi i primjeni kodeksâ ponašanja i kodeksâ prakse u skladu s ovom Uredbom, kao i smjernica Komisije;
 - ii. o evaluaciji i preispitivanju ove Uredbe u skladu s člankom 112., među ostalim u pogledu izvješća o ozbiljnim incidentima iz članka 73. i funkcioniranja baze podataka EU-a iz članka 71., o izradi delegiranih akata ili provedbenih akata te u pogledu mogućih usklađivanja ove Uredbe sa zakonodavstvom Unije o usklađivanje navedenim u Prilogu I.;
 - iii. o tehničkim specifikacijama ili postojećim normama u vezi sa zahtjevima utvrđenima u poglavlju III. odjeljku 2.;

- iv. o upotrebi usklađenih normi ili zajedničkih specifikacija iz članka 40. i 41.;
- v. o trendovima, kao što su europska globalna konkurentnost u području umjetne inteligencije, prihvaćanje umjetne inteligencije u Uniji i razvoj digitalnih vještina;
- vi. o trendovima u razvoju tipologije vrijednosnih lanaca umjetne inteligencije, posebno u pogledu posljedica koje iz toga proizlaze u vezi s odgovornošću;
- vii. o mogućoj potrebi za izmjenom Priloga III. u skladu s člankom 7. i o mogućoj potrebi za revizijom članka 5. u skladu s člankom 112., uzimajući u obzir relevantne dostupne dokaze i najnovija tehnološka dostignuća;
- (f) podupirati Komisiju u promicanju pismenosti u području umjetne inteligencije, javne svijesti o koristima, rizicima, zaštitnim mjerama, pravima i obvezama u vezi s korištenjem UI sustava te njihova razumijevanja;
- (g) olakšavati razvoj zajedničkih kriterija i zajedničko razumijevanje relevantnih koncepata predviđenih u ovoj Uredbi među tržišnim operatorima i nadležnim tijelima, među ostalim doprinošenjem razvoju referentnih vrijednosti;
- (h) surađivati, prema potrebi, s drugim institucijama, tijelima, uredima i agencijama Unije te relevantnim Unijanim stručnim skupinama i mrežama, posebno u područjima sigurnosti proizvoda, kibernetičke sigurnosti, tržišnog natjecanja, digitalnih i medijskih usluga, financijskih usluga, zaštite potrošača te zaštite podataka i temeljnih prava;
- (i) doprinositi djelotvornoj suradnji s nadležnim tijelima trećih zemalja i međunarodnim organizacijama;
- (j) pomagati nacionalnim nadležnim tijelima i Komisiji u razvoju organizacijskog i tehničkog stručnog znanja potrebnog za provedbu ove Uredbe, među ostalim doprinošenjem procjeni potreba za osposobljavanjem osoblja država članica uključenog u provedbu ove Uredbe;
- (k) pomagati Uredu za umjetnu inteligenciju u pružanju potpore nacionalnim nadležnim tijelima u uspostavi i razvoju regulatornih izoliranih okruženja za umjetnu inteligenciju te olakšavati suradnju i razmjenu informacija među regulatornim izoliranim okruženjima za umjetnu inteligenciju;
- (l) doprinositi izradi dokumenata sa smjernicama i pružati odgovarajuće savjete o tome;
- (m) savjetovati Komisiju o međunarodnim pitanjima povezanim s umjetnom inteligencijom;
- (n) davati mišljenja Komisiji o kvalificiranim upozorenjima u vezi s UI modelima opće namjene;
- (o) primati mišljenja država članica o kvalificiranim upozorenjima u vezi s UI modelima opće namjene te o nacionalnim iskustvima i nacionalnoj praksi u području praćenja i izvršavanja UI sustava, posebno sustava u koje su integrirani UI modeli opće namjene.

Članak 67.

Savjetodavni forum

1. Osniva se savjetodavni forum koji pruža tehničko stručno znanje i savjetuje Vijeće za umjetnu inteligenciju i Komisiju te doprinosi njihovim zadaćama na temelju ove Uredbe.
2. Članstvo u savjetodavnom forumu čine uravnoteženo odabrani dionici, koji uključuju industriju, *start-up* poduzeća, MSP-ove, civilno društvo i akademsku zajednicu. Članstvo u savjetodavnom forumu mora biti uravnoteženo u smislu komercijalnih i nekomercijalnih interesa, a unutar kategorije komercijalnih interesa uravnoteženo u smislu MSP-ova i ostalih poduzeća.
3. Komisija među dionicima s priznatim stručnim znanjem u području umjetne inteligencije imenuje članove savjetodavnog foruma u skladu s kriterijima iz stavka 2.

4. Mandat članova savjetodavnog foruma traje dvije godine i može se produljiti za najviše četiri godine.
5. Agencija za temeljna prava, ENISA, Europski odbor za normizaciju (CEN), Europski odbor za elektrotehničku normizaciju (CENELEC) i Europski institut za telekomunikacijske norme (ETSI) stalni su članovi savjetodavnog foruma.
6. Savjetodavni forum izrađuje svoj poslovnik. Savjetodavni forum bira dva supredsjednika među svojim članovima, u skladu s kriterijima iz stavka 2. Mandat supredsjednika traje dvije godine i može se jednom produljiti.
7. Savjetodavni forum održava sastanke najmanje dvaput godišnje. Savjetodavni forum na svoje sastanke može pozvati stručnjake i druge dionike.
8. Savjetodavni forum na zahtjev Vijeća za umjetnu inteligenciju ili Komisije može pripremati mišljenja, preporuke i pisane doprinose.
9. Savjetodavni forum može prema potrebi osnovati stalne ili privremene podskupine radi razmatranja posebnih pitanja povezanih s ciljevima ove Uredbe.
10. Savjetodavni forum priprema godišnje izvješće o svojim aktivnostima. To se izvješće objavljuje.

Članak 68.

Znanstveno povjerenstvo neovisnih stručnjaka

1. Komisija provedbenim aktom donosi odredbe o osnivanju znanstvenog povjerenstva neovisnih stručnjaka („znanstveno povjerenstvo”) čija je svrha podupirati aktivnosti izvršavanja na temelju ove Uredbe. Taj provedbeni akt donosi se u skladu s postupkom ispitivanja iz članka 98. stavka 2.
 2. Znanstveno povjerenstvo sastoji se od stručnjaka koje Komisija odabire na temelju najsuvremenijeg znanstvenog ili tehničkog stručnog znanja u području umjetne inteligencije potrebnog za obavljanje zadaća iz stavka 3. i koji moraju moći dokazati da ispunjavaju sve sljedeće uvjete:
 - (a) posjeduju posebno stručno znanje i kompetencije te znanstveno ili tehničko stručno znanje u području umjetne inteligencije;
 - (b) neovisni su od svih dobavljača UI sustava ili UI modela opće namjene;
 - (c) sposobni su aktivnosti provoditi savjesno, točno i objektivno.
- Komisija u savjetovanju s Vijećem za umjetnu inteligenciju određuje broj stručnjaka u povjerenstvu u skladu s potrebama i osigurava pravednu rodnu i geografsku zastupljenost.
3. Znanstveno povjerenstvo savjetuje i podupire Ured za umjetnu inteligenciju, posebno u pogledu sljedećih zadaća:
 - (a) podupiranja provedbe i izvršavanja ove Uredbe u pogledu UI modela i sustava opće namjene, posebno tako što:
 - i. upozorava Ured za umjetnu inteligenciju o mogućim sistemskim rizicima na razini Unije u pogledu UI modela opće namjene, u skladu s člankom 90.;
 - ii. doprinosi razvoju alata i metodologija za evaluaciju sposobnosti UI modela i sustava opće namjene, među ostalim s pomoću referentnih vrijednosti;
 - iii. pruža savjete o klasifikaciji UI modela opće namjene sa sistemskim rizikom;
 - iv. pruža savjete o klasifikaciji različitih UI modela i sustava opće namjene;

v. doprinosi razvoju alata i predložaka;

(b) podupiranja rada tijela za nadzor tržišta na njihov zahtjev;

(c) podupiranja prekograničnih aktivnosti nadzora tržišta iz članka 74. stavka 11., ne dovodeći u pitanje ovlasti tijela za nadzor tržišta;

(d) podupiranja Ureda za umjetnu inteligenciju u izvršavanju njegovih dužnosti u kontekstu zaštitnog postupka Unije u skladu s člankom 81.

4. Stručnjaci iz znanstvenog povjerenstva svoje zadaće obavljaju nepristrano i objektivno i osiguravaju povjerljivost informacija i podataka dobivenih pri obavljanju svojih zadaća i aktivnosti. Pri obavljanju svojih zadaća iz stavka 3. ne smiju tražiti ni primati upute ni od koga. Svaki stručnjak sastavlja izjavu o interesima, koja se objavljuje. Ured za umjetnu inteligenciju uspostavlja sustave i postupke za aktivno upravljanje mogućim sukobima interesa i njihovo sprečavanje.

5. Provedbeni akt iz stavka 1. uključuje odredbe o uvjetima, postupcima i detaljnim aranžmanima u skladu s kojima znanstveno povjerenstvo i njegovi članovi izdaju upozorenja i traže pomoć Ureda za umjetnu inteligenciju u obavljanju zadaća znanstvenog povjerenstva.

Članak 69.

Pristup država članica stručnjacima

1. Države članice mogu pozvati stručnjake iz znanstvenog povjerenstva da im pruže potporu u njihovim aktivnostima izvršavanja na temelju ove Uredbe.

2. Od država članica može se zahtijevati plaćanje naknada za savjete i potporu stručnjaka. Komisija provedbenim aktom iz članka 68. stavka 1. utvrđuje strukturu i visinu naknada te ljestvicu i strukturu troškova čiji je povrat moguće tražiti, uzimajući u obzir ciljeve adekvatne provedbe ove Uredbe, troškovnu učinkovitost i potrebu da se svim državama članicama osigura djelotvoran pristup stručnjacima.

3. Komisija državama članicama olakšava pravodoban pristup stručnjacima, prema potrebi, i osigurava da kombinacija potpornih aktivnosti koje provode potporna struktura Unije za testiranje umjetne inteligencije u skladu s člankom 84. i stručnjaci u skladu s ovim člankom bude učinkovito organizirana i da donosi najveću moguću dodanu vrijednost.

ODJELJAK 2.

Nacionalna nadležna tijela

Članak 70.

Imenovanje nacionalnih nadležnih tijela i jedinstvenih kontaktnih točaka

1. Za potrebe ove Uredbe svaka država članica osniva ili imenuje kao nacionalna nadležna tijela barem jedno tijelo koje provodi prijavljivanje i barem jedno tijelo za nadzor tržišta. Ta nacionalna nadležna tijela izvršavaju svoje ovlasti neovisno, nepristrano i bez predrasuda kako bi zaštitila objektivnost svojih aktivnosti i zadaća te osigurala primjenu i provedbu ove Uredbe. Članovi tih tijela suzdržavaju se od svakog djelovanja koje je nespojivo s njihovim dužnostima. Pod uvjetom da se poštuju ta načela, takve aktivnosti i zadaće može obavljati jedno ili više imenovanih tijela, u skladu s organizacijskim potrebama države članice.

2. Države članice obavješćuju Komisiju o identitetu tijela koja provode prijavljivanje i tijela za nadzor tržišta te o zadaćama tih tijela, kao i o svim kasnijim promjenama u vezi s njima. Države članice do 2. kolovoza 2025. elektroničkim komunikacijskim sredstvima objavljuju informacije o tome kako se može stupiti u kontakt s nadležnim tijelima i jedinstvenim kontaktnim točkama. Države članice imenuju tijelo za nadzor tržišta koje će djelovati kao jedinstvena kontaktna točka za ovu Uredbu i obavješćuju Komisiju o identitetu jedinstvene kontaktne točke. Komisija objavljuje popis jedinstvenih kontaktnih točaka.

3. Države članice osiguravaju da njihova nacionalna nadležna tijela imaju adekvatne tehničke, financijske i ljudske resurse i infrastrukturu za djelotvorno obavljanje svojih zadaća na temelju ove Uredbe. Nacionalna nadležna tijela osobito moraju imati dovoljno stalno raspoloživog osoblja čije kompetencije i stručno znanje obuhvaćaju temeljito razumijevanje tehnologija umjetne inteligencije, podataka i obrade podataka, zaštite osobnih podataka, kibernetičke sigurnosti, temeljnih prava i rizika za zdravlje i sigurnost te poznavanje postojećih normi i pravnih zahtjeva. Države članice jednom godišnje ocjenjuju i, ako je to potrebno, ažuriraju zahtjeve u pogledu kompetencija i resursa iz ovog stavka.
4. Nacionalna nadležna tijela poduzimaju odgovarajuće mjere kako bi se osigurala odgovarajuća razina kibernetičke sigurnosti.
5. Pri obavljanju svojih zadaća nacionalna nadležna tijela postupaju u skladu s obvezama u pogledu povjerljivosti utvrđenima u članku 78.
6. Države članice do 2. kolovoza 2025., a zatim jednom svake dvije godine izvješćuju Komisiju o stanju financijskih i ljudskih resursa nacionalnih nadležnih tijela, uz ocjenu njihove adekvatnosti. Komisija te informacije prosljeđuje Vijeću za umjetnu inteligenciju radi rasprave i utvrđivanja mogućih preporuka.
7. Komisija olakšava razmjenu iskustava među nacionalnim nadležnim tijelima.
8. Nacionalna nadležna tijela mogu pružati smjernice i savjete o provedbi ove Uredbe, posebno MSP-ovima, uključujući *start-up* poduzeća, prema potrebi uzimajući u obzir smjernice i savjete Vijeća za umjetnu inteligenciju i Komisije. Ako nacionalna nadležna tijela namjeravaju pružiti smjernice i savjete u vezi s određenim UI sustavom u područjima obuhvaćenima drugim pravom Unije, prema potrebi se savjetuju s nacionalnim nadležnim tijelima na temelju tog prava Unije.
9. Ako područje primjene ove Uredbe obuhvaća institucije, tijela, urede ili agencije Unije, Europski nadzornik za zaštitu podataka djeluje kao tijelo nadležno za njihov nadzor.

POGLAVLJE VIII.

BAZA PODATAKA EU-A ZA VISOKORIZIČNE UI SUSTAVE

Članak 71.

Baza podataka EU-a za visokorizične UI sustave iz Priloga III.

1. Komisija u suradnji s državama članicama uspostavlja i održava bazu podataka EU-a koja sadržava informacije iz stavaka 2. i 3. ovog članka o visokorizičnim UI sustavima iz članka 6. stavka 2. koji su registrirani u skladu s člancima 49. i 60. i UI sustavima koji se ne smatraju visokorizičnim na temelju članka 6. stavka 3. i koji su registrirani u skladu s člankom 6. stavkom 4. i člankom 49. Pri utvrđivanju funkcionalnih specifikacija te baze podataka Komisija se savjetuje s relevantnim stručnjacima, a pri ažuriranju funkcionalnih specifikacija te baze podataka Komisija se savjetuje s Vijećem za umjetnu inteligenciju.
2. Podatke navedene u odjeljcima A i B Priloga VIII. u bazu podataka EU-a unosi dobavljač ili, ako je primjenjivo, ovlašteni zastupnik.
3. Podatke navedene u odjeljku C Priloga VIII. u bazu podataka EU-a unosi subjekt koji uvodi sustav i koji je tijelo javne vlasti, javna agencija ili javno tijelo ili koji djeluje u ime tijela javne vlasti, javne agencije ili javnog tijela, u skladu s člankom 49. stavcima 3. i 4.
4. Uz iznimku dijela iz članka 49. stavka 4. i članka 60. stavka 4. točke (c), informacije iz baze podataka EU-a registrirane u skladu s člankom 49. moraju biti pristupačne i javno dostupne na način prilagođen korisnicima. Te bi informacije trebale biti jednostavne za snalaženje i strojno čitljive. Informacije registrirane u skladu s člankom 60. dostupne su samo tijelima za nadzor tržišta i Komisiji, osim ako je potencijalni dobavljač ili dobavljač dao privolu da te informacije budu dostupne javnosti.
5. Baza podataka EU-a sadržava osobne podatke samo ako je to potrebno za prikupljanje i obradu informacija u skladu s ovom Uredbom. Te informacije uključuju imena i kontaktne podatke pojedinaca koji su odgovorni za registraciju sustava i koji imaju pravnu ovlast za zastupanje dobavljača ili subjekta koji uvodi sustav, ovisno o slučaju.

6. Komisija je nadzornik baze podataka EU-a. Dobavljačima, potencijalnim dobavljačima i subjektima koji uvode sustav Komisija stavlja na raspolaganje adekvatnu tehničku i administrativnu potporu. Baza podataka EU-a mora ispunjavati primjenjive zahtjeve u pogledu pristupačnosti.

POGLAVLJE IX.

PRAĆENJE NAKON STAVLJANJA NA TRŽIŠTE, RAZMJENA INFORMACIJA I NADZOR TRŽIŠTA

ODJELJAK 1.

Praćenje nakon stavljanja na tržište

Članak 72.

Praćenje nakon stavljanja na tržište koje provode dobavljači i plan praćenja nakon stavljanja na tržište za visokorizične UI sustave

1. Dobavljači uspostavljaju sustav praćenja nakon stavljanja na tržište i izrađuju dokumentaciju za njega na način koji je razmjeran prirodi tehnologija umjetne inteligencije i rizicima visokorizičnog UI sustava.

2. Sustavom praćenja nakon stavljanja na tržište aktivno se i sustavno prikupljaju, dokumentiraju i analiziraju relevantni podaci koje mogu dostaviti subjekti koji uvode sustav ili koji se mogu prikupiti iz drugih izvora o učinkovitosti visokorizičnih UI sustava tijekom cijelog njihova životnog ciklusa i koji dobavljaču omogućuju evaluaciju kontinuirane usklađenosti UI sustava sa zahtjevima iz poglavlja III. odjeljka 2. Ako je to relevantno, praćenje nakon stavljanja na tržište uključuje analizu interakcije s drugim UI sustavima. Ta obveza ne obuhvaća osjetljive operativne podatke subjekata koji uvode sustav koji su tijela kaznenog progona.

3. Sustav praćenja nakon stavljanja na tržište temelji se na planu praćenja nakon stavljanja na tržište. Plan praćenja nakon stavljanja na tržište dio je tehničke dokumentacije iz Priloga IV. Komisija do 2. veljače 2026. donosi provedbeni akt s detaljnim odredbama kojima se utvrđuje predložak za plan praćenja nakon stavljanja na tržište i popis elemenata koje treba uključiti u taj plan. Taj provedbeni akt donosi se u skladu s postupkom ispitivanja iz članka 98. stavka 2.

4. Za visokorizične UI sustave obuhvaćene zakonodavstvom Unije o usklađivanju navedenim u odjeljku A Priloga I., ako su sustav i plan praćenja nakon stavljanja na tržište već uspostavljeni na temelju tog zakonodavstva, kako bi se osigurala dosljednost, izbjeglo udvostručavanje i smanjila dodatna opterećenja, dobavljači imaju mogućnost da, koristeći se predloškom iz stavka 3., potrebne elemente opisane u stavcima 1., 2. i 3. prema potrebi integriraju u sustave i planove koji već postoje na temelju tog zakonodavstva, pod uvjetom da se time postiže jednakovrijedna razina zaštite.

Prvi podstavak ovog stavka primjenjuje se i na visokorizične UI sustave iz točke 5. Priloga III. koje na tržište ili u upotrebu stavljaju financijske institucije na koje se u pogledu njihova unutarnjeg upravljanja, aranžmana ili procesa primjenjuju zahtjevi na temelju prava Unije o financijskim uslugama.

ODJELJAK 2.

Razmjena informacija o ozbiljnim incidentima

Članak 73.

Prijavljivanje ozbiljnih incidenata

1. Dobavljači visokorizičnih UI sustava stavljenih na tržište Unije prijavljuju svaki ozbiljan incident tijelima za nadzor tržišta država članica u kojima je došlo do tog incidenta.

2. Prijavljivanje iz stavka 1. provodi se odmah nakon što je dobavljač utvrdio uzročno-posljedičnu vezu između UI sustava i ozbiljnog incidenta ili razumnu vjerojatnost takve veze, a u svakom slučaju najkasnije 15 dana nakon što je dobavljač ili, ako je primjenjivo, subjekt koji uvodi sustav, saznao za ozbiljni incident.

Razdobljem za prijavljivanje iz prvog podstavka uzima se u obzir težina ozbiljnog incidenta.

3. Neovisno o stavku 2. ovog članka, u slučaju raširene povrede ili ozbiljnog incidenta kako je definiran u članku 3. točki 49. podtočki (b), prijavljivanje iz stavka 1. ovog članka provodi se odmah, a najkasnije dva dana nakon što dobavljač ili, ako je primjenjivo, subjekt koji uvodi sustav, sazna za taj incident.

4. Neovisno o stavku 2., u slučaju smrti osobe prijavljivanje se provodi odmah nakon što je dobavljač ili subjekt koji uvodi sustav utvrdio uzročno-posljedičnu vezu između visokorizičnog UI sustava i ozbiljnog incidenta ili čim je posumnjao u postojanje takve veze, a najkasnije deset dana nakon datuma na koji je dobavljač ili, ako je primjenjivo, subjekt koji uvodi sustav, saznao za ozbiljni incident.

5. Ako je to potrebno kako bi se osiguralo pravodobno prijavljivanje, dobavljač ili, ako je primjenjivo, subjekt koji uvodi sustav može podnijeti početnu prijavu koja je nepotpuna, nakon koje slijedi potpuna prijava.

6. Nakon prijavljivanja ozbiljnog incidenta u skladu sa stavkom 1. dobavljač bez odgode provodi potrebne istrage u vezi s ozbiljnim incidentom i dotičnim UI sustavom. To uključuje procjenu rizika incidenta i korektivne mjere.

Dobavljač surađuje s nadležnim tijelima i, prema potrebi, s dotičnim prijavljenim tijelom tijekom istraga iz prvog podstavka i ne provodi istragu koja uključuje izmjenu dotičnog UI sustava na način koji bi mogao utjecati na naknadnu evaluaciju uzroka incidenta prije nego što o takvom djelovanju obavijesti nadležna tijela.

7. Nakon primitka obavijesti o ozbiljnom incidentu iz članka 3. točke 49. podtočke (c) relevantno tijelo za nadzor tržišta o tome obavješćuje nacionalna tijela javne vlasti ili javna tijela iz članka 77. stavka 1. Komisija izrađuje namjenske smjernice za lakše ispunjavanje obveza utvrđenih u stavku 1. ovog članka. Te se smjernice izdaju do 2. kolovoza 2025. i redovito se ocjenjuju.

8. Tijelo za nadzor tržišta u roku od sedam dana od datuma na koji je primilo prijavu iz stavka 1. ovog članka poduzima odgovarajuće mjere, kako je predviđeno u članku 19. Uredbe (EU) 2019/1020, i slijedi postupke prijavljivanja predviđene u toj uredbi.

9. Za visokorizične UI sustave iz Priloga III. koje na tržište ili u upotrebu stavljaju dobavljači na koje se primjenjuju zakonodavni instrumenti Unije kojima se utvrđuju obveze izvješćivanja jednakovrijedne onima koje su utvrđene u ovoj Uredbi, prijavljivanje ozbiljnih incidenata ograničava se na ozbiljne incidente iz članka 3. točke 49. podtočke (c).

10. Za visokorizične UI sustave koji su sigurnosne komponente uređaja ili su sami uređaji, a obuhvaćeni su uredbama (EU) 2017/745 i (EU) 2017/746, prijava ozbiljnih incidenata ograničava se na ozbiljne incidente iz članka 3. točke 49. podtočke (c) ove Uredbe i upućuje se nacionalnom nadležnom tijelu koje su u tu svrhu odabrale države članice u kojima je došlo do incidenta.

11. Nacionalna nadležna tijela odmah prijavljuju Komisiji svaki ozbiljan incident u skladu s člankom 20. Uredbe (EU) 2019/1020, bez obzira na to jesu li u vezi s njim poduzela mjere.

ODJELJAK 3.

Izvršavanje

Članak 74.

Nadzor nad tržištem i kontrola UI sustava na tržištu Unije

1. Uredba (EU) 2019/1020 primjenjuje se na UI sustave obuhvaćene ovom Uredbom. U svrhu djelotvornog izvršavanja ove Uredbe:

- (a) smatra se da svako upućivanje na gospodarski subjekt na temelju Uredbe (EU) 2019/1020 uključuje sve operatere iz članka 2. stavka 1. ove Uredbe;
- (b) smatra se da svako upućivanje na proizvod na temelju Uredbe (EU) 2019/1020 uključuje sve UI sustave obuhvaćene područjem primjene ove Uredbe.

2. U okviru svojih obveza izvješćivanja na temelju članka 34. stavka 4. Uredbe (EU) 2019/1020 tijela za nadzor tržišta svake godine izvješćuju Komisiju i relevantna nacionalna tijela nadležna za tržišno natjecanje o svim informacijama utvrđenima tijekom aktivnosti nadzora tržišta koje bi mogle biti od interesa za primjenu prava Unije o pravilima tržišnog natjecanja. Također svake godine izvješćuju Komisiju o primjeni zabranjenih praksi do koje je došlo tijekom te godine i o poduzetim mjerama.

3. Za visokorizične UI sustave povezane s proizvodima na koje se primjenjuje zakonodavstvo Unije o usklađivanju navedeno u odjeljku A Priloga I. tijelo za nadzor tržišta za potrebe ove Uredbe tijelo je odgovorno za aktivnosti nadzora tržišta imenovano na temelju tih pravnih akata.

Odstupajući od prvog podstavka i u primjerenim okolnostima, države članice mogu imenovati drugo relevantno tijelo koje će djelovati kao tijelo za nadzor tržišta pod uvjetom da osiguraju koordinaciju s relevantnim sektorskim tijelima za nadzor tržišta odgovornima za izvršavanje zakonodavstva Unije o usklađivanju navedenog u Prilogu I.

4. Postupci iz članaka od 79. do 83. ove Uredbe ne primjenjuju se na UI sustave povezane s proizvodima na koje se primjenjuje zakonodavstvo Unije o usklađivanju navedeno u odjeljku A Priloga I. ako su tim pravnim aktima već predviđeni postupci kojima se osigurava jednakovrijedna razina zaštite i ako ti pravni akti imaju isti cilj. U takvim se slučajevima primjenjuju relevantni sektorski postupci.

5. Ne dovodeći u pitanje ovlasti tijela za nadzor tržišta na temelju članka 14. Uredbe (EU) 2019/1020, u svrhu osiguravanja djelotvornog izvršavanja ove Uredbe tijela za nadzor tržišta ovlasti iz članka 14. stavka 4. točaka (d) i (j) te uredbe mogu, prema potrebi, izvršavati na daljinu.

6. Za visokorizične UI sustave koji se stavljaju na tržište, stavljaju u upotrebu ili koje koriste financijske institucije regulirane pravom Unije o financijskim uslugama, tijelo za nadzor tržišta za potrebe ove Uredbe relevantno je nacionalno tijelo odgovorno za financijski nadzor tih institucija na temelju tog zakonodavstva ako su stavljanje na tržište, stavljanje u upotrebu ili korištenje UI sustava izravno povezani s pružanjem tih financijskih usluga.

7. Odstupajući od stavka 6., u primjerenim okolnostima i pod uvjetom da je osigurana koordinacija, država članica može odrediti drugo relevantno tijelo kao tijelo za nadzor tržišta za potrebe ove Uredbe.

Nacionalna tijela za nadzor tržišta koja nadziru regulirane kreditne institucije regulirane Direktivom 2013/36/EU, a koje sudjeluju u jedinstvenom nadzornom mehanizmu uspostavljenom Uredbom (EU) br. 1024/2013, trebala bi bez odgode izvijestiti Europsku središnju banku o svim informacijama utvrđenima tijekom njihovih aktivnosti nadzora tržišta koje bi mogle biti od interesa za zadaće bonitetnog nadzora Europske središnje banke navedene u toj uredbi.

8. Za visokorizične UI sustave iz točke 1. Priloga III. ovoj Uredbi, ako se ti sustavi upotrebljavaju u svrhu kaznenog progona, upravljanja granicama, pravosuđa i demokracije, te za visokorizične UI sustave navedene u točkama 6., 7. i 8. Priloga III. ovoj Uredbi, države članice za potrebe ove Uredbe kao tijela za nadzor tržišta imenuju ili nadležna nadzorna tijela za zaštitu podataka na temelju Uredbe (EU) 2016/679 ili Direktive (EU) 2016/680 ili bilo koje drugo tijelo imenovano u skladu s istim uvjetima, utvrđenima u člancima od 41. do 44. Direktive (EU) 2016/680. Aktivnosti nadzora tržišta ni na koji način ne smiju utjecati na neovisnost pravosudnih tijela niti smiju na drugi način utjecati na njihove aktivnosti kada djeluju u pravosudnom svojstvu.

9. Ako područje primjene ove Uredbe obuhvaća institucije, tijela, urede ili agencije Unije, Europski nadzornik za zaštitu podataka djeluje kao njihovo tijelo za nadzor tržišta, osim u odnosu na Sud Europske unije kada djeluje u svojem sudbenom svojstvu.

10. Države članice olakšavaju koordinaciju između tijela za nadzor tržišta imenovanih na temelju ove Uredbe i drugih relevantnih nacionalnih tijela koja nadziru primjenu prava Unije o usklađivanju navedenog u Prilogu I. ili drugog prava Unije koje bi moglo biti relevantno za visokorizične UI sustave iz Priloga III.

11. Tijela za nadzor tržišta i Komisija mogu predložiti zajedničke aktivnosti, uključujući zajedničke istrage, koje trebaju provesti tijela za nadzor tržišta ili tijela za nadzor tržišta zajedno s Komisijom, a čiji je cilj promicanje usklađenosti, utvrđivanje neusklađenosti, podizanje svijesti ili pružanje smjernica u vezi s ovom Uredbom u pogledu specifičnih kategorija visokorizičnih UI sustava za koje je utvrđeno da predstavljaju ozbiljan rizik u dvjema ili više država članica u skladu s člankom 9. Uredbe (EU) 2019/1020. Ured za umjetnu inteligenciju pruža koordinacijsku potporu za zajedničke istrage.

12. Ne dovodeći u pitanje ovlasti predviđene na temelju Uredbe (EU) 2019/1020 te, ako je to relevantno i ograničeno na ono što je potrebno za ispunjavanje njihovih zadaća, dobavljači tijelima za nadzor tržišta odobravaju puni pristup dokumentaciji i skupovima podataka za treniranje, validaciju i testiranje koji se upotrebljavaju za razvoj visokorizičnih UI sustava, među ostalim, prema potrebi i podložno sigurnosnim zaštitnim mjerama, putem aplikacijskih programskih sučelja ili drugih relevantnih tehničkih sredstava i alata koji omogućuju daljnji pristup.

13. Tijelima za nadzor tržišta odobrava se pristup izvornom kodu visokorizičnog UI sustava na obrazložen zahtjev i samo ako su ispunjena sljedeća dva uvjeta:

- (a) pristup izvornom kodu potreban je za ocjenjivanje sukladnosti visokorizičnog UI sustava sa zahtjevima utvrđenima u poglavlju III. odjeljku 2.; i
- (b) postupci testiranja ili revizije i provjere na temelju podataka i dokumentacije koje je dostavio dobavljač iscrpljeni su ili su se pokazali nedostatnima.

14. Sa svim informacijama ili dokumentacijom koje su tijela za nadzor tržišta dobila postupaju se u skladu s obvezama u pogledu povjerljivosti utvrđenima u članku 78.

Članak 75.

Uzajamna pomoć, nadzor tržišta i kontrola UI sustavâ opće namjene

1. Ako se UI sustav temelji na UI modelu opće namjene, a model i sustav razvija isti dobavljač, Ured za umjetnu inteligenciju ima ovlasti za praćenje i nadzor usklađenosti tog UI sustava s obvezama na temelju ove Uredbe. Za obavljanje svojih zadaća praćenja i nadzora Ured za umjetnu inteligenciju ima sve ovlasti tijela za nadzor tržišta predviđene u ovom odjeljku i u Uredbi (EU) 2019/1020.

2. Ako relevantna tijela za nadzor tržišta imaju dovoljno razloga smatrati da UI sustavi opće namjene koje subjekti koji uvode sustav mogu izravno upotrebljavati u barem jednu svrhu koja je na temelju ove Uredbe klasificirana kao visokorizična nisu usklađeni sa zahtjevima ove Uredbe, ona surađuju s Uredom za umjetnu inteligenciju kako bi provela evaluacije usklađenosti i o tome obavješćuju Vijeće za umjetnu inteligenciju i druga tijela za nadzor tržišta.

3. Ako tijelo za nadzor tržišta ne može zaključiti svoju istragu visokorizičnog UI sustava zbog toga što nema pristup određenim informacijama povezanim s UI modelom opće namjene, iako je poduzelo sve potrebne korake kako bi ih pribavilo, ono može Uredu za umjetnu inteligenciju podnijeti obrazloženi zahtjev na temelju kojeg se nalaže pristup tim informacijama. U tom slučaju Ured za umjetnu inteligenciju bez odgode, a najkasnije u roku od 30 dana, tijelu podnositelju zahtjeva dostavlja sve informacije koje Ured za umjetnu inteligenciju smatra važnima za utvrđivanje je li visokorizični UI sustav neusklađen. Tijela za nadzor tržišta štite povjerljivost informacija koje su pribavila u skladu s člankom 78. ove Uredbe. Postupak predviđen u poglavlju VI. Uredbe (EU) 2019/1020 primjenjuje se *mutatis mutandis*.

Članak 76.

Nadzor testiranja u stvarnim uvjetima koji provode tijela za nadzor tržišta

1. Tijela za nadzor tržišta imaju nadležnosti i ovlasti da osiguraju da se testiranje u stvarnim uvjetima provodi u skladu s ovom Uredbom.

2. Ako se testiranje u stvarnim uvjetima provodi za UI sustave koji se nadziru u regulatornom izoliranom okruženju za umjetnu inteligenciju na temelju članka 58., tijela za nadzor tržišta provjeravaju usklađenost s člankom 60. u okviru svoje nadzorne uloge za regulatorno izolirano okruženje za umjetnu inteligenciju. Ta tijela mogu, prema potrebi, dopustiti da dobavljač ili potencijalni dobavljač provodi testiranje u stvarnim uvjetima odstupajući od uvjeta utvrđenih u članku 60. stavku 4. točaka (f) i (g).

3. Ako su potencijalni dobavljač, dobavljač ili treća strana obavijestili tijelo za nadzor tržišta o ozbiljnom incidentu ili ono ima drugih razloga vjerovati da uvjeti iz članaka 60. i 61. nisu ispunjeni, ono može na svojem državnom području prema potrebi donijeti jednu od sljedećih odluka:

(a) suspendirati ili obustaviti testiranje u stvarnim uvjetima;

(b) zahtijevati od dobavljača ili potencijalnog dobavljača i od subjekta koji uvodi sustav ili potencijalnog subjekta koji uvodi sustav da izmijeni bilo koji aspekt testiranja u stvarnim uvjetima.

4. Ako je tijelo za nadzor tržišta donijelo odluku iz stavka 3. ovog članka ili je podnijelo prigovor u smislu članka 60. stavka 4. točke (b), u odluci ili prigovoru moraju se navesti razlozi za njih te način na koji dobavljač ili potencijalni dobavljač može osporiti odluku ili prigovor.

5. Kada je primjenjivo, ako je tijelo za nadzor tržišta donijelo odluku iz stavka 3., o razlozima njezina donošenja obavješćuje tijela za nadzor tržišta drugih država članica u kojima je UI sustav testiran u skladu s planom testiranja.

Članak 77.

Ovlasti tijela nadležnih za zaštitu temeljnih prava

1. Nacionalna tijela javne vlasti ili javna tijela koja nadziru ili izvršavaju poštovanje obveza na temelju prava Unije o zaštiti temeljnih prava, uključujući pravo na nediskriminaciju, u pogledu korištenja visokorizičnih UI sustava iz Priloga III. ovlaštena su zatražiti i pristupiti svojoj dokumentaciji izrađenoj ili vođenoj na temelju ove Uredbe na pristupačnom jeziku i u pristupačnom formatu kada je pristup toj dokumentaciji potreban za djelotvorno ispunjavanje njihovih mandata u granicama njihove jurisdikcije. Relevantno tijelo javne vlasti ili javno tijelo obavješćuje tijelo za nadzor tržišta dotične države članice o svakom takvom zahtjevu.

2. Svaka država članica do 2. studenoga 2024. određuje tijela javne vlasti ili javna tijela iz stavka 1. i objavljuje popis tih tijela. Države članice taj popis dostavljaju Komisiji i drugim državama članicama te ga ažuriraju.

3. Ako dokumentacija iz stavka 1. nije dovoljna za utvrđivanje je li došlo do povrede obveza na temelju prava Unije o zaštiti temeljnih prava, tijelo javne vlasti ili javno tijelo iz stavka 1. može tijelu za nadzor tržišta podnijeti obrazloženi zahtjev za organiziranje testiranja visokorizičnog UI sustava tehničkim sredstvima. Tijelo za nadzor tržišta u razumnom roku nakon podnošenja zahtjeva organizira testiranje u bliskoj suradnji s tijelom javne vlasti ili javnim tijelom koje je podnijelo zahtjev.

4. Sa svim informacijama ili dokumentacijom koje su nacionalna tijela javne vlasti ili javna tijela iz stavka 1. ovog članka dobila na temelju ovog članka postupa se u skladu s obvezama u pogledu povjerljivosti utvrđenima u članku 78.

Članak 78.

Povjerljivost

1. Komisija, tijela za nadzor tržišta, prijavljena tijela i sve druge fizičke ili pravne osobe uključene u primjenu ove Uredbe, u skladu s pravom Unije ili nacionalnim pravom, poštuju povjerljivost informacija i podataka dobivenih pri obavljanju svojih zadaća i aktivnosti tako da osobito štite:

- (a) prava intelektualnog vlasništva i povjerljive poslovne informacije ili poslovne tajne fizičke ili pravne osobe, uključujući izvorni kôd, osim u slučajevima iz članka 5. Direktive (EU) 2016/943 Europskog parlamenta i Vijeća ⁽⁵⁷⁾;
- (b) djelotvornu provedbu ove Uredbe, osobito za potrebe inspekcija, istraga ili revizija;
- (c) javne i nacionalne sigurnosne interese;
- (d) provedbu kaznenih ili upravnih postupaka;
- (e) podatke klasificirane na temelju prava Unije ili nacionalnog prava.

2. Tijela uključena u primjenu ove Uredbe u skladu sa stavkom 1. zahtijevaju samo one podatke koji su nužni za procjenu rizika koji predstavljaju UI sustavi i za izvršavanje svojih ovlasti u skladu s ovom Uredbom i s Uredbom (EU) 2019/1020. Ta tijela uspostavljaju adekvatne i djelotvorne mjere u području kibernetičke sigurnosti radi zaštite sigurnosti i povjerljivosti dobivenih informacija i podataka te u skladu s primjenjivim pravom Unije ili nacionalnim pravom brišu prikupljene podatke čim prestanu biti potrebni u svrhu za koju su dobiveni.

3. Ne dovodeći u pitanje stavke 1. i 2., informacije koje na povjerljivoj osnovi međusobno razmjenjuju nacionalna nadležna tijela ili nacionalna nadležna tijela i Komisija ne otkrivaju se bez prethodnog savjetovanja s nacionalnim nadležnim tijelom od kojeg informacije potječu i sa subjektom koji uvodi sustav kada tijela kaznenog progona, tijela za nadzor granica, tijela za imigraciju ili tijela za azil upotrebljavaju visokorizične UI sustave iz točaka 1., 6. ili 7. Priloga III. i kada bi se takvim otkrivanjem ugrozili javni i nacionalni sigurnosni interesi. Ta razmjena informacija ne obuhvaća osjetljive operativne podatke u vezi s aktivnostima tijela kaznenog progona, tijela za nadzor granica, tijela za imigraciju ili tijela za azil.

Ako su tijela kaznenog progona, tijela za imigraciju ili tijela za azil dobavljači visokorizičnih UI sustava iz točaka 1., 6. ili 7. Priloga III., tehnička dokumentacija iz Priloga IV. ostaje u prostorijama tih tijela. Ta tijela osiguravaju da tijela za nadzor tržišta iz članka 74. stavaka 8. i 9., ovisno o slučaju, mogu na zahtjev odmah pristupiti toj dokumentaciji ili dobiti njezin primjerak. Pristup toj dokumentaciji ili njezinim primjercima dopušten je samo osoblju tijela za nadzor tržišta koje je prošlo odgovarajući stupanj sigurnosne provjere.

4. Stavci 1., 2. i 3. ne utječu na prava ili obveze Komisije, država članica i njihovih relevantnih tijela, kao ni na obveze prijavljenih tijela u pogledu razmjene informacija i širenja upozorenja, među ostalim u kontekstu prekogranične suradnje, a ne utječu ni na obveze dotičnih stranaka da pruže informacije na temelju kaznenog prava država članica.

5. Komisija i države članice mogu, kada je to potrebno i u skladu s relevantnim odredbama međunarodnih i trgovinskih sporazuma, razmjenjivati povjerljive informacije s regulatornim tijelima trećih zemalja s kojima su sklopile bilateralne ili multilateralne aranžmane o povjerljivosti kojima se jamči odgovarajuća razina povjerljivosti.

Članak 79.

Postupak koji se na nacionalnoj razini primjenjuje na UI sustave koji predstavljaju rizik

1. UI sustavi koji predstavljaju rizik smatraju se „proizvodom koji predstavlja rizik” kako je definiran u članku 3. točki 19. Uredbe (EU) 2019/1020 u mjeri u kojoj predstavljaju rizike za zdravlje ili sigurnost osoba ili za temeljna prava osoba.

2. Ako tijelo za nadzor tržišta države članice ima dovoljno razloga smatrati da UI sustav predstavlja rizik u smislu stavka 1. ovog članka, ono evaluira usklađenost dotičnog UI sustava sa svim zahtjevima i obvezama utvrđenima u ovoj Uredbi. Posebna pozornost posvećuje se UI sustavima koji predstavljaju rizik za skupine ranjivih osoba. Ako su utvrđeni rizici za temeljna prava, tijelo za nadzor tržišta ujedno obavješćuje relevantna nacionalna tijela javne vlasti ili javna tijela iz članka 77. stavka 1. te s njima u potpunosti surađuje. Relevantni operateri prema potrebi surađuju s tijelom za nadzor tržišta i drugim nacionalnim tijelima javne vlasti ili javnim tijelima iz članka 77. stavka 1.

⁽⁵⁷⁾ Direktiva (EU) 2016/943 Europskog parlamenta i Vijeća od 8. lipnja 2016. o zaštiti neotkrivenih znanja i iskustva te poslovnih informacija (poslovne tajne) od nezakonitog pribavljanja, korištenja i otkrivanja (SL L 157, 15.6.2016., str. 1.).

Ako tijekom te evaluacije tijelo za nadzor tržišta ili, ako je primjenjivo, tijelo za nadzor tržišta u suradnji s nacionalnim tijelom javne vlasti iz članka 77. stavka 1. utvrdi da UI sustav ne ispunjava zahtjeve i obveze utvrđene u ovoj Uredbi, ono bez nepotrebne odgode od relevantnog operatera zahtijeva da poduzme sve odgovarajuće korektivne mjere kako bi UI sustav uskladio s tim zahtjevima i obvezama, povukao ga s tržišta ili ga opozvao u roku koji može propisati tijelo za nadzor tržišta, a u svakom slučaju unutar manje od 15 radnih dana ili kako je predviđeno u relevantnom zakonodavstvu Unije o usklađivanju.

Tijelo za nadzor tržišta o tome obavješćuje relevantno prijavljeno tijelo. Na mjere navedene u drugom podstavku ovog stavka primjenjuje se članak 18. Uredbe (EU) 2019/1020.

3. Ako tijelo za nadzor tržišta smatra da neusklađenost nije ograničena samo na njegovo državno područje, ono bez nepotrebne odgode obavješćuje Komisiju i druge države članice o rezultatima evaluacije i mjerama za koje je zatražilo da ih operater poduzme.

4. Operater osigurava da se poduzmu sve odgovarajuće korektivne mjere u pogledu svih dotičnih UI sustava koje je stavio na raspolaganje na tržištu Unije.

5. Ako operater UI sustava ne poduzme adekvatne korektivne mjere u roku iz stavka 2., tijelo za nadzor tržišta poduzima sve odgovarajuće privremene mjere kako bi zabranilo ili ograničilo stavljanje UI sustava na raspolaganje na svojem nacionalnom tržištu ili njegovo stavljanje u upotrebu, odnosno kako bi povuklo taj proizvod ili samostalan UI sustav s tog tržišta ili ga opozvalo. To tijelo bez nepotrebne odgode obavješćuje Komisiju i druge države članice o navedenim mjerama.

6. Obavijest iz stavka 5. uključuje sve dostupne pojedinosti, a osobito informacije potrebne za identifikaciju neusklađenog UI sustava, njegovo podrijetlo i lanac opskrbe, prirodu navodne neusklađenosti i povezanog rizika, prirodu i trajanje poduzetih nacionalnih mjera te argumente relevantnog operatera. Tijela za nadzor tržišta posebno navode je li neusklađenost posljedica jednog ili više sljedećih uzroka:

(a) ne poštuje se zabrana praksi u području umjetne inteligencije iz članka 5.;

(b) visokorizični UI sustav ne ispunjava zahtjeve utvrđene u poglavlju III. odjeljku 2.;

(c) postoje nedostaci u usklađenim normama ili zajedničkim specifikacijama iz članaka 40. i 41. kojima se stvara pretpostavka sukladnosti;

(d) izostaje usklađenost s člankom 50.

7. Tijela za nadzor tržišta koja nisu tijelo za nadzor tržišta države članice koje pokreće postupak bez nepotrebne odgode obavješćuju Komisiju i druge države članice o svim donesenim mjerama i o svim dodatnim informacijama koje su im na raspolaganju i koje se odnose na neusklađenost dotičnog UI sustava te, u slučaju neslaganja s nacionalnom mjerom o kojoj je obaviješteno, o svojim prigovorima.

8. Ako u roku od tri mjeseca od primitka obavijesti iz stavka 5. ovog članka ni tijelo za nadzor tržišta države članice ni Komisija ne podnese prigovor na privremenu mjeru koju je poduzelo tijelo za nadzor tržišta druge države članice, ta mjera smatra se opravdanom. Time se ne dovode u pitanje postupovna prava dotičnog operatera u skladu s člankom 18. Uredbe (EU) 2019/1020. Tromjesečno razdoblje iz ovog stavka skraćuje se na 30 dana u slučaju nepoštovanja zabrane praksi u području umjetne inteligencije iz članka 5. ove Uredbe.

9. Tijela za nadzor tržišta osiguravaju da se u odnosu na dotični proizvod ili UI sustav bez nepotrebne odgode poduzmu primjerene restriktivne mjere, primjerice povlačenje proizvoda ili UI sustava s njihovih tržišta.

Članak 80.

Postupak koji se primjenjuje na UI sustave koje je dobavljač u skladu s Prilogom III. klasificirao kao UI sustave koji nisu visokorizični

1. Ako tijelo za nadzor tržišta ima dovoljno razloga smatrati da UI sustav koji je dobavljač u skladu s člankom 6. stavkom 3. klasificirao kao UI sustav koji nije visokorizičan zapravo jest visokorizičan, ono provodi evaluaciju dotičnog UI sustava u vezi s njegovom klasifikacijom kao visokorizičnim UI sustavom na temelju uvjeta utvrđenih u članku 6. stavku 3. i smjernica Komisije.

2. Ako tijekom te evaluacije tijelo za nadzor tržišta utvrdi da je dotični UI sustav visokorizičan, ono od relevantnog dobavljača bez nepotrebne odgode zahtijeva da poduzme sve potrebne mjere kako bi UI sustav uskladio sa zahtjevima i obvezama utvrđenima u ovoj Uredbi te da u roku koji može propisati tijelo za nadzor tržišta poduzme odgovarajuće korektivne mjere.
3. Ako tijelo za nadzor tržišta smatra da korištenje dotičnog UI sustava nije ograničeno samo na njegovo državno područje, ono bez nepotrebne odgode Komisiju i druge države članice obavješćuje o rezultatima evaluacije i mjerama za koje je zatražilo da ih dobavljač poduzme.
4. Dobavljač osigurava da se poduzmu sve potrebne mjere kako bi se UI sustav uskladio sa zahtjevima i obvezama utvrđenima u ovoj Uredbi. Ako dobavljač dotičnog UI sustava u roku iz stavka 2. ovog članka ne uskladi taj UI sustav s navedenim zahtjevima i obvezama, izriču mu se novčane kazne u skladu s člankom 99.
5. Dobavljač osigurava da se poduzmu sve odgovarajuće korektivne mjere u pogledu svih dotičnih UI sustava koje je stavio na raspolaganje na tržištu Unije.
6. Ako dobavljač dotičnog UI sustava u roku iz stavka 2. ovog članka ne poduzme odgovarajuće korektivne mjere, primjenjuje se članak 79. stavci od 5. do 9.
7. Ako tijekom evaluacije na temelju stavka 1. ovog članka tijelo za nadzor tržišta utvrdi da je dobavljač pogrešno klasificirao UI sustav kao UI sustav koji nije visokorizičan kako bi izbjegao primjenu zahtjeva iz poglavlja III. odjeljka 2., dobavljaču se izriču novčane kazne u skladu s člankom 99.
8. Pri izvršavanju svojih ovlasti za praćenje primjene ovog članka, a u skladu s člankom 11. Uredbe (EU) 2019/1020, tijela za nadzor tržišta mogu provoditi odgovarajuće provjere, posebno uzimajući u obzir informacije pohranjene u bazi podataka EU-a iz članka 71. ove Uredbe.

Članak 81.

Zaštitni postupak Unije

1. Ako tijelo za nadzor tržišta države članice u roku od tri mjeseca od primitka obavijesti iz članka 79. stavka 5., ili u roku od 30 dana u slučaju nepoštovanja zabrane praksi u području umjetne inteligencije iz članka 5., podnese prigovore na mjeru koju je poduzelo drugo tijelo za nadzor tržišta ili ako Komisija smatra da je mjera u suprotnosti s pravom Unije, Komisija bez nepotrebne odgode započinje savjetovanje s tijelom za nadzor tržišta relevantne države članice i operaterom ili operaterima te provodi evaluaciju nacionalne mjere. Na temelju rezultata te evaluacije Komisija u roku od šest mjeseci, ili u roku od 60 dana u slučaju nepoštovanja zabrane praksi u području umjetne inteligencije iz članka 5., od obavijesti iz članka 79. stavka 5. odlučuje je li nacionalna mjera opravdana i svoju odluku priopćuje tijelu za nadzor tržišta dotične države članice. Komisija o svojoj odluci obavješćuje i sva ostala tijela za nadzor tržišta.
2. Ako Komisija smatra da je mjera koju je poduzela relevantna država članica opravdana, sve države članice osiguravaju da u vezi s dotičnim UI sustavom poduzmu primjerene restriktivne mjere, primjerice tako da zahtijevaju da se taj UI sustav bez nepotrebne odgode povuče s njihova tržišta, i o tome obavješćuju Komisiju. Ako Komisija smatra da je nacionalna mjera neopravdana, dotična država članica povlači mjeru i o tome obavješćuje Komisiju.
3. Ako se nacionalna mjera smatra opravdanom i ako se neusklađenost UI sustava pripisuje nedostacima u usklađenim normama ili zajedničkim specifikacijama iz članaka 40. i 41. ove Uredbe, Komisija primjenjuje postupak iz članka 11. Uredbe (EU) br. 1025/2012.

Članak 82.

Usklađeni UI sustavi koji predstavljaju rizik

1. Ako tijelo za nadzor tržišta države članice nakon provedene evaluacije na temelju članka 79. i savjetovanja s relevantnim nacionalnim tijelom javne vlasti iz članka 77. stavka 1. zaključi da visokorizični UI sustav, iako je u skladu s ovom Uredbom, ipak predstavlja rizik za zdravlje ili sigurnost osoba, za temeljna prava ili za druge aspekte zaštite javnog interesa, od relevantnog operatera zahtijeva da bez nepotrebne odgode i u roku koji ono može propisati poduzme sve odgovarajuće mjere kako bi se osiguralo da dotični UI sustav, kada bude stavljen na tržište ili u upotrebu, više ne predstavlja taj rizik.

2. Dobavljač ili drugi relevantni operater osigurava da se u roku koji je propisalo tijelo za nadzor tržišta države članice iz stavka 1. poduzmu korektivne mjere u pogledu dotičnih UI sustava koje je stavio na raspolaganje na tržištu Unije.
3. Države članice odmah obavješćuju Komisiju i druge države članice o zaključku na temelju stavka 1. Te informacije uključuju sve dostupne pojedinosti, a osobito podatke potrebne za identifikaciju dotičnog UI sustava, podrijetlo i lanac opskrbe tog UI sustava, prirodu s njime povezanog rizika te prirodu i trajanje poduzetih nacionalnih mjera.
4. Komisija bez nepotrebne odgode započinje savjetovanje s dotičnim državama članicama i relevantnim operaterima te provodi evaluaciju poduzetih nacionalnih mjera. Na temelju rezultata te evaluacije Komisija odlučuje je li mjera opravdana i prema potrebi predlaže druge odgovarajuće mjere.
5. Komisija svoju odluku odmah priopćuje dotičnim državama članicama i relevantnim operaterima. Komisija o njoj obavješćuje i druge države članice.

Članak 83.

Formalna neusklađenost

1. Tijelo za nadzor tržišta države članice od relevantnog dobavljača zahtijeva da određenu neusklađenost otkloni u roku koji ono može propisati ako ustanovi jedno od sljedećeg:
 - (a) oznaka CE stavljena je uz kršenje članka 48.;
 - (b) oznaka CE uopće nije stavljena;
 - (c) EU izjava o sukladnosti iz članka 47. nije sastavljena;
 - (d) EU izjava o sukladnosti iz članka 47. nije ispravno sastavljena;
 - (e) registracija u bazi podataka EU-a iz članka 71. nije provedena;
 - (f) ovlašteni zastupnik nije imenovan, ako je primjenjivo;
 - (g) tehnička dokumentacija nije dostupna.
2. Ako se neusklađenost iz stavka 1. nastavi, tijelo za nadzor tržišta dotične države članice poduzima odgovarajuće i razmjerne mjere kako bi ograničilo ili zabranilo stavljanje visokorizičnog UI sustava na raspolaganje na tržištu ili kako bi osiguralo da se taj UI sustav bez odgode opozove ili povuče s tržišta.

Članak 84.

Potporne strukture Unije za testiranje umjetne inteligencije

1. Komisija za obavljanje zadaća na temelju članka 21. stavka 6. Uredbe (EU) 2019/1020 u području umjetne inteligencije određuje jednu ili više potpornih struktura Unije za testiranje umjetne inteligencije.
2. Ne dovodeći u pitanje zadaće iz stavka 1., potporne strukture Unije za testiranje umjetne inteligencije također pružaju neovisne tehničke ili znanstvene savjete na zahtjev Vijeća za umjetnu inteligenciju, Komisije ili tijela za nadzor tržišta.

ODJELJAK 4.

Pravna sredstva

Članak 85.

Pravo na podnošenje pritužbe tijelu za nadzor tržišta

Ne dovodeći u pitanje druga upravna ili sudska pravna sredstva, svaka fizička ili pravna osoba koja ima razloga smatrati da je došlo do povrede odredaba ove Uredbe može podnijeti pritužbe relevantnom tijelu za nadzor tržišta.

U skladu s Uredbom (EU) 2019/1020 takve pritužbe uzimaju se u obzir u svrhu provođenja aktivnosti nadzora tržišta i s njima se postupa u skladu s posebnim postupcima koje su u tu svrhu utvrdila tijela za nadzor tržišta.

Članak 86.

Pravo na objašnjenje donošenja pojedinačnih odluka

1. Svaka osoba na koju se primjenjuje odluka koju subjekt koji uvodi sustav donese na temelju izlaznih podataka visokorizičnog UI sustava iz Priloga III., uz iznimku sustava navedenih u točki 2. tog priloga, a koja proizvodi pravne učinke ili na tu osobu na sličan način znatno utječe tako da ona smatra da ima negativan učinak na njezino zdravlje, sigurnost ili temeljna prava, ima pravo od subjekta koji uvodi sustav zatražiti jasna i smislena objašnjenja o ulozi UI sustava u postupku donošenja odluka i o glavnim elementima donesene odluke.

2. Stavak 1. ne primjenjuje se na korištenje UI sustava za koje iznimke od obveze iz tog stavka ili njezina ograničenja proizlaze iz prava Unije ili nacionalnog prava u skladu s pravom Unije.

3. Ovaj se članak primjenjuje samo ako pravo iz stavka 1. nije na drugi način predviđeno na temelju prava Unije.

Članak 87.

Prijava povreda i zaštita prijavitelja povreda

Direktiva (EU) 2019/1937 primjenjuje se na prijave povreda ove Uredbe i zaštitu osoba koje prijavljuju takve povrede.

ODJELJAK 5.

Nadzor, istrage, izvršavanje i praćenje u vezi s dobavljačima UI modelâ opće namjene

Članak 88.

Izvršavanje obveza dobavljača UI modelâ opće namjene

1. Komisija ima isključive ovlasti za nadzor i izvršavanje poglavlja V., uzimajući u obzir postupovna jamstva na temelju članka 94. Komisija provedbu tih zadaća povjerava Uredu za umjetnu inteligenciju, ne dovodeći u pitanje organizacijske ovlasti Komisije i podjelu nadležnosti između država članica i Unije na temelju Ugovorâ.

2. Ne dovodeći u pitanje članak 75. stavak 3., tijela za nadzor tržišta mogu od Komisije zatražiti da izvrši ovlasti utvrđene u ovom odjeljku ako je to potrebno i razmjerno kako bi im se pomoglo u ispunjavanju njihovih zadaća na temelju ove Uredbe.

Članak 89.**Mjere praćenja**

1. Za potrebe obavljanja zadaća koje su mu dodijeljene na temelju ovog odjeljka Ured za umjetnu inteligenciju može poduzimati mjere potrebne za praćenje djelotvorne provedbe ove Uredbe i usklađenosti s njome od strane dobavljača UI modela opće namjene, među ostalim i njihova poštovanja odobrenih kodeksa prakse.
2. Dobavljači niže u lancu imaju pravo podnijeti pritužbu zbog navodne povrede ove Uredbe. Pritužba mora biti propisno obrazložena, a u njoj se navodi barem sljedeće:
 - (a) kontaktna točka dotičnog dobavljača UI modela opće namjene;
 - (b) opis relevantnih činjenica, dotične odredbe ove Uredbe i razlog zašto dobavljač niže u lancu smatra da je dotični dobavljač UI modela opće namjene počinio povredu ove Uredbe;
 - (c) sve ostale informacije koje dobavljač niže u lancu koji je podnio zahtjev smatra relevantnima, uključujući, prema potrebi, informacije prikupljene na vlastitu inicijativu.

Članak 90.**Upozorenja znanstvenog povjerenstva o sistemskim rizicima**

1. Znanstveno povjerenstvo može Uredu za umjetnu inteligenciju dostaviti kvalificirano upozorenje ako ima razloga sumnjati na sljedeće:
 - (a) UI model opće namjene predstavlja konkretan utvrdiv rizik na razini Unije; ili
 - (b) UI model opće namjene ispunjava uvjete iz članka 51.
2. Slijedom takvog kvalificiranog upozorenja Komisija, putem Ureda za umjetnu inteligenciju i nakon što je obavijestila Vijeće za umjetnu inteligenciju, može izvršavati ovlasti utvrđene u ovom odjeljku u svrhu procjene tog pitanja. Ured za umjetnu inteligenciju obavješćuje Vijeće za umjetnu inteligenciju o svim mjerama u skladu s člancima od 91. do 94.
3. Kvalificirano upozorenje mora biti propisno obrazloženo, a u njemu se navodi barem sljedeće:
 - (a) kontaktna točka dobavljača dotičnog UI modela opće namjene sa sistemskim rizikom;
 - (b) opis relevantnih činjenica i razloga za upozorenje znanstvenog povjerenstva;
 - (c) sve ostale informacije koje znanstveno povjerenstvo smatra relevantnima, uključujući, prema potrebi, informacije prikupljene na vlastitu inicijativu.

Članak 91.**Ovlast za zahtijevanje dokumentacije i informacija**

1. Komisija može od dobavljača dotičnog UI modela opće namjene zahtijevati da dostavi dokumentaciju koju je dobavljač sastavio u skladu s člancima 53. i 55. ili sve dodatne informacije koje su potrebne u svrhu procjene usklađenosti dobavljača s ovom Uredbom.
2. Prije slanja zahtjeva za informacije Ured za umjetnu inteligenciju može pokrenuti strukturirani dijalog s dobavljačem UI modela opće namjene.
3. Na propisno obrazložen zahtjev znanstvenog povjerenstva Komisija može uputiti zahtjev za informacije dobavljaču UI modela opće namjene ako je pristup informacijama potreban i razmjeran za ispunjavanje zadaća znanstvenog povjerenstva u skladu s člankom 68. stavkom 2.

4. U zahtjevu za informacije navode se pravna osnova i svrha zahtjeva, preciziraju se informacije koje se zahtijevaju, određuje se rok u kojem se moraju dostaviti informacije i navode se novčane kazne predviđene u članku 101. za dostavljanje netočnih, nepotpunih ili obmanjujućih informacija.

5. Dobavljač dotičnog UI modela opće namjene ili njegov zastupnik dostavlja informacije obuhvaćene zahtjevom. U slučaju pravnih osoba, trgovačkih društava ili, ako dobavljač nema pravnu osobnost, osobe koje su ih na temelju zakona ili njihovih internih pravnih akata ovlaštene zastupati dostavljaju informacije obuhvaćene zahtjevom u ime dobavljača dotičnog UI modela opće namjene. Propisno ovlašteni odvjetnici mogu dostaviti informacije u ime svojih klijenata. Međutim, klijenti snose punu odgovornost ako su dostavljene informacije nepotpune, netočne ili obmanjujuće.

Članak 92.

Ovlast za provođenje evaluacija

1. Ured za umjetnu inteligenciju može, nakon savjetovanja s Vijećem za umjetnu inteligenciju, provoditi evaluacije dotičnog UI modela opće namjene radi sljedećeg:

- (a) procjene usklađenosti dobavljača s obvezama na temelju ove Uredbe ako su informacije prikupljene na temelju članka 91. nedostadne; ili
- (b) istrage sistemskih rizika na razini Unije u pogledu UI modelâ opće namjene sa sistemskim rizikom, posebice slijedom kvalificiranog upozorenja znanstvenog povjerenstva u skladu s člankom 90. stavkom 1. točkom (a).

2. Komisija može odlučiti imenovati neovisne stručnjake, među ostalim iz znanstvenog povjerenstva osnovanog na temelju članka 68., koji će biti zaduženi za provedbu evaluacija u njezino ime. Neovisni stručnjaci imenovani za tu zadaću moraju ispunjavati kriterije iz članka 68. stavka 2.

3. Za potrebe stavka 1. Komisija može zatražiti pristup dotičnom UI modelu opće namjene putem aplikacijskih programskih sučelja ili drugih odgovarajućih tehničkih sredstava i alata, uključujući izvorni kôd.

4. U zahtjevu za pristup navode se pravna osnova, svrha zahtjeva i razlozi za njegovo podnošenje, određuje se rok u kojem se mora omogućiti pristup i navode se novčane kazne predviđene u članku 101. ako se pristup ne omogući.

5. Dobavljač dotičnog UI modela opće namjene ili njegov zastupnik dostavlja informacije obuhvaćene zahtjevom. U slučaju pravnih osoba, trgovačkih društava ili, ako dobavljači nemaju pravnu osobnost, osobe koje su ih na temelju zakona ili njihovih internih pravnih akata ovlaštene zastupati omogućuju zatraženi pristup u ime dobavljača dotičnog UI modela opće namjene.

6. Komisija donosi provedbene akte kojima se utvrđuju detaljni aranžmani i uvjeti za evaluacije, uključujući detaljne aranžmane za uključivanje neovisnih stručnjaka i postupak za njihov odabir. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 98. stavka 2.

7. Prije nego što zatraži pristup dotičnom UI modelu opće namjene Ured za umjetnu inteligenciju može pokrenuti strukturirani dijalog s dobavljačem UI modela opće namjene kako bi prikupio više informacija o unutarnjem testiranju modela, unutarnjim zaštitnim mjerama za sprečavanje sistemskih rizika i drugim unutarnjim postupcima i mjerama koje je dobavljač poduzeo za ublažavanje takvih rizika.

Članak 93.

Ovlast za zahtijevanje mjera

1. Ako je to potrebno i primjereno, Komisija može od dobavljača zahtijevati sljedeće:

- (a) da poduzmu odgovarajuće mjere za ispunjavanje obveza utvrđenih u člancima 53. i 54.;

- (b) da provedu mjere za ublažavanje rizika ako je evaluacija provedena u skladu s člankom 92. rezultirala ozbiljnom i potkrijepljenom sumnjom na postojanje sistemskog rizika na razini Unije;
 - (c) da ograniče stavljanje modela na raspolaganje na tržištu, povuku ga ili opozovu.
2. Prije zahtijevanja mjere Ured za umjetnu inteligenciju može pokrenuti strukturirani dijalog s dobavljačem UI modela opće namjene.
3. Ako tijekom strukturiranog dijaloga iz stavka 2. dobavljač UI modela opće namjene sa sistemskim rizikom ponudi da će preuzeti obveze za provedbu mjera za ublažavanje sistemskog rizika na razini Unije, Komisija može odlukom odrediti da te obveze budu obvezujuće i navesti da nema daljnjih razloga za djelovanje.

Članak 94.

Postupovna prava gospodarskih subjekata UI modela opće namjene

Članak 18. Uredbe (EU) 2019/1020 primjenjuje se *mutatis mutandis* na dobavljače UI modela opće namjene, ne dovodeći u pitanje specifičnija postupovna prava predviđena u ovoj Uredbi.

POGLAVLJE X.

KODEKSI PONAŠANJA I SMJERNICE

Članak 95.

Kodeksi ponašanja za dobrovoljnu primjenu specifičnih zahtjeva

1. Ured za umjetnu inteligenciju i države članice potiču i olakšavaju izradu kodeksa ponašanja, uključujući povezane mehanizme upravljanja, namijenjenih poticanju dobrovoljne primjene pojedinih ili svih zahtjeva iz poglavlja III. odjeljka 2. na UI sustave koji nisu visokorizični, uzimajući u obzir dostupna tehnička rješenja i primjere najbolje prakse iz sektora koji omogućuju primjenu takvih zahtjeva.
2. Ured za umjetnu inteligenciju i države članice olakšavaju izradu kodeksa ponašanja koji se odnose na dobrovoljnu primjenu specifičnih zahtjeva na sve UI sustave, među ostalim od strane subjekata koji uvode sustav, na temelju jasnih ciljeva i ključnih pokazatelja uspješnosti za mjerenje ostvarenja tih ciljeva, koji uključuju, ali nisu ograničeni na sljedeće elemente:
- (a) primjenjive elemente predviđene u etičkim smjernicama Unije za pouzdanu umjetnu inteligenciju;
 - (b) procjenu učinka UI sustava na okolišnu održivost i njegovo svođenje na najmanju moguću mjeru, među ostalim u pogledu energetski učinkovitog programiranja i tehnika za učinkovit dizajn, treniranje i korištenje umjetne inteligencije;
 - (c) promicanje pismenosti u području umjetne inteligencije, posebice za osobe koje se bave razvojem, radom i korištenjem umjetne inteligencije;
 - (d) olakšavanje uključivog i raznolikog dizajna UI sustava, među ostalim osnivanjem uključivih i raznolikih razvojnih timova i promicanjem sudjelovanja dionika u tom procesu;
 - (e) procjenu i sprečavanje negativnog učinka UI sustava na ranjive osobe ili skupine ranjivih osoba, među ostalim u pogledu pristupačnosti za osobe s invaliditetom, kao i na rodnu ravnopravnost.
3. Kodekse ponašanja mogu izraditi pojedinačni dobavljači UI sustava ili subjekti koji uvode te sustave ili organizacije koje ih zastupaju ili i ti dobavljači ili subjekti i te organizacije, među ostalim uz sudjelovanje svih zainteresiranih dionika i njihovih predstavničkih organizacija, uključujući organizacije civilnog društva i akademsku zajednicu. Kodeksi ponašanja mogu obuhvaćati jedan UI sustav ili više njih, uzimajući u obzir sličnost namjene relevantnih sustava.
4. Pri poticanju i olakšavanju izrade kodeksa ponašanja Ured za umjetnu inteligenciju i države članice uzimaju u obzir posebne interese i potrebe MSP-ova, uključujući *start-up* poduzeća.

Članak 96.

Smjernice Komisije o provedbi ove Uredbe

1. Komisija izrađuje smjernice o praktičnoj provedbi ove Uredbe, a posebno o sljedećem:
 - (a) primjeni zahtjeva i obveza iz članaka od 8. do 15. i iz članka 25.;
 - (b) zabranjenim praksama iz članka 5.;
 - (c) praktičnoj provedbi odredaba o bitnoj izmjeni;
 - (d) praktičnoj provedbi obveza u pogledu transparentnosti utvrđenih u članku 50.;
 - (e) detaljnim informacijama o odnosu ove Uredbe sa zakonodavstvom Unije o usklađivanju iz Priloga I., kao i s drugim relevantnim pravom Unije, među ostalim u pogledu dosljednosti u njihovu izvršavanju;
 - (f) primjeni definicije UI sustava kako je utvrđena u članku 3. točki 1.

Pri izdavanju takvih smjernica Komisija posebnu pozornost posvećuje potrebama MSP-ova, uključujući *start-up* poduzeća, lokalnih tijela javne vlasti i sektora za koje postoji najveća vjerojatnost da će ova Uredba na njih utjecati.

U smjernicama iz prvog podstavka ovog stavka na odgovarajući način uzimaju se u obzir općepriznata najnovija dostignuća u području umjetne inteligencije, kao i relevantne usklađene norme i zajedničke specifikacije iz članaka 40. i 41. te usklađene norme ili tehničke specifikacije utvrđene na temelju prava Unije o usklađivanju.

2. Komisija na zahtjev država članica ili Ureda za umjetnu inteligenciju ili na vlastitu inicijativu ažurira prethodno donesene smjernice kada to smatra potrebnim.

POGLAVLJE XI.

DELEGIRANJE OVLASTI I POSTUPAK ODBORA

Članak 97.

Izvršavanje delegiranja ovlasti

1. Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji podložno uvjetima utvrđenima u ovom članku.
2. Ovlast za donošenje delegiranih akata iz članka 6. stavaka 6. i 7., članka 7. stavaka 1. i 3., članka 11. stavka 3., članka 43. stavaka 5. i 6., članka 47. stavka 5., članka 51. stavka 3., članka 52. stavka 4. i članka 53. stavaka 5. i 6. dodjeljuje se Komisiji na razdoblje od pet godina počevši od 1. kolovoza 2024. Komisija izrađuje izvješće o delegiranju ovlasti najkasnije devet mjeseci prije kraja razdoblja od pet godina. Delegiranje ovlasti prešutno se produljuje za razdoblja jednakog trajanja, osim ako se Europski parlament ili Vijeće tom produljenju usprotive najkasnije tri mjeseca prije kraja svakog razdoblja.
3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 6. stavaka 6. i 7., članka 7. stavaka 1. i 3., članka 11. stavka 3., članka 43. stavaka 5. i 6., članka 47. stavka 5., članka 51. stavka 3., članka 52. stavka 4. i članka 53. stavaka 5. i 6. Odlukom o opozivu prekida se delegiranje ovlasti koje je u njoj navedeno. Opoziv počinje proizvoditi učinke sljedećeg dana od dana objave spomenute odluke u *Službenom listu Europske unije* ili na kasniji datum naveden u spomenutoj odluci. On ne utječe na valjanost delegiranih akata koji su već na snazi.
4. Prije donošenja delegiranog akta Komisija se savjetuje sa stručnjacima koje je imenovala svaka država članica u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.

5. Čim donese delegirani akt, Komisija ga istodobno priopćuje Europskom parlamentu i Vijeću.
6. Delegirani akt donesen na temelju članka 6. stavka 6. ili stavka 7., članka 7. stavka 1. ili stavka 3., članka 11. stavka 3., članka 43. stavka 5. ili stavka 6., članka 47. stavka 5., članka 51. stavka 3., članka 52. stavka 4. ili članka 53. stavka 5. ili stavka 6. stupa na snagu samo ako ni Europski parlament ni Vijeće u roku od tri mjeseca od priopćenja tog akta Europskom parlamentu i Vijeću na njega ne podnesu prigovor ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da neće podnijeti prigovore. Taj se rok produljuje za tri mjeseca na inicijativu Europskog parlamenta ili Vijeća.

Članak 98.

Postupak odbora

1. Komisiji pomaže odbor. Navedeni odbor je odbor u smislu Uredbe (EU) br. 182/2011.
2. Pri upućivanju na ovaj stavak primjenjuje se članak 5. Uredbe (EU) br. 182/2011.

POGLAVLJE XII.

SANKCIJE

Članak 99.

Sankcije

1. U skladu s uvjetima utvrđenima u ovoj Uredbi, države članice utvrđuju pravila o sankcijama i drugim mjerama izvršavanja, koje također mogu uključivati upozorenja i nenovčane mjere, koje se primjenjuju na povrede ove Uredbe od strane operatera te poduzimaju sve potrebne mjere radi osiguranja njihove pravilne i djelotvorne provedbe, uzimajući pritom u obzir smjernice koje je Komisija izdala u skladu s člankom 96. Predviđene sankcije moraju biti učinkovite, proporcionalne i odvraćajuće. Njima se uzimaju u obzir interesi MSP-ova, uključujući *start-up* poduzeća, i njihova gospodarska održivost.
2. Države članice bez odgode, a najkasnije do datuma početka njihove primjene, obavješćuju Komisiju o pravilima o sankcijama i drugim mjerama izvršavanja iz stavka 1. te je bez odgode obavješćuju o svim njihovim naknadnim izmjenama.
3. Za nepoštovanje zabrane praksi u području umjetne inteligencije iz članka 5. izriču se upravne novčane kazne u iznosu do 35 000 000 EUR ili, ako je počinitelj poduzeće, do 7 % njegova ukupnog svjetskog godišnjeg prometa za prethodnu financijsku godinu, ovisno o tome koji je iznos veći.
4. Za neusklađenost s jednom od sljedećih odredaba povezanih s operaterima ili prijavljenim tijelima, osim onih utvrđenih u članku 5., izriču se upravne novčane kazne u iznosu do 15 000 000 EUR ili, ako je počinitelj poduzeće, do 3 % njegova ukupnog svjetskog godišnjeg prometa za prethodnu financijsku godinu, ovisno o tome koji je iznos veći:
 - (a) obvezama dobavljača na temelju članka 16.;
 - (b) obvezama ovlaštenih zastupnika na temelju članka 22.;
 - (c) obvezama uvoznika na temelju članka 23.;
 - (d) obvezama distributerâ na temelju članka 24.;
 - (e) obvezama subjekata koji uvode sustav na temelju članka 26.;
 - (f) zahtjevima i obvezama koji se odnose na prijavljena tijela na temelju članka 31., članka 33. stavaka 1., 3. i 4. ili članka 34.;
 - (g) obvezama u pogledu transparentnosti za dobavljače i subjekte koji uvode sustav na temelju članka 50.

5. Ako se prijavljenim tijelima ili nacionalnim nadležnim tijelima u odgovoru na zahtjev dostave netočne, nepotpune ili obmanjujuće informacije, izriču se upravne novčane kazne u iznosu do 7 500 000 EUR ili, ako je počinitelj poduzeće, do 1 % njegova ukupnog svjetskog godišnjeg prometa za prethodnu financijsku godinu, ovisno o tome koji je iznos veći.
6. U slučaju MSP-ova, uključujući *start-up* poduzeća, maksimalna visina svake novčane kazne iz ovog članka odgovara postotku ili iznosu iz stavaka 3., 4. i 5., ovisno o tome koji je od ta dva iznosa manji.
7. Pri odlučivanju o izricanju upravne novčane kazne i o njezinu iznosu u svakom pojedinačnom slučaju uzimaju se u obzir sve relevantne okolnosti specifične situacije te se, prema potrebi, pozornost posvećuje sljedećem:
- (a) prirodi, težini i trajanju povrede te njezinim posljedicama, uzimajući u obzir svrhu UI sustava te, prema potrebi, broj pogođenih osoba i razinu štete koju su pretrpjele;
 - (b) eventualnim upravnim novčanim kaznama koje su druga tijela za nadzor tržišta već izrekla istom operateru za istu povredu;
 - (c) eventualnim upravnim novčanim kaznama koje su druga tijela već izrekla istom operateru za povrede drugog prava Unije ili nacionalnog prava, ako su takve povrede posljedica iste aktivnosti ili propusta koji predstavljaju relevantnu povredu ove Uredbe;
 - (d) veličini, godišnjem prometu i tržišnom udjelu operatera koji je počinio povredu;
 - (e) svim ostalim otegotnim ili olakotnim čimbenicima primjenjivima na okolnosti slučaja, kao što su financijska korist ostvarena povredom ili gubici izbjegnuti, izravno ili neizravno, tom povredom;
 - (f) stupnju suradnje s nacionalnim nadležnim tijelima radi ispravljanja povrede i ublažavanja mogućih štetnih posljedica te povrede;
 - (g) stupnju odgovornosti operatera, uzimajući u obzir tehničke i organizacijske mjere koje je proveo;
 - (h) načinu na koji su nacionalna nadležna tijela doznala za povredu, osobito je li i u kojoj mjeri operater obavijestio o povredi;
 - (i) tome je li povreda počinjena namjerno ili iz nepažnje;
 - (j) svim mjerama koje je operater poduzeo kako bi ublažio štetu koju su pretrpjele pogođene osobe.
8. Svaka država članica utvrđuje pravila o tome u kojoj se mjeri tijelima javne vlasti i javnim tijelima te države članice mogu izreći upravne novčane kazne.
9. Ovisno o pravnom sustavu država članica, pravila o upravnim novčanim kaznama mogu se primjenjivati tako da novčane kazne izriču nadležni nacionalni sudovi ili druga tijela, kako je primjenjivo u tim državama članicama. Primjena takvih pravila u tim državama članicama mora imati jednakovrijedan učinak.
10. Izvršavanje ovlasti na temelju ovog članka podliježe odgovarajućim postupovnim zaštitnim mjerama u skladu s pravom Unije i nacionalnim pravom, uključujući djelotvorna sudska pravna sredstva i zakonito postupanje.
11. Države članice svake godine izvješćuju Komisiju o upravnim novčanim kaznama koje su izrekle tijekom te godine, u skladu s ovim člankom, te o svim povezanim pravnim sporovima ili sudskim postupcima.

Članak 100.

Upravne novčane kazne za institucije, tijela, urede i agencije Unije

1. Europski nadzornik za zaštitu podataka može izreći upravne novčane kazne institucijama, tijelima, uredima i agencijama Unije obuhvaćenima područjem primjene ove Uredbe. Pri odlučivanju o izricanju upravne novčane kazne i o njezinu iznosu u svakom pojedinačnom slučaju uzimaju se u obzir sve relevantne okolnosti specifične situacije i dužna se pozornost posvećuje sljedećem:

- (a) prirodi, težini i trajanju povrede te njezinim posljedicama, uzimajući u obzir svrhu dotičnog UI sustava te, prema potrebi, broj pogođenih osoba i razinu štete koju su pretrpjele;
- (b) stupnju odgovornosti institucije, tijela, ureda ili agencije Unije, uzimajući u obzir tehničke i organizacijske mjere koje su proveli;
- (c) svim mjerama koje su institucija, tijelo, ured ili agencija Unije poduzeli kako bi ublažili štetu koju su pretrpjele pogođene osobe;
- (d) stupnju suradnje s Europskim nadzornikom za zaštitu podataka radi ispravljanja povrede i ublažavanja mogućih štetnih posljedica te povrede, uključujući usklađenost sa svim mjerama koje je Europski nadzornik za zaštitu podataka prethodno izrekao dotičnoj instituciji, tijelu, uredu ili agenciji Unije u vezi s istim predmetom;
- (e) svim sličnim prijašnjim povredama od strane dotične institucije, tijela, ureda ili agencije Unije;
- (f) načinu na koji je Europski nadzornik za zaštitu podataka doznao za povredu, osobito jesu li i u kojoj mjeri institucija, tijelo, ured ili agencija Unije obavijestili o povredi;
- (g) godišnjem proračunu institucije, tijela, ureda ili agencije Unije.

2. Za nepoštovanje zabrane praksi u području umjetne inteligencije iz članka 5. izriču se upravne novčane kazne u iznosu do 1 500 000 EUR.

3. Za neusklađenost UI sustava s nekim od zahtjeva ili obveza na temelju ove Uredbe, osim onih utvrđeni u članku 5., izriču se upravne novčane kazne u iznosu do 750 000 EUR.

4. Prije donošenja odluka u skladu s ovim člankom Europski nadzornik za zaštitu podataka pruža instituciji, tijelu, uredu ili agenciji Unije protiv kojih vodi postupak mogućnost da se očituju o mogućoj povredi. Europski nadzornik za zaštitu podataka svoje odluke temelji isključivo na elementima i okolnostima o kojima su se dotične stranke mogle očitovati. Eventualni podnositelji pritužbe moraju biti blisko uključeni u postupak.

5. U postupku se u potpunosti poštuje pravo dotičnih stranaka na obranu. Stranke imaju pravo na uvid u spis Europskog nadzornika za zaštitu podataka pod uvjetom da se poštuju legitimni interesi pojedinaca ili poduzeća da štite svoje osobne podatke ili poslovne tajne.

6. Sredstva prikupljena naplatom novčanih kazni iz ovog članka doprinos su općem proračunu Unije. Novčane kazne ne smiju utjecati na djelotvorno funkcioniranje institucije, tijela, ureda ili agencije Unije kojima je izrečena novčana kazna.

7. Europski nadzornik za zaštitu podataka jednom godišnje obavješćuje Komisiju o upravnim novčanim kaznama koje je izrekao na temelju ovog članka te o svim pravnim sporovima ili sudskim postupcima koje je pokrenuo.

Članak 101.

Novčane kazne za dobavljače UI modelâ opće namjene

1. Komisija može dobavljačima UI modelâ opće namjene izreći novčane kazne koje ne premašuju 3 % njihova ukupnog svjetskog prometa na godišnjoj razini u prethodnoj financijskoj godini ili 15 000 000 EUR, ovisno o tome koji je iznos veći, ako utvrdi da je dobavljač namjerno ili iz nepažnje učinio sljedeće:

- (a) povrijedio je relevantne odredbe ove Uredbe;
- (b) nije postupio u skladu sa zahtjevom za dokumentaciju ili informacije na temelju članka 91. ili je dostavio netočne, nepotpune ili obmanjujuće informacije;
- (c) nije postupio u skladu s mjerom zahtijevanom na temelju članka 93.;

- (d) Komisiji nije omogućio pristup UI modelu opće namjene ili UI modelu opće namjene sa sistemskim rizikom radi provedbe evaluacije na temelju članka 92.

Pri određivanju iznosa novčane kazne ili periodičnog penala u obzir se uzimaju priroda, težina i trajanje povrede, vodeći pritom na odgovarajući način računa o načelima proporcionalnosti i primjerenosti. Komisija također uzima u obzir obveze preuzete u skladu s člankom 93. stavkom 3. ili preuzete u relevantnim kodeksima prakse u skladu s člankom 56.

2. Prije donošenja odluke na temelju stavka 1. Komisija dostavlja svoje preliminarne nalaze dobavljaču UI modela opće namjene i pruža mu mogućnost da se očituje.
3. Novčane kazne izrečene u skladu s ovim člankom moraju biti učinkovite, proporcionalne i odvraćajuće.
4. Informacije o novčanim kaznama izrečenima na temelju ovog članka ujedno se prema potrebi priopćuju Vijeću za umjetnu inteligenciju.
5. Sud Europske unije ima neograničenu nadležnost za preispitivanje odluka Komisije kojima se određuje novčana kazna na temelju ovog članka. On izrečenu novčanu kaznu može ukinuti, smanjiti ili povećati.
6. Komisija donosi provedbene akte koji sadržavaju detaljne aranžmane i postupovne zaštitne mjere za postupke s obzirom na moguće donošenje odluka na temelju stavka 1. ovog članka. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 98. stavka 2.

POGLAVLJE XIII.

ZAVRŠNE ODREDBE

Članak 102.

Izmjena Uredbe (EZ) br. 300/2008

U članku 4. stavku 3. Uredbe (EZ) br. 300/2008 dodaje se sljedeći podstavak:

„Pri donošenju podrobnih mjera povezanih s tehničkim specifikacijama i postupcima za odobravanje i uporabu zaštitne opreme koje se odnose na sustave umjetne inteligencije u smislu Uredbe (EU) 2024/1689 Europskog parlamenta i Vijeća (*) u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.

(*) Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”.

Članak 103.

Izmjena Uredbe (EU) br. 167/2013

U članku 17. stavku 5. Uredbe (EU) br. 167/2013 dodaje se sljedeći podstavak:

„Pri donošenju delegiranih akata na temelju prvog podstavka o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/1689 Europskog parlamenta i Vijeća (*) u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.

(*) Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”.

Članak 104.

Izmjena Uredbe (EU) br. 168/2013

U članku 22. stavku 5. Uredbe (EU) br. 168/2013 dodaje se sljedeći podstavak:

„Pri donošenju delegiranih akata na temelju prvog podstavka o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/1689 Europskog parlamenta i Vijeća (*) u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.

(*) Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”.

Članak 105.

Izmjena Direktive 2014/90/EU

U članku 8. Direktive 2014/90/EU dodaje se sljedeći stavak:

„5. Kad je riječ o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/1689 Europskog parlamenta i Vijeća (*), Komisija pri obavljanju svojih aktivnosti na temelju stavka 1. i pri donošenju tehničkih specifikacija i ispitnih normi u skladu sa stavcima 2. i 3. u obzir uzima zahtjeve iz poglavlja III. odjeljka 2. te uredbe.

(*) Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”.

Članak 106.

Izmjena Direktive (EU) 2016/797

U članku 5. Direktive (EU) 2016/797 dodaje se sljedeći stavak:

„12. Pri donošenju delegiranih akata na temelju stavka 1. i provedbenih akata na temelju stavka 11. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/1689 Europskog parlamenta i Vijeća (*) u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.

(*) Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”.

Članak 107.

Izmjena Uredbe (EU) 2018/858

U članku 5. Uredbe (EU) 2018/858 dodaje se sljedeći stavak:

„4. Pri donošenju delegiranih akata na temelju stavka 3. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/1689 Europskog parlamenta i Vijeća (*) u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.

(*) Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”.

Članak 108.

Izmjene Uredbe (EU) 2018/1139

Uredba (EU) 2018/1139 mijenja se kako slijedi:

1. u članku 17. dodaje se sljedeći stavak:

„3. Na dovodeći u pitanje stavak 2., pri donošenju provedbenih akata na temelju stavka 1. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/1689 Europskog parlamenta i Vijeća (*) u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.

(*) Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”;

2. u članku 19. dodaje se sljedeći stavak:

„4. Pri donošenju delegiranih akata na temelju stavaka 1. i 2. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/1689 u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.”;

3. u članku 43. dodaje se sljedeći stavak:

„4. Pri donošenju provedbenih akata na temelju stavaka 1. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/1689 u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.”;

4. u članku 47. dodaje se sljedeći stavak:

„3. Pri donošenju delegiranih akata na temelju stavaka 1. i 2. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/1689 u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.”;

5. u članku 57. dodaje se sljedeći podstavak:

„Pri donošenju tih provedbenih akata o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/1689 u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.”;

6. u članku 58. dodaje se sljedeći stavak:

„3. Pri donošenju delegiranih akata na temelju stavaka 1. i 2. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/1689 u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.”.

Članak 109.

Izmjena Uredbe (EU) 2019/2144

U članku 11. Uredbe (EU) 2019/2144 dodaje se sljedeći stavak:

„3. Pri donošenju provedbenih akata na temelju stavka 2. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/1689. Europskog parlamenta i Vijeća (*) u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.

(*) Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”.

Članak 110.

Izmjena Direktive (EU) 2020/1828

U Prilogu I. Direktivi (EU) 2020/1828 Europskog parlamenta i Vijeća ⁽⁵⁸⁾ dodaje se sljedeća točka:

„68. Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>).”.

Članak 111.

UI sustavi koji su već stavljeni na tržište ili u upotrebu i UI modeli opće namjene koji su već stavljeni na tržište

1. Ne dovodeći u pitanje primjenu članka 5. kako je predviđena u članku 113. stavku 3. točki (a), UI sustavi koji su komponente opsežnih informacijskih sustava uspostavljenih pravnim aktima iz Priloga X. i koji su stavljeni na tržište ili u upotrebu prije 2. kolovoza 2027. usklađuju se s ovom Uredbom do 31. prosinca 2030.

Zahtjevi utvrđeni u ovoj Uredbi uzimaju se u obzir pri evaluaciji svakog opsežnog informacijskog sustava uspostavljenog pravnim aktima iz Priloga X. koju treba provesti kako je predviđeno u tim pravnim aktima i onda kada se ti pravni akti zamjenjuju ili mijenjaju.

2. Ne dovodeći u pitanje primjenu članka 5. kako je predviđena u članku 113. stavku 3. točki (a), ova se Uredba primjenjuje na operatore visokorizičnih UI sustava, osim sustava iz stavka 1. ovog članka, koji su stavljeni na tržište ili u upotrebu prije 2. kolovoza 2026. samo ako se nakon tog datuma znatno promijeni dizajn tih sustava. U svakom slučaju, dobavljači visokorizičnih UI sustava i subjekti koji ih uvode, koji su namijenjeni korištenju od strane tijela javne vlasti, poduzimaju potrebne korake kako bi ispunili zahtjeve i obveze iz ove Uredbe do 2. kolovoza 2030.

3. Dobavljači UI modela opće namjene koji su stavljeni na tržište prije 2. kolovoza 2025. poduzimaju potrebne korake kako bi ispunili obveze utvrđene u ovoj Uredbi do 2. kolovoza 2027.

⁽⁵⁸⁾ Direktiva (EU) 2020/1828 Europskog parlamenta i Vijeća od 25. studenoga 2020. o predstavničkim tužbama za zaštitu kolektivnih interesa potrošača i stavljanju izvan snage Direktive 2009/22/EZ (SL L 409, 4.12.2020., str. 1.).

Članak 112.

Evaluacija i preispitivanje

1. Komisija jednom godišnje nakon stupanja na snagu ove Uredbe i do kraja razdoblja delegiranja ovlasti utvrđenog u članku 97. procjenjuje potrebu za izmjenom popisa iz Priloga III. i popisa zabranjenih praksi u području umjetne inteligencije utvrđenog u članku 5. Komisija zaključke te procjene podnosi Europskom parlamentu i Vijeću.
2. Komisija do 2. kolovoza 2028. i svake četiri godine nakon toga provodi evaluaciju te izvješćuje Europski parlament i Vijeće o sljedećem:
 - (a) potrebi za izmjenama radi proširenja postojećih kategorija područja ili dodavanja novih područja u Prilog III.;
 - (b) izmjenama popisa UI sustava za koje su potrebne dodatne mjere transparentnosti iz članka 50.;
 - (c) izmjenama radi povećanja djelotvornosti sustava nadzora i upravljanja.
3. Komisija do 2. kolovoza 2029. i svake četiri godine nakon toga Europskom parlamentu i Vijeću podnosi izvješće o evaluaciji i preispitivanju ove Uredbe. Izvješće uključuje ocjenu u vezi sa strukturom izvršavanja i mogućom potrebom da agencija Unije otkloni utvrđene nedostatke. Na temelju nalaza tom se izvješću, prema potrebi, prilaže prijedlog za izmjenu ove Uredbe. Ta se izvješća objavljuju.
4. U izvješćima iz stavka 2. posebna se pozornost posvećuje sljedećem:
 - (a) stanju financijskih, tehničkih i ljudskih resursa nacionalnih nadležnih tijela za djelotvorno obavljanje zadaća koje su im dodijeljene na temelju ove Uredbe;
 - (b) stanju sankcija, a posebno upravnih novčanih kazni iz članka 99. stavka 1. koje države članice primjenjuju za povrede ove Uredbe;
 - (c) donesenim usklađenim normama i zajedničkim specifikacijama razvijenima kao potpora ovoj Uredbi;
 - (d) broju poduzeća koja ulaze na tržište nakon početka primjene ove Uredbe i koliko je među njima MSP-ova.
5. Komisija do 2. kolovoza 2028. evaluira funkcioniranje Ureda za umjetnu inteligenciju, jesu li Uredu za umjetnu inteligenciju dodijeljene dostatne ovlasti i nadležnosti za ispunjavanje njegovih zadaća i bi li za pravilnu provedbu i izvršavanje ove Uredbe bilo relevantno i potrebno osnažiti Ured za umjetnu inteligenciju i njegove nadležnosti u području izvršavanja te povećati njegove resurse. Komisija podnosi izvješće o svojoj evaluaciji Europskom parlamentu i Vijeću.
6. Komisija do 2. kolovoza 2028. i svake četiri godine nakon toga podnosi izvješće o preispitivanju napretka u razvoju normizacijskih dokumenata o energetski učinkovitom razvoju UI modela opće namjene te procjenjuje potrebu za daljnjim mjerama ili djelovanjem, uključujući obvezujuće mjere ili djelovanje. To se izvješće podnosi Europskom parlamentu i Vijeću i objavljuje.
7. Komisija do 2. kolovoza 2028. i svake tri godine nakon toga evaluira učinak i djelotvornost dobrovoljnih kodeksa ponašanja namijenjenih poticanju primjene zahtjeva utvrđenih u poglavlju III. odjeljku 2. za UI sustave koji nisu visokorizični i eventualno drugih dodatnih zahtjeva za UI sustave koji nisu visokorizični, među ostalim u pogledu okolišne održivosti.
8. Za potrebe stavaka od 1. do 7. Vijeće za umjetnu inteligenciju, države članice i nacionalna nadležna tijela Komisiji dostavljaju informacije na njezin zahtjev i bez nepotrebne odgode.
9. Pri provedbi evaluacija i preispitivanja iz stavaka od 1. do 7. Komisija uzima u obzir stajališta i zaključke Vijeća za umjetnu inteligenciju, Europskog parlamenta, Vijeća i drugih relevantnih tijela ili izvora.

10. Komisija prema potrebi podnosi odgovarajuće prijedloge radi izmjene ove Uredbe, posebno uzimajući u obzir razvoj tehnologije i učinke UI sustavâ na zdravlje i sigurnost te na temeljna prava, i s obzirom na napredak informacijskog društva.

11. Radi usmjeravanja evaluacija i preispitivanja iz stavaka od 1. do 7. ovog članka Ured za umjetnu inteligenciju obvezuje se razviti objektivnu i participativnu metodologiju za evaluaciju razine rizika na temelju kriterija navedenih u relevantnim člancima i za uključivanje novih sustava na sljedeće:

- (a) popis utvrđen u Prilogu III., uključujući proširenje postojećih kategorija područja ili dodavanje novih kategorija područja u taj prilog;
- (b) popis zabranjenih praksi utvrđen u članku 5.; i
- (c) popis UI sustava za koje su potrebne dodatne mjere transparentnosti na temelju članka 50.

12. Pri svakoj izmjeni ove Uredbe na temelju stavka 10. ili relevantnih delegiranih akata ili provedbenih akata koja se odnosi na sektorsko zakonodavstvo Unije o usklađivanju navedeno u odjeljku B Priloga I. u obzir se uzimaju regulatorne posebnosti svakog sektora i postojeći mehanizmi upravljanja, ocjenjivanja sukladnosti i izvršenja te tijela koja su njime utvrđena.

13. Komisija do 2. kolovoza 2031. ocjenjuje izvršavanje ove Uredbe i o tome izvješćuje Europski parlament, Vijeće te Europski gospodarski i socijalni odbor, uzimajući u obzir prve godine primjene ove Uredbe. Na temelju zaključaka tom se izvješću prema potrebi prilaže prijedlog za izmjenu ove Uredbe u vezi sa strukturom izvršavanja i potrebom da agencija Unije otkloni utvrđene nedostatke.

Članak 113.

Stupanje na snagu i primjena

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Primjenjuje se od 2. kolovoza 2026.

Međutim:

- (a) poglavlja I. i II. primjenjuju se od 2. veljače 2025.;
- (b) poglavlje III. odjeljak 4., poglavlje V., poglavlje VII. i poglavlje XII. te članak 78. primjenjuju se od 2. kolovoza 2025., uz iznimku članka 101.;
- (c) članak 6. stavak 1. i odgovarajuće obveze iz ove Uredbe primjenjuju se od 2. kolovoza 2027.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 13. lipnja 2024.

Za Europski parlament

Predsjednica

R. METSOLA

Za Vijeće

Predsjednik

M. MICHEL

PRILOG I.

Popis zakonodavstva Unije o usklađivanju

Odjeljak A. Popis zakonodavstva Unije o usklađivanju na temelju novog zakonodavnog okvira

1. Direktiva 2006/42/EZ Europskog parlamenta i Vijeća od 17. svibnja 2006. o strojevima o izmjeni Direktive 95/16/EZ (SL L 157, 9.6.2006., str. 24.);
2. Direktiva 2009/48/EZ Europskog parlamenta i Vijeća od 18. lipnja 2009. o sigurnosti igračaka (SL L 170, 30.6.2009., str. 1.);
3. Direktiva 2013/53/EU Europskog parlamenta i Vijeća od 20. studenoga 2013. o rekreacijskim plovilima i osobnim plovilima na vodomlazni pogon i o stavljanju izvan snage Direktive Vijeća 94/25/EZ (SL L 354, 28.12.2013., str. 90.);
4. Direktiva 2014/33/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o usklađivanju zakonodavstava država članica u odnosu na dizala i sigurnosne komponente za dizala (SL L 96, 29.3.2014., str. 251.);
5. Direktiva 2014/34/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o usklađivanju zakonodavstava država članica u odnosu na opremu i zaštitne sustave namijenjene za uporabu u potencijalno eksplozivnim atmosferama (SL L 96, 29.3.2014., str. 309.);
6. Direktiva 2014/53/EU Europskog parlamenta i Vijeća od 16. travnja 2014. o usklađivanju zakonodavstava država članica o stavljanju na raspolaganje radijske opreme na tržištu i stavljanju izvan snage Direktive 1999/5/EZ (SL L 153, 22.5.2014., str. 62.);
7. Direktiva 2014/68/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o usklađivanju zakonodavstava država članica o stavljanju na raspolaganje na tržištu tlačne opreme (SL L 189, 27.6.2014., str. 164.);
8. Uredba (EU) 2016/424 Europskog parlamenta i Vijeća od 9. ožujka 2016. o žičarama i stavljanju izvan snage Direktive 2000/9/EZ (SL L 81, 31.3.2016., str. 1.);
9. Uredba (EU) 2016/425 Europskog parlamenta i Vijeća od 9. ožujka 2016. o osobnoj zaštitnoj opremi i o stavljanju izvan snage Direktive Vijeća 89/686/EEZ (SL L 81, 31.3.2016., str. 51.);
10. Uredba (EU) 2016/426 Europskog parlamenta i Vijeća od 9. ožujka 2016. o aparatima na plinovita goriva i stavljanju izvan snage Direktive 2009/142/EZ (SL L 81, 31.3.2016., str. 99.);
11. Uredba (EU) 2017/745 Europskog parlamenta i Vijeća od 5. travnja 2017. o medicinskim proizvodima, o izmjeni Direktive 2001/83/EZ, Uredbe (EZ) br. 178/2002 i Uredbe (EZ) br. 1223/2009 te o stavljanju izvan snage direktiva Vijeća 90/385/EEZ i 93/42/EEZ (SL L 117, 5.5.2017., str. 1.);
12. Uredba (EU) 2017/746 Europskog parlamenta i Vijeća od 5. travnja 2017. o *in vitro* dijagnostičkim medicinskim proizvodima te o stavljanju izvan snage Direktive 98/79/EZ i Odluke Komisije 2010/227/EU (SL L 117, 5.5.2017., str. 176.).

Odjeljak B. Popis ostalog zakonodavstva Unije o usklađivanju

13. Uredba (EZ) br. 300/2008 Europskog parlamenta i Vijeća od 11. ožujka 2008. o zajedničkim pravilima u području zaštite civilnog zračnog prometa i stavljanju izvan snage Uredbe (EZ) br. 2320/2002 (SL L 97, 9.4.2008., str. 72.);
14. Uredba (EU) br. 168/2013 Europskog parlamenta i Vijeća od 15. siječnja 2013. o homologaciji i nadzoru tržišta vozila na dva ili tri kotača i četverocikala (SL L 60, 2.3.2013., str. 52.);
15. Uredba (EU) br. 167/2013 Europskog parlamenta i Vijeća od 5. veljače 2013. o homologaciji i nadzoru tržišta traktora za poljoprivredu i šumarstvo (SL L 60, 2.3.2013., str. 1.);

16. Direktiva 2014/90/EU Europskog parlamenta i Vijeća od 23. srpnja 2014. o pomorskoj opremi i stavljanju izvan snage Direktive Vijeća 96/98/EZ (SL L 257, 28.8.2014., str. 146.);
17. Direktiva (EU) 2016/797 Europskog parlamenta i Vijeća od 11. svibnja 2016. o interoperabilnosti željezničkog sustava u Europskoj uniji (SL L 138, 26.5.2016., str. 44.);
18. Uredba (EU) 2018/858 Europskog parlamenta i Vijeća od 30. svibnja 2018. o homologaciji i nadzoru tržišta motornih vozila i njihovih prikolica te sustavâ, sastavnih dijelova i zasebnih tehničkih jedinica namijenjenih za takva vozila, o izmjeni uredaba (EZ) br. 715/2007 i (EZ) br. 595/2009 te o stavljanju izvan snage Direktive 2007/46/EZ (SL L 151, 14.6.2018., str. 1.);
19. Uredba (EU) 2019/2144 Europskog parlamenta i Vijeća od 27. studenoga 2019. o zahtjevima za homologaciju tipa za motorna vozila i njihove prikolice te za sustave, sastavne dijelove i zasebne tehničke jedinice namijenjene za takva vozila, u pogledu njihove opće sigurnosti te zaštite osoba u vozilima i nezaštićenih sudionika u cestovnom prometu, o izmjeni Uredbe (EU) 2018/858 Europskog parlamenta i Vijeća i stavljanju izvan snage uredbi (EZ) br. 78/2009, (EZ) br. 79/2009 i (EZ) br. 661/2009 Europskog parlamenta i Vijeća i uredbi Komisije (EZ) br. 631/2009, (EU) br. 406/2010, (EU) br. 672/2010, (EU) br. 1003/2010, (EU) br. 1005/2010, (EU) br. 1008/2010, (EU) br. 1009/2010, (EU) br. 19/2011, (EU) br. 109/2011, (EU) br. 458/2011, (EU) br. 65/2012, (EU) br. 130/2012, (EU) br. 347/2012, (EU) br. 351/2012, (EU) br. 1230/2012 i (EU) 2015/166 (SL L 325, 16.12.2019., str. 1.);
20. Uredba (EU) 2018/1139 Europskog parlamenta i Vijeća od 4. srpnja 2018. o zajedničkim pravilima u području civilnog zrakoplovstva i osnivanju Agencije Europske unije za sigurnost zračnog prometa i izmjeni uredbi (EZ) br. 2111/2005, (EZ) br. 1008/2008, (EU) br. 996/2010, (EU) br. 376/2014 i direktiva 2014/30/EU i 2014/53/EU Europskog parlamenta i Vijeća te stavljanju izvan snage uredbi (EZ) br. 552/2004 i (EZ) br. 216/2008 Europskog parlamenta i Vijeća i Uredbe Vijeća (EEZ) br. 3922/91 (SL L 212, 22.8.2018., str. 1.), kada je riječ o projektiranju, proizvodnji i stavljanju na tržište zrakoplova iz članka 2. stavka 1. točaka (a) i (b), u vezi s bespilotnim zrakoplovima i njihovim motorima, propelerima, dijelovima i opremi za daljinsko upravljanje tim zrakoplovima.

PRILOG II.

Popis kaznenih djela iz članka 5. stavka 1. prvog podstavka točke (h) podtočke iii.

Kaznena djela iz članka 5. stavka 1. prvog podstavka točke (h) podtočke iii.:

- terorizam,
 - trgovina ljudima,
 - seksualno iskorištavanje djece i dječja pornografija,
 - nezakonita trgovina opojnim drogama ili psihotropnim tvarima,
 - nezakonita trgovina oružjem, streljivom ili eksplozivima,
 - ubojstvo, teška tjelesna ozljeda,
 - nezakonita trgovina ljudskim organima ili tkivom,
 - nezakonita trgovina nuklearnim ili radioaktivnim materijalima,
 - otmica, protupravno oduzimanje slobode ili uzimanje talaca,
 - kaznena djela iz nadležnosti Međunarodnog kaznenog suda,
 - protupravno oduzimanje zrakoplova ili brodova,
 - silovanje,
 - kazneno djelo protiv okoliša,
 - organizirana ili oružana pljačka,
 - sabotaža,
 - sudjelovanje u zločinačkoj organizaciji uključenoj u jednoj od navedenih kaznenih djela ili više njih.
-

PRILOG III.

Visokorizični UI sustavi iz članka 6. stavka 2.

Visokorizični UI sustavi u skladu s člankom 6. stavkom 2. jesu UI sustavi u bilo kojem od sljedećih područja:

1. Biometrija, ako je njezino korištenje dopušteno na temelju relevantnog prava Unije ili nacionalnog prava:
 - (a) sustavi za daljinsku biometrijsku identifikaciju.

To ne uključuje UI sustave namijenjene za biometrijsku provjeru čija je jedina svrha potvrditi da je određena fizička osoba doista ona osoba kojom se predstavlja;
 - (b) UI sustavi namijenjeni za biometrijsku kategorizaciju, u skladu s osjetljivim ili zaštićenim atributima ili karakteristikama na temelju zaključivanja o tim atributima ili značajkama;
 - (c) UI sustavi namijenjeni za prepoznavanje emocija.
2. Kritična infrastruktura: UI sustavi namijenjeni za korištenje kao sigurnosne komponente za upravljanje kritičnom digitalnom infrastrukturom, cestovnim prometom ili opskrbom vodom, plinom, grijanjem ili električnom energijom te za njihov rad.
3. Obrazovanje i strukovno osposobljavanje:
 - (a) UI sustavi namijenjeni za odlučivanje o pristupu ili upisu ili za razvrstavanje fizičkih osoba u ustanove ili programe za obrazovanje i strukovno osposobljavanje na svim razinama;
 - (b) UI sustavi namijenjeni za evaluaciju ishoda učenja, među ostalim kad se ti ishodi upotrebljavaju za usmjeravanje procesa učenja fizičkih osoba u ustanovama za obrazovanje i strukovno osposobljavanje na svim razinama;
 - (c) UI sustavi namijenjeni za upotrebu u svrhu procjene odgovarajuće razine obrazovanja koju će pojedinci primiti ili kojoj će moći pristupiti, u kontekstu ili unutar ustanova za obrazovanje i strukovno osposobljavanje na svim razinama;
 - (d) UI sustavi namijenjeni za praćenje i otkrivanje zabranjenog postupanja učenika tijekom testiranja u kontekstu ili unutar ustanova za obrazovanje i strukovno osposobljavanje na svim razinama.
4. Zapošljavanje, kadrovsko upravljanje i pristup samozapošljavanju:
 - (a) UI sustavi namijenjeni za zapošljavanje ili odabir fizičkih osoba, posebno za postavljanje ciljanih oglasa za posao, za analizu i filtriranje prijava za posao te za evaluaciju kandidata;
 - (b) UI sustavi namijenjeni za donošenje odluka koje utječu na uvjete radnog odnosa, promaknuće ili otkazivanje radnih ugovornih odnosa, za dodjelu zadataka na osnovi individualnog ponašanja ili osobnih obilježja odnosno karakteristika te za praćenje i evaluaciju učinkovitosti i ponašanja osoba u takvim odnosima.
5. Pristup osnovnim privatnim uslugama te osnovnim javnim uslugama i naknadama i njihovo korištenje:
 - (a) UI sustavi namijenjeni za korištenje od strane tijela javne vlasti ili u njihovo ime za evaluaciju prihvatljivosti fizičkih osoba za osnovne naknade i usluge javne pomoći, uključujući zdravstvene usluge, te za dodjeljivanje, smanjenje, ukidanje ili povrat takvih naknada i usluga;
 - (b) UI sustavi namijenjeni za evaluaciju kreditne sposobnosti fizičkih osoba ili utvrđivanje njihova kreditnog rejtinga, uz iznimku UI sustava koji se upotrebljavaju za otkrivanje financijskih prijevara;
 - (c) UI sustavi namijenjeni za procjenu rizika i određivanje cijena u odnosu na fizičke osobe u slučaju životnog i zdravstvenog osiguranja;

- (d) UI sustavi namijenjeni za evaluaciju i klasifikaciju hitnih poziva fizičkih osoba ili za dispečiranje ili određivanje prioriteta pri dispečiranju hitnih službi, uključujući policiju, vatrogasce i medicinsku pomoć, kao i sustave za trijažu pacijenata u pružanju hitne skrbi.
6. Kazneni progon, ako je njihovo korištenje dopušteno na temelju relevantnog prava Unije ili nacionalnog prava:
- (a) UI sustavi namijenjeni za korištenje od strane tijela kaznenog progona ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije za potporu tijelima kaznenog progona ili u njihovo ime za procjenu rizika fizičke osobe da postane žrtva kaznenih djela;
- (b) UI sustavi namijenjeni za upotrebu od strane tijela kaznenog progona ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije za potporu tijelima kaznenog progona kao poligrafi ili slični alati;
- (c) UI sustavi namijenjeni za korištenje od strane tijela kaznenog progona ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije za potporu tijelima kaznenog progona za evaluaciju pouzdanosti dokaza tijekom istrage ili progona kaznenih djela;
- (d) UI sustavi namijenjeni za korištenje od strane tijela kaznenog progona ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije za potporu tijelima kaznenog progona za procjenu rizika fizičke osobe do počini ponovno počini kazneno djelo ne samo na osnovi izrade profila fizičkih osoba kako je navedeno u članku 3. točki 4. Direktive (EU) 2016/680 ili za procjenu osobina i karakteristika ili prethodnog kriminalnog ponašanja fizičkih osoba ili skupina;
- (e) UI sustavi namijenjeni za korištenje od strane tijela kaznenog progona ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije za potporu tijelima kaznenog progona za izradu profila fizičkih osoba kako je navedeno u članku 3. točki 4. Direktive (EU) 2016/680 tijekom otkrivanja, istrage ili progona kaznenih djela.
7. Migracije, azil i upravljanje nadzorom državne granice, ako je njihovo korištenje dopušteno na temelju relevantnog prava Unije ili nacionalnog prava:
- (a) UI sustavi namijenjeni za korištenje od strane nadležnih tijela javne vlasti ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije kao poligrafi ili slični alati;
- (b) UI sustavi namijenjeni za korištenje od strane nadležnih tijela javne vlasti ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije za procjenu rizika, uključujući rizik za sigurnost, rizik od nezakonitih migracija ili rizik za zdravlje, koji predstavlja fizička osoba koja namjerava ući ili je ušla na državno područje države članice;
- (c) UI sustavi namijenjeni za korištenje od strane nadležnih tijela javne vlasti ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije za pomoć nadležnim tijelima javne vlasti u razmatranju zahtjeva za azil, viza ili boravišnih dozvola i povezanih pritužbi u pogledu prihvatljivosti fizičkih osoba koje podnose zahtjev za određeni status, uključujući povezane procjene pouzdanosti dokaza;
- (d) UI sustavi namijenjeni za korištenje od strane nadležnih tijela javne vlasti ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije, u kontekstu migracija, azila ili upravljanja nadzorom državne granice, u svrhu otkrivanja, prepoznavanja ili identifikacije fizičkih osoba, uz iznimku provjere putnih isprava.
8. Sudovanje i demokratski procesi:
- (a) UI sustavi namijenjeni za korištenje od strane pravosudnih tijela ili u njihovo ime za pomoć pravosudnom tijelu u istraživanju i tumačenju činjenica i prava te primjeni prava na konkretan skup činjenica ili za upotrebu na sličan način u alternativnom rješavanju sporova;

- (b) UI sustavi namijenjeni za utjecanje na ishod izbora ili referendumu ili na ponašanje fizičkih osoba pri glasovanju na izborima ili referendumima. To ne uključuje UI sustave čijim izlaznim podacima fizičke osobe nisu izravno izložene, kao što su alati koji se upotrebljavaju za organizaciju, optimizaciju i strukturiranje političkih kampanja s administrativnog ili logističkog stajališta.
-

PRILOG IV.

Tehnička dokumentacija iz članka 11. stavka 1.

Tehnička dokumentacija iz članka 11. stavka 1. sadržava barem sljedeće informacije, ovisno o tome što je primjenjivo na dotični UI sustav:

1. opći opis UI sustava, uključujući:
 - (a) njegovu namjenu, ime dobavljača i verziju sustava koja odražava njegovu povezanost s prethodnim verzijama;
 - (b) način na koji je UI sustav u interakciji s hardverom ili softverom, među ostalim s drugim UI sustavima koji nisu dio samog UI sustava, ili način na koji se može upotrijebiti za takvu interakciju, ako je primjenjivo;
 - (c) verzije relevantnog softvera ili ugrađenog softvera i sve zahtjeve povezane s ažuriranjem verzija;
 - (d) opis svih oblika u kojima se UI sustav stavlja na tržište ili u upotrebu, kao što su softverski paketi ugrađeni u hardver, preuzimanja ili aplikacijska programska sučelja;
 - (e) opis hardvera na kojem bi UI sustav trebao raditi;
 - (f) ako je UI sustav komponenta proizvoda, fotografije ili ilustracije koje prikazuju vanjske značajke, oznake i unutarnju strukturu tih proizvoda;
 - (g) osnovni opis korisničkog sučelja koje se pruža subjektu koji uvodi sustav;
 - (h) upute za korištenje namijenjene subjektu koji uvodi sustav i osnovni opis korisničkog sučelja koje se pruža subjektu koji uvodi sustav, ako je primjenjivo;
2. detaljan opis elemenata UI sustava i postupka njegova razvoja, uključujući:
 - (a) metode i korake provedene u razvoju UI sustava, uključujući, ako je to relevantno, upotrebu prethodno treniranih sustava ili alata trećih strana i način na koji ih je dobavljač upotrijebio, integrirao ili izmijenio;
 - (b) specifikacije dizajna sustava, odnosno opću logiku UI sustava i algoritama; najvažnije odabire u pogledu dizajna, uključujući obrazloženja i pretpostavke, među ostalim u vezi s osobama ili skupinama osoba u vezi s kojima se sustav namjerava upotrebljavati; glavne klasifikacijske odabire; informacije o tome što bi sustav svojim dizajnom trebao optimizirati i relevantnost različitih parametara; opis očekivanih izlaznih podataka sustava i njihove kvalitete; odluke o eventualnim kompromisima u pogledu tehničkih rješenja donesenima radi ispunjavanja zahtjeva iz poglavlja III. odjeljka 2.;
 - (c) opis arhitekture sustava u kojem se objašnjava kako se softverske komponente međusobno nadopunjuju ili potpomažu te kako su integrirane u cjelokupnu obradu; računalne resurse upotrijebljene za razvoj, treniranje, testiranje i validaciju UI sustava;
 - (d) ako je to relevantno, zahtjeve u pogledu podataka u smislu tablica s opisom metodologija i tehnika treniranja te upotrijebljenih skupova podataka za treniranje, uključujući opći opis tih skupova podataka i informacije o njihovu podrijetlu, sadržaju i glavnim karakteristikama; način na koji su podaci dobiveni i odabrani; postupke označavanja (npr. za nadzirano učenje), metodologije čišćenja podataka (npr. otkrivanje netipičnih vrijednosti);
 - (e) procjenu mjera ljudskog nadzora potrebnih u skladu s člankom 14., uključujući procjenu tehničkih mjera potrebnih kako bi se subjektima koji uvode sustav olakšalo tumačenje izlaznih podataka UI sustava, u skladu s člankom 13. stavkom 3. točkom (d);
 - (f) ako je primjenjivo, detaljan opis unaprijed određenih promjena UI sustava i njegove učinkovitosti, zajedno sa svim relevantnim informacijama o tehničkim rješenjima primijenjenima radi osiguravanja kontinuirane usklađenosti UI sustava s relevantnim zahtjevima iz poglavlja III. odjeljka 2.;
 - (g) primijenjene postupke validacije i testiranja, uključujući informacije o podacima upotrijebljenima za validaciju i testiranje te njihovim glavnim karakteristikama; parametre upotrijebljene za mjerenje točnosti, otpornosti i usklađenosti s drugim relevantnim zahtjevima iz poglavlja III. odjeljka 2., kao i potencijalne diskriminirajuće učinke; evidenciju događaja tijekom testiranja i sva izvješća o testiranju s datumom i potpisom odgovornih osoba, među ostalim u vezi s unaprijed određenim promjenama iz točke (f);

- (h) uspostavljene mjere u području kibernetičke sigurnosti;
3. detaljne informacije o praćenju, funkcioniranju i kontroli UI sustava, posebno u pogledu sljedećeg: njegovih sposobnosti i ograničenja u radu, uključujući stupnjeve točnosti za konkretne osobe ili skupine osoba na kojima se sustav namjerava upotrebljavati te ukupnu očekivanu razinu točnosti u odnosu na namjenu sustava; predvidljivih neplaniranih ishoda i izvora rizika za zdravlje i sigurnost, temeljna prava i u pogledu diskriminacije s obzirom na namjenu UI sustava; mjera ljudskog nadzora potrebnih u skladu s člankom 14., uključujući tehničke mjere uspostavljene kako bi se subjektima koji uvode sustav olakšalo tumačenje izlaznih podataka UI sustava; specifikacije ulaznih podataka, prema potrebi;
 4. opis primjerenosti parametara učinkovitosti za određeni UI sustav;
 5. detaljan opis sustava upravljanja rizikom u skladu s člankom 9.;
 6. opis svih relevantnih promjena koje je dobavljač unio u sustav tijekom njegova životnog ciklusa;
 7. popis u cijelosti ili djelomično primijenjenih usklađenih normi na koje su objavljena upućivanja u *Službenom listu Europske unije*; ako nisu primijenjene takve usklađene norme, detaljan opis rješenja koja su primijenjenima radi ispunjavanja zahtjeva iz poglavlja III. odjeljka 2., uključujući popis drugih primijenjenih relevantnih normi i tehničkih specifikacija;
 8. primjerak EU izjave o sukladnosti iz članka 47.;
 9. detaljan opis sustava uspostavljenog za evaluaciju učinkovitosti UI sustava u fazi nakon stavljanja na tržište u skladu s člankom 72., uključujući plan praćenja nakon stavljanja na tržište iz članka 72. stavka 3.
-

PRILOG V.

EU izjava o sukladnosti

EU izjava o sukladnosti iz članka 47. sadržava sve sljedeće informacije:

1. ime i vrstu UI sustava te sve dodatne nedvosmislene referentne oznake koje omogućuju identifikaciju i sljedivost UI sustava;
2. ime i adresu dobavljača ili, kada je to primjenjivo, njegova ovlaštenog zastupnika;
3. izjavu da je za izdavanje EU izjave o sukladnosti iz članka 47. odgovoran isključivo dobavljač;
4. izjavu da je UI sustav sukladan s ovom Uredbom i, ako je primjenjivo, sa svim drugim relevantnim pravom Unije kojim je predviđeno izdavanje EU izjave o sukladnosti iz članka 47.;
5. ako UI sustav obuhvaća obradu osobnih podataka, izjavu da je taj UI sustav usklađen s uredbama (EU) 2016/679 i (EU) 2018/1725 te Direktivom (EU) 2016/680;
6. upućivanja na sve primijenjene relevantne usklađene norme ili druge zajedničke specifikacije u odnosu na koje se izjavljuje sukladnost;
7. ako je primjenjivo, ime i identifikacijski broj prijavljenog tijela, opis provedenog postupka ocjenjivanja sukladnosti te identifikacijsku oznaku izdane potvrde;
8. mjesto i datum izdavanja izjave, ime i funkciju osobe koja ju je potpisala, uključujući navod za koga ili u čije ime je potpisana, te potpis.

PRILOG VI.

Postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole

1. Postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole postupak je ocjenjivanja sukladnosti na temelju točaka 2., 3. i 4.
 2. Dobavljač provjerava je li uvedeni sustav upravljanja kvalitetom usklađen sa zahtjevima iz članka 17.
 3. Dobavljač pregledava informacije iz tehničke dokumentacije kako bi ocijenio usklađenost UI sustava s relevantnim temeljnim zahtjevima iz poglavlja III. odjeljka 2.
 4. Osim toga, dobavljač provjerava jesu li postupak dizajniranja i razvoja UI sustava te njegovo praćenje nakon stavljanja na tržište iz članka 72. u skladu s tehničkom dokumentacijom.
-

PRILOG VII.

Sukladnost na temelju ocjenjivanja sustava upravljanja kvalitetom i ocjenjivanja tehničke dokumentacije

1. Uvod

Sukladnost na temelju ocjenjivanja sustava upravljanja kvalitetom i ocjenjivanja tehničke dokumentacije postupak je ocjenjivanja sukladnosti na temelju točaka od 2. do 5.
2. Pregled

Odobreni sustav upravljanja kvalitetom za dizajniranje, razvoj i testiranje UI sustava na temelju članka 17. ispituje se u skladu s točkom 3. i podliježe nadzoru kako je utvrđeno u točki 5. Tehnička dokumentacija UI sustava pregledava se u skladu s točkom 4.
3. Sustav upravljanja kvalitetom
 - 3.1. Zahtjev dobavljača sadržava:
 - (a) ime i adresu dobavljača te, ako je zahtjev podnio ovlašteni zastupnik, i njegovo ime te adresu;
 - (b) popis UI sustava obuhvaćenih istim sustavom upravljanja kvalitetom;
 - (c) tehničku dokumentaciju za svaki UI sustav obuhvaćen istim sustavom upravljanja kvalitetom;
 - (d) dokumentaciju o sustavu upravljanja kvalitetom koja obuhvaća sve aspekte navedene u članku 17.;
 - (e) opis uspostavljenih postupaka kojima se osigurava da sustav upravljanja kvalitetom ostane adekvatan i djelotvoran;
 - (f) pisanu izjavu da isti zahtjev nije podnesen nijednom drugom prijavljenom tijelu.
 - 3.2. Prijavljeno tijelo ocjenjuje sustav upravljanja kvalitetom i utvrđuje udovoljava li on zahtjevima iz članka 17.

O toj se odluci obavješćuje dobavljač ili njegov ovlašteni zastupnik.

Ta obavijest sadržava zaključke ocjenjivanja sustava upravljanja kvalitetom i obrazloženu odluku o ocjeni.
 - 3.3. Dobavljač nastavlja primjenjivati i održavati odobreni sustav upravljanja kvalitetom tako da ostane adekvatan i učinkovit.
 - 3.4. Dobavljač obavješćuje prijavljeno tijelo o svakoj planiranoj promjeni odobrenog sustava upravljanja kvalitetom ili popisa UI sustava koji su njime obuhvaćeni.

Prijavljeno tijelo pregledava predložene promjene i donosi odluku o tome ispunjava li izmijenjeni sustav upravljanja kvalitetom i dalje zahtjeve iz točke 3.2. ili je potrebno ponovno ocjenjivanje.

Prijavljeno tijelo obavješćuje dobavljača o svojoj odluci. Ta obavijest sadržava zaključke pregleda promjena i obrazloženu odluku o ocjeni.
4. Kontrola tehničke dokumentacije
 - 4.1. Uz zahtjev iz točke 3. dobavljač podnosi prijavljenom tijelu koje je sâm odabrao zahtjev za ocjenjivanje tehničke dokumentacije UI sustava koji dobavljač namjerava staviti na tržište ili u upotrebu i koji je obuhvaćen sustavom upravljanja kvalitetom iz točke 3.
 - 4.2. Taj zahtjev sadržava:
 - (a) ime i adresu dobavljača;
 - (b) pisanu izjavu da isti zahtjev nije podnesen nijednom drugom prijavljenom tijelu;
 - (c) tehničku dokumentaciju iz Priloga IV.

- 4.3. Prijavljeno tijelo pregledava tu tehničku dokumentaciju. Ako je to relevantno i ograničeno na ono što je potrebno za ispunjavanje njegovih zadaća, prijavljenom tijelu odobrava se puni pristup upotrijebljenim skupovima podataka za treniranje, validaciju i testiranje, među ostalim, prema potrebi i podložno sigurnosnim zaštitnim mjerama, putem aplikacijskih programskih sučelja ili drugih relevantnih tehničkih sredstava i alata koji omogućuju daljinski pristup.
- 4.4. Pri pregledu tehničke dokumentacije prijavljeno tijelo može zatražiti da dobavljač dostavi dodatne dokaze ili provede dodatna testiranja kako bi se omogućilo pravilno ocjenjivanje sukladnosti UI sustava sa zahtjevima utvrđenima u poglavlju III. odjeljku 2. Ako prijavljeno tijelo nije zadovoljno testiranjima koja je proveo dobavljač, ono prema potrebi samo izravno provodi adekvatna testiranja.
- 4.5. Ako je to potrebno za ocjenjivanje sukladnosti visokorizičnog UI sustava sa zahtjevima utvrđenima u poglavlju III. odjeljku 2., nakon što su svi drugi razumni načini provjere sukladnosti iscrpljeni ili su se pokazali nedostatnima, i na obrazložen zahtjev, prijavljenom tijelu također se odobrava pristup modelima za treniranje i istreniranim modelima UI sustava, uključujući njegove relevantne parametre. Na taj pristup primjenjuje se postojeće pravo Unije u području zaštite intelektualnog vlasništva i poslovnih tajni.
- 4.6. O odluci prijavljenog tijela obavješćuje se dobavljač ili njegov ovlašteni zastupnik. Ta obavijest sadržava zaključke ocjenjivanja tehničke dokumentacije i obrazloženu odluku o ocjeni.

Ako je UI sustav sukladan sa zahtjevima iz poglavlja III. odjeljka 2., prijavljeno tijelo izdaje potvrdu Unije o ocjenjivanju tehničke dokumentacije. Ta potvrda sadržava ime i adresu dobavljača, zaključke pregleda, uvjete valjanosti potvrde (ako postoje) i podatke potrebne za identifikaciju dotičnog UI sustava.

Potvrda i njezini prilozi sadržavaju sve relevantne informacije potrebne za omogućivanje evaluacije sukladnosti UI sustava i, prema potrebi, za kontrolu UI sustava tijekom korištenja.

Ako UI sustav nije sukladan sa zahtjevima iz poglavlja III. odjeljka 2., prijavljeno tijelo odbija izdati potvrdu Unije o ocjenjivanju tehničke dokumentacije te o tome obavješćuje podnositelja zahtjeva, uz detaljno obrazloženje odbijanja.

Ako UI sustav ne ispunjava zahtjev u pogledu podataka upotrijebljenih za njegovo treniranje, prije podnošenja zahtjeva za novo ocjenjivanje sukladnosti bit će potrebno ponovno treniranje dotičnog UI sustava. U tom slučaju obrazložena odluka prijavljenog tijela o odbijanju izdavanja potvrde Unije o ocjenjivanju tehničke dokumentacije sadržava konkretne argumente o kvaliteti podataka upotrijebljenih za treniranje UI sustava, a posebno o razlozima za utvrđivanje neusklađenosti.

- 4.7. Svaku promjenu UI sustava koja bi mogla utjecati na usklađenost UI sustava sa zahtjevima ili na njegovu namjenu ocjenjuje prijavljeno tijelo koje je izdalo potvrdu Unije o ocjenjivanju tehničke dokumentacije. Dobavljač obavješćuje to prijavljeno tijelo o svojoj namjeri da uvede neku od navedenih promjena ili ako na neki drugi način sazna za pojavu takvih promjena. Prijavljeno tijelo ocjenjuje planirane promjene i odlučuje je li zbog njih potrebno novo ocjenjivanje sukladnosti u skladu s člankom 43. stavkom 4. ili se za njih može izdati dodatak potvrdi Unije o ocjenjivanju tehničke dokumentacije. U potonjem slučaju prijavljeno tijelo ocjenjuje promjene, obavješćuje dobavljača o svojoj odluci te, ako promjene odobri, dobavljaču izdaje dodatak potvrdi Unije o ocjenjivanju tehničke dokumentacije.
5. Nadzor nad odobrenim sustavom upravljanja kvalitetom
- 5.1. Svrha je nadzora koji provodi prijavljeno tijelo iz točke 3. osigurati da dobavljač ispunjava uvjete odobrenog sustava upravljanja kvalitetom.
- 5.2. Za potrebe ocjenjivanja dobavljač prijavljenom tijelu omogućuje pristup prostorima u kojima se odvijaju dizajniranje, razvoj i testiranje UI sustava. Osim toga, dobavljač prijavljenom tijelu daje sve potrebne informacije.
- 5.3. Prijavljeno tijelo provodi periodične revizije kako bi potvrdilo da dobavljač provodi i primjenjuje sustav upravljanja kvalitetom te dobavljaču dostavlja izvješće o reviziji. U okviru tih revizija prijavljeno tijelo može provesti dodatna testiranja UI sustava za koje je izdana potvrda Unije o ocjenjivanju tehničke dokumentacije.

PRILOG VIII.

Informacije koje se moraju dostaviti pri registraciji visokorizičnih UI sustava u skladu s člankom 49.

Odjeljak A – Informacije koje moraju dostaviti dobavljači visokorizičnih UI sustava u skladu s člankom 49. stavkom 1.

Za visokorizične UI sustave koji se moraju registrirati u skladu s člankom 49. stavkom 1. dostavljaju se, a nakon toga ažuriraju, sljedeće informacije:

1. ime, adresa i kontaktni podaci dobavljača;
2. ako informacije dostavlja druga osoba u ime dobavljača, ime, adresa i kontaktni podaci te osobe;
3. ime, adresa i kontaktni podaci ovlaštenog zastupnika, ako je primjenjivo;
4. trgovačko ime UI sustava i sve dodatne nedvosmislene referentne oznake koje omogućuju identifikaciju i sljedivost UI sustava;
5. opis namjene UI sustava te komponenti i funkcija koje podržava taj UI sustav;
6. osnovni i sažet opis informacija koje sustav upotrebljava (podaci, ulazne vrijednosti) i njegova logika funkcioniranja;
7. status UI sustava (stavljen na tržište ili u upotrebi; više nije stavljen na tržište / u upotrebi, opozvan);
8. vrsta, broj i datum isteka potvrde koju je izdalo prijavljeno tijelo te ime ili identifikacijski broj tog prijavljenog tijela, ako je primjenjivo;
9. skenirani primjerak potvrde iz točke 8., ako je primjenjivo;
10. imena država članica u kojima je UI sustav stavljen na tržište, u upotrebu ili na raspolaganje u Uniji;
11. primjerak EU izjave o sukladnosti iz članka 47.;
12. upute za korištenje u elektroničkom formatu; te se informacije ne dostavljaju za visokorizične UI sustave u području kaznenog progona ili migracija, azila i upravljanja nadzorom državne granice iz Priloga III. točaka 1., 6. i 7.;
13. URL adresa za dodatne informacije (nije obvezno).

Odjeljak B – Informacije koje moraju dostaviti dobavljači visokorizičnih UI sustava u skladu s člankom 49. stavkom 2.

Za UI sustave koji se moraju registrirati u skladu s člankom 49. stavkom 2. dostavljaju se, a nakon toga ažuriraju, sljedeće informacije:

1. ime, adresa i kontaktni podaci dobavljača;
2. ako informacije dostavlja druga osoba u ime dobavljača, ime, adresa i kontaktni podaci te osobe;
3. ime, adresa i kontaktni podaci ovlaštenog zastupnika, ako je primjenjivo;
4. trgovačko ime UI sustava i sve dodatne nedvosmislene referentne oznake koje omogućuju identifikaciju i sljedivost UI sustava;
5. opis namjene UI sustava;
6. uvjet ili uvjeti iz članka 6. stavka 3. na temelju kojih se UI sustav ne smatra visokorizičnim;
7. kratak sažetak obrazloženja zašto se UI sustav ne smatra visokorizičnim pri primjeni postupka iz članka 6. stavka 3.;
8. status UI sustava (stavljen na tržište ili u upotrebi; više nije stavljen na tržište / u upotrebi, opozvan);
9. imena država članica u kojima je UI sustav stavljen na tržište, u upotrebu ili na raspolaganje u Uniji.

Odjeljak C – Informacije koje moraju dostaviti subjekti koji uvode visokorizične UI sustave u skladu s člankom 49. stavkom 3.

Za visokorizične UI sustave koji se moraju registrirati u skladu s člankom 49. stavkom 3. dostavljaju se, a nakon toga ažuriraju, sljedeće informacije:

1. ime, adresa i kontaktni podaci subjekta koji uvodi sustav;
 2. ime, adresa i kontaktni podaci osobe koja dostavlja informacije u ime subjekta koji uvodi sustav;
 3. URL adresa unosa UI sustava u bazu podataka EU-a od strane njegova dobavljača;
 4. sažetak nalaza procjene učinka na temeljna prava provedene u skladu s člankom 27.;
 5. sažetak procjene učinka na zaštitu podataka provedene u skladu s člankom 35. Uredbe (EU) 2016/679 ili člankom 27. Direktive (EU) 2016/680 kako je navedeno u članku 26. stavku 8. ove Uredbe, ako je primjenjivo.
-

PRILOG IX.

Informacije koje se moraju dostaviti pri registraciji visokorizičnih UI sustava iz priloga III. u vezi s testiranjem u stvarnim uvjetima u skladu s člankom 60.

U vezi s testiranjem u stvarnim uvjetima koje se mora registrirati u skladu s člankom 60. dostavljaju se, a nakon toga ažuriraju, sljedeće informacije:

1. jedinstveni identifikacijski broj na razini Unije za testiranje u stvarnim uvjetima;
 2. ime i kontaktni podaci dobavljača ili potencijalnog dobavljača i subjekata koji uvode sustav koji sudjeluju u testiranju u stvarnim uvjetima;
 3. kratak opis UI sustava i njegove namjene te druge informacije potrebne za identifikaciju sustava;
 4. sažetak glavnih karakteristika plana testiranja u stvarnim uvjetima;
 5. informacije o suspenziji ili obustavi testiranja u stvarnim uvjetima.
-

PRILOG X.

Zakonodavni akti Unije o opsežnim informacijskim sustavima u području slobode, sigurnosti i pravde

1. Schengenski informacijski sustav

- (a) Uredba (EU) 2018/1860 Europskog parlamenta i Vijeća od 28. studenoga 2018. o upotrebi Schengenskog informacijskog sustava za vraćanje državljana trećih zemalja s nezakonitim boravkom (SL L 312, 7.12.2018., str. 1.);
- (b) Uredba (EU) 2018/1861 Europskog parlamenta i Vijeća od 28. studenoga 2018. o uspostavi, radu i upotrebi Schengenskog informacijskog sustava (SIS) u području granične kontrole i o izmjeni Konvencije o provedbi Schengenskog sporazuma te o izmjeni i stavljanju izvan snage Uredbe (EZ) br. 1987/2006 (SL L 312, 7.12.2018., str. 14.);
- (c) Uredba (EU) 2018/1862 Europskog parlamenta i Vijeća od 28. studenoga 2018. o uspostavi, radu i upotrebi Schengenskog informacijskog sustava (SIS) u području policijske suradnje i pravosudne suradnje u kaznenim stvarima, izmjeni i stavljanju izvan snage Odluke Vijeća 2007/533/PUP i stavljanju izvan snage Uredbe (EZ) br. 1986/2006 Europskog parlamenta i Vijeća i Odluke Komisije 2010/261/EU (SL L 312, 7.12.2018., str. 56.).

2. Vizni informacijski sustav

- (a) Uredba (EU) 2021/1133 Europskog parlamenta i Vijeća od 7. srpnja 2021. o izmjeni uredaba (EU) br. 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 i (EU) 2019/818 u pogledu utvrđivanja uvjeta za pristup drugim informacijskim sustavima EU-a za potrebe viznog informacijskog sustava (SL L 248, 13.7.2021., str. 1.);
- (b) Uredba (EU) 2021/1134 Europskog parlamenta i Vijeća od 7. srpnja 2021. o izmjeni uredaba (EZ) br. 767/2008, (EZ) br. 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 i (EU) 2019/1896 Europskog parlamenta i Vijeća te o stavljanju izvan snage odluka Vijeća 2004/512/EZ i 2008/633/PUP u svrhu reforme viznog informacijskog sustava (SL L 248, 13.7.2021., str. 11.).

3. Eurodac

Uredba (EU) 2024/1358 Europskog parlamenta i Vijeća od 14. svibnja 2024. o uspostavi sustava „Eurodac” za usporedbu biometrijskih podataka radi djelotvorne primjene uredaba (EU) 2024/1315 i (EU) 2024/1350 Europskog parlamenta i Vijeća i Direktive Vijeća 2001/55/EZ te radi utvrđivanja identiteta državljana treće zemlje i osoba bez državljanstva s nezakonitim boravkom i o zahtjevima tijela za izvršavanje zakonodavstva država članica i Europolu za usporedbu s podacima iz Eurodaca u svrhu izvršavanja zakonodavstva, o izmjeni uredaba (EU) 2018/1240 i (EU) 2019/818 Europskog parlamenta i Vijeća te o stavljanju izvan snage Uredbe (EU) br. 603/2013 Europskog parlamenta i Vijeća (SL L, 2024/1358, 22.5.2024., ELI: <http://data.europa.eu/eli/reg/2024/1358/oj>) .

4. Sustav ulaska/izlaska

Uredba (EU) 2017/2226 Europskog parlamenta i Vijeća od 30. studenoga 2017. o uspostavi sustava ulaska/izlaska (EES) za registraciju podataka o ulasku i izlasku te podataka o odbijanju ulaska za državljane trećih zemalja koji prelaze vanjske granice država članica i određivanju uvjeta za pristup EES-u za potrebe izvršavanja zakonodavstva te o izmjeni Konvencije o provedbi Schengenskog sporazuma i uredbi (EZ) br. 767/2008 i (EU) br. 1077/2011 (SL L 327, 9.12.2017., str. 20.).

5. Europski sustav za informacije o putovanjima i odobravanje putovanja

- (a) Uredba (EU) 2018/1240 Europskog parlamenta i Vijeća od 12. rujna 2018. o uspostavi europskog sustava za informacije o putovanjima i odobravanje putovanja (ETIAS) i izmjeni uredaba (EU) br. 1077/2011, (EU) br. 515/2014, (EU) 2016/399, (EU) 2016/1624 i (EU) 2017/2226 (SL L 236, 19.9.2018., str. 1.);
- (b) Uredba (EU) 2018/1241 Europskog parlamenta i Vijeća od 12. rujna 2018. o izmjeni Uredbe (EU) 2016/794 u svrhu uspostave europskog sustava za informacije o putovanjima i odobravanje putovanja (ETIAS) (SL L 236, 19.9.2018., str. 72.).

6. Europski informacijski sustav kaznene evidencije za državljane trećih zemalja i osobe bez državljanstva
Uredba (EU) 2019/816 Europskog parlamenta i Vijeća od 17. travnja 2019. o uspostavi centraliziranog sustava za utvrđivanje država članica koje imaju podatke o osuđujućim presudama protiv državljana trećih zemalja i osoba bez državljanstva (sustav ECRIS-TCN) za dopunu Europskog informacijskog sustava kaznene evidencije te o izmjeni Uredbe (EU) 2018/1726 (SL L 135, 22.5.2019., str. 1.).
 7. Interoperabilnost
 - (a) Uredba (EU) 2019/817 Europskog parlamenta i Vijeća od 20. svibnja 2019. o uspostavi okvira za interoperabilnost informacijskih sustava EU-a u području granica i viza i izmjeni uredaba (EZ) br. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 i (EU) 2018/1861 Europskog parlamenta i Vijeća te odluka Vijeća 2004/512/EZ i 2008/633/PUP (SL L 135, 22.5.2019., str. 27.);
 - (b) Uredba (EU) 2019/818 Europskog parlamenta i Vijeća od 20. svibnja 2019. o uspostavi okvira za interoperabilnost informacijskih sustava EU-a u području policijske i pravosudne suradnje, azila i migracija i izmjeni uredaba (EU) 2018/1726, (EU) 2018/1862 i (EU) 2019/816 (SL L 135, 22.5.2019., str. 85.).
-

PRILOG XI.

Tehnička dokumentacija iz članka 53. stavka 1. točke (a) – tehnička dokumentacija za dobavljače UI modela opće namjene

Odjeljak 1.

Informacije koje moraju dostaviti svi dobavljači UI modela opće namjene

Tehnička dokumentacija iz članka 53. stavka 1. točke (a) sadržava barem sljedeće informacije, ovisno o veličini i profilu rizika modela:

1. Opći opis UI modela opće namjene, uključujući:
 - (a) zadaće koje bi model trebao obavljati te vrstu i prirodu UI sustava u koje se može integrirati;
 - (b) primjenjive politike u pogledu prihvatljivog korištenja;
 - (c) datum stavljanja na tržište i metode distribucije;
 - d) arhitekturu i broj parametara;
 - (e) modalitet (npr. tekst, slika) i format ulaznih i izlaznih podataka;
 - (f) licenciju.
2. Detaljan opis elemenata modela iz točke 1. i relevantne informacije o postupku njegova razvoja, uključujući sljedeće elemente:
 - (a) tehnička sredstva (npr. upute za korištenje, infrastruktura, alati) potrebna za integraciju UI modela opće namjene u UI sustave;
 - (b) specifikacije dizajna modela i postupka treniranja, uključujući metodologije i tehnike treniranja, najvažnije odabire u pogledu dizajna, uključujući obrazloženja i pretpostavke; informacije o tome što bi model svojim dizajnom trebao optimizirati i relevantnost različitih parametara, ako je primjenjivo;
 - (c) informacije o podacima upotrijebljenima za treniranje, testiranje i validaciju, ako je primjenjivo, uključujući vrstu i podrijetlo podataka i metodologije skrbi o podacima (npr. čišćenje, filtriranje itd.), količinu podataka, njihov opseg i glavne karakteristike; način na koji su podaci dobiveni i odabrani, kao i sve druge mjere za otkrivanje neprimjerenosti izvora podataka i metode za otkrivanje utvrdivih pristranosti, ako je primjenjivo;
 - (d) računalne resurse upotrijebljene za treniranje modela (npr. broj matematičkih operacija nad s brojevima s pomičnim zarezom), vrijeme treniranja i druge relevantne pojedinosti povezane s treniranjem;
 - (e) poznatu ili procijenjenu potrošnju energije modela.

Kad je riječ o točki (e), ako je potrošnja energije modela nepoznata, potrošnja energije može se temeljiti na informacijama o upotrijebljenim računalnim resursima.

Odjeljak 2.

Dodatne informacije koje moraju dostaviti dobavljači UI modela opće namjene sa sistemskim rizikom

1. Detaljan opis strategija evaluacije, uključujući rezultate evaluacije, na temelju dostupnih javnih evaluacijskih protokola i alata ili drugih metodologija evaluacije. Strategije evaluacije uključuju evaluacijske kriterije, parametre i metodologiju za utvrđivanje ograničenja.
2. Ako je primjenjivo, detaljan opis mjera uspostavljenih u svrhu provedbe unutarnjeg i/ili vanjskog neprijateljskog testiranja (npr. penetracijsko testiranje) i prilagodaba modela, uključujući usklađivanje i doradu.

3. Ako je primjenjivo, detaljan opis arhitekture sustava koji objašnjava kako se softverske komponente međusobno nadopunjuju ili potpomažu te kako su integrirane u cjelokupnu obradu.
-

PRILOG XII.

Informacije o transparentnosti iz članka 53. stavka 1. točke (b) – tehnička dokumentacija koju dobavljači UI modela opće namjene stavljaju na raspolaganje dobavljačima niže u lancu koji integriraju model u svoj UI sustav

Informacije iz članka 53. stavka 1. točke (b) sadržavaju barem sljedeće elemente:

1. opći opis UI modela opće namjene, uključujući:
 - (a) zadaće koje bi model trebao obavljati te vrstu i prirodu UI sustava u koje se može integrirati;
 - (b) primjenjive politike u pogledu prihvatljivog korištenja;
 - (c) datum stavljanja na tržište i metode distribucije;
 - (d) način na koji je model u interakciji s hardverom ili softverom koji nije dio samog modela ili na koji se može upotrijebiti za takvu interakciju, ako je primjenjivo;
 - (e) verzije relevantnog softvera povezanog s korištenjem UI modela opće namjene, ako je primjenjivo;
 - (f) arhitekturu i broj parametara;
 - (g) modalitet (npr. tekst, slika) i format ulaznih i izlaznih podataka;
 - (h) licenciju za model;
2. opis elemenata UI modela i postupka njegova razvoja, uključujući:
 - (a) tehnička sredstva (npr. upute za korištenje, infrastruktura, alati) potrebna za integraciju UI modela opće namjene u UI sustave;
 - (b) modalitet (npr. tekst, slika itd.) i format ulaznih i izlaznih podataka te njihova maksimalna veličina (npr. veličina kontekstualnog prozora itd.);
 - (c) informacije o podacima upotrijebljenima za treniranje, testiranje i validaciju, ako je primjenjivo, uključujući vrstu i podrijetlo podataka i metodologije skrbi o podacima.

PRILOG XIII.

Kriteriji za određivanje UI modela opće namjene sa sistemskim rizikom iz članka 51.

Kako bi utvrdila ima li određeni UI model opće namjene sposobnosti ili učinak jednakovrijedne onima iz članka 51. stavka 1. točke (a), Komisija uzima u obzir sljedeće kriterije:

- (a) broj parametara modela;
 - (b) kvalitetu ili veličinu skupa podataka, primjerice mjereno tokenima;
 - (c) količinu računanja upotrijebljenu za treniranje modela, izmjerenu u matematičkim operacijama nad brojevima s pomičnim zarezom ili izraženu kombinacijom drugih varijabli kao što su procijenjeni troškovi treniranja, procijenjeno vrijeme potrebno za treniranje ili procijenjena potrošnja energije za treniranje;
 - (d) ulazne i izlazne modalitete modela, kao što su pretvaranje teksta u tekst (veliki jezični modeli), pretvaranje teksta u sliku, multimodalnost i najnoviji pragovi za utvrđivanje sposobnosti visokog učinka za svaki modalitet, kao i specifičnu vrstu ulaznih i izlaznih podataka (npr. biološke sekvence);
 - (e) referentne vrijednosti i evaluacije sposobnosti modela, što uključuje uzimanje u obzir broja zadataka bez dodatnog treniranja, prilagodljivost za učenje novih, različitih zadataka, njegovu razinu autonomije i skalabilnosti, alate kojima ima pristup;
 - (f) ima li model zbog svojeg dosega znatan utjecaj na unutarnje tržište, što se pretpostavlja ako je stavljen na raspolaganje najmanje 10 000 registriranih poslovnih korisnika s poslovnim nastanom u Uniji;
 - (g) broj registriranih krajnjih korisnika.
-