



EUROPSKA
KOMISIJA

Bruxelles, 21.4.2021.
COM(2021) 206 final

2021/0106 (COD)

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

**O UTVRĐIVANJU USKLAĐENIH PRAVILA O UMJETNOJ INTELIGENCIJI (AKT
O UMJETNOJ INTELIGENCIJI) I IZMJENI ODREĐENIH ZAKONODAVNIH
AKATA UNIJE**

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

OBRAZLOŽENJE

1. KONTEKST PRIJEDLOGA

1.1. Razlozi i ciljevi prijedloga

Ovo obrazloženje priloženo je Prijedlogu uredbe o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji). Umjetna inteligencija (UI) skup je tehnologija koja se brzo razvija i može donijeti niz gospodarskih i društvenih koristi u cijelom spektru industrijskih grana i društvenih aktivnosti. Budući da umjetna inteligencija poboljšava predviđanje, optimizaciju operacija i raspodjelu resursa te personalizira pružanje usluga, njezino korištenje može pridonijeti ostvarenju rezultata koji pogoduju društvu i okolišu, a poduzećima i europskom gospodarstvu donijeti ključne konkurentske prednosti. Takvo je djelovanje prije svega potrebno u sektorima s velikim utjecajem, uključujući klimatske promjene, okoliš i zdravlje, javni sektor, financije, mobilnost, unutarnje poslove i poljoprivredu. Međutim, isti elementi i tehnike koji pokreću socioekonomske koristi UI-ja mogu prouzročiti nove rizike ili negativne posljedice za pojedince ili društvo. S obzirom na brzinu tehnoloških promjena i moguće poteškoće, EU se obvezuje da će nastojati postići uravnotežen pristup. U najboljem je interesu Unije da zadrži tehnološko vodstvo i pobrine se da Europljani ostvaruju koristi od novih tehnologija koje se razvijaju i funkcioniraju u skladu s vrijednostima, temeljnim pravima i načelima Unije.

Ovim se prijedlogom ostvaruje politička obveza predsjednice von der Leyen, koja je u političkim smjernicama za Komisiju od 2019. do 2024. naslovljenima „Ambicioznija Unija”¹ najavila da će Komisija predstaviti propise za koordinirani europski pristup ljudskim i etičkim implikacijama UI-ja. Nakon te najave Komisija je 19. veljače 2020. objavila Bijelu knjigu o UI-ju – Europski pristup izvrsnosti i izgradnji povjerenja². U Bijeloj knjizi utvrđuju se opcije politike o načinima postizanja dvostrukog cilja promicanja prihvatanja UI-ja i suzbijanja rizika povezanih s određenim uporabama te tehnologije. Ovim se prijedlogom pravnog okvira za pouzdani UI želi ostvariti drugi cilj, koji se odnosi na razvoj ekosustava povjerenja. Prijedlog se temelji na vrijednostima i temeljnim pravima EU-a te se njime nastoji uliti povjerenje građanima i drugim korisnicima da prihvaćaju rješenja koja se temelje na UI-ju, a poduzeća potaknuti da ta rješenja razvijaju. UI bi trebao biti alat u službi čovjeka i pozitivna snaga u društvu koja će s vremenom poboljšati dobrobit građana. Stoga bi pravila za UI koji je dostupan na tržištu Unije ili na neki drugi način utječe na njezine stanovnike trebala biti antropocentrična kako bi se građani mogli pouzdati u to da se ta tehnologija upotrebljava sigurno i u skladu s pravom, uključujući poštovanje temeljnih prava. Nakon što je objavila Bijelu knjigu Komisija je pokrenula opsežno savjetovanje s dionicima, koji su se odazvali u velikom broju i uglavnom podržali regulatorne intervencije za rješavanje problema i nedoumica izazvanih sve većom uporabom UI-ja.

Prijedlog je i odgovor na izričite zahtjeve Europskog parlamenta i Europskog vijeća, koji su više puta pozivali na zakonodavne mjere kojima se osigurava funkcionalno unutarnje tržište za sustave umjetne inteligencije („UI sustavi”) te kojima se na razini Unije adekvatno odgovara na koristi i rizike UI-ja. Njime se pridonosi Unijinu cilju globalnog vodstva u

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

² Europska komisija, Bijela knjiga o umjetnoj inteligenciji – Europski pristup izvrsnosti i izgradnji povjerenja, COM(2020) 65 final, 2020.

razvoju sigurne, pouzdane i etične umjetne inteligencije, koji je odredilo Europsko vijeće³, te se štite etička načela u skladu s izričitim zahtjevom Europskog parlamenta⁴.

Europsko vijeće upozorilo je 2017. na „svijest o hitnosti suočavanja s novim trendovima”, uključujući „pitanja kao što su umjetna inteligencija [...], uz istodobno osiguravanje visoke razine zaštite podataka, digitalnih prava i etičkih standarda”⁵. Vijeće je u zaključcima iz 2019. o koordiniranom planu za razvoj i upotrebu umjetne inteligencije europskog podrijetla⁶ dodatno naglasilo da je važno osigurati potpuno poštovanje prava europskih građana i pozvalo da se postojeće relevantno zakonodavstvo preispita kako bi bilo prikladno za nove mogućnosti i probleme koje donosi UI. Europsko vijeće ujedno je pozvalo na jasno utvrđivanje primjena UI-ja koje bi se trebale smatrati visokorizičnima⁷.

U najnovijim zaključcima od 21. listopada 2020. ponovno je pozvalo na rješavanje problema netransparentnosti, složenosti, pristranosti, određenog stupnja nepredvidivosti i djelomično autonomnog ponašanja određenih UI sustava kako bi se osigurala njihova usklađenost s temeljnim pravima i olakšalo provođenje pravnih propisa⁸.

Europski parlament isto je tako bio iznimno aktivan u području UI-ja. U listopadu 2020. donio je nekoliko rezolucija povezanih s UI-jem, među ostalim o etičnosti⁹, odgovornosti¹⁰ i autorskom pravu¹¹. Zatim je 2021. donio rezolucije o UI-ju u kaznenim stvarima¹² te u obrazovnom, kulturnom i audiovizualnom sektoru¹³. U Rezoluciji o okviru etičkih aspekata umjetne inteligencije, robotike i s njima povezanih tehnologija Europski parlament posebno je Komisiji preporučio da predloži zakonodavne mjere kojima bi se iskoristile mogućnosti i koristi UI-ja te osigurala zaštita etičkih načela. Rezolucija sadržava tekst zakonodavnog prijedloga uredbe o etičkim načelima za razvoj, primjenu i uporabu UI-ja, robotike i s njima povezanih tehnologija. U skladu s političkom obvezom koju je predsjednica von der Leyen preuzela u političkim smjernicama u pogledu rezolucija koje je donio Europski parlament na temelju članka 225. UFEU-a, u ovom se prijedlogu uzima u obzir prethodno navedena

³ Europsko vijeće, [Izvanredni sastanak Europskog vijeća \(1. i 2. listopada 2020.\) – zaključci](#), EUCO 13/20, 2020., str. 6.

⁴ 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).

⁵ Europsko vijeće, [Sastanak Europskog vijeća \(19. listopada 2017.\) – zaključci](#), EUCO 14/17, 2017., str. 8.

⁶ Vijeće Europske unije, [Umjetna inteligencija b\) Zaključci o koordiniranom planu o umjetnoj inteligenciji – usvajanje](#) 6177/19, 2019.

⁷ Europsko vijeće, [Izvanredni sastanak Europskog vijeća \(1. i 2. listopada 2020.\) – zaključci](#), EUCO 13/20, 2020.

⁸ Vijeće Europske unije, [Zaključci predsjedništva – Povelja o temeljnim pravima u kontekstu umjetne inteligencije i digitalnih promjena](#), 11481/20, 2020.

⁹ Rezolucija Europskog parlamenta od 20. listopada 2020. o okviru etičkih aspekata umjetne inteligencije, robotike i s njima povezanih tehnologija, [2020/2012\(INL\)](#).

¹⁰ Rezolucija Europskog parlamenta od 20. listopada 2020. o sustavu građanskopravne odgovornosti za umjetnu inteligenciju, [2020/2014\(INL\)](#).

¹¹ Rezolucija Europskog parlamenta od 20. listopada 2020. o pravima intelektualnog vlasništva za razvoj tehnologija umjetne inteligencije, [2020/2015\(INI\)](#).

¹² Nacrt izvješća Europskog parlamenta o umjetnoj inteligenciji u kaznenom pravu i njezinoj primjeni od strane policije i pravosudnih tijela u kaznenim stvarima, [2020/2016\(INI\)](#).

¹³ Nacrt izvješća Europskog parlamenta o umjetnoj inteligenciji u obrazovnom, kulturnom i audiovizualnom sektoru, [2020/2017\(INI\)](#). Komisija je u tom pogledu donijela Akcijski plan za digitalno obrazovanje 2021.–2027.: Prilagodba obrazovanja i osposobljavanja digitalnom dobu, u kojoj se predviđa razvoj etičkih smjernica o UI-ju i uporabi podataka u obrazovanju – Komunikacija Komisije COM(2020) 624 final.

rezolucija Europskog parlamenta uz potpuno poštovanje načela proporcionalnosti, supsidijarnosti i bolje izrade zakonodavstva.

U tom političkom kontekstu Komisija predstavlja predloženi regulatorni okvir o umjetnoj inteligenciji sa sljedećim **posebnim ciljevima**:

- da su UI sustavi koji se stavljaju na tržište Unije i upotrebljavaju sigurni i usklađeni s postojećim pravom o temeljnim pravima i vrijednostima Unije,
- pravna sigurnost kako bi se olakšala ulaganja i inovacije u području UI-ja,
- poboljšanje upravljanja i djelotvorne provedbe postojećih propisa o temeljnim pravima i sigurnosnim zahtjevima primjenjivima na UI sustave,
- olakšavanje razvoja jedinstvenog tržišta za zakonite, sigurne i pouzdane primjene UI-ja te sprečavanje fragmentacije tržišta.

Kako bi se ti ciljevi ostvarili, u ovom se prijedlogu iznosi uravnotežen i proporcionalan horizontalni pristup UI-ju koji je ograničen na minimalne zahtjeve potrebne za rješavanje rizika i problema povezanih s UI-jem, bez nepotrebnog ograničavanja ili ometanja tehnološkog razvoja ili nerazmjernog povećanja troškova stavljanja UI rješenja na tržište na neki drugi način. Prijedlogom se uspostavlja otporan i fleksibilan pravni okvir. S jedne je strane, s obzirom na temeljne regulatorne odabire, sveobuhvatan i otporan na buduće promjene, što uključuje i na načelima temeljene zahtjeve koje bi UI sustavi trebali ispunjavati. S druge se strane njime uvodi proporcionalan regulatorni sustav čija je okosnica dobro definiran regulatorni pristup koji se temelji na riziku i ne stvara nepotrebna ograničenja za trgovinu, dok je pravna intervencija prilagođena konkretnim situacijama u kojima postoji opravdan razlog za zabrinutost ili u kojima se razumno može očekivati da će se u bliskoj budućnosti pojaviti takva zabrinutost. Pravni okvir istodobno uključuje fleksibilne mehanizme koji omogućuju da ga se dinamično prilagođava razvoju novih tehnologija i pojavi novih problematičnih okolnosti.

Prijedlogom se utvrđuju usklađena pravila za razvoj, stavljanje na tržište i uporabu UI sustava u Uniji, i to na temelju proporcionalnog pristupa koji se temelji na riziku. U njemu se predlaže jedinstvena i dugoročno održiva definicija UI-ja. Zabranjuju se određene iznimno štetne prakse UI-ja jer su protivne vrijednostima Unije te se predlažu specifična ograničenja i zaštitne mjere u pogledu određenih primjena sustavâ za daljinsku biometrijsku identifikaciju za potrebe kaznenog progona. U prijedlogu se utvrđuje temeljita metodologija procjene rizika za definiranje „visokorizičnih” UI sustava koji predstavljaju značajne rizike za zdravlje i sigurnost ili temeljna prava osoba. Ti UI sustavi morat će ispunjavati skup horizontalnih obveznih zahtjeva za pouzdani UI i zadovoljiti na ocjenjivanjima sukladnosti prije nego što se budu mogli staviti na tržište Unije. Ujedno se uvode predvidljive, proporcionalne i jasne obveze za dobavljače i korisnike tih sustava kako bi UI sustavi tijekom cijelog životnog vijeka bili sigurni i u skladu s postojećim propisima o zaštiti temeljnih prava. Za određene UI sustave predlažu se samo minimalne obveze u pogledu transparentnosti, posebno kad je riječ o uporabi *chatbotova* ili uvjerljivog krivotvorenog sadržaja („deep fake”).

Predložena pravila provodit će se u okviru sustava upravljanja država članica na temelju već postojećih struktura, ali i mehanizma suradnje na razini Unije uspostavom Europskog odbora za umjetnu inteligenciju. Predlažu se i dodatne mjere za potporu inovacijama, posebno u obliku regulatornih izoliranih okruženja i drugih mjera za smanjenje regulatornog opterećenja i potporu malim i srednjim poduzećima („MSP-ovi”) te novoosnovanim (*start-up*) poduzećima.

1.2. Dosljednost s postojećim odredbama politike u tom području

Horizontalna priroda prijedloga zahtijeva potpunu dosljednost s postojećim zakonodavstvom Unije koje se primjenjuje na sektore u kojima se već upotrebljavaju visokorizični UI sustavi ili u kojima će se vjerojatno upotrebljavati u bliskoj budućnosti.

Prijedlog je dosljedan i s Poveljom Europske unije o temeljnim pravima i postojećim sekundarnim zakonodavstvom Unije o zaštiti podataka, zaštiti potrošača, nediskriminaciji i rodnoj ravnopravnosti. Prijedlogom se ne dovode u pitanje Opća uredba o zaštiti podataka (Uredba (EU) 2016/679) ni Direktiva o zaštiti podataka pri izvršavanju zakonodavstva (Direktiva (EU) 2016/680), već se dopunjuju usklađenim pravilima primjenjivima na projektiranje, razvoj i uporabu određenih visokorizičnih UI sustava te ograničenjima za određene uporabe sustava za daljinsku biometrijsku identifikaciju. Nadalje, prijedlogom se dopunjuje postojeće pravo Unije o nediskriminaciji posebnim zahtjevima kojima se nastoji što više smanjiti rizik od algoritamske diskriminacije, posebno u pogledu organizacije i kvalitete skupova podataka za razvoj UI sustava, te obvezama koje se odnose na testiranje, upravljanje rizikom, vođenje dokumentacije i ljudski nadzor tijekom cijelog životnog vijeka UI sustava. Prijedlogom se ne dovodi u pitanje primjena prava Unije u području tržišnog natjecanja.

Kad je riječ o visokorizičnim UI sustavima koji su sigurnosni sastavni dijelovi proizvoda, ovaj će se prijedlog integrirati u postojeće sektorsko propise o sigurnosti kako bi se osigurala dosljednost, spriječilo udvostručavanje i što više smanjila dodatna opterećenja. Točnije, za visokorizične UI sustave povezane s proizvodima koji su obuhvaćeni propisima novog zakonodavnog okvira (npr. strojevi, medicinski proizvodi, igračke) zahtjevi za UI sustave utvrđeni u ovom prijedlogu provjeravat će se u okviru postojećih postupaka ocjenjivanja sukladnosti na temelju relevantnih propisa novog zakonodavnog okvira. Kad je riječ o interakciji zahtjeva, iako bi sigurnosni rizici specifični za UI sustave trebali biti obuhvaćeni zahtjevima iz ovog prijedloga, propisima novog zakonodavnog okvira nastoji se osigurati općenita sigurnost konačnog proizvoda, pa mogu sadržavati posebne zahtjeve o sigurnoj integraciji UI sustava u konačan proizvod. Prijedlog uredbe o strojevima, koji se donosi istog dana kao i ovaj prijedlog, u potpunosti je u skladu s tim pristupom. Ovaj se prijedlog ne bi izravno primjenjivao na visokorizične UI sustave povezane s proizvodima obuhvaćenima relevantnim zakonodavnim propisima starog pristupa (npr. zrakoplovstvo, automobili). Međutim, pri donošenju relevantnog provedbenog ili delegiranog zakonodavnog propisa na temelju tih akata morat će se uzeti u obzir *ex ante* temeljni zahtjevi za visokorizične UI sustave koji su utvrđeni u ovom prijedlogu.

Kad je riječ o UI sustavima koje pružaju ili upotrebljavaju regulirane kreditne institucije, tijela nadležna za nadziranje propisa Unije o financijskim uslugama trebala bi biti određena kao nadležna tijela za nadzor nad zahtjevima ovog prijedloga kako bi se osigurala usklađena provedba obveza iz ovog prijedloga i propisa o financijskim uslugama u kojima su UI sustavi u određenoj mjeri implicitno regulirani s obzirom na sustav internog upravljanja kreditnih institucija. Kako bi se dosljednost dodatno povećala, postupak ocjenjivanja sukladnosti i neke od postupovnih obveza dobavljača iz ovog prijedloga integrirani su u postupke koji se temelje na Direktivi 2013/36/EU o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru¹⁴.

¹⁴ 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 (Tekst značajan za EGP), SL L 176, 27.6.2013., str. 338.–436.

Ovaj je prijedlog dosljedan i s primjenjivim propisima Unije o uslugama, među ostalim o uslugama posredovanja koje su regulirane Direktivom 2000/31/EZ o elektroničkoj trgovini¹⁵ i s nedavnim prijedlogom Komisije o Aktu o digitalnim uslugama¹⁶.

Kad je riječ o UI sustavima koji su sastavni dijelovi opsežnih informacijskih sustava u području slobode, sigurnosti i pravde kojima upravlja Agencija Europske unije za operativno upravljanje opsežnim informacijskim sustavima (eu-LISA), prijedlog se neće primjenjivati na UI sustave koji su stavljeni na tržište ili u uporabu prije isteka jedne godine od datuma primjene ove Uredbe, osim ako zamjena ili izmjena tih pravnih akata dovede do znatne promjene u konceptu ili namjeni tih UI sustava.

1.3. Dosljednost u odnosu na druge politike Unije

Ovaj je prijedlog dio šireg sveobuhvatnog paketa mjera za rješavanje problema koji proizlaze iz razvoja i uporabe UI-ja, kako je razmotreno u Bijeloj knjizi o UI-ju. Stoga je osigurana dosljednost i komplementarnost s drugim tekućim ili planiranim inicijativama Komisije kojima se također nastoje riješiti ti problemi, među ostalim s revizijom sektorskog zakonodavstva o proizvodima (npr. Direktiva o strojevima, Direktiva o općoj sigurnosti proizvoda) i inicijativama kojima se rješavaju pitanja odgovornosti povezana s novim tehnologijama, uključujući UI sustave. Tim će se inicijativama nadograditi i dopuniti ovaj prijedlog kako bi se postigla pravna jasnoća i poticao razvoj ekosustava povjerenja u UI u Europi.

Prijedlog je usklađen i s općom digitalnom strategijom Komisije u pogledu doprinosa promicanju tehnologije u interesu građana, jednog od triju glavnih stupova smjernica i ciljeva politike najavljenih u Komunikaciji „Izgradnja digitalne budućnosti Europe”¹⁷. Njime se utvrđuje usklađen, djelotvoran i proporcionalan okvir s ciljem da se UI razvija tako da se poštuju prava ljudi i stječe njihovo povjerenje te time Europu pripremi za digitalno doba i sljedećih deset godina pretvori u **digitalno desetljeće**¹⁸.

Nadalje, promicanje inovacija koje se temelje na umjetnoj inteligenciji blisko je povezano s **Aktom o upravljanju podacima**¹⁹, **Direktivom o otvorenim podacima**²⁰ i drugim inicijativama u okviru **strategije EU-a za podatke**²¹, kojima će se uspostaviti pouzdani mehanizmi i usluge za ponovnu uporabu, razmjenu i objedinjavanje podataka koji su neophodni za razvoj visokokvalitetnih UI modela koji se temelje na podacima.

Prijedlogom se znatno jača i uloga Unije u oblikovanju globalnih normi i standarda te promicanju pouzdanog UI-ja koji je dosljedan vrijednostima i interesima Unije. Njime se Uniji daje snažan temelj za daljnju suradnju s vanjskim partnerima, uključujući treće zemlje, i u međunarodnim forumima o pitanjima koja se odnose na UI.

¹⁵ Direktiva 2000/31/EZ Europskog parlamenta i Vijeća od 8. lipnja 2000. o određenim pravnim aspektima usluga informacijskog društva na unutarnjem tržištu, posebno elektroničke trgovine (Direktiva o elektroničkoj trgovini), SL L 178, 17.7.2000., str. 1.–16.

¹⁶ Vidjeti Prijedlog UREDBE EUROPSKOG PARLAMENTA I VIJEĆA o jedinstvenom tržištu digitalnih usluga (Akt o digitalnim uslugama) i izmjeni Direktive 2000/31/EZ, COM(2020) 825 final.

¹⁷ Komunikacija Komisije, Izgradnja digitalne budućnosti Europe, COM(2020) 67 final.

¹⁸ [Digitalni kompas 2030.: europski pristup za digitalno desetljeće.](#)

¹⁹ Prijedlog uredbe o europskom upravljanju podacima (Akt o upravljanju podacima), [COM\(2020\) 767.](#)

²⁰ Direktiva (EU) 2019/1024 Europskog parlamenta i Vijeća od 20. lipnja 2019. o otvorenim podacima i ponovnoj uporabi informacija javnog sektora, PE/28/2019/REV/1, SL L 172, 26.6.2019., str. 56.–83.

²¹ [Komunikacija Komisije, Europska strategija za podatke, COM\(2020\) 66 final.](#)

2. PRAVNA OSNOVA, SUPSIDIJARNOST I PROPORCIONALNOST

2.1. Pravna osnova

Pravna je osnova prijedloga prvenstveno članak 114. Ugovora o funkcioniranju Europske unije (UFEU), kojim se predviđa donošenje mjera za osiguravanje uspostave i funkcioniranja unutarnjeg tržišta.

Ovaj je prijedlog ključan dio EU-ove strategije jedinstvenog digitalnog tržišta. Njime se prvenstveno želi osigurati pravilno funkcioniranje unutarnjeg tržišta uspostavljanjem usklađenih pravila, ponajprije o razvoju, stavljanju na tržište Unije te uporabi proizvoda i usluga u kojima se koriste tehnologije UI-ja ili koji se nude kao samostalni UI sustavi. Neke države članice već razmatraju nacionalna pravila kojima bi osigurale sigurnost UI-ja te njegov razvoj i uporabu u skladu s obvezama u području temeljnih prava. To će vjerojatno izazvati dva glavna problema: i. fragmentaciju unutarnjeg tržišta s obzirom na osnovne elemente, posebno u pogledu zahtjeva za proizvode i usluge s UI-jem, njihovo stavljanje na tržište, uporabu, odgovornost i nadzor koji provode tijela javne vlasti te ii. znatno slabljenje pravne sigurnosti za dobavljače i korisnike UI sustava u vezi s primjenom postojećih i novih pravila na te sustave u Uniji. S obzirom na znatan prekogranični promet proizvoda i usluga ta se dva problema najbolje mogu riješiti usklađivanjem zakonodavstva EU-a.

Naime, u prijedlogu se utvrđuju zajednički obvezni zahtjevi koji se primjenjuju na projektiranje i razvoj određenih UI sustava prije nego što se stave na tržište, a koji će se dodatno operacionalizirati s pomoću usklađenih tehničkih standarda. U prijedlogu se rješava i situacija nakon stavljanja UI sustava na tržište tako što se usklađuje način provođenja *ex post* kontrola.

Osim toga, budući da ovaj prijedlog sadržava određena posebna pravila o zaštiti pojedinaca u pogledu obrade osobnih podataka, prije svega ograničenja uporabe UI sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona, dio ove Uredbe koji se odnosi na ta posebna pravila primjereno je temeljiti na članku 16. UFEU-a.

2.2. Supsidijarnost (za neisključivu nadležnost)

Zbog prirode UI-ja, koji se često oslanja na velike i raznolike skupove podataka i može biti ugrađen u bilo kakve proizvode ili usluge u slobodnom prometu na unutarnjem tržištu, države članice ne mogu same djelotvorno ostvariti ciljeve ovog prijedloga. Nadalje, mnoštvo novih potencijalno neujednačenih nacionalnih pravila otežat će neometani promet proizvoda i usluga povezanih s UI sustavima u cijelom EU-u i neće djelotvorno jamčiti sigurnost i zaštitu temeljnih prava i vrijednosti Unije u različitim državama članicama. Nacionalni pristupi rješavanju tih problema samo će prouzročiti dodatnu pravnu nesigurnost i zapreke te usporiti prihvatanje UI-ja na tržištu.

Ciljevi ovog prijedloga mogu se bolje ostvariti na razini Unije kako bi se spriječila daljnja fragmentacija jedinstvenog tržišta na potencijalno proturječne nacionalne okvire koji onemogućavaju slobodan promet robe i usluga u koje je ugrađen UI. Čvrst europski regulatorni okvir za pouzdan UI osigurat će i ravnopravne uvjete i zaštititi sve građane te pritom ojačati konkurentnost Europe i industrijske temelje u području UI-ja. Samo zajedničko djelovanje na razini Unije omogućuje zaštitu digitalne suverenosti Unije te iskorištavanje njezinih alata i regulatornih ovlasti za oblikovanje globalnih pravila i standarda.

2.3. Proporcionalnost

Prijedlog se temelji na postojećim pravnim okvirima te je proporcionalan i potreban za postizanje svojih ciljeva jer slijedi pristup koji se temelji na riziku i nameće regulatorna

opterećenja samo u slučajevima u kojima bi UI mogao ozbiljno ugroziti temeljna prava i sigurnost. Za UI sustave koji nisu visokorizični nameću se samo vrlo ograničene obveze u pogledu transparentnosti, koje se, primjerice, odnose na davanje upozorenja kad se UI sustav kad koristi u interakciji s ljudima. Za visokorizične UI sustave nužni su zahtjevi u pogledu visokokvalitetnih podataka, dokumentacije i sljedivosti, transparentnosti, ljudskog nadzora, točnosti i otpornosti kako bi se smanjili rizici za temeljna prava i sigurnost koji proizlaze iz UI-ja i koji nisu obuhvaćeni drugim postojećim pravnim okvirima. Usklađene norme te prateće smjernice i alati za postizanje usklađenosti pomoći će dobavljačima i korisnicima da ispune zahtjeve iz prijedloga i minimiziraju troškove. Troškovi koje snose operateri proporcionalni su ostvarenim ciljevima te ekonomskim i reputacijskim koristima koje operateri mogu očekivati od ovog prijedloga.

2.4. Odabir instrumenta

Izbor uredbe kao pravnog instrumenta opravdan je potrebom za ujednačenom primjenom novih pravila, kao što su definicija UI-ja, zabrana određenih štetnih praksi koje su omogućene UI-jem i klasifikacija određenih UI sustava. Izravna primjenjivost Uredbe u skladu s člankom 288. UFEU-a smanjit će pravnu rascjepkanost i olakšati razvoj jedinstvenog tržišta za zakonite, sigurne i pouzdane UI sustave. To će se prije svega postići uvođenjem usklađenog skupa temeljnih zahtjeva koji se odnose na UI sustave klasificirane kao visokorizične i obveza za dobavljače i korisnike tih sustava, čime će se poboljšati zaštita temeljnih prava te osigurati pravna sigurnost i za operatere i za potrošače.

Odredbe uredbe pritom nisu pretjerano preskriptivne i ostavljaju prostora za različite razine djelovanja država članica u pogledu elemenata kojima se ne ugrožavaju ciljevi inicijative, osobito unutarnje organizacije sustava nadzora tržišta i primjene mjera za poticanje inovacija.

3. REZULTATI EX POST EVALUACIJA, SAVJETOVANJA S DIONICIMA I PROCJENA UČINKA

3.1. Savjetovanje s dionicima

Ovaj je prijedlog rezultat opsežnog savjetovanja sa svim važnim dionicima, u kojem su primijenjena opća načela i minimalni standardi za savjetovanje Komisije sa zainteresiranim stranama.

Internetsko javno savjetovanje pokrenuto je 19. veljače 2020., kad je objavljena i Bijela knjiga o umjetnoj inteligenciji, a trajalo je do 14. lipnja 2020. Cilj savjetovanja bilo je prikupljanje stajališta i mišljenja o Bijeloj knjizi. Bilo je namijenjeno svim zainteresiranim dionicima iz javnog i privatnog sektora, uključujući vlade, lokalna tijela, komercijalne i nekomercijalne organizacije, socijalne partnere, stručnjake, članove akademske zajednice i građane. Nakon što je analizirala sve primljene odgovore Komisija je na svojim internetskim stranicama objavila sažetak rezultata i pojedinačne odgovore²².

Primljeno je ukupno 1 215 odgovora, od kojih su 352 pristigla iz poduzeća ili poslovnih organizacija/udruženja, 406 od pojedinaca (92 % pojedinaca bilo je iz EU-a), 152 iz akademskih/istraživačkih ustanova i 73 iz tijela javne vlasti. Sudjelovalo je 160 predstavnika civilnog društva (među kojima je bilo devet organizacija potrošača, 129 nevladinih organizacija i 22 sindikata), a 72 ispitanika označena su kao „ostali”. Od 352 predstavnika poslovnog i industrijskog sektora njih 222 bila su poduzeća i predstavnici poslovnog sektora, od toga su 41,5 % bila mikropoduzeća te mala i srednja poduzeća. Ostali su bili poslovna

²²

[Ovdje su dostupni svi rezultati savjetovanja.](#)

udruženja. Ukupno je 84 % odgovora poslovnog i industrijskog sektora pristiglo iz EU-27. Ovisno o pitanju, između 81 i 598 ispitanika iskoristilo je mogućnost slobodnog unošenja teksta za pisanje komentara. Na internetskom portalu EUSurvey dostavljeno je više od 450 dokumenata o stajalištu, ili kao dodatak odgovorima iz upitnika (više od 400) ili u obliku samostalnih doprinosa (više od 50).

Dionici se općenito slažu da je potrebno djelovati. Velika većina dionika slaže se da postoje zakonodavne praznine ili da je potrebno novo zakonodavstvo. Međutim, više je dionika upozorilo Komisiju da je potrebno spriječiti udvostručavanje, proturječne obveze i prekomjerne propise. U mnogo je komentara istaknuta važnost tehnološki neutralnog i proporcionalnog regulatornog okvira.

Dionici su uglavnom zatražili usku, jasnu i preciznu definiciju UI-ja. Dionici su naglasili i da je osim pojašnjenja pojma UI-ja važno definirati „rizik”, „visoki rizik”, „niski rizik”, „daljinsku biometrijsku identifikaciju” i „štetu”.

Većina ispitanika izričito podržava pristup koji se temelji na riziku. Smatralo se da je okvir koji se temelji na riziku bolja opcija od opće regulacije svih UI sustava. Vrste rizika i prijetnji trebale bi se temeljiti na sektorskom pristupu u kojem se svaki slučaj razmatra zasebno. Pri izračunu rizika trebao bi se uzeti u obzir i utjecaj na prava i sigurnost.

Regulatorna izolirana okruženja mogla bi biti vrlo korisna za promicanje UI-ja i pojedini ih dionici podupiru, posebno poslovna udruženja.

Više od 50 % ispitanika koji su izrazili mišljenje o modelima provedbe, a posebno oni iz poslovnih udruženja, podržalo je kombinaciju *ex ante* samoprocjene rizika i *ex post* provedbe za visokorizične UI sustave.

3.2. Prikupljanje i primjena stručnog znanja

Prijedlog se temelji na dvogodišnjoj analizi i bliskoj suradnji dionika, uključujući članove akademske zajednice, poduzeća, socijalne partnere, nevladine organizacije, države članice i građane. Pripremni rad počeo je 2018. osnivanjem **stručne skupine na visokoj razini za UI**, koja je imala uključiv i širok sastav od 52 poznata stručnjaka zadužena za savjetovanje Komisije o provedbi strategije Komisije za umjetnu inteligenciju. Komisija je u travnju 2019. podržala²³ glavne zahtjeve utvrđene u etičkim smjernicama stručne skupine na visokoj razini za pouzdani UI²⁴, koje su revidirane kako bi se uzelo u obzir više od 500 podnesaka dionika. Glavni zahtjevi u skladu su s raširenim i zajedničkim pristupom primijenjenim u mnoštvu etičkih kodeksa i načela koje su razvile brojne privatne i javne organizacije u Europi i drugdje, prema kojem bi razvoj i uporabu UI-ja trebala usmjeravati određena osnovna načela koja se temelje na vrijednostima. Zahvaljujući popisu za procjenu pouzdane umjetne inteligencije²⁵ ti su zahtjevi primijenjeni u pokusnom postupku s više od 350 organizacija.

Osim toga, osnovan je **Savez za UI**²⁶ kao platforma na kojoj približno 4 000 dionika može raspravljati o tehnološkim i društvenim implikacijama UI-ja, a jednom godišnje održava se i skup o UI-ju.

²³ Europska komisija, [Izgradnja povjerenja u antropocentričnu umjetnu inteligenciju](#), COM(2019) 168.

²⁴ Stručna skupina na visokoj razini, [Etičke smjernice za pouzdani UI](#), 2019.

²⁵ Stručna skupina na visokoj razini, [Popis za procjenu pouzdane umjetne inteligencije u svrhu samoprocjene](#), 2020.

²⁶ Savez za UI forum je više dionika koji je pokrenut u lipnju 2018., Savez za UI <https://ec.europa.eu/digital-single-market/en/european-ai-alliance>.

Taj uključivi pristup dodatno je razrađen u **Bijeloj knjizi** o UI-ju i o njemu su pristigli komentari više od 1 250 dionika, uključujući više od 450 dodatnih dokumenata o stajalištu. Komisija je kao rezultat toga objavila početnu procjenu učinka, koja je pak privukla više od 130 komentara²⁷. Organizirani su i **dodatne radionice i događanja za dionike**, čiji rezultati podupiru analizu u procjeni učinka i opcije politike izložene u ovom prijedlogu²⁸. Naručena je i **vanjska studija** kojom su prikupljeni podaci za procjenu učinka.

3.3. Procjena učinka

Komisija je u skladu sa svojom politikom „bolje regulative” provela procjenu učinka ovog prijedloga, koju je ispitao Komisijin Odbor za nadzor regulative. Odbor za nadzor regulative sastao se 16. prosinca 2020. i izdao negativno mišljenje. Nakon što je provedena znatna revizija procjene učinka radi uvažavanja komentara i njezina ponovnog podnošenja, Odbor za nadzor regulative izdao je 21. ožujka 2021. pozitivno mišljenje. Mišljenja Odbora za nadzor regulative, preporuke i objašnjenje toga kako su uzeti u obzir prikazani su u Prilogu 1. procjeni učinka.

Komisija je razmotrila različite opcije politike kako bi postigla opći cilj prijedloga: **osiguravanje pravilnog funkcioniranja jedinstvenog tržišta** stvaranjem uvjeta za razvoj i uporabu pouzdanog UI-ja u Uniji.

Procijenjene su četiri opcije politike različitog stupnja regulatorne intervencije:

- **opcija 1:** zakonodavni instrument EU-a kojim se uspostavlja program dobrovoljnog označivanja,
- **opcija 2:** sektorski, *ad-hoc* pristup,
- **opcija 3:** horizontalni zakonodavni instrument EU-a primjenom proporcionalnog pristupa koji se temelji na riziku,
- **opcija 3+:** horizontalni zakonodavni instrument EU-a primjenom proporcionalnog pristupa koji se temelji na riziku + kodeksi ponašanja za UI sustave koji nisu visokorizični,
- **opcija 4:** horizontalni zakonodavni instrument EU-a kojim se utvrđuju obvezni zahtjevi za sve UI sustave, bez obzira na rizik koji predstavljaju.

U skladu s utvrđenom metodologijom Komisije svaka je opcija politike evaluirana u odnosu na gospodarske i društvene učinke, s posebnim naglaskom na temeljnim pravima. Najpoželjnija je opcija 3+, regulatorni okvir namijenjen isključivo visokorizičnim UI sustavima, uz mogućnost da se svi dobavljači UI sustava koji nisu visokorizični pridržavaju kodeksa ponašanja. Zahtjevi će se odnositi na podatke, dokumentaciju i sljedivost, pružanje informacija i transparentnost, ljudski nadzor, otpornost i točnost te bi bili obvezni za visokorizične UI sustave. Poduzeća koja bi uvela kodekse ponašanja za druge UI sustave učinila bi to dobrovoljno.

Smatralo se da je najpoželjnija opcija prikladna za ispunjavanje ciljeva prijedloga na najdjelotvorniji način. Najpoželjnjom opcijom zahtijeva se ograničen, ali i djelotvoran skup mjera od proizvođača i korisnika UI-ja, čime se smanjuju rizici od kršenja temeljnih prava i sigurnosti ljudi te se potiču djelotvoran nadzor i provedba jer se zahtjevi odnose samo na sustave s visokim rizikom od takvih kršenja. Stoga ta opcija omogućuje najniže troškove

²⁷ Europska komisija, [*Početna procjena učinka prijedloga pravnog akta Europskog parlamenta i Vijeća o utvrđivanju zahtjeva u pogledu umjetne inteligencije.*](#)

²⁸ Za pojedinosti o svim savjetovanjima koja su provedena vidjeti Prilog 2. procjeni učinka.

usklađivanja, pa se izbjegava nepotrebno usporavanje primjene zbog viših cijena i troškova usklađivanja. Kako bi se uklonili mogući nedostaci za MSP-ove, ta opcija uključuje nekoliko odredaba za potporu njihovoj usklađenosti i smanjenju troškova, uključujući stvaranje regulatornih izoliranih okruženja i obveze da se pri određivanju naknada za ocjenjivanje sukladnosti uzmu u obzir interesi MSP-ova.

Najpoželjnija opcija povećat će povjerenje građana u UI, poduzeća će dobiti pravnu sigurnost, a države članice neće imati razloga za jednostrano djelovanje koje bi fragmentiralo jedinstveno tržište. Zahvaljujući većoj potražnji zbog većeg povjerenja, većem broju dostupnih ponuda zbog pravne sigurnosti i nepostojanju zapreka prekograničnom kretanju UI sustava, jedinstveno tržište UI-ja vjerojatno će procvasti. Europska unija nastaviti će razvijati brzorastući UI ekosustav inovativnih usluga i proizvoda koji uključuju UI tehnologiju ili samostalnih UI sustava, što će dovesti do veće digitalne autonomije.

Poduzeća ili tijela javne vlasti koja razvijaju ili upotrebljavaju aplikacije UI-ja koje su vrlo rizične za sigurnost ili temeljna prava građana morala bi ispunjavati posebne zahtjeve i obveze. Ispunjavanje tih zahtjeva podrazumijevalo bi troškove od približno 6 000 EUR do 7 000 EUR za nabavu prosječno visokorizičnog UI sustava od približno 170 000 EUR do 2025. Korisnici UI-ja snosili bi i godišnje troškove za vrijeme posvećeno ljudskom nadzoru ondje gdje je on potreban, ovisno o slučaju primjene. Ti su troškovi procijenjeni na približno 5 000 EUR do 8 000 EUR na godinu. Troškovi provjere za dobavljače visokorizičnog UI-ja mogli bi iznositi dodatnih 3 000 EUR do 7 500 EUR. Poduzeća ili tijela javne vlasti koja razvijaju ili upotrebljavaju aplikacije UI-ja koje nisu klasificirane kao visokorizične imala bi tek minimalne obveze obavješćivanja. Međutim, mogla bi se odlučiti pridružiti drugima i zajedno s njima donijeti kodeks ponašanja kako bi ispunila odgovarajuće zahtjeve i osigurala pouzdanost svojih UI sustava. U tom bi slučaju troškovi iznosili najviše onoliko koliko iznose za visokorizične UI sustave, ali najvjerojatnije bi bili niži.

Učinci opcija politike na različite kategorije dionika (gospodarski subjekti/poslovni sektor, tijela za ocjenjivanje sukladnosti, tijela za normizaciju i druga javna tijela, pojedinci/gr građani, istraživači) detaljno su objašnjeni u Prilogu 3. procjeni učinka koja je priložena ovom prijedlogu.

3.4. Primjerenost i pojednostavnjenje propisa

U prijedlogu se utvrđuje obveza koja će se primjenjivati na dobavljače i korisnike visokorizičnih UI sustava. Dobavljačima koji razvijaju i stavljaju takve sustave na tržište Unije stvoriti će pravnu sigurnost i spriječiti zapreke prekograničnom pružanju usluga i proizvoda povezanih s UI-jem. Poduzećima koja koriste UI podići će povjerenje među klijentima. Kad je riječ o nacionalnim javnim upravama, povećat će se javno povjerenje u uporabu UI-ja i ojačati mehanizmi provedbe (uvođenjem europskog koordinacijskog mehanizma, osiguravanjem odgovarajućih kapaciteta i olakšavanjem revizija UI sustava uvođenjem novih zahtjeva u pogledu dokumentacije, sljedivosti i transparentnosti). Nadalje, tim će se okvirom predvidjeti posebne mjere za potporu inovacijama, uključujući regulatorna izolirana okruženja i posebne mjere kojima se malim korisnicima i dobavljačima visokorizičnih UI sustava pruža potpora u ispunjavanju novih pravila.

Prijedlog je posebno usmjeren i na jačanje konkurentnosti Europe i industrijskih temelja u području UI-ja. Osigurava se potpuna usklađenost s postojećim sektorskim zakonodavstvom Unije koje se primjenjuje na UI sustave (npr. na proizvode i usluge), čime će se omogućiti veća jasnoća i pojednostavniti provedba novih pravila.

3.5. Temeljna prava

Uporaba UI-ja s njegovim specifičnim karakteristikama (npr. netransparentnost, složenost, ovisnost o podacima, autonomno ponašanje) može nepovoljno utjecati na brojna temeljna prava utvrđena u Povelji Europske unije o temeljnim pravima („Povelja”). Ovim se prijedlogom želi osigurati visoka razina zaštite tih temeljnih prava i nastoje se riješiti različiti izvori rizika s pomoću jasno definiranog pristupa koji se temelji na riziku. Zahvaljujući skupu zahtjeva za pouzdani UI i proporcionalnim obvezama za sve sudionike lanca vrijednosti, prijedlogom će se poboljšati i promicati zaštita prava zaštićenih Poveljom: pravo na ljudsko dostojanstvo (članak 1.), poštovanje privatnog života i zaštita osobnih podataka (članci 7. i 8.), nediskriminacija (članak 21.) te ravnopravnost žena i muškaraca (članak 23.). Njime se nastoji spriječiti odvrćajući učinak na prava na slobodu izražavanja (članak 11.) i slobodu okupljanja (članak 12.) te osigurati zaštitu prava na djelotvoran pravni lijek i na pošteno suđenje, prava na obranu i pretpostavku nedužnosti (članci 47. i 48.) i opće načelo dobre uprave. Nadalje, kako je primjenjivo u određenim područjima, prijedlog će pozitivno utjecati na prava brojnih posebnih skupina, kao što su prava radnika na poštene i pravične radne uvjete (članak 31.), visoka razina zaštite potrošača (članak 38.), prava djeteta (članak 24.) i integracija osoba s invaliditetom (članak 26.). Relevantno je i pravo na visoku razinu zaštite okoliša i poboljšavanje kvalitete okoliša (članak 37.), među ostalim u pogledu zdravlja i sigurnosti ljudi. Obveze koje se odnose na *ex ante* ispitivanje, upravljanje rizikom i ljudski nadzor isto će tako olakšati poštovanje drugih temeljnih prava jer će se rizik od pogrešnih ili pristranih odluka potpomognutih UI-jem u važnim područjima kao što su obrazovanje i osposobljavanje, zapošljavanje, važne usluge, kazneni progon i sudstvo svesti na najmanju moguću mjeru. Ako i dalje bude kršenja temeljnih prava, omogućit će se djelotvorna pravna zaštita za pogođene osobe tako što će se osigurati transparentnost i sljedivost UI sustava u kombinaciji sa snažnim *ex post* kontrolama.

Prijedlogom se uvode određena ograničenja slobode poduzetništva (članak 16.) i slobode umjetnosti i znanosti (članak 13.) radi usklađenosti s prevladavajućim razlozima od javnog interesa kao što su zdravlje, sigurnost, zaštita potrošača i zaštita drugih temeljnih prava („odgovorne inovacije”) pri razvoju i uporabi visokorizične UI tehnologije. Ta su ograničenja proporcionalna i ograničena na najmanju moguću razinu potrebnu za sprečavanje i smanjenje ozbiljnih sigurnosnih rizika i mogućih kršenja temeljnih prava.

Veće obveze u pogledu transparentnosti neće nerazmjerno utjecati ni na pravo na zaštitu intelektualnog vlasništva (članak 17. stavak 2.) jer će biti ograničene samo na minimalne informacije koje su nužne da bi pojedinci ostvarili pravo na djelotvoran pravni lijek i na potrebnu razinu transparentnosti nadzornih tijela i tijela kaznenog progona u skladu s njihovim ovlastima. Svako otkrivanje informacija provodit će se u skladu s relevantnim propisima u tom području, među ostalim s Direktivom 2016/943 o zaštiti neotkrivenih znanja i iskustva te poslovnih informacija (poslovne tajne) od nezakonitog pribavljanja, korištenja i otkrivanja. Ako se tijelima javne vlasti i prijavljenim tijelima mora dati pristup povjerljivim informacijama ili izvornom kodu kako bi ispitala usklađenost s bitnim obvezama, ona se obvezuju na zaštitu povjerljivosti.

4. UTJECAJ NA PRORAČUN

Države članice morat će imenovati nadzorna tijela koja će biti zadužena za provedbu zakonodavnih zahtjeva. Njihova nadzorna funkcija mogla bi se temeljiti na postojećim aranžmanima, koji primjerice vrijede za tijela za ocjenjivanje sukladnosti ili nadzor tržišta, ali zahtijevala bi odgovarajuće stručno tehnološko znanje i financijska sredstva. Ovisno o već

postojećoj strukturi u svakoj državi članici, to bi moglo podrazumijevati od 1 do 25 ekvivalenata punog radnog vremena po državi članici.

Detaljan pregled uključenih troškova nalazi se u „financijskom izvještaju” povezanom s ovim prijedlogom.

5. DRUGI ELEMENTI

5.1. Planovi provedbe i mehanizmi praćenja, evaluacije i izvješćivanja

Neophodno je predvidjeti robustan mehanizam praćenja i evaluacije kako bi se osiguralo uspješno ostvarenje ciljeva prijedloga. Komisija će biti zadužena za praćenje učinaka prijedloga. Uspostavit će sustav za registraciju samostalnih visokorizičnih aplikacija UI-ja u javnoj bazi podataka na razini EU-a. Ta će registracija nadležnim tijelima, korisnicima i drugim zainteresiranim osobama omogućiti i da provjere je li visokorizični UI sustav u skladu sa zahtjevima utvrđenima u prijedlogu i da provode pojačani nadzor nad UI sustavima koji su rizičniji za temeljna prava. Kako bi se prikupili podaci za tu bazu podataka, dobavljači UI-ja morat će dostavljati smislene informacije o svojim sustavima i ocjenjivanju sukladnosti koje je provedeno na tim sustavima.

Usto, dobavljači UI-ja bit će dužni nacionalnim nadležnim tijelima prijavljivati ozbiljne incidente ili neispravnosti kojima se krše obveze u području temeljnih prava čim saznaju za njih te o svim provedenim povratima ili povlačenjima UI sustava s tržišta. Nacionalna nadležna tijela zatim će istražiti te incidente ili neispravnosti, prikupiti sve potrebne informacije i redovito ih prenositi Komisiji uz odgovarajuće metapodatke. Komisija će dopuniti te informacije o incidentima opsežnom analizom cjelokupnog tržišta UI-ja.

Komisija će objaviti izvješće u kojem se evaluiira i preispituje predloženi okvir za UI pet godina od datuma početka njegove primjene.

5.2. Detaljno obrazloženje posebnih odredaba prijedloga

5.2.1. PODRUČJE PRIMJENE I DEFINICIJE (GLAVA I.)

U **glavi I.** definiraju se predmet uredbe i područje primjene novih pravila koja obuhvaćaju stavljanje na tržište, stavljanje u uporabu i korištenje UI sustava. Utvrđuju se i definicije koje se upotrebljavaju u cijelom instrumentu. Nastoji se da definicija UI sustava u pravnom okviru bude što tehnološki neutralnija i otpornija na buduće promjene, uzimajući pritom u obzir brz tehnološke i tržišne promjene povezane s UI-jem. Kako bi se osigurala potrebna pravna sigurnost, glava I. dopunjena je Prilogom I. s detaljnim popisom pristupa i tehnika za razvoj UI-ja, koji će Komisija prilagođavati u skladu s novim tehnološkim kretanjima. Jasno su definirani i važni sudionici u cijelom lancu vrijednosti UI-ja, kao što su dobavljači i korisnici UI sustava koji obuhvaćaju i javne i privatne operatore kako bi se osigurali jednaki uvjeti.

5.2.2. ZABRANJENE PRAKSE U PODRUČJU UMJETNE INTELIGENCIJE (GLAVA II.)

U **glavi II.** utvrđuje se popis zabranjenog UI-ja. Uredba se temelji na pristupu temeljenom na riziku, pri čemu se razlikuju uporabe UI-ja kojima se stvara i. neprihvatljiv rizik, ii. visoki rizik i iii. nizak ili minimalan rizik. Popis zabranjenih praksi u glavi II. obuhvaća sve UI sustave čija se uporaba smatra neprihvatljivom jer je protivna vrijednostima Unije, na primjer zbog kršenja temeljnih prava. Zabrane se odnose na prakse koje imaju znatan potencijal za manipuliranje osobama primjenom subliminalnih tehnika koje djeluju na nesvjesnoj razini ili iskorištavanje slabosti specifičnih ranjivih skupina kao što su djeca ili osobe s invaliditetom kako bi se bitno promijenilo njihovo ponašanje na način koji će njima ili drugim osobama vjerojatno prouzročiti psihološku ili tjelesnu štetu. Druge manipulativne ili izrabljivačke prakse koje utječu na odrasle i koje bi UI sustavi mogli olakšati mogle bi se obuhvatiti

postojećim propisima o zaštiti podataka, zaštiti potrošača i digitalnim uslugama kojima se osigurava pravilno informiranje pojedinaca i slobodno odlučivanje o podvrgavanju izradi profila ili drugim praksama koje bi mogle utjecati na njihovo ponašanje. Prijedlogom se zabranjuje i društveno vrednovanje u opće svrhe koje se temelji na UI-ju i provode ga tijela javne vlasti. Naposljetku, zabranjuje se i primjena sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona, osim ako se primjenjuju određene ograničene iznimke.

5.2.3. VISOKORIZIČNI UI SUSTAVI (GLAVA III.)

Glava III. sadržava posebna pravila za UI sustave koji stvaraju visok rizik za zdravlje i sigurnost ili temeljna prava pojedinaca. U skladu s pristupom temeljenom na riziku ti visokorizični UI sustavi dopušteni su na europskom tržištu ako su u skladu s određenim obveznim zahtjevima i *ex ante* ocjenjivanjem sukladnosti. UI sustavi klasificiraju se kao visokorizični na temelju njihove namjene, u skladu s postojećim zakonodavstvom u području sigurnosti proizvoda. Stoga klasifikacija UI sustava kao visokorizičnog ne ovisi samo o njegovoj funkciji, nego i o njegovoj konkretnoj namjeni i načinima uporabe.

U poglavlju 1. glave III. navode se pravila klasifikacije i utvrđuju dvije glavne kategorije visokorizičnih UI sustava:

- UI sustavi koji su namijenjeni za uporabu kao sigurnosni sastavni dijelovi proizvoda koji podliježu *ex ante* ocjenjivanju sukladnosti koje provode treće strane,
- ostali samostalni UI sustavi koji ponajprije imaju posljedice na temeljna prava i koji su izričito navedeni u Prilogu III.

Popis visokorizičnih UI sustava u Prilogu III. sadržava ograničen broj UI sustava čiji su se rizici već ostvarili ili će se vjerojatno ostvariti u bliskoj budućnosti. Kako bi se osiguralo da se Uredba može prilagoditi novim primjenama i aplikacijama UI-ja, Komisija može proširiti popis visokorizičnih UI sustava koji se upotrebljavaju unutar određenih unaprijed utvrđenih područja tako da primijeni skup kriterija i metodologiju procjene rizika.

U poglavlju 2. utvrđuju se pravni zahtjevi za visokorizične UI sustave u pogledu podataka i upravljanja podacima, dokumentacije i vođenja evidencije, transparentnosti i informiranja korisnika, ljudskog nadzora, otpornosti, točnosti i sigurnosti. Predloženi minimalni zahtjevi već su razina prema kojoj djeluju mnogi revni operateri te su rezultat dviju godina pripremnog rada provedenog na temelju etičkih smjernica stručne skupine na visokoj razini²⁹, a probno ih je primijenilo više od 350 organizacija³⁰. Uvelike su usklađeni i s drugim međunarodnim preporukama i načelima, čime se osigurava da je predloženi okvir za UI spojiv s onima koje su donijeli međunarodni trgovinski partneri EU-a. Točna tehnička rješenja za postizanje usklađenosti s tim zahtjevima mogu se osigurati standardima ili drugim tehničkim specifikacijama ili se mogu razviti na neki drugi način u skladu s općim inženjerskim ili znanstvenim spoznajama i prema slobodnoj odluci dobavljača UI sustava. Ta je fleksibilnost posebno važna jer dobavljačima UI sustava omogućuje da odaberu način na koji će ispuniti zahtjeve, uzimajući u obzir najnovija dostignuća te tehnološki i znanstveni napredak u tom području.

²⁹ Stručna skupina na visokoj razini za umjetnu inteligenciju, [Etičke smjernice za pouzdani UI](#), 2019.

³⁰ Podržala ih je i Komisija u svojoj Komunikaciji o antropocentričnom pristupu UI-ju iz 2019.

U poglavlju 3. utvrđuje se jasan skup horizontalnih obveza za dobavljače visokorizičnih UI sustava. Utvrđuju se i proporcionalne obveze za korisnike i druge sudionike u lancu vrijednosti UI-ja (npr. uvoznici, distributeri, ovlašteni zastupnici).

U poglavlju 4. utvrđuje se okvir za prijavljena tijela koja će sudjelovati kao neovisne treće strane u postupcima ocjenjivanja sukladnosti, dok se u poglavlju 5. detaljno opisuju postupci ocjenjivanja sukladnosti za svaku vrstu visokorizičnog UI sustava. Pristupom koji uključuje ocjenjivanje sukladnosti nastoji se što više smanjiti opterećenje za gospodarske subjekte, ali i za prijavljena tijela, čiji će se kapacitet s vremenom morati postupno povećavati. UI sustavi namijenjeni za uporabu kao sigurnosni sastavni dijelovi proizvoda koji su regulirani propisima novog zakonodavnog okvira (npr. strojevi, igračke, medicinski proizvodi itd.) podlijeгат će istim *ex ante* i *ex post* mehanizmima sukladnosti i provedbe kao i proizvodi čiji su sastavni dijelovi. Ključna je razlika u tome što će se *ex ante* i *ex post* mehanizmima osigurati usklađenost ne samo sa zahtjevima utvrđenima u sektorskom zakonodavstvu nego i sa zahtjevima utvrđenima u ovoj Uredbi.

Za samostalne visokorizične UI sustave iz Priloga III. uspostaviti će se novi sustav sukladnosti i provedbe. To je u skladu s modelom propisa novog zakonodavnog okvira, odnosno primjenom unutarnjih kontrolnih provjera koje obavljaju dobavljači, uz iznimku sustava za daljinsku biometrijsku identifikaciju koji bi podlijeгali ocjenjivanjima sukladnosti koje provode treće strane. Opsežno *ex ante* ocjenjivanje sukladnosti s pomoću unutarnjih provjera, u kombinaciji s dosljednom *ex post* provedbom, moglo bi biti djelotvorno i razumno rješenje za te sustave s obzirom na ranu fazu regulatorne intervencije i činjenicu da je sektor UI-ja vrlo inovativan i da se stručno znanje za revizije tek počelo gomilati. Ocjenjivanje primjenom unutarnjih provjera za „samostalne” visokorizične UI sustave zahtijevalo bi potpunu, djelotvornu i pravilno dokumentiranu *ex ante* usklađenost sa svim zahtjevima iz Uredbe i usklađenost s pouzdanim sustavima upravljanja kvalitetom i rizikom te praćenjem nakon stavljanja na tržište. Nakon što dobavljač provede odgovarajuće ocjenjivanje sukladnosti, trebao bi registrirati te samostalne visokorizične UI sustave u bazi podataka EU-a, koju će voditi Komisija, kako bi se poboljšali javna transparentnost i nadzor te ojačao *ex post* nadzor koji provode nadležna tijela. S druge strane, kako bi se osigurala dosljednost s postojećim propisima o sigurnosti proizvoda, ocjenjivanje sukladnosti UI sustava koji su sigurnosni sastavni dijelovi proizvoda slijedit će sustav s postupcima ocjenjivanja sukladnosti koje provode treće strane, a koji je već uspostavljen relevantnim propisima o sigurnosti proizvoda. Bit će potrebna nova *ex ante* ponovna ocjenjivanja sukladnosti u slučaju bitnih izmjena UI sustava (osobito promjena koje prelaze ono što je dobavljač unaprijed odredio u svojoj tehničkoj dokumentaciji i što je provjereno u trenutku *ex ante* ocjenjivanja sukladnosti).

5.2.4. OBVEZE U POGLEDU TRANSPARENTNOSTI ZA ODREĐENE UI SUSTAVE (GLAVA IV.)

Glava IV. odnosi se na određene UI sustave kako bi se uzeli u obzir posebni rizici od manipulacije koje predstavljaju. Obveze u pogledu transparentnosti primjenjuju se za sustave koji: i. komuniciraju s ljudima, ii. služe za otkrivanje emocija ili određivanje povezanosti sa (socijalnim) kategorijama na temelju biometrijskih podataka ili iii. stvaraju sadržaj ili manipuliraju njime („deep fakes”). Ako su osobe u interakciji s UI sustavom ili se izvodi automatizirano prepoznavanje njihovih emocija ili karakteristika, mora ih se o tome obavijestiti. Ako se UI sustav upotrebljava za stvaranje ili manipuliranje slikovnim sadržajem, audiosadržajem ili videosadržajem u kojem postoji znatna sličnost s autentičnim sadržajem, trebala bi postojati obveza navođenja da je taj sadržaj stvoren automatiziranim sredstvima, uz iznimke u zakonite svrhe (kazneni progon, sloboda izražavanja). To pojedincima omogućuje da donose utemeljene odluke ili odustanu od sudjelovanja u određenim situacijama.

5.2.5. MJERE ZA POTPORU INOVACIJAMA (GLAVA V.)

U **glavi V.** pridonosi se cilju stvaranja pravnog okvira koji je prilagođen inovacijama, spreman na buduće promjene i otporan na poremećaje. U tu se svrhu nacionalna nadležna tijela potiču na uspostavu regulatornih izoliranih okruženja i utvrđuje se osnovni okvir za upravljanje, nadzor i odgovornost. Regulatornim izoliranim okruženjima za UI uspostavlja se kontrolirano okruženje za testiranje inovativnih tehnologija u ograničenom vremenu na temelju plana testiranja dogovorenog s nadležnim tijelima. Glava V. sadržava i mjere za smanjenje regulatornog opterećenja za MSP-ove i novoosnovana (*start-up*) poduzeća.

5.2.6. UPRAVLJANJE I PROVEDBA (GLAVE VI., VII. I VIII.)

U **glavi VI.** utvrđuju se sustavi upravljanja na razini Unije i nacionalnoj razini. Na razini unije na temelju prijedloga osniva se Europski odbor za umjetnu inteligenciju („Odbor”), koji čine predstavnici država članica i Komisije. Odbor će olakšati neometanu, djelotvornu i usklađenu provedbu ove Uredbe tako što će doprinosti djelotvornoj suradnji nacionalnih nadzornih tijela i Komisije te će Komisiji pružati savjete i stručno znanje. Ujedno će prikupljati i razmjenjivati najbolje primjere iz prakse među državama članicama.

Na nacionalnoj razini države članice morat će odrediti jedno ili više nacionalnih nadležnih tijela, a među njima i nacionalno nadzorno tijelo, za nadzor primjene i provedbe Uredbe. Europski nadzornik za zaštitu podataka djelovat će kao nadležno tijelo za nadzor nad institucijama, agencijama i tijelima Unije obuhvaćenima područjem primjene ove Uredbe.

Glavom VII. želi se olakšati praćenje koje provode Komisija i nacionalna tijela, i to uspostavom baze podataka na razini EU-a za samostalne visokorizične UI sustave koji ponajprije imaju posljedice na temeljna prava. Tom bazom podataka upravljat će Komisija, a podatke koji će se u nju unositi dostavljat će dobavljači UI sustava, koji će morati registrirati svoje sustave prije nego što ih stave na tržište ili na drugi način stave u uporabu.

U **glavi VIII.** utvrđuju se obveze praćenja i izvješćivanja za dobavljače UI sustava u pogledu praćenja nakon stavljanja na tržište te prijavljivanja i istraživanja incidenata i neispravnosti povezanih s UI-jem. Tijela za nadzor tržišta ujedno bi kontrolirala tržište i istraživala usklađenost s obvezama i zahtjevima za sve visokorizične UI sustave koji su već stavljeni na tržište. Tijela za nadzor tržišta imala bi sve ovlasti na temelju Uredbe (EU) 2019/1020 o nadzoru tržišta. *Ex post* provedbom trebalo bi se osigurati da nakon stavljanja UI sustava na tržište tijela javne vlasti imaju ovlasti i resurse da interveniraju ako UI sustavi izazivaju neočekivane rizike koji zahtijevaju brzo djelovanje. Pratit će i ispunjavaju li operateri odgovarajuće obveze utvrđene u Uredbi. U prijedlogu nije predviđeno automatsko osnivanje dodatnih tijela na razini država članica. Države članice stoga mogu imenovati (i osloniti se na stručno znanje) postojećih sektorskih tijela, kojima bi se dale i ovlasti za praćenje i provođenje odredbi Uredbe.

Svime time ne dovode se u pitanje postojeći sustav ni dodjela ovlasti za *ex post* provedbu obveza u pogledu temeljnih prava u državama članicama. Ako je to potrebno za izvršavanje njihovih ovlasti, postojeća nadzorna tijela i tijela kaznenog progona imat će i ovlast zatražiti svu dokumentaciju vođenu na temelju ove Uredbe te joj pristupiti, a prema potrebi će moći i zatražiti od tijela za nadzor tržišta da organiziraju testiranje visokorizičnog UI sustava tehničkim sredstvima.

5.2.7. KODEKSI PONAŠANJA (GLAVA IX.)

U **glavi IX.** utvrđuje se okvir za izradu kodeksa ponašanja kojima se nastoji potaknuti dobavljače UI sustava koji nisu visokorizični da dobrovoljno primjenjuju obvezne zahtjeve za visokorizične UI sustave (kako je navedeno u glavi III.). Dobavljači UI sustava koji nisu visokorizični mogu i sami izraditi i uvesti kodekse ponašanja. Ti kodeksi mogu uključivati i

dobrovoljne obveze koje se, primjerice, odnose na okolišnu održivost, pristupačnost za osobe s invaliditetom, sudjelovanje dionika u projektiranju i razvoju UI sustava te raznolikost razvojnih timova.

5.2.8. *ZAVRŠNE ODREDBE (GLAVE X., XI. I XII.)*

U **glavi X.** ističe se da su sve strane dužne poštovati povjerljivost informacija i podataka te se utvrđuju pravila za razmjenu informacija dobivenih tijekom provedbe Uredbe. Glava X. uključuje i mjere za osiguravanje djelotvorne provedbe Uredbe primjenom djelotvornih, proporcionalnih i odvraćajućih sankcija za kršenje odredaba.

U **glavi XI.** utvrđuju se pravila za izvršavanje delegiranih i provedbenih ovlasti. Prijedlogom se Komisija ovlašćuje da prema potrebi donosi provedbene akte kako bi se osigurala ujednačena provedba Uredbe ili delegirane akte radi ažuriranja ili dopunjavanja popisa iz priloga od I. do VII.

Glava XII. sadržava obvezu prema kojoj Komisija mora redovito procjenjivati potrebu za ažuriranjem Priloga III. i sastavljati redovita izvješća o evaluaciji i preispitivanju Uredbe. U njoj se utvrđuju i završne odredbe, uključujući diferencirano prijelazno razdoblje za početni datum primjenjivosti Uredbe kako bi se svim uključenim stranama olakšala neometana provedba.

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA**O UTVRĐIVANJU USKLAĐENIH PRAVILA O UMJETNOJ INTELIGENCIJI (AKT O UMJETNOJ INTELIGENCIJI) I IZMJENI ODREĐENIH ZAKONODAVNIH AKATA UNIJE**

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 nacрта zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora³¹,

uzimajući u obzir mišljenje Odbora regija³²,

u skladu s redovnim zakonodavnim postupkom,

budući da:

- (1) Svrha je ove Uredbe poboljšati funkcioniranje unutarnjeg tržišta utvrđivanjem ujednačenog pravnog okvira, posebno za razvoj, stavljanje na tržište i uporabu umjetne inteligencije u skladu s vrijednostima Unije. Uredbom je obuhvaćeno nekoliko prevladavajućih razloga od općeg interesa, kao što je visoka razina zaštite zdravlja, sigurnosti i temeljnih prava, te se njome osigurava slobodno prekogranično kretanje robe i usluga koje se temelje na UI-ju, čime se sprečava da države članice nameću ograničenja na razvoj, stavljanje na tržište i uporabu UI sustava osim ako je to izričito odobreno ovom Uredbom.
- (2) Sustavi umjetne inteligencije (UI sustavi) mogu se lako upotrebljavati u različitim sektorima gospodarstva i društva, među ostalim preko granica, te se kretati unutar Unije. Neke su države članice već razmotrile donošenje nacionalnih pravila kojima bi zajamčile sigurnost umjetne inteligencije te njezin razvoj i uporabu u skladu s obvezama u području temeljnih prava. Različita nacionalna pravila mogu uzrokovati fragmentaciju unutarnjeg tržišta i smanjiti pravnu sigurnost za operatere koji razvijaju ili upotrebljavaju UI sustave. Stoga bi u cijeloj Uniji trebalo osigurati dosljednu i visoku razinu zaštite, dok bi razlike koje otežavaju slobodno kretanje UI sustava te povezanih proizvoda i usluga unutar unutarnjeg tržišta trebalo spriječiti utvrđivanjem jedinstvenih 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 posebna pravila o zaštiti pojedinaca pri obradi osobnih podataka u vezi s ograničenjima uporabe UI sustava za daljinsku biometrijsku identifikaciju u

³¹ SL C [...], [...], str. [...].

³² SL C [...], [...], str. [...].

stvarnom vremenu na javnim mjestima za potrebe kaznenog progona dio ove Uredbe koji se odnosi na ta posebna pravila primjereno je temeljiti na članku 16. UFEU-a. S obzirom na ta posebna pravila i pozivanje na članak 16. UFEU-a, primjereno je zatražiti mišljenje Europskog odbora za zaštitu podataka.

- (3) Umjetna inteligencija skupina je tehnologija koja se brzo razvija i može pridonijeti nizu gospodarskih i društvenih koristi u cijelom spektru sektora i društvenih aktivnosti. Zahvaljujući boljem predviđanju, optimizaciji operacija i dodjele resursa te personalizaciji digitalnih rješenja koja su dostupna pojedincima i organizacijama, uporaba umjetne inteligencije može poduzećima omogućiti ključne konkurentske prednosti i pridonijeti društveno i ekološki korisnim rezultatima, na primjer u zdravstvenoj zaštiti, poljoprivredi, obrazovanju i osposobljavanju, upravljanju infrastrukturuom, energetici, prometu i logistici, javnim uslugama, sigurnosti, pravosuđu, učinkovitom korištenju resursa i energije te ublažavanju klimatskih promjena i prilagodbi tim promjenama.
- (4) Međutim, ovisno o okolnostima njezine specifične primjene i uporabe, umjetna inteligencija može stvoriti rizike i uzrokovati štetu javnim interesima i pravima koja su zaštićena pravom Unije. Takva šteta može biti materijalna i nematerijalna.
- (5) Stoga je potreban pravni okvir kojim se utvrđuju usklađena pravila o umjetnoj inteligenciji kako bi se poticali razvoj, uporaba i prihvatanje umjetne inteligencije na unutarnjem tržištu kojima se istodobno ostvaruje visoka razina zaštite javnih interesa, kao što su zdravlje i sigurnost te zaštita temeljnih prava koja su priznata i zaštićena pravom Unije. Kako bi se postigao taj cilj, trebalo bi utvrditi pravila kojima se uređuje stavljanje na tržište i stavljanje u uporabu određenih UI sustava, te tako osigurati neometano funkcioniranje unutarnjeg tržišta i omogućiti da načela slobodnog kretanja robe i usluga pogoduju tim sustavima. Ovom se Uredbom, zahvaljujući tim pravilima, pridonosi Unijinu cilju globalnog vodstva u razvoju sigurne, pouzdane i etične umjetne inteligencije koji je odredilo Europsko vijeće³³ i osigurava se zaštita etičkih načela u skladu s izričitim zahtjevom Europskog parlamenta³⁴.
- (6) Trebalo bi jasno definirati pojam UI sustava kako bi se osigurala pravna sigurnost i pritom omogućila fleksibilnost za prilagođavanje budućem tehnološkom napretku. Ta bi se definicija trebala temeljiti na ključnim funkcionalnim karakteristikama softvera, a posebno na sposobnosti da za zadani skup ciljeva koje odredi čovjek generira izlazne rezultate kao što su sadržaj, predviđanja, preporuke ili odluke koji utječu na okolinu s kojom je sustav u interakciji, bilo u fizičkoj ili digitalnoj dimenziji. UI sustavi mogu se projektirati tako da rade s različitom razinom autonomije i da se upotrebljavaju samostalno ili kao sastavni dio nekog proizvoda, bez obzira na to je li sustav fizički integriran u proizvod (ugrađen) ili izvršava funkciju proizvoda bez integriranja u njega (neugrađen). Definiciju UI sustava trebalo bi dopuniti popisom posebnih tehnika i pristupa primijenjenih u njegovu razvoju, koji bi trebalo ažurirati s obzirom na tržišne i tehnološke promjene, i to delegiranim aktima Komisije za izmjenu tog popisa.
- (7) Pojam biometrijskih podataka koji se upotrebljava u ovoj Uredbi u skladu je s pojmom biometrijskih podataka kako je definiran člankom 4. točkom 14. Uredbe (EU)

³³ Europsko vijeće, Izvanredni sastanak Europskog vijeća (1. i 2. listopada 2020.) – zaključci, EUCO 13/20, 2020., str. 6.

³⁴ 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).

2016/679 Europskog parlamenta i Vijeća³⁵, člankom 3. točkom 18. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća³⁶ i člankom 3. točkom 13. Direktive (EU) 2016/680 Europskog parlamenta i Vijeća³⁷ te bi se trebao tumačiti dosljedno tim odredbama.

- (8) Pojam sustava za daljinsku biometrijsku identifikaciju koji se upotrebljava u ovoj Uredbi trebalo bi definirati funkcionalno, kao UI sustav namijenjen za daljinsko identificiranje pojedinaca usporedbom biometrijskih podataka osobe s biometrijskim podacima iz referentne baze podataka, pri čemu se ne može unaprijed znati hoće li ciljana osoba biti prisutna i može li je se identificirati, bez obzira na tehnologiju, postupke ili vrste biometrijskih podataka koji se upotrebljavaju. S obzirom na njihove različite karakteristike i različite načine korištenja, ali i na različite prisutne rizike, trebalo bi razlikovati sustav za daljinsku biometrijsku identifikaciju u stvarnom vremenu i sustav za naknadnu daljinsku biometrijsku identifikaciju. U sustavima za daljinsku biometrijsku identifikaciju u stvarnom vremenu prikupljanje biometrijskih podataka, usporedba i identifikacija odvijaju se trenutačno, gotovo trenutačno ili u svakom slučaju bez znatnog kašnjenja. Reguliranjem kratkih kašnjenja trebalo bi onemogućiti zaobilaženje pravila ove Uredbe o uporabi tih UI sustava u stvarnom vremenu. Sustavi u stvarnom vremenu uključuju uporabu materijala snimljenog „uživo” ili „gotovo uživo”, kao što je videozapis snimljen kamerom ili drugim uređajem sa sličnom funkcijom. S druge strane, u sustavima za naknadnu identifikaciju biometrijski su podaci već prethodno prikupljeni te se usporedba i identifikacija vrše tek nakon znatnog kašnjenja. To uključuje materijal snimljen prije nego što je sustav upotrijebljen za identifikaciju predmetnih pojedinaca, kao što su fotografije ili videozapisi snimljeni nadzornim kamerama ili privatnim uređajima.
- (9) Pojam javnog mjesta za potrebe ove Uredbe trebalo bi shvatiti kao svako fizičko mjesto koje je dostupno javnosti, bez obzira na to je li u privatnom ili javnom vlasništvu. Dakle, taj pojam ne obuhvaća mjesta koja su privatne naravi i obično nisu slobodno dostupna trećim stranama, među ostalim ni tijelima kaznenog progona, osim ako su te strane izričito pozvane ili im je odobren pristup; to su primjerice stambeni objekti, privatni klubovi, uredi, skladišta i tvornice. Nisu obuhvaćeni ni internetski prostori jer oni nisu fizički prostori. Međutim, samo to što se nekom mjestu može pristupiti po određenim uvjetima, kao što su ulaznice ili dobna ograničenja, ne znači da to mjesto nije javno u smislu ove Uredbe. Prema tome, uz javna mjesta kao što su ulice, odgovarajući dijelovi vladinih zgrada i većina prometne infrastrukture, i mjesta kao što su kina, kazališta, trgovine i trgovački centri obično su javna. Ipak, to je li određeno mjesto javno trebalo bi utvrditi u svakom slučaju posebno i pritom uzeti u obzir specifične okolnosti konkretne situacije.

³⁵ 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.).

³⁶ 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.)

³⁷ 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 (Direktiva o zaštiti podataka pri izvršavanju zakonodavstva) (SL L 119, 4.5.2016., str. 89.).

- (10) Kako bi se osigurali jednaki uvjeti i djelotvorna zaštita prava i sloboda pojedinaca u cijeloj Uniji, pravila utvrđena u ovoj Uredbi 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 korisnike UI sustava s poslovnim nastanom u Uniji.
- (11) Određeni bi UI sustavi zbog svojeg digitalnog karaktera trebali biti obuhvaćeni područjem primjene ove Uredbe čak i ako nisu stavljeni ni na tržište ni u uporabu niti se upotrebljavaju u Uniji. To se, primjerice, odnosi na operatera s poslovnim nastanom u Uniji koji od operatera s poslovnim nastanom izvan Unije naruči određene usluge povezane sa zadaćom koju obavlja UI sustav koji bi pripadao u visokorizične sustave i koji bi mogao utjecati na pojedince u Uniji. U tim bi okolnostima UI sustav kojim se služi operater izvan Unije mogao obrađivati podatke koji su zakonito prikupljeni u Uniji i preneseni iz nje te dostaviti izlazni rezultat UI sustava koji se temelji na toj obradi operateru ugovaratelju u Uniji, a da taj UI sustav nije stavljen ni na tržište ni u uporabu niti se upotrebljava u Uniji. Kako bi se spriječilo zaobilaženje ove Uredbe i osigurala djelotvorna zaštita pojedinaca u Uniji, ova bi se Uredba trebala primjenjivati i na dobavljače i korisnike UI sustava koji imaju poslovni nastan u trećoj zemlji ako se u Uniji upotrebljavaju izlazni rezultati tih sustava. Međutim, kako bi se uzeli u obzir postojeći aranžmani i specifične potrebe za 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 koje djeluju u okviru međunarodnih sporazuma koji su na nacionalnoj ili europskoj razini sklopljeni s Unijom ili njezinim državama članicama za suradnju u područjima kaznenog progona i pravosuđa. Riječ je o bilateralnim sporazumima sklopljenima između država članica i trećih zemalja ili između Europske unije, Europolu i drugih agencija EU-a te trećih zemalja i međunarodnih organizacija.
- (12) Ova bi se Uredba trebala primjenjivati i na institucije, urede, tijela i agencije Unije ako djeluju kao dobavljači ili korisnici UI sustava. UI sustave koji se razvijaju ili upotrebljavaju isključivo u vojne svrhe trebalo bi izostaviti iz područja primjene ove Uredbe ako je ta uporaba u isključivoj nadležnosti zajedničke vanjske i sigurnosne politike uređene na temelju glave V. Ugovora o Europskoj uniji (UEU). Ovom Uredbom ne bi se trebale dovoditi u pitanje odredbe o odgovornosti pružatelja posredničkih usluga iz Direktive 2000/31/EZ Europskog parlamenta i Vijeća [kako je izmijenjena Aktom o digitalnim uslugama].
- (13) Kako bi se osigurala dosljedna i visoka razina zaštite javnih interesa u pogledu zdravlja, sigurnosti i temeljnih prava, trebalo bi utvrditi zajedničke normativne standarde za sve visokorizične UI sustave. Ti bi standardi trebali biti dosljedni s Poveljom Europske unije o temeljnim pravima (Povelja) te bi trebali biti nediskriminirajući i usklađeni s međunarodnim trgovinskim obvezama Unije.
- (14) Kako bi se uveo proporcionalan i djelotvoran skup obvezujućih pravila za UI sustave, trebalo bi slijediti jasno definiran pristup koji se temelji 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 prakse u području umjetne inteligencije, utvrditi zahtjeve za visokorizične UI sustave i obveze za relevantne operatore te utvrditi obveze u pogledu transparentnosti za određene UI sustave.
- (15) Osim brojnih korisnih primjena umjetne inteligencije, ta se tehnologija može i zloupotrijebiti te omogućiti nove i moćne alate za manipulativne i izrabljivačke prakse te prakse socijalne kontrole. Takve su prakse iznimno štetne i trebalo bi ih zabraniti jer su protivne Unijanim vrijednostima poštovanja ljudskog dostojanstva, slobode,

ravnopravnosti, demokracije i vladavine prava te temeljnim pravima Unije, uključujući pravo na nediskriminaciju, zaštitu podataka i privatnost te prava djeteta.

- (16) Trebalo bi zabraniti stavljanje na tržište, stavljanje u uporabu ili primjenu određenih UI sustava kojima se želi promijeniti čovjekovo ponašanje, čime se može izazvati tjelesna ili psihološka šteta. U takvim UI sustavima primjenjuju se subliminalni elementi koje pojedinci ne mogu percipirati ili se iskorištavaju ranjivosti koje djeca i odrasli mogu imati zbog svoje dobi te fizičkih ili mentalnih poteškoća. Pritom se njima želi bitno promijeniti ponašanje osobe na način koji uzrokuje ili bi mogao uzrokovati štetu toj ili nekoj drugoj osobi. Ta se namjera ne može pretpostaviti ako mijenjanje ljudskog ponašanja proizlazi iz čimbenika koji su izvan UI sustava i kontrole dobavljača ili korisnika. Zabrana ne bi trebala kočiti istraživanja u zakonite svrhe koja se odnose na takve UI sustave ako ta istraživanja ne uključuju uporabu UI sustava u odnosima između ljudi i strojeva koji bi mogli naštetiti pojedincima i ako se provode u skladu s priznatim etičkim standardima za znanstvena istraživanja.
- (17) UI sustavi koji omogućuju društveno vrednovanje pojedinaca u opće svrhe koje provode tijela javne vlasti ili koje se provodi u njihovo ime mogu prouzročiti diskriminatorne krajnje ishode i isključivanje 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 vjerodostojnost pojedinaca na temelju njihova društvenog ponašanja u različitim kontekstima ili poznatih ili predviđenih osobnih obilježja ili obilježja osobnosti. Društveni rejting dobiven takvim UI sustavima može uzrokovati štetno ili nepovoljno postupanje prema pojedincima ili cijelim skupinama pojedinaca u društvenim kontekstima koji nisu povezani s kontekstom u kojima su podaci izvorno generirani ili prikupljeni ili štetno postupanje koje je nerazmjerno ili neopravdano u odnosu na težinu posljedica njihova društvenog ponašanja. Stoga bi takve UI sustave trebalo zabraniti.
- (18) Uporaba UI sustava za daljinsku biometrijsku identifikaciju pojedinaca u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona smatra se znatnim kršenjem prava i sloboda uključenih osoba u onoj mjeri u kojoj može utjecati na privatni život velikog dijela stanovništva, pobuditi doživljaj stalnog nadzora i neizravno odvratiti od ostvarenja slobode okupljanja i drugih temeljnih prava. Osim toga, neposrednost učinka i ograničene mogućnosti za dodatne provjere ili ispravke uporabe takvih sustava koji funkcioniraju u „stvarnom vremenu” nose povećane rizike za prava i slobode osoba koje su obuhvaćene aktivnostima kaznenog progona.
- (19) Stoga bi trebalo zabraniti uporabu tih sustava za potrebe kaznenog progona, osim u trima iscrpno navedenima i usko definiranim situacijama u kojima je ta uporaba nužna za ostvarenje znatnog javnog interesa čija važnost premašuje rizike. Te situacije uključuju potragu za potencijalnim žrtvama kaznenih djela, uključujući nestalu djecu, određene prijetnje životu ili tjelesnoj sigurnosti pojedinaca ili prijetnje terorističkog napada te otkrivanje, lociranje, identifikaciju ili progon počinitelja kaznenih djela ili osumnjičenika za kaznena djela iz Okvirne odluke Vijeća 2002/584/PUP³⁸ ako su ta kaznena djela u državi članici kažnjiva najvišom kaznom zatvora ili oduzimanjem slobode od najmanje tri godine i kako su utvrđena pravom te države članice. Takvim pragom za kaznu zatvora ili oduzimanje slobode u skladu s nacionalnim pravom pomaže se osigurati da bi ta djela trebala biti dovoljno teška da se potencijalno

³⁸

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

opravda uporaba sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu. Nadalje, od 32 kaznena djela navedena u Okvirnoj odluci Vijeća 2002/584/PUP neka će u praksi vjerojatno biti relevantniji od drugih, u smislu da će da će primjena daljinske biometrijske identifikacije u stvarnom vremenu biti predvidljivo potrebna i razmjerna u veoma različitoj mjeri za otkrivanje, lociranje, identifikaciju ili progon počinitelja različitih navedenih kaznenih djela ili osumnjičenika za ta kaznena djela te s obzirom na vjerojatne razlike u težini, vjerojatnosti i razmjeru štete ili mogućih negativnih posljedica.

- (20) Kako bi se osigurala odgovorna i proporcionalna uporaba tih sustava, važno je i utvrditi da bi u svakoj od tih triju iscrpno navedenih i usko definiranih situacija trebalo uzeti u obzir određene elemente, osobito u pogledu prirode situacije zbog koje zahtijeva njihova uporaba i posljedica uporabe za prava i slobode svih uključenih osoba te na zaštitne mjere i uvjete propisane za tu uporabu. Osim toga, za uporabu sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona trebala bi vrijediti odgovarajuća vremenska i prostorna ograničenja, osobito s obzirom na dokaze ili indikacije koji se odnose na prijetnje, žrtve ili počinitelje. Referentna baza podataka osoba trebala bi biti prikladna za svaki slučaj primjene u svakoj od triju prethodno navedenih situacija.
- (21) Za svaku uporabu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona trebalo bi pribaviti izričito i posebno odobrenje pravosudnog tijela ili neovisnog upravnog tijela države članice. Takvo bi se odobrenje u načelu trebalo pribaviti prije uporabe, osim u propisno opravdanim hitnim situacijama, odnosno situacijama u kojima je potreba za uporabom tih sustava takva da je praktično i objektivno nemoguće dobiti odobrenje prije početka uporabe. U takvim hitnim situacijama uporaba bi trebala biti ograničena na apsolutno nužni minimum te podlijehati odgovarajućim zaštitnim mjerama i uvjetima, kako je utvrđeno u nacionalnom pravu i kako je odredilo samo tijelo kaznenog progona u kontekstu svakog pojedinačnog hitnog primjera uporabe. Osim toga, tijelo kaznenog progona u takvim bi situacijama trebalo tražiti pribavljanje odobrenja što prije, uz navođenje razloga zbog kojih se ono nije moglo zatražiti ranije.
- (22) Nadalje, primjereno je u kontekstu iscrpnog okvira utvrđenog ovom Uredbom propisati da bi takva uporaba na državnom području države članice u skladu s ovom Uredbom trebala biti moguća samo ako i u mjeri u kojoj je ta država članica odlučila izričito predvidjeti mogućnost odobrenja takve uporabe u svojim detaljnim pravilima nacionalnog prava. Stoga države članice u skladu s ovom Uredbom 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 odobrena uporaba utvrđena u ovoj Uredbi.
- (23) Uporaba UI sustavâ za daljinsku biometrijsku identifikaciju pojedinaca u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona nužno uključuje obradu biometrijskih podataka. Pravila ove Uredbe kojima se, uz određene iznimke, zabranjuje takva uporaba, 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 takva uporaba i obrada biometrijskih podataka. Stoga bi takva uporaba i obrada trebala biti moguća samo u onoj mjeri u kojoj je u skladu s okvirom utvrđenim ovom Uredbom, pri čemu ne bi trebao postojati prostor, izvan tog okvira, da nadležna tijela koja djeluju za potrebe 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 iz članka 8. Direktive (EU) 2016/680. Međutim, uporaba sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u druge svrhe osim kaznenog progona, i kad ih upotrebljavaju nadležna tijela, ne bi trebala biti obuhvaćena posebnim okvirom o takvoj uporabi za potrebe kaznenog progona utvrđenim ovom Uredbom. Takva uporaba u druge svrhe osim kaznenog progona stoga ne bi trebala podlijetati zahtjevu za odobrenje u skladu s ovom Uredbom te važećim detaljnim pravilima nacionalnog prava kojima se može provoditi.

- (24) Svaka obrada biometrijskih podataka i drugih osobnih podataka povezana s uporabom UI sustavâ za biometrijsku identifikaciju, osim obrade povezane s uporabom sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona kako je uređeno ovom Uredbom, uključujući slučajeve kad te sustave upotrebljavaju nadležna tijela na javnim mjestima u druge svrhe osim kaznenog progona, i dalje bi trebala ispunjavati sve zahtjeve koji proizlaze iz članka 9. stavka 1. Uredbe (EU) 2016/679, članka 10. stavka 1. Uredbe (EU) 2018/1725 i članka 10. Direktive (EU) 2016/680, ovisno o slučaju.
- (25) 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 člankom 5. stavkom 1. točkom (d) i člankom 5. stavcima 2. i 3. ove Uredbe donesene 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 traži usklađenost s odredbama utvrđenima na temelju članka 16. UFEU-a.
- (26) 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 člankom 5. stavkom 1. točkom (d) i člankom 5. stavcima 2. i 3. ove Uredbe donesene 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.
- (27) Visokorizični UI sustavi trebali bi se stavljati na tržište Unije ili u uporabu samo ako ispunjavaju određene obvezne zahtjeve. Tim bi se zahtjevima trebalo osigurati da visokorizični UI sustavi koji su dostupni u Uniji ili čiji se izlazni rezultati na drugi način upotrebljavaju u Uniji ne predstavljaju neprihvatljiv rizik za važne javne interese Unije koji su priznati i zaštićeni pravom Unije. 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 ograničenje trebalo minimizirati bilo kakvo potencijalno ograničenje u pogledu međunarodne trgovine.
- (28) Krajnji ishodi uporabe UI sustava mogli bi nepovoljno utjecati na zdravlje i sigurnost osoba, osobito ako su ti sustavi sastavni dio proizvodâ. U skladu s ciljevima zakonodavstva Unije o usklađivanju, kako bi se olakšalo slobodno kretanje proizvoda na unutarnjem tržištu i kako bi se osiguralo da se na tržište stavljaju samo sigurni i sukladni proizvodi, važno je da se propisno spriječe i smanje mogući sigurnosni rizici od proizvoda kao cjeline zbog njegovih digitalnih sastavnih dijelova, 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 posebno visoki, sve sofisticiraniji dijagnostički sustavi i sustavi koji pomažu ljudima u odlučivanju trebali bi biti pouzdani i točni. Razmjer nepovoljnog utjecaja 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 te nediskriminaciju, zaštitu potrošača, prava radnika, prava osoba s invaliditetom, 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 da djeca imaju posebna prava utvrđena člankom 24. Povelje EU-a i Konvencijom Ujedinjenih naroda o pravima djeteta (podrobnije razrađena u Općoj napomeni br. 25 Odbora UN-a za prava djeteta o digitalnom okruženju), kojima se zahtijeva da se vodi računa o ranjivosti djece te da se osiguraju zaštita i skrb potrebni za njihovu dobrobit. Pri procjeni ozbiljnosti štete koju UI sustav može prouzročiti, među ostalim u pogledu zdravlja i sigurnosti osoba, trebalo bi uzeti u obzir i temeljno pravo na visoku razinu zaštite okoliša koje je utvrđeno Poveljom i provodi se u politikama Unije.

- (29) Kad je riječ o visokorizičnim UI sustavima koji su sigurnosni sastavni dijelovi proizvodâ ili sustavâ ili koji su sami proizvodi ili sustavi obuhvaćeni područjem primjene Uredbe (EZ) br. 300/2008 Europskog parlamenta i Vijeća³⁹, Uredbe (EU) br. 167/2013 Europskog parlamenta i Vijeća⁴⁰, Uredbe (EU) br. 168/2013 Europskog parlamenta i Vijeća⁴¹, Direktive 2014/90/EU Europskog parlamenta i Vijeća⁴², Direktive (EU) 2016/797 Europskog parlamenta i Vijeća⁴³, Uredbe (EU) 2018/858 Europskog parlamenta i Vijeća⁴⁴, Uredbe (EU) 2018/1139 Europskog parlamenta i Vijeća⁴⁵ i Uredbe (EU) 2019/2144 Europskog parlamenta i Vijeća⁴⁶, primjereno je

³⁹ 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.).

⁴⁰ 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.).

⁴¹ 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.).

⁴² 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.).

⁴³ 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.).

⁴⁴ 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.).

⁴⁵ 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.).

⁴⁶ 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,

izmijeniti te akte kako bi se osiguralo da Komisija, na temelju tehničkih i regulatornih posebnosti svakog sektora te bez uplitanja u postojeće mehanizme upravljanja, ocjenjivanja sukladnosti i provedbe te rad tijela koja su njima utvrđena, pri donošenju svih relevantnih budućih delegiranih ili provedbenih akata na temelju tih akata uzima u obzir obvezne zahtjeve za visokorizične UI sustave utvrđene u ovoj Uredbi.

- (30) Kad je riječ o UI sustavima koji su sigurnosni sastavni dijelovi proizvoda ili su sami proizvodi, a obuhvaćeni su područjem primjene određenog zakonodavstva Unije o usklađivanju, primjereno ih je klasificirati među visokorizične na temelju ove Uredbe ako se za predmetni proizvod provodi postupak ocjenjivanja sukladnosti koji provodi tijelo za ocjenjivanje sukladnosti kao treća strana u skladu s relevantnim zakonodavstvom Unije o usklađivanju. Konkretno, takvi su proizvodi strojevi, igračke, dizala, oprema i zaštitni sustavi za uporabu 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.
- (31) Klasifikacija UI sustava kao visokorizičnog u skladu s ovom Uredbom ne bi nužno trebala značiti da se proizvod čiji je sigurnosni sastavni dio UI sustav ili pak sam UI sustav kao proizvod smatra „visokorizičnim” na temelju kriterija utvrđenih u relevantnom zakonodavstvu Unije o usklađivanju koje se primjenjuje na taj proizvod. To se posebno odnosi na Uredbu (EU) 2017/745 Europskog parlamenta i Vijeća⁴⁷ i Uredbu (EU) 2017/746 Europskog parlamenta i Vijeća⁴⁸ ako ocjenjivanje sukladnosti srednjerizičnih i visokorizičnih proizvoda provodi treća strana.
- (32) Kad je riječ o samostalnim UI sustavima, odnosno visokorizičnim UI sustavima koji nisu sigurnosni sastavni dijelovi proizvoda ili koji su sami proizvodi, primjereno ih je klasificirati kao visokorizične ako, s obzirom na njihovu namjenu, kod njih postoji velik rizik od štete za zdravlje i sigurnost ili temeljna prava osoba, uzimajući u obzir i ozbiljnost moguće štete i njezinu vjerojatnost pojavljivanja, te ako se upotrebljavaju u nekoliko posebnih unaprijed definiranih područja navedenih u Uredbi. Identifikacija tih sustava temelji se na istoj metodologiji i kriterijima predviđenima i za sve buduće izmjene popisa visokorizičnih UI sustava.
- (33) Tehničke netočnosti UI sustava namijenjenih daljinskoj biometrijskoj identifikaciji pojedinaca mogu prouzročiti pristrane rezultate i imati diskriminacijske učinke. To je posebno relevantno kad je riječ o dobi, etničkom podrijetlu, spolu ili invaliditetu. Stoga bi sustave za daljinsku biometrijsku identifikaciju u stvarnom vremenu i sustave za naknadnu daljinsku biometrijsku identifikaciju trebalo klasificirati kao visokorizične. S obzirom na rizike koje predstavljaju, na obje vrste sustava za daljinsku biometrijsku identifikaciju trebali bi se primjenjivati posebni zahtjevi u pogledu funkcija bilježenja događaja i ljudskog nadzora.
- (34) Kad je riječ o upravljanju kritičnom infrastrukturuom i njezinu radu, primjereno je klasificirati kao visokorizične one UI sustave koji su namijenjeni uporabi kao sigurnosni sastavni dijelovi u cestovnom prometu i upravljanju njime te opskrbi

(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.).

⁴⁷ 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.).

⁴⁸ 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.).

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.

- (35) UI sustavi koji se upotrebljavaju u obrazovanju ili strukovnom osposobljavanju, posebno za razvrstavanje osoba u ustanove za obrazovanje i strukovno osposobljavanje ili za određivanje pristupa tim ustanovama ili pak za ocjenjivanje osoba na testiranjima tijekom obrazovanja ili kao preduvjet za obrazovanje, trebaju se smatrati visokorizičnima jer mogu odrediti obrazovni i profesionalni tijek života osobe i stoga utjecati na njezinu mogućnost da osigura vlastita sredstva za život. Ako se projektiraju i upotrebljavaju na nepravilan način, takvi sustavi mogu kršiti pravo na obrazovanje i osposobljavanje i pravo na nediskriminaciju te mogu održati povijesne diskriminacijske uzorke.
- (36) UI sustavi koji se upotrebljavaju za zapošljavanje, kadrovsko upravljanje i pristup samozapošljavanju, posebno za pronalaženje i odabir osoba, za donošenje odluka o promaknućima i otkazima te za dodjeljivanje zadataka, praćenje ili evaluaciju osoba u ugovornim odnosima povezanim s poslom, isto bi tako trebali biti klasificirani kao visokorizični jer bi mogli znatno utjecati na buduće mogućnosti za razvoj karijere i životne uvjete tih osoba. Relevantni radni ugovorni odnosi trebali bi uključivati zaposlenike i osobe koje pružaju usluge posredstvom platformi kako je navedeno u programu rada Komisije za 2021. Takve se osobe u načelu ne bi trebale smatrati korisnicima u smislu ove Uredbe. U procesu zapošljavanja i pri evaluaciji, promicanju ili zadržavanju osoba u radnim ugovornim odnosima takvi sustavi mogu održati povijesne uzorke diskriminacije, primjerice žena, određenih dobni skupina, osoba s invaliditetom ili osoba određenog rasnog ili etničkog podrijetla ili spolne orijentacije. UI sustavi koji se upotrebljavaju za praćenje uspješnosti i ponašanja tih osoba mogu utjecati i na njihova prava na zaštitu osobnih podataka i privatnost.
- (37) Još jedno područje u kojem UI sustavima treba posvetiti posebnu pozornost jest korištenje i dostupnost određenih privatnih i javnih usluga i pogodnosti nužnih za potpuno sudjelovanje u društvu ili poboljšanje životnog standarda osoba. Točnije, UI sustave koji se upotrebljavaju za ocjenu kreditnog rejtinga ili kreditne sposobnosti pojedinaca trebalo bi klasificirati kao visokorizične UI sustave jer određuju pristup tih osoba financijskim sredstvima ili osnovnim uslugama kao što su stanovanje, električna energija i telekomunikacijske usluge. UI sustavi koji se upotrebljavaju u tu svrhu mogu prouzročiti diskriminaciju osoba ili skupina te nastaviti povijesne uzorke diskriminacije, primjerice na temelju rasnog ili etničkog podrijetla, invaliditeta, dobi, spolne orijentacije, ili mogu stvoriti nove oblike diskriminacije. Uzimajući u obzir vrlo ograničenu razinu utjecaja i dostupne alternative na tržištu, primjereno je izuzeti UI sustave za potrebe ocjene kreditne sposobnosti i kreditnog rejtinga kad ih u uporabu stavljaju mali dobavljači za vlastite potrebe. Pojedinci koji tijelima javne vlasti podnose zahtjev za naknade i usluge javne pomoći ili ih primaju obično ovise o tim naknadama i uslugama te su u ranjivu položaju u odnosu na nadležna tijela. Ako nadležna tijela upotrebljavaju UI sustave za određivanje treba li takve naknade i usluge odbiti, smanjiti, ukinuti ili treba li tražiti njihov povrat, ti sustavi mogu znatno utjecati na životne uvjete tih osoba i mogu kršiti njihova temeljna prava, kao što su pravo na socijalnu zaštitu, nediskriminaciju, ljudsko dostojanstvo ili djelotvoran pravni lijek. Te bi sustave stoga trebalo klasificirati kao visokorizične. Međutim, ova Uredba ne bi trebala otežavati razvoj i primjenu inovativnih pristupa u javnoj upravi, koja bi imala izravnu korist od šire uporabe usklađenih i sigurnih UI sustava, pod uvjetom da ti sustavi ne podrazumijevaju velik rizik za pravne i fizičke osobe.

Naposljetku, UI sustavi koji se upotrebljavaju za dispečiranje ili određivanje prioriteta pri dispečiranju hitnih službi isto bi se trebali smatrati visokorizičnima jer donose odluke u situacijama koje su kritične za život i zdravlje osoba te za njihovu imovinu.

- (38) Postupcima tijela kaznenog progona koji uključuju određene uporabe UI sustava svojstvena je znatna neravnoteža moći, pa mogu dovesti do nadzora, uhićenja ili oduzimanja slobode pojedinaca, kao i do drugih nepovoljnih utjecaja na temeljna prava zajamčena Poveljom. Naime, ako UI sustav nije učen visokokvalitetnim podacima, ne ispunjava odgovarajuće zahtjeve u pogledu točnosti ili otpornosti ili nije pravilno projektiran i testiran prije stavljanja na tržište ili u uporabu, on može izdvajati ljude na diskriminatoran ili na drukčije netočan ili nepravedan način. Nadalje, ostvarivanje važnih postupovnih temeljnih prava, kao što su pravo na djelotvoran pravni lijek i na pošteno suđenje te pravo na obranu i pretpostavku nedužnosti, moglo bi biti otežano, osobito ako takvi UI sustavi nisu dovoljno transparentni i objašnjivi te kad o njima ne postoji dovoljno dokumentacije. Stoga je primjereno klasificirati kao visokorizične one UI sustave koji su namijenjeni uporabi u kontekstu kaznenog progona kad su točnost, pouzdanost i transparentnost posebno važne kako bi se izbjegli nepovoljni utjecaji, zadržalo povjerenje javnosti te osigurala odgovornost i učinkovita pravna zaštita. S obzirom na prirodu tih postupaka i s njima povezane rizike, među visokorizične UI sustave trebalo bi osobito klasificirati UI sustave namijenjene tijelima kaznenog progona za pojedinačne procjene rizika, poligrafe i slične alate ili za utvrđivanje emocionalnog stanja pojedinca, za otkrivanje „deep fake” sadržaja, za procjenu pouzdanosti dokaza u kaznenim postupcima, za predviđanje počinjenja ili ponavljanja stvarnog ili potencijalnog kaznenog djela na temelju izrade profila pojedinaca ili procjenu osobina ličnosti i karakteristika ili prijašnjeg kriminalnog ponašanja pojedinaca ili skupina, za izradu profila tijekom otkrivanja, istrage ili progona kaznenih djela, kao i za analitiku kaznenih djela koja se odnosi na pojedince. UI sustavi posebno namijenjeni za upravne postupke poreznih i carinskih tijela ne bi se trebali smatrati visokorizičnim UI sustavima koje tijela kaznenog progona upotrebljavaju u svrhu sprečavanja, otkrivanja, istrage i progona kaznenih djela.
- (39) UI sustavi koji se upotrebljavaju u upravljanju migracijama, azilom i granicama 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, posebno njihovih prava na slobodno kretanje, nediskriminaciju, zaštitu privatnog života i osobnih podataka, međunarodnu zaštitu i dobru upravu. Stoga je primjereno klasificirati kao visokorizične one UI sustave namijenjene tijelima javne vlasti nadležnima za zadaće u području upravljanja migracijama, azilom i granicama, kao što su poligrafi i slični alati ili sustavi za utvrđivanje emocionalnog stanja pojedinca, za procjenu određenih rizika koje predstavljaju pojedinci koji ulaze na državno područje države članice ili podnose zahtjev za vizu ili azil, za provjeru vjerodostojnosti relevantnih dokumenata pojedinaca, za pomaganje nadležnim tijelima javne vlasti pri razmatranju zahtjeva za azil, vize i boravišne dozvole te s tim povezanih pritužbi s obzirom na cilj da se utvrdi prihvatljivost pojedinca koji podnosi zahtjev za taj status. UI sustavi koji se upotrebljavaju u upravljanju migracijama, azilom i granicama obuhvaćeni ovom Uredbom trebali bi biti u skladu s relevantnim postupovnim zahtjevima utvrđenima

Direktivom 2013/32/EU Europskog parlamenta i Vijeća⁴⁹, Uredbom (EZ) br. 810/2009 Europskog parlamenta i Vijeća⁵⁰ i drugim relevantnim propisima.

- (40) Određene UI sustave namijenjene pravosuđu 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 pravni lijek i na pošteno suđenje. Točnije, radi smanjenja rizika od mogućih pristranosti, pogrešaka i netransparentnosti, primjereno je klasificirati kao visokorizične one UI sustave koji su namijenjeni za pomoć pravosudnim tijelima u istraživanju i tumačenju činjenica i prava te primjeni prava na konkretan skup činjenica. Međutim, takva se kvalifikacija 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, administrativne zadaće ili raspodjela resursa.
- (41) Činjenica da je UI sustav klasificiran kao visokorizičan na temelju ove Uredbe ne bi se trebala tumačiti kao indikator da je uporaba sustava nužno zakonita na temelju drugih pravnih akata Unije ili nacionalnog prava koje je usklađeno s pravom Unije, primjerice o zaštiti osobnih podataka, o uporabi poligrafa i sličnih alata ili drugih sustava kojima se utvrđuje emocionalno stanje pojedinaca. Svaka takva uporaba trebala 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, ovisno o slučaju, posebne kategorije osobnih podataka.
- (42) Kako bi se smanjili rizici visokorizičnih UI sustava koji su stavljeni na tržište Unije ili na drugi način stavljeni u uporabu na tržištu Unije za korisnike i zahvaćene osobe, trebali bi se primjenjivati određeni obvezni zahtjevi s obzirom na namjenu sustava i sustav upravljanja rizikom koji uspostavlja dobavljač.
- (43) Zahtjevi bi se trebali primjenjivati na visokorizične UI sustave u pogledu kvalitete korištenih skupova podataka, tehničke dokumentacije i vođenja evidencije, transparentnosti i pružanja informacija korisnicima, ljudskog nadzora te otpornosti, točnosti i kibernsigurnosti. Ti su zahtjevi potrebni kako bi se uspješno smanjili rizici za zdravlje, sigurnost i temeljna prava, ovisno o namjeni sustava, a druge mjere kojima se manje ograničava trgovina nisu u razumnoj mjeri dostupne, čime se izbjegavaju neopravdana ograničenja u području trgovine.
- (44) Visokokvalitetni podaci ključni su za sposobnost mnogih UI sustava, posebno kad se upotrebljavaju tehnike s učenjem modelâ, s ciljem da visokorizični UI sustav funkcionira kako je predviđeno i sigurno te da ne postane izvor diskriminacije koja je zabranjena pravom Unije. Za vrlo kvalitetne skupove podataka za učenje, validaciju i testiranje potrebna je primjena odgovarajuće prakse upravljanja podacima. Skupovi podataka za učenje, validaciju i testiranje trebali bi biti dovoljno relevantni, reprezentativni i bez pogrešaka te bi trebali biti potpuni s obzirom na namjenu sustava. Trebali bi imati i odgovarajuća statistička obilježja, među ostalim u odnosu na osobe

⁴⁹ 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.).

⁵⁰ 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.).

ili skupine osoba za koje se visokorizični UI sustav namjerava rabiti. Naročito bi u skupovima podataka za učenje, validaciju i testiranje trebalo uzeti u obzir, u mjeri u kojoj to iziskuje njihova namjena, obilježja, karakteristike ili elemente specifične za zemljopisno, bihevioralno ili radno okruženje ili kontekst u kojem je previđena uporaba UI sustava. Kako bi se prava drugih osoba zaštitila od moguće diskriminacije zbog pristranosti UI sustavâ, dobavljači bi trebali moći obrađivati i posebne kategorije osobnih podataka, kao pitanje od znatnog javnog interesa, kako bi se osiguralo praćenje, otkrivanje i ispravljanje pristranosti povezanih s visokorizičnim UI sustavima.

- (45) Kad je riječ o razvoju visokorizičnih UI sustava, određeni dionici, kao što su dobavljači, prijavljena tijela i drugi relevantni subjekti, na primjer centri za digitalne inovacije, centri za testiranje i eksperimentiranje te istraživači, trebali bi imati pristup visokokvalitetnim skupovima podataka i upotrebljavati ih u okviru svojih područja aktivnosti 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 važni za osiguravanje pouzdanog, odgovornog i nediskriminirajućeg pristupa visokokvalitetnim podacima za učenje, validaciju i testiranje UI sustavâ. Na primjer, u području zdravstva zajednički europski prostor za zdravstvene podatke olakšat će nediskriminirajući pristup zdravstvenim podacima i učenje algoritama umjetne inteligencije tim skupovima podataka tako da se očuvaju privatnost, sigurnost, pravovremenost, transparentnost i pouzdanost uz odgovarajuće institucijsko upravljanje. Relevantna nadležna tijela, uključujući sektorska, koja pružaju ili olakšavaju pristup podacima, mogu olakšati i pružanje visokokvalitetnih podataka za učenje, validaciju i testiranje UI sustava.
- (46) Informacije o tome kako su visokorizični UI sustavi razvijeni te kakav im je radni učinak tijekom cijelog životnog vijeka ključne su za provjeru usklađenosti sa zahtjevima iz ove Uredbe. Za to je potrebno vođenje evidencije i dostupnost tehničke dokumentacije koja sadržava informacije potrebne za procjenu usklađenosti UI sustava s relevantnim zahtjevima. Te bi informacije trebale uključivati opće karakteristike, mogućnosti i ograničenja sustava, algoritme, podatke, postupke učenja, testiranja i validacije koji su upotrijebljeni, kao i dokumentaciju o relevantnom sustavu upravljanja rizikom. Tehnička dokumentacija trebala bi se redovito ažurirati.
- (47) Kako bi se riješio problem netransparentnosti koja može određene UI sustave učiniti neshvatljivima ili presloženima za pojedince, visokorizični UI sustavi trebali bi biti u određenoj mjeri transparentni. Korisnici bi trebali moći tumačiti izlazne rezultate sustava i upotrebljavati ih na odgovarajući način. Visokorizični UI sustavi stoga bi trebali biti popraćeni odgovarajućom dokumentacijom i uputama za uporabu sa sažetom i jasnim informacijama, među ostalim, prema potrebi, u pogledu mogućih rizika povezanih s temeljnim pravima i diskriminacijom.
- (48) Visokorizične UI sustave trebalo bi projektirati i razvijati na način da pojedinci mogu nadzirati njihovo funkcioniranje. U tu bi svrhu dobavljač sustava prije njegova stavljanja na tržište ili u uporabu trebao utvrditi odgovarajuće mjere ljudskog nadzora. Prema potrebi bi takvim mjerama posebno trebalo osigurati da su u sustav ugrađena operativna ograničenja koja sam sustav ne može promijeniti i da reagira na ljudske operatere te da pojedinci koji su zaduženi za ljudski nadzor imaju potrebne kompetencije i da su osposobljeni i ovlašteni za obavljanje te zadaće.
- (49) Visokorizični UI sustavi trebali bi imati ujednačen učinak u cijelom životnom vijeku te imati odgovarajuću razinu točnosti, otpornosti i kibersigurnosti u skladu s

općepriznatim najnovijim dostignućima. Korisnici bi trebali biti obaviješteni o razini i parametrima točnosti.

- (50) Tehnička otpornost ključni je zahtjev za visokorizične UI sustave. Trebali bi biti otporni na rizike povezane s ograničenjima sustava (npr. pogreške, kvarovi, nedosljednosti, neočekivane situacije), kao i na zlonamjerne radnje koje mogu ugroziti sigurnost UI sustava i dovesti do štetnog ili na neki drugi način nepoželjnog ponašanja. Nedostatna zaštita od tih rizika mogla uzrokovati posljedice za sigurnost ili negativno utjecati na temeljna prava, primjerice zbog pogrešnih odluka ili krivih ili pristranih izlaznih rezultata UI sustava.
- (51) Kibersigurnost je ključna za otpornost UI sustava na pokušaje zlonamjernih trećih strana koje iskorištavaju slabe točke sustava da bi im izmijenili način uporabe, ponašanje, sposobnost ili da bi ugrozili njihove sigurnosne mehanizme. Kibernapadima na UI sustave moguće je iskoristiti resurse svojstvene umjetnoj inteligenciji, kao što su skupovi podataka za učenje (npr. trovanje podataka) ili poučeni modeli (npr. neprijateljski napadi) ili iskoristiti slabe točke digitalnih resursa UI sustava ili osnovne IKT infrastrukture. Kako bi se osigurala razina kibersigurnosti koja odgovara rizicima, dobavljači visokorizičnih UI sustava trebali bi poduzeti odgovarajuće mjere, prema potrebi uzimajući u obzir i osnovnu infrastrukturu IKT-a.
- (52) U okviru zakonodavstva Unije o usklađivanju, pravila koja se primjenjuju na stavljanje na tržište, stavljanje u uporabu i korištenje visokorizičnih UI sustava trebala bi biti usklađena s Uredbom (EZ) br. 765/2008 Europskog parlamenta i Vijeća⁵¹ o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta, Odlukom br. 768/2008/EZ Europskog parlamenta i Vijeća⁵² o zajedničkom okviru za stavljanje na tržište proizvoda i Uredbom (EU) 2019/1020 Europskog parlamenta i Vijeća⁵³ o nadzoru tržišta i sukladnosti proizvoda („novi zakonodavni okvir za stavljanje proizvoda na tržište”).
- (53) Primjereno je da određena fizička ili pravna osoba, koja je definirana kao dobavljač, preuzme odgovornost za stavljanje visokorizičnog UI sustava na tržište ili u uporabu, bez obzira na to je li ta fizička ili pravna osoba ista osoba koja je projektirala ili razvila sustav.
- (54) Dobavljač bi trebao uspostaviti pouzdan sustav upravljanja kvalitetom, osigurati realizaciju obveznog postupka ocjenjivanja sukladnosti, sastaviti relevantnu dokumentaciju i uspostaviti pouzdan sustav praćenja nakon stavljanja na tržište. Tijela javne vlasti koja stavljaju visokorizične UI sustave u uporabu za vlastite potrebe mogu donijeti i primjenjivati 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 predmetnog tijela javne vlasti.

⁵¹ Uredba (EZ) br. 765/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište i o stavljanju izvan snage Uredbe (EEZ) br. 339/93 (SL L 218, 13.8.2008., str. 30.).

⁵² 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.).

⁵³ 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 (Tekst značajan za EGP) (SL L 169, 25.6.2019., str. 1.–44.).

- (55) Ako se visokorizični UI sustav koji je sigurnosni sastavni dio proizvoda obuhvaćenog sektorskim propisima relevantnog novog zakonodavnog okvira ne stavlja na tržište ili u uporabu neovisno o proizvodu, proizvođač konačnog proizvoda, kako je definirano propisima relevantnog novog zakonodavnog okvira, trebao bi ispunjavati obveze dobavljača utvrđene u ovoj Uredbi, a posebno osigurati da UI sustav ugrađen u konačni proizvod ispunjava zahtjeve iz ove Uredbe.
- (56) Kako bi se omogućilo izvršenje 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 UI sustava. Stoga, ako se uvoznik ne može identificirati, dobavljači s poslovnim nastanom izvan Unije pisanim ovlaštenjem imenuju ovlaštenog zastupnika s poslovnim nastanom u Uniji prije stavljanja svojih UI sustava na raspolaganje u Uniji.
- (57) U skladu s načelima novog zakonodavnog okvira trebalo bi utvrditi posebne obveze za relevantne gospodarske subjekte, kao što su uvoznici i distributeri, kako bi se postigla pravna sigurnost i olakšalo usklađivanje tih relevantnih subjekata s propisima.
- (58) S obzirom na prirodu UI sustavâ i rizike za sigurnost i temeljna prava koji se potencijalno mogu povezati s njihovom uporabom, među ostalim u pogledu potrebe da se osigura propisno praćenje sposobnosti UI sustava u stvarnim uvjetima, primjereno je utvrditi posebne odgovornosti za korisnike. Korisnici bi ponajprije visokorizične UI sustave trebali upotrebljavati u skladu s uputama za uporabu te bi, prema potrebi, trebalo propisati određene druge obveze u pogledu praćenja funkcioniranja UI sustavâ i vođenja evidencije.
- (59) Primjereno je predvidjeti da bi korisnik UI sustava trebao biti fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo u okviru čije se nadležnosti koristi UI sustav, osim ako se koristi u osobnoj neprofesionalnoj djelatnosti.
- (60) S obzirom na složenost lanca vrijednosti umjetne inteligencije, relevantne treće strane, posebno one uključene u prodaju i nabavu softvera, softverskih alata i sastavnih dijelova, prethodno poučenih modela i podataka ili pružatelji mrežnih usluga, trebali bi prema potrebi surađivati s dobavljačima i korisnicima kako bi im omogućili da ispune obveze iz ove Uredbe te s nadležnim tijelima uspostavljenima na temelju ove Uredbe.
- (61) Normizacija bi trebala imati ključnu ulogu u pružanju tehničkih rješenja dobavljačima kako bi se osigurala usklađenost s ovom Uredbom. Sukladnost s usklađenim normama kako je utvrđeno u Uredbi (EU) br. 1025/2012 Europskog parlamenta i Vijeća⁵⁴ trebala bi biti sredstvo kojim će dobavljači dokazivati sukladnost sa zahtjevima iz ove Uredbe. Međutim, Komisija bi mogla donijeti zajedničke tehničke specifikacije za područja u kojima ne postoje usklađene norme ili u kojima one nisu dovoljne.
- (62) Kako bi se osigurala visoka razina pouzdanosti visokorizičnih UI sustava, ti bi sustavi trebali podlijegati ocjenjivanju sukladnosti prije njihova stavljanja na tržište ili u uporabu.

⁵⁴ 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.).

- (63) Kako bi se opterećenje za operatere 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 postupka ocjenjivanja sukladnosti koji je već predviđen tim zakonodavstvom. Primjenjivost zahtjevâ iz ove Uredbe stoga ne bi trebala utjecati na specifičnu logiku, metodologiju ili opću strukturu ocjenjivanja sukladnosti na temelju relevantnih specifičnih propisa relevantnog novog zakonodavnog okvira. Taj se pristup u potpunosti odražava u međudjelovanju ove Uredbe i [Uredbe o strojevima]. Iako zahtjevi iz ove Uredbe obuhvaćaju sigurnosne rizike UI sustava za sigurnosne funkcije u strojevima, određenim posebnim zahtjevima iz [Uredbe o strojevima] osigurat će se sigurna integracija UI sustava u strojeve općenito kako se ne bi ugrozila sigurnost strojeva u cjelini. U [Uredbi o strojevima] primjenjuje se ista definicija UI sustava kao i u ovoj Uredbi.
- (64) S obzirom na bogato 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 trebali provoditi dobavljači na vlastitu odgovornost, osim u slučaju kad su UI sustavi namijenjeni za daljinsku biometrijsku identifikaciju osoba, za što je potrebno predvidjeti sudjelovanje prijavljenog tijela u ocjenjivanju sukladnosti, pod uvjetom da ti sustavi nisu zabranjeni.
- (65) Za ocjenjivanja sukladnosti UI sustava namijenjenih za daljinsku biometrijsku identifikaciju osoba koje provodi treća strana nacionalna nadležna tijela trebala bi na temelju ove Uredbe imenovati prijavljena tijela, pod uvjetom da ispunjavaju niz zahtjeva, ponajprije u pogledu neovisnosti, sposobnosti i nepostojanja sukoba interesa.
- (66) U skladu s uvriježenim pojmom bitne izmjene za proizvode uređene zakonodavstvom Unije o usklađivanju, primjereno je da se za UI sustav provede novi postupak ocjenjivanja sukladnosti kad god nastupi promjena koja bi mogla utjecati na usklađenost sustava s ovom Uredbom ili promjena namjene sustava. Usto, kad je riječ o UI sustavima koji „uče” i nakon što su stavljeni na tržište ili u uporabu (tj. automatski prilagođavaju način obavljanja funkcija), potrebno je propisati pravila kojima se utvrđuje da se izmjene algoritma i njegovih sposobnosti koje je dobavljač unaprijed odredio i koje se ocjenjuju u trenutku ocjenjivanja sukladnosti ne bi trebale smatrati bitnom izmjenom.
- (67) 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. Države članice ne bi trebale stvarati neopravdane zapreke stavljanju na tržište ili u uporabu visokorizičnih UI sustava koji ispunjavaju zahtjeve utvrđene ovom Uredbom i nose oznaku CE.
- (68) U određenim okolnostima brza dostupnost inovativnih tehnologija može biti ključna za zdravlje i sigurnost osoba te za društvo u cjelini. Stoga je primjereno da u iznimnim okolnostima povezanim s javnom sigurnošću ili zaštitom života i zdravlja pojedinaca te zaštitom industrijskog i trgovačkog vlasništva države članice mogu odobriti stavljanje na tržište ili u uporabu UI sustava za koje nije proveden postupak ocjenjivanja sukladnosti.

- (69) Kako bi se olakšao rad Komisije i država članica u području umjetne inteligencije te povećala transparentnost prema javnosti, od dobavljača visokorizičnih UI sustava koji nisu povezani s proizvodima obuhvaćenima relevantnim postojećim zakonodavstvom Unije o usklađivanju trebalo bi zahtijevati da registriraju svoj visokorizični UI sustav u bazi podataka EU-a, koju će uspostaviti i voditi Komisija. Komisija bi trebala biti voditelj obrade za tu bazu podataka, u skladu s Uredbom (EU) 2018/1725 Europskog parlamenta i Vijeća⁵⁵. Kako bi ta baza bila posve funkcionalna od puštanja u rad, postupak njezina uspostavljanja trebao bi uključivati razradu funkcionalnih specifikacija, što je Komisijina zadaća, te neovisno revizorsko izvješće.
- (70) Kod određenih UI sustava namijenjenih interakciji s pojedincima ili generiranju sadržaja mogu postojati posebni rizici u pogledu lažnog predstavljanja ili obmanjivanja, bez obzira na to smatraju li se visokorizičnima. Uporaba tih sustava stoga bi u određenim okolnostima trebala podlijevati posebnim obvezama u pogledu transparentnosti, ne dovodeći u pitanje zahtjeve i obveze za visokorizične UI sustave. Pojedinci bi prije svega trebali biti obaviješteni da su u interakciji s UI sustavom, osim ako je to očito iz okolnosti i konteksta uporabe. Osim toga, pojedince bi trebalo obavijestiti kad su izloženi sustavu za prepoznavanje emocija ili sustavu za biometrijsku kategorizaciju. Takve informacije i obavijesti trebale bi se davati u oblicima koji su pristupačni osobama s invaliditetom. Nadalje, korisnici koji upotrebljavaju UI sustav za generiranje ili manipuliranje slikovnim sadržajem, audiosadržajem ili videosadržajem u kojem postoji znatna sličnost s postojećim osobama, mjestima ili događajima te koji bi se nekoj osobi netočno činio vjerodostojnim moraju navesti da je taj sadržaj umjetno stvoren ili da je njime manipulirano označivanjem izlaznih rezultata UI sustava na odgovarajući način i navođenjem njihova umjetnog podrijetla.
- (71) Umjetna inteligencija skup je tehnologija koje se vrlo brzo razvijaju, što zahtijeva nove oblike regulatornog nadzora i siguran prostor za eksperimentiranje, a da se pritom inovacije razvijaju na odgovoran način te da se integriraju odgovarajuće zaštitne mjere i mjere za smanjenje rizika. Kako bi se osigurao pravni okvir koji je otvoren prema inovacijama, spreman za buduće promjene i otporan na poremećaje, nacionalna nadležna tijela jedne ili više država članica trebalo bi poticati da uspostave regulatorno izolirano okruženje za umjetnu inteligenciju radi lakšeg razvoja i testiranja inovativnih UI sustava pod strogim regulatornim nadzorom prije stavljanja tih sustava na tržište ili u uporabu.
- (72) Ciljevi regulatornih izoliranih okruženja trebali bi biti poticanje inovacija u području umjetne inteligencije uspostavom kontroliranog okruženja za eksperimentiranje i testiranje u fazi razvoja i prije stavljanja na tržište s ciljem da se: osigura usklađenost inovativnih UI sustava s ovom Uredbom i drugim relevantnim zakonodavstvom Unije i država članica, poveća pravna sigurnost za inovatore, poboljša nadzor nadležnih tijela i njihovo razumijevanje mogućnosti, novih rizika i učinaka uporabe umjetne inteligencije te ubrza pristup tržištima, među ostalim uklanjanjem zapreka za mala i srednja poduzeća (MSP-ovi) te novoosnovana (*start-up*) poduzeća. Radi ujednačene provedbe u cijeloj Uniji i ekonomije razmjera, primjereno je uspostaviti zajednička pravila za primjenu regulatornih izoliranih okruženja i okvir za suradnju relevantnih tijela uključenih u nadzor izoliranih okruženja. Ovom bi se Uredbom trebala dati

⁵⁵

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.).

pravna osnova za uporabu osobnih podataka prikupljenih u druge svrhe za razvoj određenih UI sustava u javnom interesu u regulatornom izoliranom okruženju za umjetnu inteligenciju, u skladu s člankom 6. stavkom 4. Uredbe (EU) 2016/679 i člankom 6. Uredbe (EU) 2018/1725, i ne dovodeći u pitanje članak 4. stavak 2. Direktive (EU) 2016/680. Sudionici u izoliranom okruženju trebali bi osigurati odgovarajuće zaštitne mjere i surađivati s nadležnim tijelima, među ostalim tako da slijede njihove smjernice, postupaju žurno i u dobroj vjeri kako bi se smanjili bilo kakvi veliki rizici za sigurnost i temeljna prava mogući tijekom razvoja i eksperimentiranja u izoliranom okruženju. Nadležna tijela trebala bi uzeti u obzir ponašanje sudionika u izoliranom okruženju kad odlučuju o izricanju upravne novčane kazne na temelju članka 83. stavka 2. Uredbe 2016/679 i članka 57. Direktive (EU) 2016/680.

- (73) Kako bi se promicale i štitile inovacije, posebno je važno uzeti u obzir interese malih dobavljača i korisnika UI sustava. Radi toga bi države članice trebale osmisliti inicijative usmjerene na te operatere, među ostalim u pogledu širenja svijesti i informiranja. Usto, prijavljena tijela trebala bi uzeti u obzir posebne interese i potrebe malih dobavljača kad određuju naknade za ocjenjivanje sukladnosti. Dobavljači i drugi operateri, posebno oni manje, 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 općenito razumije najveći mogući broj prekograničnih korisnika.
- (74) Kako bi se rizici za provedbu koji proizlaze iz nedostatka znanja i iskustva na tržištu sveli na najmanju moguću mjeru te kako bi se dobavljačima i prijavljenim tijelima olakšalo ispunjavanje obveza iz ove Uredbe, Komisija i države članice trebale bi pridonijeti njezinoj provedbi uspostavljanjem platforme za umjetnu inteligenciju na zahtjev, europskih centara za digitalne inovacije te centara za testiranje i eksperimentiranje na nacionalnoj razini ili razini EU-a. U okviru svojih misija i područja kompetentnosti ponajprije mogu pružati tehničku i znanstvenu potporu dobavljačima i prijavljenim tijelima.
- (75) 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 u skladu s Uredbom (EU) 2017/745 i Uredbom (EU) 2017/746.
- (76) Kako bi se olakšala nesmetana, učinkovita i usklađena provedba ove Uredbe, trebalo bi uspostaviti Europski odbor za umjetnu inteligenciju. Odbor bi trebao biti odgovoran za niz savjetodavnih zadaća, uključujući davanje mišljenja, preporuka, savjeta ili smjernica o pitanjima povezanim s provedbom ove Uredbe, među ostalim o tehničkim specifikacijama ili postojećim normama povezanim sa zahtjevima iz ove Uredbe, te za davanje savjeta i pomaganje Komisiji u vezi sa specifičnim pitanjima koja se odnose na umjetnu inteligenciju.
- (77) Države članice imaju ključnu ulogu u primjeni i provedbi ove Uredbe. Svaka bi država članica zato trebala odrediti jedno ili više nacionalnih nadležnih tijela za potrebe nadziranja primjene i provedbe ove Uredbe. Kako bi se povećala učinkovitost organizacije u državama članicama i uspostavila službena kontaktna točka za javne i

druge partnere na razini država članica i Unije, u svakoj bi državi članici jedno nacionalno tijelo trebalo imenovati kao nacionalno nadzorno tijelo.

- (78) Kako bi dobavljači visokorizičnih UI sustava mogli uzeti u obzir iskustvo stečeno uporabom visokorizičnih UI sustava za poboljšanje svojih sustava te za projektiranje i razvoj ili kako bi mogli pravovremeno poduzeti korektivne mjere, svi bi dobavljači trebali uspostaviti sustav praćenja nakon stavljanja na tržište. 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 uporabu. U tom bi kontekstu od dobavljača trebalo zahtijevati i da uspostave sustav za prijavljivanje relevantnim tijelima svih ozbiljnih incidenata ili povreda nacionalnog prava i prava Unije kojima se štite temeljna prava koji su posljedica uporabe njihovih UI sustava.
- (79) Kako bi se osigurala odgovarajuća i učinkovita provedba zahtjeva i obveza utvrđenih ovom Uredbom, odnosno zakonodavstvom Unije o usklađivanju, u cijelosti bi se trebao primjenjivati sustav nadzora tržišta i sukladnosti proizvoda uspostavljen Uredbom (EU) 2019/1020. Ako je to potrebno za njihov mandat, pristup svoj dokumentaciji izrađenoj na temelju ove Uredbe trebala bi imati i nacionalna tijela javne vlasti ili javnopravna tijela koja nadziru primjenu prava Unije o zaštiti temeljnih prava, uključujući tijela za ravnopravnost.
- (80) Zakonodavstvo Unije o financijskim uslugama uključuje pravila i zahtjeve o internom 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 provedba obveza iz ove Uredbe te relevantnih pravila i zahtjeva iz zakonodavstva Unije o financijskim uslugama, tijela odgovorna za nadzor i provedbu zakonodavstva o financijskim uslugama, uključujući prema potrebi Europsku središnju banku, trebala bi biti imenovana nadležnim tijelima za potrebe nadziranja provedbe ove Uredbe, uključujući aktivnosti nadzora tržišta, kad je riječ o UI sustavima koje pružaju ili upotrebljavaju financijske institucije koje su regulirane i pod nadzorom. Kako bi se dodatno poboljšala usklađenost ove Uredbe i pravila koja se primjenjuju na kreditne institucije regulirane na temelju Direktive 2013/36/EU Europskog parlamenta i Vijeća⁵⁶, primjereno je i integrirati postupak ocjenjivanja sukladnosti i 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 dobavljačkih sustava upravljanja kvalitetom i obveze praćenja za korisnike visokorizičnih UI sustava u mjeri u kojoj se primjenjuju na kreditne institucije uređene Direktivom 2013/36/EU.
- (81) Razvoj UI sustava koji nisu visokorizični u skladu sa zahtjevima ove Uredbe može dovesti do šire primjene pouzdane umjetne inteligencije u Uniji. Dobavljače UI sustava koji nisu visokorizični trebalo bi poticati na izradu kodeksa ponašanja kako bi se povećalo dobrovoljno ispunjavanje obveznih zahtjeva za visokorizične UI sustave. Dobavljače bi trebalo poticati i da dobrovoljno ispunjavaju dodatne zahtjeve koji se, primjerice, odnose na okolišnu održivost, pristupačnost za osobe s invaliditetom, sudjelovanje dionika u projektiranju i razvoju UI sustava te raznolikost razvojnih

⁵⁶ 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.).

timova. Komisija može osmisliti inicijative, među ostalim na sektorskoj razini, za lakše smanjivanje tehničkih zapreka prekograničnoj razmjeni podataka u svrhu razvoja umjetne inteligencije, među ostalim u području infrastrukture za pristup podacima te semantičke i tehničke interoperabilnosti različitih vrsta podataka.

- (82) Važno je da UI sustavi povezani s proizvodima koji nisu visokorizični prema ovoj Uredbi, pa ne moraju ispunjavati njezine zahtjeve, ipak budu sigurni kad se stavljaju na tržište ili u uporabu. Kako bi se pridonijelo tom cilju, Direktiva 2001/95/EZ Europskog parlamenta i Vijeća⁵⁷ primjenjivala bi se kao sigurnosni mehanizam.
- (83) 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.
- (84) Države članice trebale bi poduzeti sve potrebne mjere za provedbu odredaba ove Uredbe, među ostalim određivanjem učinkovitih, proporcionalnih i odvraćajućih sankcija za povrede tih odredaba. Za određene specifične povrede države članice trebale bi uzeti u obzir odstupanja i kriterije utvrđene u ovoj Uredbi. Europski nadzornik za zaštitu podataka trebao bi imati ovlast izreći novčane kazne institucijama, agencijama i tijelima Unije obuhvaćenima područjem primjene ove Uredbe.
- (85) Kako bi se regulatorni okvir mogao prilagođavati prema potrebi, Komisiji bi trebalo delegirati ovlast za donošenje akata u skladu s člankom 290. UFEU-a radi izmjene tehnika i pristupa iz Priloga I. za definiranje UI sustava, zakonodavstva Unije o usklađivanju iz Priloga II., visokorizičnih UI sustava iz Priloga III., odredaba o tehničkoj dokumentaciji iz Priloga IV., sadržaja EU izjave o sukladnosti iz Priloga V., odredaba o postupku ocjenjivanja sukladnosti iz priloga VI. i VII. te 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. Posebno je važno da Komisija u pripremnom radu provede odgovarajuća savjetovanja, među ostalim na stručnoj razini, te da se ta savjetovanja provedu u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu od 13. travnja 2016. o boljoj izradi zakonodavstva⁵⁸. Konkretno, s ciljem osiguravanja ravnopravnog sudjelovanja u pripremi delegiranih akata, Europski parlament i Vijeće primaju sve dokumente istodobno kad i stručnjaci iz država članica te njihovi stručnjaci sustavno imaju pristup sastancima stručnih skupina Komisije koji se odnose na pripremu delegiranih akata.
- (86) 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 Vijeća⁵⁹.
- (87) S obzirom na to da cilj ove Uredbe ne mogu dostatno ostvariti države članice i da se zbog opsega ili učinaka djelovanja na bolji način može ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti utvrđenim u članku 5. UFEU-a.

⁵⁷ Direktiva 2001/95/EZ Europskog parlamenta i Vijeća od 3. prosinca 2001. o općoj sigurnosti proizvoda (SL L 11, 15.1.2002., str. 4.).

⁵⁸ SL L 123, 12.5.2016., str. 1.

⁵⁹ 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.).

U skladu s načelom proporcionalnosti utvrđenim u tom članku ova Uredba ne prelazi ono što je potrebno za ostvarivanje tog cilja.

- (88) Ova bi se Uredba trebala primjenjivati od... [*OP – please insert the date established in Art. 85*]. Međutim, infrastruktura povezana s upravljanjem i sustavom za ocjenjivanje sukladnosti trebala bi biti spremna za uporabu prije tog datuma, pa bi se odredbe o prijavljenim tijelima i strukturama upravljanja trebale primjenjivati od... [*OP – please insert the date – three months following the entry into force of this Regulation*]. Usto, države članice trebale bi utvrditi pravila i obavijestiti Komisiju o sankcijama, 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 [*OP – please insert the date – twelve months following the entry into force of this Regulation*].
- (89) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka i Europskim odborom za zaštitu podataka u skladu s člankom 42. stavkom 2. Uredbe (EU) 2018/1725 te su oni dali mišljenje o [...],

DONIJELI SU OVU UREDBU:

GLAVA I.

OPĆE ODREDBE

Članak 1.

Predmet

Ovom se Uredbom utvrđuju:

- (a) usklađena pravila za stavljanje na tržište, stavljanje u uporabu i korištenje sustava umjetne inteligencije („UI sustavi”) u Uniji;
- (a) zabrane određenih praksi u području umjetne inteligencije;
- (b) posebni zahtjevi za visokorizične UI sustave i obveze za operatere takvih sustava;
- (c) usklađena pravila o transparentnosti za UI sustave namijenjene za interakciju s pojedincima, sustave za prepoznavanje emocija i sustave za biometrijsku kategorizaciju te UI sustave za generiranje slikovnog sadržaja, audiosadržaja i videosadržaja te manipuliranje njime;
- (d) pravila o praćenju i nadzoru tržišta.

Članak 2.

Područje primjene

1. Ova Uredba primjenjuje se na:

- (a) dobavljače koji stavljaju na tržište ili u uporabu UI sustave u Uniji, bez obzira na to imaju li ti dobavljači poslovni nastan u Uniji ili u trećoj zemlji;
- (b) korisnike UI sustava koji se nalaze u Uniji;
- (c) dobavljače i korisnike UI sustava koji se nalaze u trećoj zemlji ako se izlazni rezultati sustava upotrebljavaju u Uniji.

2. Na visokorizične UI sustave koji su sigurnosni sastavni dio proizvoda ili sustava ili koji su sami proizvodi ili sustavi i obuhvaćeni su područjem primjene sljedećih akata primjenjuje se samo članak 84. ove Uredbe:
 - (a) Uredba (EZ) br. 300/2008;
 - (b) Uredba (EU) br. 167/2013;
 - (c) Uredba (EU) br. 168/2013;
 - (d) Direktiva 2014/90/EU;
 - (e) Direktiva (EU) 2016/797;
 - (f) Uredba (EU) 2018/858;
 - (g) Uredba (EU) 2018/1139;
 - (h) Uredba (EU) 2019/2144.
3. Ova se Uredba ne primjenjuje na UI sustave koji su razvijeni ili se koriste isključivo u vojne svrhe.
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 organizacije koriste UI sustave u okviru međunarodnih sporazuma za suradnju s Unijom ili s jednom ili više država članica u područjima kaznenog progona i pravosuđa.
5. Ova Uredba ne utječe na primjenu odredaba o odgovornosti posrednih davatelja usluga utvrđenih u poglavlju II. odjeljku 4. Direktive 2000/31/EZ Europskog parlamenta i Vijeća⁶⁰ [kako će se zamijeniti odgovarajućim odredbama Akta o digitalnim uslugama].

Članak 3. Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

- (1) „sustav umjetne inteligencije” ili „UI sustav” znači softver koji je razvijen pomoću barem jedne tehnike ili pristupa iz Priloga I. i koji može, za zadani skup ciljeva koje odredi čovjek, generirati izlazne rezultate, kao što su sadržaj, predviđanja, preporuke ili odluke, koji utječu na okruženja s kojima su u interakciji;
- (2) „dobavljač” znači fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje razvija UI sustav ili ima UI sustav razvijen s ciljem njegova stavljanja na tržište ili stavljanja u uporabu pod vlastitim imenom ili žigom, uz plaćanje ili besplatno;
- (3) „mali dobavljač” znači dobavljač koji je mikropoduzeće ili malo poduzeće u smislu Preporuke Komisije 2003/361/EZ⁶¹;

⁶⁰ Direktiva 2000/31/EZ Europskog parlamenta i Vijeća od 8. lipnja 2000. o određenim pravnim aspektima usluga informacijskog društva na unutarnjem tržištu, posebno elektroničke trgovine (Direktiva o elektroničkoj trgovini) (SL L 178, 17.7.2000., str. 1.).

⁶¹ Preporuka Komisije od 6. svibnja 2003. o definiciji mikro, malih i srednjih poduzeća (SL L 124, 20.5.2003., str. 36.).

- (4) „korisnik” znači svaka fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje koristi UI sustav u okviru svoje nadležnosti, osim ako se UI sustav koristi u osobnoj neprofesionalnoj djelatnosti;
- (5) „ovlašteni zastupnik” znači svaka fizička ili pravna osoba s poslovnim nastanom u Uniji koju je dobavljač UI sustava napisмено ovlastio da u njegovo ime izvršava i provodi obveze i postupke utvrđene u ovoj Uredbi;
- (6) „uvoznik” znači svaka fizička ili pravna osoba s poslovnim nastanom u Uniji koja stavlja na tržište ili u uporabu UI sustav s imenom ili žigom fizičke ili pravne osobe s poslovnim nastanom izvan Unije;
- (7) „distributer” znači svaka fizička ili pravna osoba u opskrbnom lancu koja nije dobavljač ni uvoznik i koja stavlja UI sustav na tržište Unije ne utječući na njegova svojstva;
- (8) „operater” znači dobavljač, korisnik, ovlašteni zastupnik, uvoznik i distributer;
- (9) „stavljanje na tržište” znači prvo stavljanje UI sustava na raspolaganje na tržištu Unije;
- (10) „stavljanje na raspolaganje na tržištu” znači svaka isporuka UI sustava za distribuciju ili uporabu na tržištu Unije u okviru komercijalne djelatnosti, uz plaćanje ili besplatno;
- (11) „stavljanje u uporabu” znači isporuka UI sustava za prvu uporabu na tržištu Unije u skladu s njegovom namjenom izravno korisniku ili za vlastite potrebe;
- (12) „namjena” znači uporaba za koju je dobavljač namijenio UI sustav, uključujući specifični kontekst i uvjete uporabe, kako je određena u informacijama koje je dobavljač naveo u uputama za uporabu, promotivnim ili prodajnim materijalima i izjavama te u tehničkoj dokumentaciji;
- (13) „razumno predvidljiva kriva uporaba” znači uporaba UI sustava na način koji nije u skladu s njegovom namjenom, ali može biti posljedica razumno predvidljivog čovjekova ponašanja ili interakcije s drugim sustavima;
- (14) „sigurnosni sastavni dio proizvoda ili sustava” znači sastavni dio proizvoda ili sustava koji ima sigurnosnu funkciju u tom proizvodu ili sustavu ili čiji kvar ili neispravnost ugrožava zdravlje i sigurnost osoba ili imovine;
- (15) „upute za uporabu” znači informacije kojima dobavljač u prvom redu informira korisnika o namjeni i pravilnoj uporabi UI sustava, što uključuje specifično zemljopisno, bihevioralno ili radno okruženje u kojem je predviđena uporaba visokorizičnog UI sustava;
- (16) „povrat UI sustava” znači svaka mjera čija je svrha vraćanje dobavljaču UI sustava stavljenog na raspolaganje korisnicima;
- (17) „povlačenje UI sustava” znači svaka mjera čija je svrha sprečavanje distribucije, izlaganja i ponude UI sustava;
- (18) „sposobnost 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 provjerava jesu li ispunjeni zahtjevi iz glave III. poglavlja 2. ove Uredbe koji se odnose na 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 imenovano 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 stavljanja u uporabu koja utječe na sukladnost UI sustava sa zahtjevima iz glave III. poglavlja 2. ove Uredbe ili koja prouzroči promjenu namjene prema kojoj je UI sustav bio ocijenjen;
- (24) „oznaka sukladnosti CE” ili „oznaka CE” znači oznaka kojom dobavljač označuje da je UI sustav sukladan sa zahtjevima iz glave III. poglavlja 2. ove Uredbe i drugom primjenjivom zakonodavstvu Unije o usklađivanju uvjeta za stavljanje proizvoda na tržište („zakonodavstvo Unije o usklađivanju”) kojim se propisuje označivanje tom oznakom;
- (25) „praćenje nakon stavljanja na tržište” znači sve aktivnosti dobavljača UI sustava kojima proaktivno prikupljaju i analiziraju iskustva stečena korištenjem UI sustava koje stavljaju na tržište ili u uporabu radi utvrđivanja potencijalne potrebe za hitnim poduzimanjem nužnih korektivnih ili preventivnih radnji;
- (26) „tijelo za nadzor tržišta” znači nacionalno tijelo nadležno za provedbu aktivnosti i poduzimanje mjera na temelju Uredbe (EU) 2019/1020;
- (27) „usklađena norma” znači europska norma kako je definirana u članku 2. stavku 1. točki (c) Uredbe (EU) br. 1025/2012;
- (28) „zajedničke specifikacije” znači dokument koji nije norma a sadržava tehnička rješenja koja služe kao sredstvo za ispunjavanje određenih zahtjeva i obveza na temelju ove Uredbe;
- (29) „podaci za učenje” znači podaci koji se upotrebljavaju za učenje UI sustava prilagođavanjem njegovih poučivih parametara, uključujući težinske faktore neuronske mreže;
- (30) „podaci za validaciju” znači podaci koji se upotrebljavaju za evaluaciju poučenog UI sustava te za ugađanje njegovih nepoučivih parametara i njegova procesa učenja, među ostalim, kako bi se izbjegla prenaučenost, pritom skup podataka za validaciju može biti zaseban skup podataka ili varijabilni ili fiksni dio skupa podataka za učenje;
- (31) „podaci za testiranje” znači podaci koji se upotrebljavaju za neovisnu evaluaciju poučenog i validiranog UI sustava kako bi se potvrdilo očekivanu sposobnost tog sustava prije njegova stavljanja na tržište ili stavljanja u uporabu;
- (32) „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;
- (33) „biometrijski podaci” znači osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci;
- (34) „sustav za prepoznavanje emocija” znači UI sustav namijenjen za prepoznavanje emocija ili namjera pojedinaca ili izvođenje zaključaka o njihovim emocijama ili namjerama na temelju njihovih biometrijskih podataka;

- (35) „sustav za biometrijsku kategorizaciju” znači UI sustav namijenjen za razvrstavanje pojedinaca prema određenim kategorijama kao što su spol, dob, boja kose, boja očiju, tetovaže, etničko podrijetlo i seksualna ili politička orijentacija na temelju njihovih biometrijskih podataka;
- (36) „sustav za daljinsku biometrijsku identifikaciju” znači UI sustav namijenjen za daljinsko identificiranje pojedinaca usporedbom biometrijskih podataka osobe s biometrijskim podacima iz referentne baze podataka, pri čemu korisnik UI sustava ne može unaprijed znati hoće li osoba biti prisutna i može li je se identificirati;
- (37) „sustav za daljinsku biometrijsku identifikaciju u stvarnom vremenu” znači sustav za daljinsku biometrijsku identifikaciju koji bez znatnog kašnjenja prikuplja biometrijske podatke, vrši usporedbe i provodi identifikaciju. To uz trenutačnu identifikaciju obuhvaća i identifikaciju s ograničenim kratkim kašnjenjima kako bi se spriječilo zaobilaženje propisa;
- (38) „sustav za naknadnu daljinsku biometrijsku identifikaciju” znači sustav za daljinsku biometrijsku identifikaciju koji nije sustav za daljinsku biometrijsku identifikaciju u stvarnom vremenu;
- (39) „javno mjesto” znači svako fizičko mjesto dostupno javnosti, bez obzira na to vrijede li za pristup određeni uvjeti;
- (40) „tijelo kaznenog progona” znači:
- (a) svako tijelo javne vlasti nadležno za sprečavanje, istragu, otkrivanje ili progon kaznenih djela ili izvršavanje 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 izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje;
- (41) „kazneni progon” znači aktivnosti koje provode tijela za izvršavanje zakonodavstva radi sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanje kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje;
- (42) „nacionalno nadzorno tijelo” znači tijelo kojem država članica povjeri odgovornost za: provedbu i primjenu ove Uredbe, koordinaciju aktivnosti povjerenih toj državi članici, obavljanje funkcije jedinstvene kontaktne točke za Komisiju te zastupanje države članice u Europskom odboru za umjetnu inteligenciju;
- (43) „nacionalno nadležno tijelo” znači nacionalno nadzorno tijelo, tijelo koje provodi prijavljivanje i tijelo za nadzor tržišta;
- (44) „ozbiljan incident” znači svaki incident koji je izravno ili neizravno doveo, mogao dovesti ili može dovesti do bilo kojeg od sljedećeg:
- (a) smrti osobe ili znatne štete za zdravlje osobe, imovinu ili okoliš,
 - (b) ozbiljnog i nepovratnog poremećaja u upravljanju kritičnom infrastrukturuom i njezinu radu.

Članak 4.
Izmjene Priloga I.

Komisija je ovlaštena donositi delegirane akte u skladu s člankom 73. radi ažuriranja popisa tehnika i pristupa u Prilogu I. s obzirom na tržišne i tehnološke novine koje su po karakteristikama slične tehnikama i propisima na tom popisu.

GLAVA II.

ZABRANJENE PRAKSE U PODRUČJU UMJETNE INTELIGENCIJE

Članak 5.

1. Zabranjuju se sljedeće prakse u području umjetne inteligencije:
 - (a) stavljanje na tržište, stavljanje u uporabu ili korištenje UI sustava u kojem se primjenjuju subliminalne tehnike zbog kojih osoba nesvjesno bitno mijenja svoje ponašanje na način koji toj ili drugoj osobi uzrokuje ili bi mogao prouzročiti tjelesnu ili psihološku štetu;
 - (b) stavljanje na tržište, stavljanje u uporabu ili korištenje UI sustava koji iskorištava bilo koju slabost određene skupine osoba zbog njihove dobi ili tjelesnog ili mentalnog oštećenja radi bitnog mijenjanja ponašanja osobe koja pripada toj skupini na način koji toj ili drugoj osobi uzrokuje ili bi mogao uzrokovati tjelesnu ili psihološku štetu;
 - (c) stavljanje na tržište, stavljanje u uporabu ili korištenje UI sustava tijelima javne vlasti ili u njihovo ime u svrhu vrednovanja ili klasifikacije vjerodostojnosti pojedinaca u određenom razdoblju na temelju njihova društvenog ponašanja ili poznatih ili predviđenih osobnih obilježja ili obilježja osobnosti, pri čemu njihov društveni rejting uzrokuje barem jedno od sljedećeg:
 - i. štetno ili nepovoljno postupanje prema određenim pojedincima ili cijelim skupinama pojedinaca u društvenim kontekstima koji nisu povezani s kontekstima u kojima su podaci izvorno generirani ili prikupljeni;
 - ii. štetno ili nepovoljno postupanje prema određenim pojedincima ili cijelim skupinama pojedinaca koje je neopravdano ili nerazmjerno njihovu društvenom ponašanju ili težini njegovih posljedica;
 - (d) uporaba sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona, osim ako i u mjeri u kojoj je takvo korištenje nužno isključivo radi jednog od sljedećih ciljeva:
 - i. ciljane potrage za konkretnim potencijalnim žrtvama kaznenih djela, uključujući nestalu djecu;
 - ii. sprečavanja konkretne, znatne i neposredne prijetnje životu ili tjelesnoj sigurnosti pojedinaca ili terorističkog napada;
 - iii. otkrivanja, lociranja, identifikacije ili progona počinitelja kaznenog djela ili osumnjičenika za kazneno djelo iz članka 2. stavka 2. Okvirne odluke Vijeća 2002/584/PUP⁶² koje je u državi članici kažnjivo najvišom

⁶²

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

kaznom zatvora ili oduzimanjem slobode od najmanje tri godine, kako je utvrđeno pravom te države članice.

2. Za uporabu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona radi bilo kojeg cilja iz stavka 1. točke (d) u obzir se uzimaju sljedeći elementi:
 - (a) priroda situacije zbog koje se pojavila mogućnost uporabe, osobito težina, vjerojatnost i razmjer štete koja bi nastala nekorištenjem sustava;
 - (b) posljedice uporabe sustava na prava i slobode svih zahvaćenih osoba, osobito težina, vjerojatnost i razmjer tih posljedica.

Usto, uporaba sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona radi bilo kojeg cilja iz stavka 1. točke (d) mora biti u skladu s nužnim i razmjernim zaštitnim mjerama i uvjetima uporabe, osobito u pogledu vremenskih, zemljopisnih i osobnih ograničenja.

3. Kad je riječ o stavku 1. točki (d) i stavku 2., za svaku pojedinačnu uporabu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu za potrebe kaznenog progona potrebno je prethodno odobrenje sudskog tijela ili neovisnog upravnog tijela države članice u kojoj će se sustav uporabiti, a koje se izdaje na obrazložen zahtjev i u skladu s detaljnim pravilima nacionalnog prava iz stavka 4. U propisno opravdanim hitnim situacijama, međutim, uporaba sustava može početi bez odobrenja i odobrenje se može zatražiti tek tijekom ili nakon uporabe.

Nadležno pravosudno ili upravno tijelo izdaje odobrenje samo ako je uvjereno, na temelju objektivnih dokaza ili jasnih naznaka koje su mu iznesene, da je konkretna uporaba sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu nužna i razmjerna za postizanje jednog od ciljeva iz stavka 1. točke (d), navedenog u zahtjevu. Pri odlučivanju o zahtjevu nadležno sudsko ili upravno tijelo uzima u obzir elemente iz stavka 2.

4. Država članica može odlučiti propisati mogućnost potpunog ili djelomičnog odobrenja uporabe sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima za potrebe kaznenog progona uz ograničenja i pod uvjetima iz stavka 1. točke (d) te stavaka 2. i 3. Ta država članica u svojem nacionalnom pravu utvrđuje potrebna detaljna pravila o podnošenju zahtjeva za odobrenja iz stavka 3. te izdavanje, izvršavanje i nadzor tih odobrenja. U tim se pravilima određuje i za se koje ciljeve iz stavka 1. točke (d), što znači i za koja kaznena djela iz njegove podtočke iii., nadležnim tijelima može odobriti uporaba tih sustava za potrebe kaznenog progona.

GLAVA III.

VISOKORIZIČNI UI SUSTAVI

POGLAVLJE 1.

KLASIFIKACIJA VISOKORIZIČNIH UI SUSTAVA

Članak 6.

Pravila klasifikacije visokorizičnih UI sustava

1. UI sustav smatra se visokorizičnim ako su ispunjena oba sljedeća uvjeta, bez obzira na to stavlja li se UI sustav na tržište ili u uporabu neovisno o proizvodima iz točaka (a) i (b):
 - (a) UI sustav namijenjen je za uporabu kao sigurnosni sastavni dio proizvoda ili je sam po sebi proizvod koji je obuhvaćen zakonodavstvom Unije o usklađivanju iz Priloga II.;
 - (b) za proizvod kojeg je UI sustav sigurnosni sastavni dio ili UI sustav koji je sam po sebi proizvod zahtijeva se ocjenjivanje sukladnosti koje provodi treća strana radi stavljanja na tržište ili stavljanja u uporabu tog proizvoda na temelju zakonodavstva Unije o usklađivanju iz Priloga II.
2. Među visokorizične sustave, uz one iz stavka 1., ubrajaju se i UI sustavi iz Priloga III.

Članak 7.

Izmjene Priloga III.

1. Komisija je ovlaštena donositi delegirane akte u skladu s člankom 73. u svrhu ažuriranja popisa iz Priloga III. dodavanjem visokorizičnih UI sustava ako su ispunjena oba sljedeća uvjeta:
 - (a) UI sustavi namijenjeni su za uporabu u bilo kojem području iz točaka od 1. do 8. Priloga III.;
 - (b) kod tih UI sustava postoji rizik od štete za zdravlje i sigurnost ili rizik od nepovoljnog utjecaja na temeljna prava koji je, u smislu ozbiljnosti i vjerojatnosti pojavljivanja, najmanje jednak riziku od štete ili nepovoljnog utjecaja koji postoji kod visokorizičnih UI sustava već navedenih u Prilogu III.
2. Kad za potrebe stavka 1. procjenjuje postoji li kod UI sustava rizik od štete za zdravlje i sigurnost ili rizik od nepovoljnog utjecaja na temeljna prava koji je najmanje jednak riziku od štete koji postoji kod visokorizičnih UI sustava koji su već navedeni u Prilogu III., Komisija uzima u obzir sljedeće kriterije:
 - (a) namjenu UI sustava;
 - (b) stupanj u kojem se UI sustav rabi ili će se vjerojatno rabiti;
 - (c) stupanj u kojem je uporaba UI sustava već prouzročila štetu zdravlju ili sigurnosti ili nepovoljan utjecaj na temeljna prava ili u kojem izaziva snažnu zabrinutost da bi mogla prouzročiti takvu štetu ili nepovoljan utjecaj, kako je

potvrđen izvješćima ili dokumentiranim navodima koji su podneseni nacionalnim nadležnim tijelima;

- (d) potencijalne razmjere takve štete ili takvog nepovoljnog utjecaja, osobito u smislu intenziteta i mogućnosti da zahvati mnogo osoba;
- (e) stupanj ovisnosti potencijalno oštećenih osoba ili osoba potencijalno izloženih nepovoljnom utjecaju o krajnjem ishodu uporabe UI sustava, osobito ako taj ishod nije razumno moguće ne prihvatiti zbog praktičnih ili pravnih razloga;
- (f) stupanj u kojem su potencijalno oštećene osobe ili osobe potencijalno izložene nepovoljnom utjecaju u ranjivu položaju u odnosu na korisnika UI sustava, osobito zbog neravnoteže moći, znanja, gospodarskih ili socijalnih okolnosti ili dobi;
- (g) stupanj u kojem je krajnji ishod uporabe UI sustava lako poništiv, pri čemu se krajnji ishodi koji utječu na zdravlje ili sigurnost osoba ne smatraju lako poništivima;
- (h) stupanj u kojem postojeći propisi 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 znatno smanjenje tih rizika.

POGLAVLJE 2.

ZAHTJEVI ZA VISOKORIZIČNE UI SUSTAVE

Članak 8.

Ispunjavanje zahtjeva

1. Visokorizični UI sustavi moraju ispunjavati zahtjeve utvrđene u ovom poglavlju.
2. Kod osiguravanja ispunjavanja tih zahtjeva u obzir se uzimaju namjena visokorizičnog UI sustava i sustav upravljanja rizicima iz članka 9.

Članak 9.

Sustav upravljanja rizicima

1. Za visokorizične UI sustave uspostavlja se, primjenjuje i održava sustav upravljanja rizicima te se o njemu vodi dokumentacija.
2. Sustav upravljanja rizicima sastoji se od kontinuiranog iterativnog procesa koji se izvodi cijeli životni vijek visokorizičnog UI sustava i koji je potrebno redovito sustavno ažurirati. Čine ga sljedeći koraci:
 - (a) identificiranje i analiza poznatih i predvidljivih rizika povezanih sa svakim visokorizičnim UI sustavom;
 - (b) procjenjivanje i evaluacija rizika koji mogu nastati pri uporabi visokorizičnog UI sustava u skladu s njegovom namjenom i u uvjetima razumno predvidljive krive uporabe;
 - (c) evaluacija drugih potencijalnih rizika na temelju analize podataka prikupljenih sustavom praćenja nakon stavljanja na tržište iz članka 61.;

- (d) donošenje odgovarajućih mjera za upravljanje rizicima u skladu s odredbama sljedećih stavaka.
3. U mjerama upravljanja rizicima iz stavka 2. točke (d) uzimaju se u obzir učinci i moguće interakcije koji proizlaze iz kombinirane primjene zahtjeva iz ovog poglavlja. U obzir se uzimaju i općepriznata najnovija dostignuća, među ostalim kako su izražena u relevantnim usklađenim normama ili zajedničkim specifikacijama.
4. Mjere upravljanja rizicima iz stavka 2. točke (d) takve su da eventualni preostali rizik povezan sa svakom pojedinom opasnošću te cjelokupni preostali rizik visokorizičnih UI sustava mora biti ocijenjen kao prihvatljiv, pod uvjetom da se visokorizični UI sustav rabi u skladu sa svojom namjenom ili u uvjetima razumno predvidljive krive uporabe. Korisnike se mora obavijestiti o tim preostalim rizicima.
- Kao najprikladnije mjere upravljanja rizicima utvrđuju se one kojima se osigurava sljedeće:
- (a) uklanjanje rizika ili svođenje rizika na najmanju moguću mjeru odgovarajućim projektiranjem i razvojem;
 - (b) prema potrebi, poduzimanje odgovarajućih mjera za smanjenje i kontrolu rizika koji se ne mogu ukloniti;
 - (c) pružanje odgovarajućih informacija korisnicima u skladu s člankom 13., osobito o rizicima iz stavka 2. točke (b) ovog članka i, prema potrebi, osposobljavanje korisnika.
- Kod uklanjanja ili smanjenja rizika povezanih s uporabom visokorizičnog UI sustava u obzir se uzimaju tehničko znanje, iskustvo, obrazovanje i osposobljavanje koje se očekuje od korisnika te predviđeno okruženje za uporabu sustava.
5. Da bi se utvrdile najprikladnije mjere upravljanja rizicima, visokorizični UI sustavi se testiraju. Testiranjem se provjerava da visokorizični UI sustavi postojano rade u skladu s namjenom i da ispunjavaju zahtjeve utvrđene u ovom poglavlju.
6. Postupci testiranja moraju biti prikladni za postizanje namjene UI sustava i ne trebaju obuhvaćati više nego što je potrebno za postizanje te namjene.
7. Visokorizični UI sustavi testiraju se prema potrebi u bilo kojem trenutku razvojnog procesa, a u svakom slučaju prije stavljanja na tržište ili stavljanja u uporabu. Testiranje se provodi u odnosu na preliminarno definirane parametre i probabilističke pragove koji su primjereni za namjenu visokorizičnog UI sustava.
8. Pri uvođenju sustava upravljanja rizicima opisanog u stavcima od 1. do 7. posebno se vodi računa o vjerojatnosti da će visokorizični UI sustav utjecati na djecu ili da će mu djeca imati pristup.
9. Za kreditne institucije regulirane Direktivom 2013/36/EU aspekti opisani u stavcima 1. do 8. dio su postupaka upravljanja rizicima koje te institucije uspostavljaju na temelju članka 74. te direktive.

Članak 10.

Podaci i upravljanje podacima

1. Visokorizični UI sustavi koji koriste tehnike s učenjem modelâ pomoću podataka razvijaju se na temelju skupova podataka za učenje, validaciju i testiranje koji ispunjavaju kriterije kvalitete iz stavaka od 2. do 5.

2. Na skupove podataka za učenje, validaciju i testiranje primjenjuju se odgovarajuće prakse upravljanja podacima. Te se prakse ponajprije odnose na:
 - (a) relevantne odluke o organizaciji podataka;
 - (b) prikupljanje podataka;
 - (c) relevantne postupke obrade za pripremu podataka, kao što su obilježavanje, označivanje, čišćenje, obogaćivanje i agregiranje;
 - (d) formuliranje relevantnih pretpostavki, osobito s obzirom na informacije koje bi podaci trebali mjeriti i predstavljati;
 - (e) prethodnu procjenu raspoloživosti, količine i prikladnosti potrebnih skupova podataka;
 - (f) pregled s obzirom na moguće pristranosti;
 - (g) utvrđivanje svih mogućih nepotpunosti i nedostataka podataka te načina na koje se te nepotpunosti i nedostaci mogu ukloniti.
3. Skupovi podataka za učenje, validaciju i testiranje su relevantni, reprezentativni, bez pogrešaka i potpuni. Imaju odgovarajuća statistička obilježja, prema potrebi i u odnosu na osobe ili skupine osoba za koje se visokorizični UI sustav namjerava rabiti. Te se karakteristike skupova podataka mogu postići na razini pojedinačnih skupova podataka ili njihove kombinacije.
4. U skupovima podataka za učenje, validaciju i testiranje u obzir se uzimaju, u mjeri u kojoj to iziskuje namjena, karakteristike ili elementi specifični za zemljopisno, bihevioralno ili radno okruženje u kojem je previđena uporaba visokorizičnog UI sustava.
5. Dobavljači visokorizičnih UI sustava mogu, u mjeri u kojoj je to nužno kako bi se osiguralo praćenje, otkrivanje i ispravljanje pristranosti povezanih s tim sustavima, obrađivati posebne 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, ovisno o odgovarajućim zaštitnim mjerama koje se odnose na temeljna prava i slobode pojedinaca, uključujući tehnička ograničenja ponovne uporabe i uporabe vrhunskih sigurnosnih mjera i mjera zaštite privatnosti, kao što je pseudonimizacija ili enkripcija u slučaju da anonimizacija može znatno omesti željenu svrhu.
6. Za razvoj visokorizičnih UI sustava koji ne koriste tehnike s učenjem modelâ primjenjuju se odgovarajuće prakse upravljanja podacima kojima se osigurava usklađenost tih sustava sa stavkom 2.

Članak 11.

Tehnička dokumentacija

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

Tehnička dokumentacija sastavlja se tako da se njome dokaže da visokorizični UI sustav ispunjava zahtjeve iz ovog poglavlja te da se nacionalnim nadležnim tijelima i prijavljenim tijelima pruže sve potrebne informacije za ocjenjivanje sukladnosti UI sustava s tim zahtjevima. Minimalno sadržava elemente utvrđene u Prilogu IV.

2. U slučaju stavljanja na tržište ili stavljanja u uporabu visokorizičnog UI sustava povezanog s proizvodom na koji se primjenjuju pravni akti iz odjeljka A Priloga II. sastavlja se jedinstvena tehnička dokumentacija koja sadržava sve informacije iz Priloga IV. i informacije potrebne na temelju tih pravnih akata.
3. Kako bi se osiguralo da tehnička dokumentacija sadržava sve potrebne informacije za ocjenjivanje sukladnosti sustava sa zahtjevima iz ovog poglavlja, Komisija je ovlaštena donositi delegirane akte u skladu s člankom 73. radi izmjene, prema potrebi, Priloga IV. s obzirom na tehnički napredak.

Članak 12. Evidentiranje

1. Visokorizični UI sustavi projektiraju se i razvijaju tako da imaju funkciju automatskog bilježenja događaja („dnevnicu događaja”) tijekom svojeg rada. Te funkcije bilježenja događaja moraju biti u skladu s priznatim standardima ili zajedničkim specifikacijama.
2. Funkcije bilježenja događaja takve su da osiguravaju razinu sljedivosti funkcioniranja UI sustava tijekom njegova životnog ciklusa koja je primjerena namjeni tog sustava.
3. Točnije, funkcije bilježenja događaja omogućuju praćenje rada visokorizičnog UI sustava s obzirom na pojavu situacija zbog kojih UI sustav može predstavljati rizik u smislu članka 65. stavka 1. ili koje mogu dovesti do bitne izmjene te olakšavaju praćenje nakon stavljanja na tržište iz članka 61.
4. Funkcije bilježenja događaja visokorizičnih UI sustava iz stavka 1. točke (a) Priloga III bilježe najmanje:
 - (a) razdoblje svake uporabe sustava (datum i vrijeme početka te datum i vrijeme završetka svake uporabe);
 - (b) referentnu bazu podataka s kojom je sustav usporedio ulazne podatke;
 - (c) ulazne podatke za koje je pretragom pronađen rezultat;
 - (d) identitet pojedinaca koji su sudjelovali u provjeri rezultata iz članka 14. stavka 5.

Članak 13. Transparentnost i informiranje korisnika

1. Visokorizični UI sustavi projektiraju se i razvijaju tako da njihov rad bude dovoljno transparentan da korisnici mogu tumačiti izlazne rezultate sustava i primjereno ih koristiti. Osigurava se odgovarajuća vrsta i stupanj transparentnosti kako bi se ispunile relevantne obveze korisnika i dobavljača utvrđene u poglavlju 3. ove glave.
2. Visokorizičnim UI sustavima prilažu se upute za uporabu u odgovarajućem digitalnom ili drugom formatu sa sažetim, potpunim, točnim i jasnim informacijama koje su korisnicima važne, pristupačne i razumljive.
3. U informacijama iz stavka 2. navode se:
 - (a) identitet i kontaktni podaci dobavljača i, prema potrebi, njegova ovlaštenog zastupnika;

- (b) karakteristike, mogućnosti i ograničenja sposobnosti visokorizičnog UI sustava, uključujući:
 - i. njegovu namjenu
 - ii. razine točnosti, otpornosti i kibersigurnosti iz članka 15. u odnosu na koje je visokorizični UI sustav testiran i potvrđen i koje se mogu očekivati te sve poznate i predvidljive okolnosti koje mogu utjecati na tu očekivanu razinu točnosti, stabilnosti i kibersigurnosti;
 - iii. sve poznate i predvidljive okolnosti povezane s uporabom visokorizičnog UI sustava u skladu s njegovom namjenom ili u uvjetima razumno predvidljive krive uporabe koje mogu prouzročiti rizike za zdravlje i sigurnost ili temeljna prava;
 - iv. sposobnost sustava u odnosu na osobe ili skupine osoba za koje se sustav namjerava rabiti;
 - v. prema potrebi, specifikacije ulaznih podataka ili sve druge važne informacije o korištenim skupovima podataka za učenje, validaciju i testiranje, uzimajući u obzir namjenu UI sustava;
- (c) promjene visokorizičnog UI sustava i njegove sposobnosti koje je dobavljač unaprijed odredio u trenutku početnog ocjenjivanja sukladnosti, ako ih ima;
- (d) mjere ljudskog nadzora iz članka 14., uključujući tehničke mjere uvedene kako bi se korisnicima olakšalo tumačenje izlaznih rezultata UI sustava;
- (e) očekivani životni vijek visokorizičnog UI sustava i sve potrebne mjere održavanja i brige kako bi se osiguralo pravilno funkcioniranje UI sustava, što se odnosi i na softverska ažuriranja.

Članak 14. Ljudski nadzor

1. Visokorizični UI sustavi projektiraju se i razvijaju, među ostalim ugrađujući odgovarajuće alate u korisničko sučelje, tako da ih pojedinci mogu djelotvorno nadzirati tijekom uporabe.
2. Cilj je ljudskog nadzora sprečavanje ili minimiziranje rizika za zdravlje, sigurnost ili temeljna prava koji se mogu pojaviti tijekom uporabe visokorizičnog UI sustava u skladu s namjenom ili u uvjetima razumno predvidljive krive uporabe, osobito ako su takvi rizici prisutni unatoč primjeni drugih zahtjeva iz ovog poglavlja.
3. Ljudski nadzor osigurava se svim ili bilo kojim sljedećim mjerama:
 - (a) mjerama koje dobavljač utvrđuje i ugrađuje, ako je tehničko izvedivo, u visokorizični UI sustav prije stavljanja na tržište ili stavljanja u uporabu;
 - (b) mjerama koje dobavljač utvrđuje prije stavljanja na tržište ili stavljanja u uporabu visokorizičnog UI sustava a koje su primjerene da ih provodi korisnik.
4. Mjere iz stavka 3. omogućuju pojedincima kojima je povjeren ljudski nadzor da, ovisno o okolnostima:
 - (a) posve razumiju mogućnosti i ograničenja visokorizičnog UI sustava te da pravilno prate njegov rad kako bi se znakovi nepravilnosti, disfunkcija i neočekivanih rezultata mogli što prije otkriti i ispraviti;

- (b) budu svjesni moguće tendencije nevoljnog ili pretjeranog oslanjanja na izlazne rezultate visokorizičnog UI sustava („automatizacijska pristranost”), osobito visokorizičnih UI sustava koji se rabe za davanje informacija ili preporuka na temelju kojih odluke donose pojedinci;
 - (c) točno protumače izlazni rezultat visokorizičnog UI sustava, uzimajući u obzir karakteristike sustava te dostupne alate i metode za tumačenje;
 - (d) u bilo kojoj situaciji odustanu od korištenja visokorizičnog UI sustava ili drukčije zanemare, zaobiđu ili ponište izlazni rezultat visokorizičnog UI sustava;
 - (e) interveniraju u rad visokorizičnog UI sustava ili ga prekinu pritiskom na gumb za zaustavljanje ili sličnim postupkom.
5. Za visokorizične UI sustave iz točke 1. podtočke (a) Priloga III. mjerama iz stavka 3. mora se usto osigurati da korisnik ne poduzima nikakvu radnju niti donosi ikakvu odluku na temelju identifikacije koja je rezultat sustava ako je nisu provjerila i potvrdila barem dva pojedinca.

Članak 15.

Točnost, otpornost i kibersigurnost

1. Visokorizični UI sustavi projektiraju se i razvijaju tako da imaju odgovarajuću razinu točnosti, otpornosti i kibersigurnosti s obzirom na namjenu te da im je u tim aspektima radni učinak tijekom životnog ciklusa ujednačen.
2. Razine točnosti i relevantni parametri točnosti visokorizičnih UI sustava navode se u popratnim uputama za uporabu.
3. Visokorizični UI sustavi moraju biti otporni na greške, kvarove ili nedosljednosti koje se mogu dogoditi unutar sustava ili okruženja u kojem sustav radi, osobito zbog njihove interakcije s pojedincima ili drugim sustavima.

Otpornost visokorizičnih UI sustava može se riješiti tehničkom redundancijom, što može uključivati pričuvene ili zaštitne planove.

Visokorizični UI sustavi koji nastavljaju učiti nakon stavljanja na tržište ili stavljanja u uporabu razvijaju se tako da se osigura da se na izlazne rezultate koji bi mogli biti pristrani jer su kao ulazni podaci za buduće operacije korišteni izlazni rezultati („povratne veze”) primjenjuju odgovarajuće mjere za smanjenje te mogućnosti.

4. Visokorizični UI sustavi moraju biti otporni na pokušaje neovlaštenih trećih strana da im izmijene uporabu ili sposobnost iskorištavanjem slabih točaka sustava.

Tehnička rješenja za kibersigurnost visokorizičnih UI sustava moraju biti primjerena relevantnim okolnostima i rizicima.

Tehnička rješenja za prevladavanje specifičnih slabih točaka UI-ja obuhvaćaju, prema potrebi, mjere za sprečavanje i obuzdavanje napada kojima je cilj manipuliranje skupom podataka za učenje („trovanje podataka”), ulaznim podacima kako bi model načinio pogrešku („neprijateljski primjeri”) ili nedostacima modela.

POGLAVLJE 3.

OBVEZE DOBAVLJAČA I KORISNIKA VISOKORIZIČNIH UI SUSTAVA I DRUGIH STRANA

Članak 16.

Obveze dobavljača visokorizičnih UI sustava

Dobavljači visokorizičnih UI sustava dužni su:

- (a) pobrinuti se da njihovi visokorizični UI sustavi ispunjavaju zahtjeve iz poglavlja 2. ove glave;
- (b) imati uspostavljen sustav upravljanja kvalitetom koji je u skladu s člankom 17.;
- (c) sastaviti tehničku dokumentaciju visokorizičnog UI sustava;
- (d) čuvati dnevnike događaja koje automatski generiraju njihovi visokorizični UI sustavi ako su oni pod njihovom kontrolom;
- (e) pobrinuti se da visokorizični UI sustav prije stavljanja na tržište ili stavljanja u uporabu prođe relevantni postupak ocjenjivanja sukladnosti;
- (f) ispuniti obveze registracije iz članka 51.;
- (g) poduzeti potrebne korektivne mjere ako visokorizični UI sustav nije sukladan sa zahtjevima iz poglavlja 2. ove glave;
- (h) o neusklađenosti i svim poduzetim korektivnim mjerama obavijestiti nacionalna nadležna tijela država članica u kojima su UI sustav stavili na raspolaganje ili u uporabu i, prema potrebi, prijavljeno tijelo;
- (i) označiti svoje visokorizične UI sustave oznakom CE kako bi iskazali sukladnost s ovom Uredbom u skladu s člankom 49.
- (j) na zahtjev nacionalnog nadležnog tijela, dokazati sukladnost visokorizičnog UI sustava sa zahtjevima iz poglavlja 2. ove glave.

Članak 17.

Sustav upravljanja kvalitetom

1. Dobavljači visokorizičnih UI sustava dužni su uspostaviti 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 te on 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 koje treba provoditi u projektiranju te nadzoru i provjeri projektiranja visokorizičnog UI sustava
 - (c) tehnike, postupke i sustavne aktivnosti koje treba provoditi u razvoju te kontroli kvalitete i osiguranju kvalitete visokorizičnog UI sustava;

- (d) postupke pregleda, testiranja i validacije koje treba provesti prije, tijekom i poslije razvoja visokorizičnog UI sustava te učestalost kojom se moraju provoditi,
 - (e) tehničke specifikacije, uključujući norme, koje treba primijeniti i, ako relevantne usklađene norme nisu u cijelosti primijenjene, sredstva kojima treba osigurati sukladnost visokorizičnog UI sustava sa zahtjevima iz poglavlja 2. ove glave;
 - (f) sustave i postupke za upravljanje podacima, uključujući 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 i za potrebe stavljanja na tržište ili stavljanja u uporabu visokorizičnih UI sustava;
 - (g) sustav upravljanja rizicima iz članka 9.;
 - (h) uspostavu, primjenu i održavanje sustava praćenja nakon stavljanja na tržište u skladu s člankom 61.;
 - (i) postupke povezane s prijavljivanjem ozbiljnih incidenata i neispravnosti u skladu s člankom 62.;
 - (j) postupke komunikacije s nacionalnim nadležnim tijelima i drugim nadležnim tijelima, uključujući sektorska, te pružanje ili olakšavanje pristupa podacima, prijavljenim tijelima, drugim operaterima, klijentima ili drugim zainteresiranim stranama;
 - (k) sustave i postupke za arhiviranje sve važne dokumentacije i svih važnih informacija;
 - (l) upravljanje resursima, uključujući mjere koje se odnose na sigurnost opskrbe;
 - (m) okvir za odgovornost kojim se utvrđuje odgovornost uprave i drugog osoblja za sve aspekte navedene u ovom stavku.
2. Aspekti iz stavka 1. primjenjuju se razmjerno veličini dobavljačeve organizacije.
3. Za dobavljače koji su kreditne institucije regulirane Direktivom 2013/36/EU obveza uspostave sustava upravljanja kvalitetom smatra se ispunjenom ako poštuju pravila o sustavima, procesima i mehanizmima internog upravljanja u skladu s člankom 74. te direktive. U tom se kontekstu u obzir uzimaju sve usklađene norme iz članka 40. ove Uredbe.

Članak 18.

Obveza sastavljanja tehničke dokumentacije

1. Dobavljači visokorizičnih UI sustava dužni su sastaviti tehničku dokumentaciju iz članka 11. u skladu s Prilogom IV.
2. Dobavljači koji su kreditne institucije regulirane Direktivom 2013/36/EU vode tehničku dokumentaciju kao dio dokumentacije o sustavima, procesima i mehanizmima internog upravljanja u skladu s člankom 74. te direktive.

Članak 19.
Ocjenjivanje sukladnosti

1. Dobavljači visokorizičnih UI sustava dužni su se pobrinuti da njihovi sustavi prije stavljanja na tržište ili stavljanja u uporabu prođu relevantni postupak ocjenjivanja u skladu s postupkom iz članka 43. Ako se na temelju tog ocjenjivanja dokaže da UI sustav ispunjava zahtjeve iz poglavlja 2. ove glave, dobavljači sastavljaju EU izjavu o sukladnosti u skladu s člankom 48. i označuju UI sustav oznakom sukladnosti CE u skladu s člankom 49.
2. Za visokorizične UI sustave iz točke 5. podtočke (b) Priloga III., koje na tržište ili u uporabu stavljaju dobavljači koji su kreditne institucije regulirane Direktivom 2013/36/EU, ocjenjivanje sukladnosti provodi se u okviru postupka iz članaka od 97. do 101. te direktive.

Članak 20.
Automatski generirani dnevници događaja

1. Dobavljači visokorizičnih UI sustava dužni su čuvati dnevnik događaja koje automatski generiraju njihovi visokorizični UI sustavi u mjeri u kojoj su takvi dnevници događaja pod njihovom kontrolom na temelju ugovornog odnosa s korisnikom ili druge pravne osnove. Dnevници događaja čuvaju se tijekom razdoblja koje je primjereno s obzirom na namjenu visokorizičnog UI sustava i primjenjivih pravnih obveza na temelju prava Unije ili nacionalnog prava.
2. Dobavljači koji su kreditne institucije regulirane Direktivom 2013/36/EU čuvaju dnevnik događaja koje automatski generiraju njihovi visokorizični UI sustavi kao dio dokumentacije u skladu s člankom 74. te direktive.

Članak 21.
Korektivne mjere

Dobavljači visokorizičnih UI sustava koji smatraju ili imaju razloga smatrati da visokorizični UI sustav koji su stavili na tržište ili u uporabu nije sukladan s ovom Uredbom odmah poduzimaju potrebne korektivne radnje kako bi, prema potrebi, postigli sukladnost tog sustava ili ga povukli ili proveli njegov povrat. O dotičnom visokorizičnom UI sustavu obavješćuju distributere i, prema potrebi i na odgovarajući način, ovlaštenog zastupnika i uvoznike.

Članak 22.
Obveza obavješćivanja

Ako visokorizični UI sustav predstavlja rizik u smislu članka 65. stavka 1. i dobavljač sustava zna za taj rizik, taj dobavljač odmah obavješćuje nacionalna nadležna tijela država članica u kojima je stavio sustav na raspolaganje i, prema potrebi, prijavljeno tijelo koje je izdalo potvrdu za taj visokorizični UI sustav, osobito o neusklađenosti i svim poduzetim korektivnim mjerama.

Članak 23.
Suradnja s nadležnim tijelima

Dobavljači visokorizičnih UI sustava nacionalnom nadležnom tijelu na njegov zahtjev pružaju sve informacije i dokumentaciju potrebne za dokazivanje sukladnosti visokorizičnog UI sustava sa zahtjevima iz poglavlja 2. ove glave na službenom jeziku Unije koji odredi dotična

država članica. Na obrazloženi zahtjev nacionalnog nadležnog tijela dobavljači tom tijelu daju i pristup dnevnicima događaja koje je automatski generirao visokorizični UI sustav u mjeri u kojoj su takve dnevници događaja pod njihovom kontrolom na temelju ugovornog odnosa s korisnikom ili druge pravne osnove.

Članak 24.

Obveze proizvođača proizvoda

Ako se visokorizični UI sustav povezan s proizvodima na koje se primjenjuju pravni akti iz odjeljka A Priloga II. stavlja na tržište ili u uporabu zajedno s proizvodom proizvedenim u skladu s tim pravnim aktima i pod imenom proizvođača tog proizvoda, proizvođač proizvoda preuzima odgovornost za usklađenost UI sustava s ovom Uredbom i u pogledu UI sustava ima iste obveze koje su ovom Uredbom propisane dobavljaču.

Članak 25.

Ovlašteni zastupnici

1. Prije stavljanja svojih sustava na raspolaganje na tržištu Unije, ako se uvoznik ne može identificirati, dobavljači s poslovnim nastanom izvan Unije pisanim ovlaštenjem imenuju ovlaštenog zastupnika s poslovnim nastanom Uniji.
2. Ovlašteni zastupnik obavlja zadaće navedene u ovlaštenju koje je dobio od dobavljača. Ovlaštenjem se ovlaštenom zastupniku daje ovlast da obavlja sljedeće zadaće:
 - (a) ima na raspolaganju primjerak EU izjave o sukladnosti i tehničke dokumentacije za nacionalna nadležna tijela i nacionalna tijela iz članka 63. stavka 7.;
 - (b) nacionalnom nadležnom tijelu, na obrazloženi zahtjev, daje sve informacije i dokumentaciju potrebne za dokazivanje sukladnosti visokorizičnog UI sustava sa zahtjevima iz poglavlja 2. ove glave; to uključuje i davanje pristupa dnevnicima događaja koje automatski generira visokorizični UI sustav u mjeri u kojoj su takvi dnevници događaja pod dobavljačevom kontrolom na temelju ugovornog odnosa s korisnikom ili druge pravne osnove.
 - (c) na obrazloženi zahtjev surađuje s nadležnim nacionalnim tijelima u svim radnjama koje ta tijela poduzimaju u vezi s visokorizičnim UI sustavom.

Članak 26.

Obveze uvoznika

1. Prije stavljanja visokorizičnog UI sustava na tržište uvoznici takvog sustava dužni su se pobrinuti da je:
 - (a) dobavljač tog UI sustava proveo odgovarajući postupak ocjenjivanja sukladnosti;
 - (b) dobavljač sastavio tehničku dokumentaciju u skladu s Prilogom IV.;
 - (c) sustav označen oznakom sukladnosti te da su mu priložene potrebna dokumentacija i upute za upotrebu.
2. Ako uvoznik smatra ili ima razloga smatrati da visokorizični UI sustav nije sukladan s ovom Uredbom, ne stavlja taj sustav na tržište dok ga se ne učini sukladnim. Ako

visokorizični UI sustav predstavlja rizik u smislu članka 65. stavka 1., uvoznik o tome obavješćuje dobavljača UI sustava i tijela za nadzor tržišta.

3. Uvoznici na visokorizičnom UI sustavu ili, ako to nije moguće, na ambalaži ili popratnoj dokumentaciji, ovisno o slučaju, navode svoje ime, registrirano trgovačko ime ili registrirani žig i adresu na koju im se moguće obratiti u vezi s tim sustavom.
4. Dok je visokorizični UI sustav pod njihovom odgovornošću, uvoznici su se dužni pobrinuti da uvjeti skladištenja ili prijevoza, ovisno o slučaju, ne ugrožavaju njegovo ispunjavanje zahtjeva iz poglavlja 2. ove glave.
5. Uvoznici nacionalnim nadležnim tijelima na obrazloženi zahtjev daju sve potrebne informacije i dokumentaciju za dokazivanje sukladnosti visokorizičnog UI sustava sa zahtjevima iz poglavlja 2. ove glave na jeziku koji dotično nacionalno nadležno tijelo razumije bez poteškoća; to uključuje i davanje pristupa dnevnicima događaja koje automatski generira visokorizični UI sustav u mjeri u kojoj su takvi dnevnici događaja pod dobavljačevom kontrolom na temelju ugovornog odnosa s korisnikom ili druge pravne osnove. S tim tijelima surađuju i u svim radnjama koje nacionalno nadležno tijelo poduzme u vezi s tim sustavom.

Članak 27. Obveze distributera

1. Prije stavljanja visokorizičnog UI sustava na tržište distributeri su dužni provjeriti ima li taj visokorizični UI sustav potrebnu oznaku sukladnosti CE, popratnu dokumentaciju i upute za uporabu te jesu li dobavljač i uvoznik sustava, ovisno o slučaju, ispunili obveze utvrđene u ovoj Uredbi.
2. Ako distributer smatra ili ima razloga smatrati da visokorizični UI sustav nije sukladan sa zahtjevima iz poglavlja 2. ove glave, ne stavlja taj sustav na tržište dok ga se ne učini sukladnim s tim zahtjevima. Ako taj sustav predstavlja rizik u smislu članka 65. stavka 1., distributer o tome obavješćuje, ovisno o slučaju, dobavljača ili uvoznika tog sustava.
3. Dok je visokorizični UI sustav pod njihovom odgovornošću, distributeri su se dužni pobrinuti da uvjeti skladištenja ili prijevoza, ovisno o slučaju, ne ugrožavaju njegovo ispunjavanje zahtjeva iz poglavlja 2. ove glave.
4. Ako distributer smatra ili ima razloga smatrati da visokorizični UI sustav koji je stavio na raspolaganje na tržištu nije sukladan sa zahtjevima iz poglavlja 2. ove glave, poduzima korektivne mjere potrebne da se taj sustav učini sukladnim s tim zahtjevima ili da se provede njegovo povlačenje ili povrat ili osigurava da te korektivne mjere poduzme, ovisno o slučaju, uvoznik ili drugi relevantni operater. Ako visokorizični UI sustav predstavlja rizik u smislu članka 65. stavka 1., distributer o tome odmah obavješćuje nacionalna nadležna tijela država članica u kojima je proizvod stavio na raspolaganje navodeći pojedinosti, osobito o nesukladnosti i svim poduzetim korektivnim radnjama.
5. Dobavljači visokorizičnih UI sustava nacionalnom nadležnom tijelu na njegov obrazloženi zahtjev daju sve informacije i dokumentaciju potrebne za dokazivanje sukladnosti visokorizičnog sustava sa zahtjevima iz poglavlja 2. ove glave. Distributeri s tim nacionalnim nadležnim tijelom surađuju i u svim radnjama koje to tijelo poduzme.

Članak 28.

Obveze distributera, uvoznika, korisnika ili ostalih trećih strana

1. Svi distributeri, uvoznici, korisnici ili ostale treće strane smatraju se dobavljačima za potrebe ove Uredbe i podliježu obvezama dobavljača na temelju članka 16. u bilo kojoj od sljedećih okolnosti:
 - (a) ako visokorizični UI sustav stavljaju na tržište ili u uporabu pod svojim imenom ili žigom;
 - (b) ako promijene namjenu visokorizičnog UI sustava koji je već stavljen na tržište ili u uporabu;
 - (c) ako učine bitnu izmjenu visokorizičnog UI sustava.
2. Ako nastupe okolnosti iz stavka 1. točke (b) ili (c), dobavljač koji je prvobitno stavio visokorizični UI sustav na tržište ili u uporabu više se ne smatra dobavljačem za potrebe ove Uredbe.

Članak 29.

Obveze korisnika visokorizičnih UI sustava

1. Korisnici visokorizičnih UI sustava koriste takve sustave prema uputama za uporabu priloženima sustavima i u skladu sa stavcima 2. i 5.
2. Obvezama iz stavka 1. ne dovode se u pitanje druge obveze korisnika na temelju prava Unije ili nacionalnog prava ni diskrecijsko pravo korisnika da organizira svoje resurse i aktivnosti za potrebe provedbe mjera ljudskog nadzora koje je naveo dobavljač.
3. Ne dovodeći u pitanje stavak 1., korisnik osigurava, u mjeri u kojoj ima kontrolu nad ulaznim podacima, da su ulazni podaci relevantni s obzirom na namjenu visokorizičnog UI sustava.
4. Korisnici prate rad visokorizičnog UI sustava prema uputama za uporabu. Ako imaju razloga smatrati da zbog uporabe u skladu s uputama za uporabu UI sustav može predstavljati rizik u smislu članka 65. stavka 1., o tome obavješćuju dobavljača ili distributera i privremeno obustavljaju uporabu sustava. Dobavljaču ili distributeru dužni su prijaviti i svaki ozbiljan incident ili svaku neispravnost u smislu članka 62. i prekidaju uporabu UI sustava. Ako korisnik ne može stupiti u kontakt s dobavljačem, članak 62. primjenjuje se *mutatis mutandis*.

Za korisnike koji su kreditne institucije regulirane Direktivom 2013/36/EU obveza praćenja iz prvog podstavka smatra se ispunjenom ako poštuju pravila o sustavima, procesima i mehanizmima internog upravljanja u skladu s člankom 74. te direktive.
5. Korisnici visokorizičnih UI sustava dužni su čuvati dnevničke događaja koje automatski generira visokorizični UI sustav u mjeri u kojoj su takvi dnevnički događaji pod njihovom kontrolom. Dnevnički događaji čuvaju se tijekom razdoblja koje je primjereno s obzirom na namjenu visokorizičnog UI sustava i primjenjivih pravnih obveza na temelju prava Unije ili nacionalnog prava.

Korisnici koji su kreditne institucije regulirane Direktivom 2013/36/EU čuvaju dnevničke događaje kao dio dokumentacije o sustavima, procesima i mehanizmima internog upravljanja u skladu s člankom 74. te direktive.

6. Korisnici visokorizičnih UI sustava dužni su služiti informacijama iz članka 13. da bi ispunili obvezu procjene učinka na zaštitu podataka na temelju, prema potrebi, članka 35. Uredbe (EU) 2016/679 ili članka 27. Direktive (EU) 2016/680.

POGLAVLJE 4.

TIJELA KOJA PROVODE PRIJAVLJIVANJE I PRIJAVLJENA TIJELA

Članak 30.

Tijela koja provode prijavljivanje

1. Svaka država članica imenuje ili osniva tijelo koje provodi prijavljivanje, koje je odgovorno za utvrđivanje i provedbu postupaka potrebnih za ocjenjivanje, imenovanje, prijavljivanje i praćenje tijela za ocjenjivanje sukladnosti.
2. Države članice kao tijelo za prijavljivanje mogu imenovati nacionalno akreditacijsko tijelo kako je navedeno u Uredbi (EZ) br. 765/2008.
3. Tijela koja provode prijavljivanje moraju se osnovati, organizirati i raditi tako da ne bude sukoba interesa s tijelima za ocjenjivanje sukladnosti te da budu zajamčene objektivnost i nepristranost njihovih aktivnosti.
4. Tijela koja provode prijavljivanje moraju se organizirati tako da odluke povezane s prijavljivanjem tijela za ocjenjivanje sukladnosti donose odgovorne osobe različite od osoba koje su provele ocjenjivanje tih tijela.
5. Tijela koja provode prijavljivanje ne nude niti obavljaju aktivnosti koje obavljaju tijela za ocjenjivanje sukladnosti, kao ni usluge savjetovanja na tržišnoj ili konkurentskoj osnovi.
6. Tijela koja provode prijavljivanje štite povjerljivost dobivenih informacija.
7. Tijela koja provode prijavljivanje moraju na raspolaganju imati dovoljan broj stručnog osoblja za propisno obavljanje svojih zadaća.
8. Tijela koja provode prijavljivanje osiguravaju da se ocjenjivanje sukladnosti provodi razmjerno, izbjegavajući nepotrebno opterećenje za dobavljače, te da prijavljena tijela obavljaju svoje aktivnosti uzimajući u obzir veličinu poduzeća, sektor u kojem ono posluje, njegovu strukturu i stupanj složenosti dotičnog UI sustava.

Članak 31.

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. Tom zahtjevu za prijavljivanje prilaže se opis aktivnosti ocjenjivanja sukladnosti, modula ili modulâ za ocjenjivanje sukladnosti i tehnologija umjetne inteligencije za koje to 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 to tijelo za ocjenjivanje sukladnosti ispunjava zahtjeve iz članka 33. Dodaju se svi valjani dokumenti koji se odnose na postojeća imenovanja prijavljenog tijela koje je podnijelo zahtjev u skladu s bilo kojim drugim zakonodavstvom Unije o usklađivanju.

3. Ako dotično tijelo za ocjenjivanje sukladnosti ne može predočiti potvrdu o akreditaciji, tijelu koje provodi prijavljivanje dostavlja sve dokumente potrebne za provjeru, priznavanje i redovno praćenje njegove usklađenosti sa zahtjevima iz članka 33. Za prijavljena tijela koja su imenovana u skladu s bilo kojim drugim zakonodavstvom Unije o usklađivanju, svi dokumenti i potvrde povezani s tim imenovanjima mogu se, prema potrebi, upotrijebiti u postupku njihova imenovanja u skladu s ovom Uredbom.

Članak 32.

Postupak prijavljivanja

1. Tijela koja provode prijavljivanje mogu prijaviti samo tijela za ocjenjivanje sukladnosti koja ispunjavaju zahtjeve iz članka 33.
2. Tijela koja provode prijavljivanje dostavljaju prijavu Komisiji i drugim državama članicama putem alata za elektroničko prijavljivanje koji je razvila i kojim upravlja Komisija.
3. Prijava mora sadržavati potpune informacije o aktivnostima ocjenjivanja sukladnosti, modulu ili modulima ocjenjivanja sukladnosti te obuhvaćenim tehnologijama umjetne inteligencije.
4. Dotično tijelo za ocjenjivanje sukladnosti može obavljati aktivnosti prijavljenog tijela samo ako Komisija ili druge države članice ne podnesu prigovor u roku od mjesec dana od prijavljivanja.
5. Tijela koja provode prijavljivanje obavješćuju Komisiju i druge države članice o svim relevantnim naknadnim promjenama prijave.

Članak 33.

Prijavljena tijela

1. Prijavljena tijela provjeravaju sukladnost visokorizičnog UI sustava u skladu s postupcima ocjenjivanja sukladnosti iz članka 43.
2. Prijavljena tijela ispunjavaju organizacijske zahtjeve te zahtjeve koji se odnose na upravljanje kvalitetom, resurse i procese koji su nužni za obavljanje njihovih zadaća.
3. Organizacijskom strukturom, podjelom odgovornosti, linijama izvješćivanja i radom prijavljenih tijela mora se osigurati povjerenje u aktivnosti ocjenjivanja sukladnosti koje provode prijavljena tijela i u njihove rezultate.
4. Prijavljena tijela neovisna su o dobavljaču visokorizičnog UI sustava za koji provode aktivnosti ocjenjivanja sukladnosti. Osim toga, prijavljena tijela neovisna su o svim drugim operaterima koji imaju gospodarski interes u visokorizičnom UI sustavu koji se ocjenjuje, kao i o svim konkurentima dobavljača.
5. Prijavljena tijela moraju se organizirati i raditi tako da budu zajamčene 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 te u svojim aktivnostima ocjenjivanja.
6. Prijavljena tijela provode dokumentirane postupke kojima se osigurava da njihovo osoblje, odbori, društva kćeri, podizvođači i sva povezana tijela ili osoblje vanjskih tijela poštuju povjerljivost informacija koje prime tijekom obavljanja aktivnosti

ocjenjivanja sukladnosti, osim ako je otkrivanje tih informacija zakonska obveza. Osoblje prijavljenih tijela obvezno je čuvati profesionalnu tajnu za sve informacije dobivene tijekom obavljanja zadaća u skladu s ovom Uredbom, osim prema tijelima koja provode prijavljivanje za državu članicu u kojoj prijavljena tijela obavljaju svoje aktivnosti.

7. Prijavljena tijela moraju imati procedure za obavljanje aktivnosti kojima se uzima u obzir veličina poduzeća, sektor u kojem ono posluje, njegova struktura i stupanj složenosti dotičnog UI sustava.
8. Prijavljena tijela na odgovarajući se način osiguravaju od odgovornosti za svoje aktivnosti ocjenjivanja sukladnosti, osim ako u skladu s nacionalnim pravom odgovornost preuzima dotična država članica ili je ta država članica izravno odgovorna za ocjenjivanje sukladnosti.
9. Prijavljena tijela moraju biti sposobna, s najvećom razinom profesionalnog integriteta i nužnim kompetencijama u određenom području, provoditi sve svoje zadaće koje proizlaze iz ove Uredbe, bilo da je riječ o zadaćama koje provode sama prijavljena tijela ili o zadaćama koje se provode u njihovo ime i pod njihovom odgovornošću.
10. Prijavljena tijela moraju imati dostatne unutarnje kompetencije da mogu djelotvorno evaluirati zadaće koje u njihovo ime obavljaju vanjske strane. Zbog toga, u svakom trenutku te za svaki postupak ocjenjivanja sukladnosti i svaki tip visokorizičnog UI sustava za koji je imenovano, prijavljeno tijelo mora stalno imati na raspolaganju dovoljno administrativnog, tehničkog i znanstvenog osoblja koji posjeduju iskustvo i znanje povezano s relevantnim tehnologijama umjetne inteligencije, podacima i obradom podataka te sa zahtjevima iz poglavlja 2. ove glave.
11. 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 najnovijim informacijama o njima.
12. Prijavljena tijela tijelu koje provodi prijavljivanje iz članka 30. stavljaju na raspolaganje i na zahtjev dostavljaju svu relevantnu dokumentaciju, uključujući dokumentaciju dobavljača, kako bi mu omogućila da provodi svoje aktivnosti ocjenjivanja, imenovanja, prijavljivanja, praćenja i nadzora te olakšala ocjenjivanje opisano u ovom poglavlju.

Članak 34.

Društva kćeri i podizvođači prijavljenih tijela

1. Ako prijavljeno tijelo određene zadaće povezane s ocjenjivanjem sukladnosti povjeri podizvođačima ili ih prenese društvu kćeri, mora osigurati da taj podizvođač ili to društvo kći ispunjava zahtjeve iz članka 33. te o tome obavijestiti tijelo koje provodi prijavljivanje.
2. Prijavljena tijela preuzimaju punu odgovornost za zadaće koje obavljaju podizvođači ili društva kćeri bez obzira na mjesto njihova poslovnog nastana.
3. Aktivnosti se mogu povjeriti podizvođaču ili ih može provoditi društvo kći samo uz suglasnost dobavljača.

4. Prijavljena tijela tijelu koje provodi prijavljivanje drže na raspolaganju relevantne dokumente koji se odnose na ocjenjivanje kvalifikacija podizvođača ili društva kćeri i poslova koje oni obavljaju u skladu s ovom Uredbom.

Članak 35.

Identifikacijski brojevi i popisi prijavljenih tijela imenovanih u skladu s ovom Uredbom

1. Komisija prijavljenim tijelima dodjeljuje identifikacijski broj. Dodjeljuje im samo jedan takav broj, čak i ako je određeno tijelo prijavljeno na temelju više akata Unije.
2. Komisija objavljuje popis tijela prijavljenih na temelju ove Uredbe, uključujući identifikacijske brojeve koji su im dodijeljeni i aktivnosti za koje su prijavljena. Komisija osigurava redovito ažuriranje tog popisa.

Članak 36.

Promjene u prijavama

1. Ako tijelo koje provodi prijavljivanje posumnja ili je obaviješteno o tome da određeno prijavljeno tijelo više ne ispunjava zahtjeve utvrđene u članku 33. 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 iznese svoje primjedbe. Ako tijelo koje provodi prijavljivanje zaključi da prijavljeno tijelo pod istragom više ne ispunjava zahtjeve utvrđene u članku 33. ili da ne ispunjava svoje obveze, tijelo koje provodi prijavljivanje ograničava, suspendira ili povlači prijavu, ovisno o ozbiljnosti neispunjavanja zahtjeva ili obveza. Usto, o tome odmah obavješćuje Komisiju i druge države članice.
2. U slučaju ograničenja, suspenzije ili povlačenja prijave, ili ako je prijavljeno tijelo prestalo s radom, tijelo koje provodi prijavljivanje poduzima odgovarajuće mjere kako bi osiguralo da dokumentaciju tog prijavljenog tijela preuzme drugo prijavljeno tijelo ili da ona bude na raspolaganju odgovornim tijelima koja provode prijavljivanje na njihov zahtjev.

Članak 37.

Osporavanje stručnosti prijavljenih tijela

1. Komisija prema potrebi istražuje sve slučajeve u kojima postoje razlozi za sumnju u usklađenost prijavljenog tijela sa zahtjevima utvrđenima u članku 33.
2. Tijelo koje provodi prijavljivanje Komisiji na zahtjev dostavlja sve relevantne informacije koje se odnose na prijavu dotičnog prijavljenog tijela.
3. Komisija osigurava da se sa svim povjerljivim informacijama dobivenima tijekom njezinih istraga na temelju ovog članka postupa na odgovarajući način.
4. Ako Komisija utvrdi da prijavljeno tijelo ne zadovoljava ili je prestalo zadovoljavati zahtjeve iz članka 33., donosi obrazloženu odluku kojom od države članice koja provodi prijavljivanje zahtijeva da poduzme potrebne korektivne mjere, uključujući povlačenje prijave ako je to potrebno. Taj provedbeni akt donosi se u skladu s postupkom ispitivanja iz članka 74. stavka 2.

Članak 38.
Koordinacija prijavljenih tijela

1. Komisija osigurava da se, za područja obuhvaćena ovom Uredbom, uspostave i pravilno provode primjerena koordinacija i suradnja prijavljenih tijela koja se bave postupcima ocjenjivanja sukladnosti UI sustava u skladu s ovom Uredbom, i to u okviru sektorske skupine prijavljenih tijela.
2. Države članice osiguravaju da tijela koja su prijavile sudjeluju u radu te skupine, izravno ili preko imenovanih predstavnika.

Članak 39.
Tijela za ocjenjivanje sukladnosti iz trećih zemalja

Tijela za ocjenjivanje sukladnosti uspostavljena u skladu s pravom određene treće zemlje s kojom je Unija sklopila sporazum mogu biti ovlaštena za obavljanje aktivnosti prijavljenih tijela u skladu s ovom Uredbom.

POGLAVLJE 5.

NORME, OCJENJIVANJE SUKLADNOSTI, POTVRDE, REGISTRACIJA

Članak 40.
Usklađene norme

Za visokorizične UI sustave koji su sukladni s usklađenim normama ili dijelovima usklađenih normi na koje su objavljena upućivanja u *Službenom listu Europske unije* pretpostavlja se da su sukladni sa zahtjevima iz poglavlja 2. ove glave u mjeri u kojoj te norme obuhvaćaju dotične zahtjeve.

Članak 41.
Zajedničke specifikacije

1. Ako usklađene norme iz članka 40. ne postoje ili ako Komisija smatra da relevantne usklađene norme nisu dovoljne ili da je potrebno uzeti u obzir određena pitanja sigurnosti ili temeljnih prava, Komisija može provedbenim aktima donijeti zajedničke specifikacije u pogledu zahtjeva iz poglavlja 2. ove glave. Ti provedbeni akti donose se u skladu s postupkom ispitivanja iz članka 74. stavka 2.
2. Komisija pri pripremi zajedničkih specifikacija iz stavka 1. prikuplja stajališta relevantnih tijela ili stručnih skupina osnovanih u skladu s relevantnim sektorskim zakonodavstvom Unije.
3. Za visokorizične UI sustave koji su sukladni sa zajedničkim specifikacijama iz stavka 1. pretpostavlja se da su sukladni sa zahtjevima iz poglavlja 2. ove glave u mjeri u kojoj te zajedničke specifikacije obuhvaćaju dotične zahtjeve.
4. Ako dobavljači ne ispunjavaju zajedničke specifikacije iz stavka 1., moraju propisno obrazložiti da su usvojili tehnička rješenja koja su barem ekvivalentna tim specifikacijama.

Članak 42.

Pretpostavka sukladnosti s određenim zahtjevima

1. Uzimajući u obzir njihovu namjenu, za visokorizične UI sustave koji su poučeni i testirani na podacima o specifičnom zemljopisnom, bihevioralnom ili radnom okruženju u kojem je predviđena njihova uporaba pretpostavlja se da ispunjavaju zahtjev iz članka 10. stavka 4.
2. Za visokorizične UI sustave koji su certificirani ili za koje je izdana izjava o sukladnosti u okviru programa kibersigurnosti u skladu s Uredbom (EU) 2019/881 Europskog parlamenta i Vijeća⁶³ i na koje su objavljena upućivanja u *Službenom listu Europske unije* pretpostavlja se da ispunjavaju kibersigurnosne zahtjeve iz članka 15. ove Uredbe ako kibersigurnosni certifikat ili izjava o sukladnosti ili njihovi dijelovi obuhvaćaju te zahtjeve.

Članak 43.

Ocjenjivanje sukladnosti

1. Za visokorizične UI sustave navedene u točki 1. Priloga III., ako je dobavljač pri dokazivanju da visokorizični UI sustav ispunjava zahtjeve iz poglavlja 2. ove glave primijenio usklađene norme iz članka 40. ili, ako je primjenjivo, zajedničke specifikacije iz članka 41., dobavljač primjenjuje jedan od sljedećih postupaka:
 - (a) postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole iz Priloga VI.;
 - (b) postupak ocjenjivanja sukladnosti na temelju ocjenjivanja sustava upravljanja kvalitetom i ocjenjivanja tehničke dokumentacije, uz sudjelovanje prijavljenog tijela, iz Priloga VII.

Ako dobavljač pri dokazivanju da visokorizični UI sustav ispunjava zahtjeve iz poglavlja 2. ove glave nije primijenio ili je samo djelomično primijenio usklađene norme iz članka 40. ili ako takve usklađene norme ne postoje i nisu dostupne zajedničke specifikacije iz članka 41., dobavljač primjenjuje postupak ocjenjivanja sukladnosti utvrđen u Prilogu VII.

Za potrebe postupka ocjenjivanja sukladnosti iz Priloga VII. dobavljač može odabrati bilo koje prijavljeno tijelo. Međutim, ako sustav u uporabu namjeravaju staviti tijela kaznenog progona, tijela za imigraciju ili tijela za azil odnosno institucije, tijela ili agencije EU-a, kao prijavljeno tijelo djeluje tijelo za nadzor tržišta iz članka 63. stavka 5. ili 6., ovisno o slučaju.

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. Za visokorizične UI sustave iz točke 5. podtočke (b) Priloga III., koje su na tržište ili u uporabu stavile kreditne institucije regulirane Direktivom 2013/36/EU, ocjenjivanje sukladnosti provodi se u okviru postupka iz članaka od 97. do 101. te direktive.
3. Za visokorizične UI sustave na koje se primjenjuju pravni akti navedeni u Prilogu II. odjeljku A dobavljač primjenjuje relevantno ocjenjivanje sukladnosti u skladu s tim

⁶³ 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. 1.).

pravnim aktima. Na te visokorizične UI sustave primjenjuju se zahtjevi iz poglavlja 2. ove glave i dio su dotičnog ocjenjivanja. Primjenjuju se i točke 4.3., 4.4., 4.5. i peti odlomak točke 4.6. Priloga VII.

Za potrebe tog ocjenjivanja prijavljena tijela koja su prijavljena u skladu s navedenim pravnim aktima imaju pravo kontrolirati sukladnost visokorizičnih UI sustava sa zahtjevima iz poglavlja 2. ove glave, pod uvjetom da je u kontekstu postupka prijavljivanja u skladu s tim pravnim aktima ocijenjeno ispunjavaju li dotična prijavljena tijela zahtjeve utvrđene u članku 33. stavcima 4., 9. i 10.

Ako je pravnim aktima navedenima u Prilogu II. odjeljku A 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 dotičnu mogućnost može iskoristiti samo ako je primijenio i usklađene norme ili, ako je to primjenjivo, zajedničke specifikacije iz članka 41. koje obuhvaćaju zahtjeve iz poglavlja 2. ove glave.

4. Za visokorizične UI sustave provodi se novi postupak ocjenjivanja sukladnosti kad god se bitno izmijene, neovisno o tome namjerava li se izmijenjeni sustav dalje distribuirati ili ga nastavlja upotrebljavati isti korisnik.

Za visokorizične UI sustave koji i dalje uče nakon stavljanja na tržište ili stavljanja u uporabu, promjene visokorizičnog UI sustava i njegove sposobnosti 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 73. u svrhu ažuriranja priloga VI. i VII. kako bi se dodali elementi postupaka ocjenjivanja sukladnosti koji postanu potrebni s obzirom na tehnički napredak.
6. Komisija je ovlaštena za donošenje delegiranih akata radi izmjene stavaka 1. i 2. 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 ili minimiziranju rizika za zdravlje i sigurnost te zaštitu temeljnih prava koje takvi sustavi predstavljaju, kao i dostupnost dostatnih kapaciteta i resursa među prijavljenim tijelima.

Članak 44.

Potvrde

1. Potvrde koje izdaju prijavljena tijela u skladu s prilogom VII. izdaju se na službenom jeziku Unije koji odredi država članica u kojoj prijavljeno tijelo ima poslovni nastan ili na službenom jeziku Unije koji je inače prihvatljiv prijavljenom tijelu.
2. Potvrde vrijede za razdoblje koje je u njima navedeno, a ono ne može biti dulje od pet godina. Na zahtjev dobavljača valjanost potvrde može se produljivati za daljnja razdoblja koja nisu dulja od pet godina, i to na temelju ponovnog ocjenjivanja u skladu s primjenjivim postupcima ocjenjivanja sukladnosti.
3. Ako ustanovi da UI sustav više ne ispunjava zahtjeve iz poglavlja 2. ove glave, prijavljeno tijelo, uzimajući u obzir načelo proporcionalnosti, suspendira ili povlači izdanu potvrdu ili uvodi ograničenja za nju, osim ako se s pomoću primjerenih

korektivnih mjera koje dobavljač sustava poduzme u primjerenom roku koji utvrdi prijavljeno tijelo osigura da UI sustav ispunjava te zahtjeve. Prijavljeno tijelo daje obrazloženje za svoju odluku.

Članak 45.

Žalbe na odluke prijavljenih tijela

Države članice stranama koje imaju legitiman interes u odlukama prijavljenih tijela moraju omogućiti pokretanje žalbenog postupka protiv tih odluka.

Članak 46.

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, 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 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 drugim provedenim aktivnostima, uključujući prekogranične aktivnosti i povjeravanje aktivnosti podizvođačima.
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 EU-a 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 tehnologije umjetne inteligencije dostavlja relevantne informacije o pitanjima u vezi s negativnim i, na zahtjev, pozitivnim rezultatima ocjenjivanja sukladnosti.

Članak 47.

Odstupanje od postupka ocjenjivanja sukladnosti

1. Odstupajući od članka 43., svako tijelo za nadzor tržišta može odobriti stavljanje na tržište ili u uporabu određenih visokorizičnih UI sustava na državnom području dotične države članice zbog iznimnih razloga javne sigurnosti ili zaštite života i zdravlja ljudi, zaštite okoliša i zaštite ključne industrijske i infrastrukturne imovine. Trajanje tog odobrenja mora biti ograničeno na razdoblje provedbe potrebnih

postupaka ocjenjivanja sukladnosti i isteći po dovršetku tih postupaka. Ti se postupci dovršavaju bez nepotrebne odgode.

2. Odobrenje iz stavka 1. izdaje se samo ako tijelo za nadzor tržišta zaključi da visokorizični UI sustav ispunjava zahtjeve iz poglavlja 2. ove glave. Tijelo za nadzor tržišta obavješćuje Komisiju i druge države članice o svim odobrenjima izdanima u skladu sa stavkom 1.
3. Ako u roku od 15 kalendarskih dana od primitka informacija iz stavka 2. 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.
4. Ako u roku od 15 kalendarskih dana od primitka obavijesti iz stavka 2. određena država članica podnese prigovore 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 2. neutemeljen, Komisija bez odgode započinje savjetovanje s relevantnom državom članicom; u savjetovanju sudjeluju i dotični operator ili operateri te im se omogućuje da iznesu svoja stajališta. Komisija ih uzima u obzir i odlučuje je li odobrenje opravdano. Komisija svoju odluku upućuje dotičnoj državi članici i relevantnom operateru ili operaterima.
5. Ako se odobrenje smatra neopravdanim, tijelo za nadzor tržišta dotične države članice povlači to odobrenje.
6. Odstupajući od stavaka od 1. do 5., za visokorizične UI sustave koji su namijenjeni za uporabu kao sigurnosni sastavni dijelovi proizvoda ili su sami proizvodi obuhvaćeni Uredbom (EU) 2017/745 i Uredbom (EU) 2017/746, članak 59. Uredbe (EU) 2017/745 i članak 54. Uredbe (EU) 2017/746 primjenjuju se i u pogledu odstupanja od ocjenjivanja usklađenosti sa zahtjevima iz poglavlja 2. ove glave.

Članak 48.

EU izjava o sukladnosti

1. Dobavljač sastavlja pisanu EU izjavu o sukladnosti za svaki UI sustav i drži je na raspolaganju nacionalnim nadležnim tijelima u razdoblju od 10 godina nakon što je taj UI sustav stavljen na tržište ili u uporabu. U EU izjavi o sukladnosti navodi se za koji je UI sustav ona sastavljena. Relevantnim nacionalnim nadležnim tijelima na zahtjev se daje primjerak EU izjave o sukladnosti.
2. U EU izjavi o sukladnosti navodi se da dotični visokorizični UI sustav ispunjava zahtjeve iz poglavlja 2. ove glave. EU izjava o sukladnosti sadržava informacije utvrđene u Prilogu V. i prevodi se na službeni jezik ili jezike Unije koje zahtijeva jedna ili više država članica u kojima se visokorizični UI sustav stavlja na raspolaganje.
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 u skladu sa svim zakonodavnim aktima Unije koji se primjenjuju 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 iz poglavlja 2. ove glave. Dobavljač prema potrebi ažurira EU izjavu o sukladnosti.
5. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 73. u svrhu ažuriranja sadržaja EU izjave o sukladnosti utvrđenog u Prilogu V. kako bi se dodali elementi koji postanu potrebni s obzirom na tehnički napredak.

Članak 49.

Oznaka sukladnosti CE

1. Oznaka CE stavlja se na visokorizične UI sustave tako da je 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.
2. Oznaka CE iz stavka 1. ovog članka podliježe općim načelima iz članka 30. Uredbe (EZ) br. 765/2008.
3. Ako je to primjenjivo, uz oznaku CE navodi se identifikacijski broj prijavljenog tijela koje je odgovorno za postupke ocjenjivanja sukladnosti iz članka 43. Taj identifikacijski broj navodi se i u svakom promotivnom materijalu u kojem se naznačuje da dotični visokorizični UI sustav ispunjava zahtjeve za oznaku CE.

Članak 50.

Čuvanje dokumenata

U razdoblju od 10 godina nakon što je UI sustav stavljen na tržište ili u uporabu dobavljač na raspolaganju nacionalnim nadležnim tijelima 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 48.

Članak 51.

Registracija

Prije stavljanja na tržište ili u uporabu visokorizičnog UI sustava iz članka 6. stavka 2., dobavljač ili, prema potrebi, ovlašteni zastupnik registrira taj sustav u bazi podataka EU-a iz članka 60.

GLAVA IV.

OBVEZE U POGLEDU TRANSPARENTNOSTI ZA ODREĐENE UI SUSTAVE

Članak 52.

Obveze u pogledu transparentnosti za određene UI sustave

1. Dobavljači osiguravaju da su UI sustavi koji su namijenjeni interakciji s pojedincima osmišljeni i razvijeni tako da pojedinci budu svjesni da su u interakciji s UI sustavom, osim ako je to očito iz okolnosti i konteksta uporabe. Ta se obveza ne primjenjuje na UI sustave koji su zakonski odobreni za otkrivanje, sprečavanje, istragu i kazneni progon kaznenih djela, osim ako su ti sustavi dostupni javnosti za prijavu kaznenog djela.
2. Korisnici sustava za prepoznavanje emocija ili sustava za biometrijsku kategorizaciju informiraju pojedince koji su izloženi tom sustavu o njegovu radu. Ta se obveza ne primjenjuje na UI sustave za biometrijsku kategorizaciju koji su zakonski dopušteni za otkrivanje, sprečavanje i istragu kaznenih djela.
3. Korisnici UI sustava koji stvara ili manipulira slikovnim sadržajem, audiosadržajem ili videosadržajem u kojem postoji znatna sličnost s postojećim osobama, predmetima, mjestima ili drugim subjektima ili događajima te koji bi se nekoj osobi netočno činio vjerodostojnim ili istinitim („deep fake”) moraju navesti da je taj sadržaj umjetno stvoren ili da je njime manipulirano.

Međutim, prvi podstavak ne primjenjuje se ako je uporaba zakonski odobrena za otkrivanje, sprečavanje, istragu i kazneni progon kaznenih djela ili je nužna za ostvarivanje prava na slobodu izražavanja i prava na slobodu umjetnosti i znanosti zajamčenih Poveljom EU-a o temeljnim pravima, pri čemu se primjenjuju odgovarajuće mjere za zaštitu prava i sloboda trećih strana.
4. Stavci 1., 2. i 3. ne utječu na zahtjeve i obveze iz glave III. ove Uredbe.

GLAVA V.

MJERE ZA POTPORU INOVACIJAMA

Članak 53.

Regulatorna izolirana okruženja za umjetnu inteligenciju

1. Regulatorna izolirana okruženja za umjetnu inteligenciju koja su uspostavili jedno ili više nadležnih tijela država članica ili Europski nadzornik za zaštitu podataka služe kao kontrolirano okruženje koje olakšava razvoj, testiranje i validaciju inovativnih UI sustava tijekom određenog vremena prije njihova stavljanja na tržište ili u uporabu u skladu s posebnim planom. To se odvija pod izravnim nadzorom i vodstvom nadležnih tijela kako bi se osiguralo ispunjavanje zahtjeva ove Uredbe i, prema potrebi, drugog zakonodavstva Unije i država članica koje se prati u relevantnom izoliranom okruženju.
2. Države članice moraju osigurati da, ako inovativni UI sustavi obuhvaćaju obradu osobnih podataka ili na neki drugi način spadaju pod nadzor drugih nacionalnih tijela ili nadležnih tijela koja pružaju ili podržavaju pristup podacima, nacionalna tijela za

zaštitu podataka i dotična druga nacionalna tijela budu povezana s radom regulatornog izoliranog okruženja za umjetnu inteligenciju.

3. Regulatorna izolirana okruženja za umjetnu inteligenciju ne utječu na nadzorne i korektivne ovlasti nadležnih tijela. Ako se tijekom razvoja i testiranja takvih sustava uoče znatni rizici za zdravlje, sigurnost i temeljna prava, ti se rizici moraju odmah smanjiti, a ako to nije moguće, mora se prekinuti postupak razvoja i testiranja sve dok se oni ne smanje.
4. U skladu s primjenjivim zakonodavstvom Unije i država članica o odgovornosti, sudionici regulatornog izoliranog okruženja za umjetnu inteligenciju i dalje su odgovorni za svaku štetu nanесenu trećim stranama koja je posljedica eksperimentiranja u izoliranom okruženju.
5. Nadležna tijela država članica koja su uspostavila regulatorna izolirana okruženja za umjetnu inteligenciju koordiniraju svoje aktivnosti i surađuju u okviru Europskog odbora za umjetnu inteligenciju. Odboru i Komisiji podnose godišnja izvješća o rezultatima provedbe tih programa, uključujući dobre primjere iz prakse, stečena iskustva i preporuke za uspostavu tih programa te, prema potrebi, o primjeni ove Uredbe i drugog zakonodavstva Unije koje se prati u relevantnom izoliranom okruženju.
6. Modaliteti i uvjeti funkcioniranja regulatornih izoliranih okruženja za umjetnu inteligenciju, uključujući kriterije prihvatljivosti i postupak za podnošenje zahtjeva, odabir, sudjelovanje u izoliranom okruženju i izlazak iz njega, te prava i obveze sudionika utvrđuju se u provedbenim aktima. Ti provedbeni akti donose se u skladu s postupkom ispitivanja iz članka 74. stavka 2.

Članak 54.

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

1. Osobni podaci koji su zakonito prikupljeni u druge svrhe u regulatornom izoliranom okruženju za umjetnu inteligenciju obrađuju se za potrebe razvoja i testiranja određenih inovativnih UI sustava pod sljedećim uvjetima:
 - (a) dotični inovativni UI sustavi razvijaju se za zaštitu znatnog javnog interesa u jednom ili više sljedećih područja:
 - i. sprečavanje, istraga, otkrivanje ili progon kaznenih djela ili izvršavanje kaznenopravnih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje, pod kontrolom i odgovornošću nadležnih tijela. Obrada se temelji na pravu države članice ili Unije;
 - ii. javna sigurnost i javno zdravlje, uključujući sprečavanje, kontrolu i liječenje bolesti;
 - iii. visoka razina zaštite i poboljšanja kvalitete okoliša;
 - (b) podaci koji se obrađuju potrebni su za ispunjavanje jednog ili više zahtjeva iz glave III. poglavlja 2. ako se ti zahtjevi ne mogu djelotvorno ispuniti obradom anonimiziranih, sintetičkih ili drugih neosobnih podataka;
 - (c) postoje djelotvorni mehanizmi praćenja kojima se utvrđuje mogu li se tijekom eksperimentiranja u izoliranom okruženju pojaviti bilo kakvi veliki rizici za

temeljna prava ispitanika te mehanizmi za odgovor kojima se ti rizici mogu brzo smanjiti i, prema potrebi, zaustaviti obrada;

- (d) svi osobni podaci koji se obrađuju u izoliranom okruženju nalaze se u funkcionalno odvojenom, izoliranom i zaštićenom okruženju za obradu podataka pod kontrolom sudionika i samo ovlaštene osobe imaju pristup tim podacima;
 - (e) osobni podaci koji se obrađuju ne smiju se slati ni prenositi drugim stranama niti im one smiju pristupiti na bilo koji drugi način;
 - (f) obrada osobnih podataka u izoliranom okruženju ne smije dovesti do mjera ili odluka koje utječu na ispitanike;
 - (g) osobni podaci koji se obrađuju u izoliranom okruženju brišu se nakon završetka sudjelovanja u izoliranom okruženju ili završetka razdoblja čuvanja osobnih podataka;
 - (h) dnevници događaja u okviru obrade osobnih podataka u izoliranom okruženju čuvaju se tijekom razdoblja sudjelovanja u izoliranom okruženju i godinu dana nakon završetka sudjelovanja, isključivo u svrhu ispunjavanja obveza u pogledu odgovornosti i dokumentacije na temelju ovog članka ili drugog primjenjivog zakonodavstva Unije ili država članica te samo onoliko dugo koliko je potrebno za to;
 - (i) zajedno s rezultatima testiranja kao dio tehničke dokumentacije iz Priloga IV. čuva se potpuni i detaljni opis procesa i temelja učenja, 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.
2. Stavkom 1. ne dovodi se u pitanje zakonodavstvo Unije ili država članica kojim je zabranjena obrada u druge svrhe osim onih koje su izričito navedene u tom zakonodavstvu.

Članak 55.

Mjere za male dobavljače i korisnike

1. Države članice poduzimaju sljedeće mjere:
- (a) malim dobavljačima i novoosnovanim poduzećima daju prioritetni pristup regulatornim izoliranim okruženjima za umjetnu inteligenciju ako ispunjavaju uvjete prihvatljivosti;
 - (b) organiziraju posebne aktivnosti informiranja o primjeni ove Uredbe prilagođene potrebama malih dobavljača i korisnika;
 - (c) ako je to primjereno, uvode namjenski kanal za komunikaciju s malim dobavljačima i korisnicima te drugim inovatorima radi pružanja smjernica i odgovaranja na upite o provedbi ove Uredbe.
2. Pri određivanju naknada za ocjenjivanje sukladnosti u skladu s člankom 43. uzimaju se u obzir posebni interesi i potrebe malih dobavljača i naknade se smanjuju razmjerno njihovoj veličini i veličini tržišta.

GLAVA VI.

UPRAVLJANJE

POGLAVLJE 1.

EUROPSKI ODBOR ZA UMJETNU INTELIGENCIJU

Članak 56.

Osnivanje Europskog odbora za umjetnu inteligenciju

1. Osniva se „Europski odbor za umjetnu inteligenciju” („Odbor”).
2. Odbor pruža savjete i pomoć Komisiji kako bi:
 - (a) doprinosio djelotvornoj suradnji nacionalnih nadzornih tijela i Komisije u vezi s pitanjima obuhvaćenima ovom Uredbom;
 - (b) koordinirao smjernice i analize Komisije i nacionalnih nadzornih tijela te drugih nadležnih tijela povezane s novim pitanjima koja se pojave na unutarnjem tržištu o stvarima obuhvaćenima ovom Uredbom te doprinosio tim smjernicama i analizama;
 - (c) pomagao nacionalnim nadzornim tijelima i Komisiji u osiguravanju dosljedne primjene ove Uredbe.

Članak 57.

Struktura Odbora

1. Odbor se sastoji od nacionalnih nadzornih tijela, koja predstavljaju voditelji ili ekvivalentni visoki dužnosnici tih tijela, i Europskog nadzornika za zaštitu podataka. Na sastanke se mogu pozvati druga nacionalna tijela ako se raspravlja o pitanjima koja su im važna.
2. Na temelju suglasnosti Komisije Odbor usvaja svoj poslovnik običnom većinom članova. Poslovnik sadržava i operative aspekte povezane s izvršavanjem zadaća Odbora navedenih u članku 58. Odbor prema potrebi može osnovati podskupine za razmatranje konkretnih pitanja.
3. Odborom predsjedava Komisija. Komisija saziva sastanke i priprema dnevni red u skladu sa zadaćama Odbora na temelju ove Uredbe i s poslovníkom Odbora. Komisija pruža administrativnu i analitičku podršku aktivnostima Odbora na temelju ove Uredbe.
4. Odbor na svoje sastanke može pozvati vanjske stručnjake i promatrače te može razmjenjivati informacije sa zainteresiranim trećim stranama radi obavješćivanja o svojim aktivnostima, koliko je to primjereno. U tu svrhu Komisija može olakšati razmjenu informacija između Odbora i drugih tijela, ureda, agencija i savjetodavnih skupina Unije.

Članak 58.

Zadace Odbora

Pri pružanju savjeta i pomoći Komisiji u kontekstu članka 56. stavka 2. Odbor posebno:

- (a) prikuplja i prenosi stručno znanje i najbolje primjere iz prakse među državama članicama;
- (b) doprinosi ujednačenim administrativnim praksama u državama članicama, među ostalim za funkcioniranje regulatornih izoliranih okruženja iz članka 53.;
- (c) izdaje mišljenja, preporuke ili pisane doprinose o pitanjima povezanim s provedbom ove Uredbe, a posebno:
 - i. o tehničkim specifikacijama ili postojećim normama u vezi sa zahtjevima iz glave III. poglavlja 2.;
 - ii. o uporabi usklađenih normi ili zajedničkih specifikacija iz članaka 40. i 41.;
 - iii. o pripremi smjernica, uključujući smjernice za određivanje upravnih novčanih kazni iz članka 71.

POGLAVLJE 2.

NACIONALNA NADLEŽNA TIJELA

Članak 59.

Imenovanje nacionalnih nadležnih tijela

1. Svaka država članica osniva ili imenuje nacionalna nadležna tijela koja će biti zadužena za primjenu i provedbu ove Uredbe. Nacionalna nadležna tijela moraju se organizirati tako da budu zajamčene objektivnost i nepristranost njihovih aktivnosti i zadaća.
2. Svaka država članica među nacionalnim nadležnim tijelima imenuje jedno nacionalno nadzorno tijelo. Nacionalno nadzorno tijelo djeluje kao tijelo koje provodi prijavljivanje i tijelo za nadzor tržišta, osim ako država članica ima organizacijske i administrativne razloge za imenovanje više tijela.
3. Države članice obavješćuju Komisiju o imenovanom tijelu ili tijelima i, prema potrebi, razlozima za imenovanje više tijela.
4. Države članice osiguravaju da nacionalna nadležna tijela imaju dostatne financijske i ljudske resurse za obavljanje svojih zadaća u skladu s ovom Uredbom. Konkretno, nacionalna nadležna tijela moraju imati dovoljno stalno raspoloživog osoblja čije kompetencije i stručno znanje obuhvaćaju temeljito razumijevanje tehnologija umjetne inteligencije, podataka i obrade podataka, temeljnih prava i rizika za zdravlje i sigurnost te poznavanje postojećih normi i pravnih zahtjeva.
5. Države članice jednom godišnje izvješćuju Komisiju o stanju financijskih i ljudskih resursa nacionalnih nadležnih tijela i pritom ocjenjuju njihovu dostatnost. Komisija te informacije prosljeđuje Odboru radi rasprave i utvrđivanja mogućih preporuka.
6. Komisija nacionalnim nadležnim tijelima olakšava razmjenu iskustava.
7. Nacionalna nadležna tijela mogu pružati smjernice i savjete o provedbi ove Uredbe, među ostalim i malim dobavljačima. Ako nacionalna nadležna tijela namjeravaju pružiti smjernice i savjete za određeni UI sustav iz područja obuhvaćenih drugim zakonodavstvom Unije, prema potrebi se savjetuju s nadležnim nacionalnim tijelima u skladu s tim drugim zakonodavstvom Unije. Osim toga, države članice mogu uspostaviti jednu središnju kontaktnu točku za komunikaciju s operaterima.

8. Ako područje primjene ove Uredbe obuhvaća institucije, agencije i tijela Unije, Europski nadzornik za zaštitu podataka djeluje kao tijelo nadležno za njihov nadzor.

GLAVA VII.

BAZA PODATAKA EU-A ZA SAMOSTALNE VISOKORIZIČNE UI SUSTAVE

Članak 60.

Baza podataka EU-a za samostalne visokorizične UI sustave

1. Komisija u suradnji s državama članicama uspostavlja i vodi bazu podataka EU-a koja sadržava informacije iz stavka 2. o visokorizičnim UI sustavima iz članka 6. stavka 2. koji su registrirani u skladu s člankom 51.
2. Dobavljači u bazu podataka EU-a unose podatke navedene u Prilogu VIII. Komisija im pruža tehničku i administrativnu podršku.
3. Informacije unesene u bazu podataka EU-a dostupne su javnosti.
4. Baza podataka EU-a sadržava osobne podatke samo u mjeri u kojoj je to potrebno za prikupljanje i obradu informacija u skladu s ovom Uredbom. Te informacije obuhvaćaju imena i kontaktne podatke pojedinaca koji su odgovorni za registraciju sustava i koji imaju pravnu ovlast za zastupanje dobavljača.
5. Komisija je nadzornik baze podataka EU-a. Osim toga, ona dobavljačima osigurava primjerenu tehničku i administrativnu podršku.

GLAVA VIII.

PRAĆENJE NAKON STAVLJANJA NA TRŽIŠTE, RAZMJENA INFORMACIJA, NADZOR TRŽIŠTA

POGLAVLJE 1.

PRAĆENJE NAKON STAVLJANJA NA TRŽIŠTE

Članak 61.

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 relevantnih 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 su dostavili korisnici ili koji su prikupljeni iz drugih izvora o sposobnosti visokorizičnih UI sustava tijekom njihova životnog vijeka te dobavljaču omogućuje da evaluiira kontinuiranu usklađenost UI sustava sa zahtjevima iz glave III. poglavlja 2.
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 mora donijeti provedbeni akt s detaljnim odredbama kojima se utvrđuje predložak za plan praćenja nakon stavljanja na tržište i popis elemenata koje treba uključiti u plan.

4. Za visokorizične UI sustave obuhvaćene pravnim aktima iz Priloga II., ako su sustav i plan praćenja nakon stavljanja na tržište već uspostavljeni u skladu s tim zakonodavstvom, elementi opisani u stavcima 1., 2. i 3. na primjeren se način integriraju u taj sustav i plan.

Prvi podstavak primjenjuje se i na visokorizične UI sustave iz točke 5. podtočke (b) Priloga III. koje na tržište ili u uporabu stavljaju kreditne institucije regulirane Direktivom 2013/36/EU.

POGLAVLJE 2.

RAZMJENA INFORMACIJA O INCIDENTIMA I NEISPRAVNOSTIMA

Članak 62.

Prijavljivanje ozbiljnih incidenata i neispravnosti

1. Dobavljači visokorizičnih UI sustava stavljenih na tržište Unije tijelima za nadzor tržišta država članica u kojima je došlo do incidenta ili kršenja prijavljuju svaki ozbiljni incident ili neispravnost tih sustava koji čini kršenje obveza na temelju prava Unije namijenjenih zaštiti temeljnih prava.

Takva se prijava radi čim dobavljač utvrdi uzročnu povezanost između UI sustava i incidenta ili neispravnosti ili razumnu vjerojatnost takve povezanosti, a u svakom slučaju najkasnije 15 dana nakon što dobavljač sazna za ozbiljan incident ili neispravnost.

2. Nakon primitka prijave u vezi s kršenjem obveza na temelju prava Unije namijenjenih zaštiti temeljnih prava, tijelo za nadzor tržišta o tome obavještuje nacionalna tijela javne vlasti ili javnopravna tijela iz članka 64. stavka 3. Komisija izrađuje namjenske smjernice za lakše ispunjavanje obveza iz stavka 1. Te se smjernice izdaju najkasnije 12 mjeseci nakon stupanja na snagu ove Uredbe.
3. Za visokorizične UI sustave iz točke 5. podtočke (b) Priloga III. koje na tržište ili u uporabu stavljaju dobavljači koji su kreditne institucije regulirane Direktivom 2013/36/EU i za visokorizične UI sustave koji su sigurnosni sastavni dijelovi proizvoda ili su sami proizvodi obuhvaćeni Uredbom (EU) 2017/745 i Uredbom (EU) 2017/746, prijava ozbiljnih incidenata ili neispravnosti ograničava se na one koji čine kršenje obveza na temelju prava Unije namijenjenih zaštiti temeljnih prava.

POGLAVLJE 3.

IZVRŠENJE

Članak 63.

Nadzor nad tržištem i kontrola UI sustava na tržištu Unije

1. Uredba (EU) 2019/1020 primjenjuje se na UI sustave obuhvaćene ovom Uredbom. Međutim, u svrhu djelotvornog izvršenja ove Uredbe:

- (a) smatra se da svako upućivanje na gospodarski subjekt na temelju Uredbe (EU) 2019/1020 uključuje sve operatere iz glave III. poglavlja 3. 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. Nacionalno nadzorno tijelo redovito izvješćuje Komisiju o ishodima relevantnih aktivnosti nadzora tržišta. Nacionalno nadzorno tijelo bez odgode dostavlja Komisiji i relevantnim nacionalnim tijelima za tržišno natjecanje sve informacije utvrđene tijekom aktivnosti nadzora tržišta koje bi mogle biti od interesa za primjenu prava Unije o tržišnom natjecanju.
 - 3. Za visokorizične UI sustave povezane s proizvodima na koje se primjenjuju pravni akti navedeni u odjeljku A Priloga II., tijelo za nadzor tržišta je za potrebe ove Uredbe tijelo odgovorno za aktivnosti nadzora tržišta imenovano na temelju tih pravnih akata.
 - 4. Za UI sustave koji se stavljaju na tržište, stavljaju u uporabu ili ih koriste financijske institucije regulirane zakonodavstvom Unije o financijskim uslugama, tijelo za nadzor tržišta je za potrebe ove Uredbe relevantno tijelo odgovorno za financijski nadzor tih institucija na temelju tog zakonodavstva.
 - 5. Za UI sustave navedene u točki 1. podtočki (a), ako se ti sustavi upotrebljavaju za kazneni progon, te točkama 6. i 7. Priloga III., države članice za potrebe ove Uredbe kao tijela za nadzor tržišta imenuju ili nadležna nadzorna tijela za zaštitu podataka na temelju Direktive (EU) 2016/680 ili Uredbe 2016/679 ili nacionalna nadležna tijela koja nadziru aktivnosti tijela kaznenog progona, tijela za imigraciju ili tijela za azil koja stavljaju u uporabu ili koriste te sustave.
 - 6. Ako područje primjene ove Uredbe obuhvaća institucije, agencije i tijela Unije, Europski nadzornik za zaštitu podataka djeluje kao njihovo tijelo za nadzor tržišta.
 - 7. Države članice olakšavaju koordinaciju između tijela za nadzor tržišta imenovanih na temelju ove Uredbe i drugih relevantnih nacionalnih tijela koja nadziru primjenu zakonodavstva Unije o usklađivanju iz Priloga II. ili drugog zakonodavstva Unije koje bi moglo biti relevantno za visokorizične UI sustave iz Priloga III.

Članak 64.

Pristup podacima i dokumentaciji

- 1. Tijelima za nadzor tržišta odobrava se, u kontekstu njihovih aktivnosti, potpuni pristup skupovima podataka za učenje, validaciju i testiranje koje je dobavljač koristio, među ostalim putem aplikacijskih programskih sučelja („API”) ili drugih odgovarajućih tehničkih sredstava i alata koji omogućuju daljinski pristup.
- 2. Ako je to potrebno za ocjenjivanje sukladnosti visokorizičnog UI sustava sa zahtjevima iz glave III. poglavlja 2., tijelima za nadzor tržišta na obrazložen se zahtjev odobrava pristup izvornom kodu UI sustava.
- 3. Nacionalna tijela javne vlasti ili javnopravna tijela koja nadziru ili izvršavaju poštovanje obveza na temelju prava Unije kojima se štite temeljna prava u pogledu uporabe visokorizičnih UI sustava iz Priloga III. ovlaštena su zatražiti i pristupiti svakoj dokumentaciji izrađenoj ili vođenoj na temelju ove Uredbe kada je pristup toj dokumentaciji potreban za ispunjavanje nadležnosti na temelju njihova mandata unutar okvira njihove jurisdikcije. Relevantno tijelo javne vlasti ili javnopravno tijelo

obavješćuje tijelo za nadzor tržišta dotične države članice o svakom takvom zahtjevu.

4. Najkasnije tri mjeseca nakon stupanja na snagu ove Uredbe svaka država članica mora odrediti tijela javne vlasti ili javnopravna tijela iz stavka 3. i objaviti popis na internetskoj stranici nacionalnog nadzornog tijela. Države članice dostavljaju taj popis Komisiji i svim drugim državama članicama te ga ažuriraju.
5. Ako dokumentacija iz stavka 3. nije dovoljna za utvrđivanje je li došlo do kršenja obveza na temelju prava Unije namijenjenih zaštiti temeljnih prava, tijelo javne vlasti ili javnopravno tijelo iz stavka 3. može tijelu za nadzor tržišta podnijeti obrazloženi zahtjev za organiziranje testiranja visokorizičnog UI sustava tehničkim sredstvima. Tijelo za nadzor tržišta organizira testiranje uz blisku suradnju tijela javne vlasti ili javnopravnog tijela koje je podnijelo zahtjev u razumnom roku nakon podnošenja zahtjeva.
6. Sa svim informacijama i dokumentacijom koje su nacionalna tijela javne vlasti ili javnopravna tijela iz stavka 3. dobila u skladu s odredbama ovog članka postupa se sukladno obvezama povjerljivosti utvrđenima u članku 70.

Članak 65.

Postupak za UI sustave koji predstavljaju rizik na nacionalnoj razini

1. UI sustavi koji predstavljaju rizik smatraju se proizvodom koji predstavlja rizik definiranim u članku 3. točki 19. Uredbe (EU) 2019/1020 s obzirom na rizike za zdravlje ili sigurnost ili zaštitu temeljnih prava osoba.
2. Ako tijelo za nadzor tržišta države članice ima dovoljno razloga smatrati da UI sustav predstavlja rizik iz stavka 1., ono evaluira usklađenost dotičnog UI sustava sa svim zahtjevima i obvezama utvrđenima u ovoj Uredbi. Osim toga, ako postoje rizici za zaštitu temeljnih prava, tijelo za nadzor tržišta obavješćuje relevantna nacionalna tijela javne vlasti ili javnopravna tijela iz članka 64. stavka 3. Relevantni operateri prema potrebi surađuju s tijelima za nadzor tržišta i drugim nacionalnim tijelima javne vlasti ili javnopravnim tijelima iz članka 64. stavka 3.

Ako tijekom te evaluacije tijelo za nadzor tržišta utvrdi da UI sustav ne ispunjava zahtjeve i obveze utvrđene ovom Uredbom, ono bez odgode zahtijeva da relevantni operater poduzme sve odgovarajuće korektivne mjere kako bi UI sustav uskladio s tim zahtjevima i obvezama, povukao ga s tržišta ili osigurao njegov povrat u razumnom roku, razmjerno prirodi rizika, prema onome što tijelo propiše.

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

3. Ako smatra da neusklađenost nije ograničena samo na područje njegove države, tijelo za nadzor tržišta dostavlja Komisiji i drugim državama članicama informacije o rezultatima evaluacije i mjerama koje je zahtijevalo od operatera.
4. Operater osigurava provedbu svih odgovarajućih korektivnih mjera u pogledu svih dotičnih UI sustava koje je stavio na raspolaganje na tržištu bilo gdje u Uniji.
5. Ako operater UI sustava ne poduzme prikladne korektivne mjere u roku navedenom u stavku 2., tijelo za nadzor tržišta poduzima sve prikladne privremene mjere kako bi zabranilo ili ograničilo stavljanje UI sustava na raspolaganje na svojem nacionalnom

tržištu, odnosno povuklo taj proizvod s tog tržišta ili osiguralo njegov povrat. To je tijelo dužno o tim mjerama bez odgode obavijestiti Komisiju i druge države članice.

6. Informacije iz stavka 5. uključuju sve dostupne pojedinosti, posebno podatke nužne za identifikaciju neusklađenog UI sustava, njegovo podrijetlo, prirodu navodne neusklađenosti i povezanog rizika, prirodu i trajanje poduzetih nacionalnih mjera te argumente relevantnog operatera. Tijela za nadzor tržišta posebno naznačuju je li neusklađenost posljedica jednog ili više sljedećih uzroka:
 - (a) UI sustav ne ispunjava zahtjeve iz glave III. poglavlja 2.;
 - (b) postoje nedostaci u usklađenim normama ili zajedničkim specifikacijama iz članaka 40. i 41. kojima se stvara pretpostavka sukladnosti.
7. Tijela za nadzor tržišta država članica, osim tijela za nadzor tržišta države članice koje pokreće postupak, bez 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 prijavljenom nacionalnom mjerom, o svojim prigovorima.
8. Ako u roku od tri mjeseca od primitka informacija navedenih u stavku 5. nijedna država članica ni Komisija ne podnese prigovor na privremenu mjeru koju je poduzela država članica, mjera se smatra opravdanom. Time se ne dovode u pitanje postupovna prava dotičnog operatera u skladu s člankom 18. Uredbe (EU) 2019/1020.
9. Tijela za nadzor tržišta svih država članica dužna su osigurati da se bez odgode poduzmu prikladne restriktivne mjere u odnosu na dotični proizvod, primjerice povlačenje proizvoda s njihovih tržišta.

Članak 66.

Zaštitni postupak Unije

1. Ako država članica u roku od tri mjeseca od primitka obavijesti iz članka 65. stavka 5. podnese prigovore na mjeru koju je poduzela druga država članica ili ako Komisija smatra da je mjera u suprotnosti s pravom Unije, Komisija bez odgode započinje savjetovanje s relevantnom državom članicom i operaterom ili operaterima te evaluiira nacionalnu mjeru. Na temelju rezultata te evaluacije Komisija u roku od devet mjeseci od obavijesti iz članka 65. stavka 5. odlučuje je li nacionalna mjera opravdana te o toj odluci obavješćuje dotičnu državu članicu.
2. Ako se nacionalna mjera smatra opravdanom, sve države članice poduzimaju mjere potrebne kako bi osigurale da se nesukladni UI sustav povuče s njihovih tržišta, te o tome obavješćuju Komisiju. Ako se nacionalna mjera smatra neopravdanom, dotična država članica mora povući mjeru.
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 67.

Usklađeni UI sustavi koji predstavljaju rizik

1. Ako tijelo za nadzor tržišta države članice nakon provedene evaluacije na temelju članka 65. ustanovi da UI sustav koji je u skladu s ovom Uredbom ipak predstavlja

rizik za zdravlje ili sigurnost osoba, za ispunjavanje obveza na temelju prava Unije ili nacionalnog prava namijenjenih zaštiti temeljnih prava ili za druge aspekte zaštite javnog interesa, od relevantnog operatera zahtijeva da poduzme sve odgovarajuće mjere kako bi osigurao da dotični UI sustav nakon stavljanja na tržište ili u uporabu više ne predstavlja rizik, povukao ga s tržišta ili osigurao njegov povrat u razumnom roku, razmjerno prirodi rizika, prema onome što tijelo propiše.

2. Dobavljač ili drugi relevantni operateri osiguravaju poduzimanje korektivnih mjera u pogledu svih dotičnih UI sustava koje su stavili na raspolaganje na tržištu bilo gdje u Uniji u roku koji je propisalo tijelo za nadzor tržišta države članice iz stavka 1.
3. Država članica odmah obavješćuje Komisiju i druge države članice. Te informacije uključuju sve dostupne pojedinosti, a posebno podatke nužne za identifikaciju dotičnog UI sustava, njegovo podrijetlo i lanac opskrbe, prirodu povezanog rizika te prirodu i trajanje poduzetih nacionalnih mjera.
4. Komisija bez odgode započinje savjetovanje s državama članicama i relevantnim operaterom te evaluira poduzete nacionalne mjere. Na temelju rezultata te evaluacije, Komisija odlučuje jesu li poduzete mjere opravdane i, prema potrebi, predlaže prikladne mjere.
5. Komisija svoju odluku upućuje državama članicama.

Članak 68.

Formalna neusklađenost

1. Tijelo za nadzor tržišta države članice zahtijeva od relevantnog dobavljača da otkloni tu neusklađenost ako ustanovi jedno od sljedećega:
 - (a) oznaka sukladnosti nije stavljena u skladu s člankom 49.;
 - (b) oznaka sukladnosti nije stavljena;
 - (c) EU izjava o sukladnosti nije sastavljena;
 - (d) EU izjava o sukladnosti nije ispravno sastavljena;
 - (e) identifikacijski broj prijavljenog tijela koje je uključeno u postupak ocjenjivanja sukladnosti, ako je primjenjivo, nije stavljen;
2. Ako se neusklađenost iz stavka 1. nastavi, dotična država članica poduzima sve odgovarajuće mjere kako bi ograničila ili zabranila stavljanje visokorizičnog UI sustava na raspolaganje na tržištu ili kako bi osigurala njegov povrat ili povlačenje s tržišta.

GLAVA IX.

KODEKSI PONAŠANJA

Članak 69.

Kodeksi ponašanja

1. Komisija i države članice potiču i olakšavaju izradu kodeksa ponašanja namijenjenih poticanju da se na UI sustave koji nisu visokorizični dobrovoljno primjenjuju zahtjevi iz glave III. poglavlja 2. na temelju tehničkih specifikacija i rješenja koji su prikladni za osiguravanje usklađenosti s takvim zahtjevima s obzirom na namjenu sustavâ.

2. Komisija i Odbor potiču i olakšavaju izradu kodeksa ponašanja namijenjenih poticanju da se na UI sustave dobrovoljno primjenjuju zahtjevi koji se odnose primjerice na okolišnu održivost, pristupačnost za osobe s invaliditetom, sudjelovanje dionika u projektiranju i razvoju UI sustava te raznolikost razvojnih timova na temelju jasnih ciljeva i ključnih pokazatelja uspješnosti za mjerenje ostvarenja tih ciljeva.
3. Kodekse ponašanja mogu sastavljati pojedinačni dobavljači UI sustava i/ili organizacije koje ih zastupaju, među ostalim uz sudjelovanje korisnika i svih zainteresiranih dionika i njihovih predstavničkih organizacija. Kodeksi ponašanja mogu obuhvaćati jedan ili više UI sustava uzimajući u obzir sličnost namjene relevantnih sustava.
4. Pri poticanju i olakšavanju izrade kodeksâ ponašanja Komisija i Odbor uzimaju u obzir posebne interese i potrebe malih dobavljača i novoosnovanih poduzeća.

GLAVA X.

POVJERLJIVOST I SANKCIJE

Članak 70. Povjerljivost

1. Nacionalna nadležna tijela i prijavljena tijela uključena u primjenu ove Uredbe moraju poštovati povjerljivost informacija i podataka koje dobiju 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 slučajeva iz članka 5. Direktive (EU) 2016/943 o zaštiti neotkrivenih znanja i iskustva te poslovnih informacija (poslovne tajne) od nezakonitog pribavljanja, korištenja i otkrivanja;
 - (b) djelotvornu provedbu ove Uredbe, posebice za potrebe inspekcija, istraga ili revizija; (c) javne i nacionalne sigurnosne interese;
 - (c) integritet kaznenih ili upravnih postupaka.
2. Ne dovodeći u pitanje stavak 1., informacije koje na povjerljivoj osnovi međusobno razmjenjuju nacionalna nadležna tijela te nacionalna nadležna tijela i Komisija ne smiju se otkrivati bez prethodnog savjetovanja s izvornim nacionalnim nadležnim tijelom i korisnikom kada tijela kaznenog progona, tijela za imigraciju ili tijela za azil upotrebljavaju visokorizične UI sustave iz točaka 1., 6. i 7. Priloga III. ako bi se takvim otkrivanjem ugrozili javni i nacionalni sigurnosni interesi.

Ako su tijela kaznenog progona, tijela za imigraciju ili tijela za azil dobavljači visokorizičnih UI sustava iz točaka 1., 6. i 7. Priloga III., tehnička dokumentacija iz Priloga IV. ostaje u prostorima tih tijela. Ta tijela osiguravaju da tijela za nadzor tržišta iz članka 63. stavaka 5. i 6., ovisno o slučaju, mogu na zahtjev odmah pristupiti dokumentaciji ili dobiti njezin primjerak. Pristup toj dokumentaciji ili bilo kojem njezinu primjerku dopušten je samo osoblju tijela za nadzor tržišta koje je prošlo odgovarajući stupanj sigurnosne provjere.

3. Stavci 1. i 2. ne utječu na prava i obveze Komisije, država članica i prijavljenih tijela u pogledu razmjene informacija i širenja upozorenja ni na obveze dotičnih stranaka da pruže informacije na temelju kaznenog prava država članica.
4. Komisija i države članice mogu po potrebi razmjenjivati povjerljive informacije s regulatornim tijelima trećih zemalja s kojima su sklopile bilateralne ili multilateralne sporazume o povjerljivosti kojima se jamči odgovarajuća razina povjerljivosti.

*Članak 71.
Sankcije*

1. U skladu s uvjetima utvrđenima u ovoj Uredbi, države članice utvrđuju pravila o sankcijama, uključujući upravne novčane kazne, koja se primjenjuju na povrede ove Uredbe i poduzimaju sve potrebne mjere kako bi osigurale njihovu pravilnu i djelotvornu provedbu. Predviđene sankcije moraju biti učinkovite, proporcionalne i odvraćajuće. Njima se osobito uzimaju u obzir interesi malih dobavljača i novoosnovanih poduzeća te njihova gospodarska održivost.
2. Države članice obavješćuju Komisiju o tim pravilima i tim mjerama te je bez odgode obavješćuju o svim naknadnim izmjenama koje na njih utječu.
3. Za sljedeće povrede izriču se upravne novčane kazne u iznosu do 30 000 000 EUR ili, ako je počinitelj povrede poduzeće, do 6 % njegova ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome koji je iznos veći:
 - (a) nepoštovanje zabrane praksi u području umjetne inteligencije iz članka 5.;
 - (b) neusklađenost UI sustava sa zahtjevima utvrđenima u članku 10.
4. Za neusklađenost UI sustava s bilo kojim zahtjevima ili obvezama iz ove Uredbe, osim onih utvrđenih u člancima 5. i 10., izriču se upravne novčane kazne u iznosu do 20 000 000 EUR ili, ako je počinitelj povrede poduzeće, do 4 % njegova ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome koji je iznos veći.
5. Za dostavljanje netočnih, nepotpunih ili obmanjujućih informacija prijavljenim tijelima i nacionalnim nadležnim tijelima kao odgovor na zahtjev izriču se upravne novčane kazne u iznosu do 10 000 000 EUR ili, ako je počinitelj povrede poduzeće, do 2 % njegova ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome koji je iznos veći.
6. Pri odlučivanju o iznosu upravne novčane kazne u svakom pojedinom 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;
 - (b) eventualnim upravnim novčanim kaznama koje su druga tijela za nadzor tržišta već izrekla istom operateru za istu povredu;
 - (c) veličini i tržišnom udjelu operatera koji je počinio povredu;
7. Svaka država članica utvrđuje pravila o tome mogu li se i u kojoj mjeri tijelima javne vlasti i javnopravnim tijelima te države članice izreći upravne novčane kazne.
8. 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, ovisno o slučaju u tim državama članicama. Primjena takvih pravila u tim državama članicama mora imati istovjetan učinak.

Članak 72.

Upravne novčane kazne za institucije, agencije i tijela Unije

1. Europski nadzornik za zaštitu podataka može izreći upravne novčane kazne institucijama, agencijama i tijelima Unije obuhvaćenima područjem primjene ove Uredbe. Pri odlučivanju o izricanju upravne novčane kazne i o njezinu iznosu u svakom pojedinom 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;
 - (b) suradnji s Europskim nadzornikom za zaštitu podataka radi ispravljanja povrede i ublažavanja mogućih štetnih posljedica povrede, uključujući poštovanje svih mjera koje je Europski nadzornik za zaštitu podataka prethodno izrekao dotičnoj instituciji ili agenciji ili tijelu Unije u vezi s istim predmetom;
 - (c) svim sličnim prijašnjim povredama koje je počinila dotična institucija, agencija ili tijelo Unije;
2. Upravne novčane kazne u iznosu do 500 000 EUR izriču se za sljedeće povrede:
 - (a) nepoštovanje zabrane praksi u području umjetne inteligencije iz članka 5.;
 - (b) neusklađenost UI sustava sa zahtjevima utvrđenima u članku 10.
3. Za neusklađenost UI sustava s bilo kojim zahtjevima ili obvezama iz ove Uredbe, osim onih utvrđenih u člancima 5. i 10., izriču se upravne novčane kazne u iznosu do 250 000 EUR.
4. Prije donošenja odluka u skladu s ovim člankom Europski nadzornik za zaštitu podataka pruža instituciji, agenciji ili tijelu Unije protiv kojeg vodi postupak mogućnost da se očituje o mogućoj povredi. Europski nadzornik za zaštitu podataka temelji svoje odluke isključivo na elementima i okolnostima o kojima su se stranke mogle očitovati. Podnositelji pritužbe, ako postoje, moraju biti uključeni u postupke.
5. U postupcima se u potpunosti mora poštovati pravo stranaka na obranu. Imaju pravo na uvid u spis Europskog nadzornika za zaštitu podataka uz uvjet da se poštuju legitimni interesi pojedinaca ili poduzeća da štite svoje osobne podatke ili poslovne tajne.
6. Sredstva ostvarena naplatom novčanih kazni iz ovog članka prihod su općeg proračuna Unije.

GLAVA XI.

DELEGIRANJE OVLASTI I POSTUPAK ODBORA

Članak 73.

Izvršavanje delegiranja ovlasti

1. Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji podložno uvjetima utvrđenima u ovom članku.

2. Delegiranje ovlasti iz članka 4., članka 7. stavka 1., članka 11. stavka 3., članka 43. stavaka 5. i 6. i članka 48. stavka 5. dodjeljuje se Komisiji na neodređeno razdoblje počevši od [*datuma stupanja na snagu ove Uredbe*].
3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 4., članka 7. stavka 1., članka 11. stavka 3., članka 43. stavaka 5. i 6. i članka 48. stavka 5. Odlukom o opozivu prestaje delegiranje ovlasti koje je u njoj navedeno. Odluka o opozivu počinje proizvoditi učinke sljedećeg dana od dana njezine objave u *Službenom listu Europske unije* ili na kasniji datum određen u spomenutoj odluci. Ona ne utječe na valjanost delegiranih akata koji su već na snazi.
4. Čim donese delegirani akt, Komisija ga istodobno priopćuje Europskom parlamentu i Vijeću.
5. Bilo koji delegirani akt donesen na temelju članka 4., članka 7. stavka 1., članka 11. stavka 3., članka 43. stavaka 5. i 6. i članka 48. stavka 5. stupa na snagu samo ako Europski parlament ili Vijeće u roku od tri mjeseca od priopćenja tog akta Europskom parlamentu i Vijeću na njega ne podnesu nikakav prigovor, ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da neće uložiti prigovore. Taj se rok produljuje za tri mjeseca na inicijativu Europskog parlamenta ili Vijeća.

Članak 74.
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.

GLAVA XII.

ZAVRŠNE ODREDBE

Članak 75.
Izmjena Uredbe (EZ) br. 300/2008

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

„Pri donošenju detaljnih mjera povezanih s tehničkim specifikacijama i postupcima za odobravanje i uporabu zaštitne opreme koje se odnose na sustave umjetne inteligencije u smislu Uredbe (EU) YYYY/XX [o umjetnoj inteligenciji] Europskog parlamenta i Vijeća* uzimaju se u obzir zahtjevi utvrđeni u glavi III. poglavlju 2. te uredbe.”

* Uredba (EU) YYYY/XX [o umjetnoj inteligenciji] (SL ...).”

Članak 76.
Izmjena Uredbe (EU) br. 167/2013

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

„Pri donošenju delegiranih akata u skladu s prvim podstavkom o sustavima umjetne inteligencije koji su sigurnosni sastavni dijelovi u smislu Uredbe (EU) YYYY/XX [o umjetnoj

inteligenciji] Europskog parlamenta i Vijeća* uzimaju se u obzir zahtjevi iz glave III. poglavlja 2. te uredbe.

* Uredba (EU) YYY/XX [o umjetnoj inteligenciji] (SL ...).”

Članak 77.

Izmjena Uredbe (EU) br. 168/2013

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

„Pri donošenju delegiranih akata u skladu s prvim podstavkom o sustavima umjetne inteligencije koji su sigurnosni sastavni dijelovi u smislu Uredbe (EU) YYY/XX o [umjetnoj inteligenciji] Europskog parlamenta i Vijeća* uzimaju se u obzir zahtjevi iz glave III. poglavlja 2. te uredbe.

* Uredba (EU) YYY/XX [o umjetnoj inteligenciji] (SL ...).”

Članak 78.

Izmjena Direktive 2014/90/EU

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

„4. Kad je riječ o sustavima umjetne inteligencije koji su sigurnosni sastavni dijelovi u smislu Uredbe (EU) YYY/XX [o umjetnoj inteligenciji] Europskog parlamenta i Vijeća*, pri obavljanju svojih aktivnosti u skladu sa stavkom 1. i pri donošenju tehničkih specifikacija i ispitnih normi u skladu sa stavcima 2. i 3. Komisija uzima u obzir zahtjeve utvrđene u glavi III. poglavlju 2. te uredbe.

* Uredba (EU) YYY/XX [o umjetnoj inteligenciji] (SL ...).”

Članak 79.

Izmjena Direktive (EU) 2016/797

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

„12. Pri donošenju delegiranih akata u skladu sa stavkom 1. i provedbenih akata u skladu sa stavkom 11. o sustavima umjetne inteligencije koji su sigurnosni sastavni dijelovi u smislu Uredbe (EU) YYY/XX o [umjetnoj inteligenciji] Europskog parlamenta i Vijeća* uzimaju se u obzir zahtjevi iz glave III. poglavlja 2. te uredbe.

* Uredba (EU) YYY/XX [o umjetnoj inteligenciji] (SL ...).”

Članak 80.

Izmjena Uredbe (EU) 2018/858

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

„4. Pri donošenju delegiranih akata u skladu sa stavkom 3. o sustavima umjetne inteligencije koji su sigurnosni sastavni dijelovi u smislu Uredbe (EU) YYY/XX [o umjetnoj inteligenciji]

Europskog parlamenta i Vijeća* uzimaju se u obzir zahtjevi iz glave III. poglavlja 2. te uredbe.

* Uredba (EU) YYYY/XX [o umjetnoj inteligenciji] (SL ...).”

*Članak 81.
Izmjena Uredbe (EU) 2018/1139*

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

1. U članku 17. dodaje se sljedeći stavak:

„3. Ne dovodeći u pitanje stavak 2., pri donošenju provedbenih akata u skladu sa stavkom 1. o sustavima umjetne inteligencije koji su sigurnosni sastavni dijelovi u smislu Uredbe (EU) YYYY/XX [o umjetnoj inteligenciji] Europskog parlamenta i Vijeća* uzimaju se u obzir zahtjevi iz glave III. poglavlja 2. te uredbe.

* Uredba (EU) YYYY/XX [o umjetnoj inteligenciji] (SL ...).”

2. U članku 19. dodaje se sljedeći stavak:

„4. Pri donošenju delegiranih akata u skladu sa stavcima 1. i 2. o sustavima umjetne inteligencije koji su sigurnosni sastavni dijelovi u smislu Uredbe (EU) YYYY/XX [o umjetnoj inteligenciji] uzimaju se u obzir zahtjevi iz glave III. poglavlja 2. te uredbe.”

3. U članku 43. dodaje se sljedeći stavak:

„4. Pri donošenju provedbenih akata u skladu sa stavkom 1. o sustavima umjetne inteligencije koji su sigurnosni sastavni dijelovi u smislu Uredbe (EU) YYYY/XX [o umjetnoj inteligenciji] uzimaju se u obzir zahtjevi iz glave III. poglavlja 2. te uredbe.”

4. U članku 47. dodaje se sljedeći stavak:

„3. Pri donošenju delegiranih akata u skladu sa stavcima 1. i 2. o sustavima umjetne inteligencije koji su sigurnosni sastavni dijelovi u smislu Uredbe (EU) YYYY/XX [o umjetnoj inteligenciji] uzimaju se u obzir zahtjevi iz glave III. poglavlja 2. te uredbe.”

5. U članku 57. dodaje se sljedeći stavak:

„Pri donošenju tih provedbenih akata o sustavima umjetne inteligencije koji su sigurnosni sastavni dijelovi u smislu Uredbe (EU) YYYY/XX [o umjetnoj inteligenciji] uzimaju se u obzir zahtjevi iz glave III. poglavlja 2. te uredbe.”

6. U članku 58. dodaje se sljedeći stavak:

„3. Pri donošenju delegiranih akata u skladu sa stavcima 1. i 2. o sustavima umjetne inteligencije koji su sigurnosni sastavni dijelovi u smislu Uredbe (EU) YYYY/XX [o umjetnoj inteligenciji] uzimaju se u obzir zahtjevi iz glave III. poglavlja 2. te uredbe.”

*Članak 82.
Izmjena Uredbe (EU) 2019/2144*

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

„3. Pri donošenju provedbenih akata u skladu sa stavkom 2. o sustavima umjetne inteligencije koji su sigurnosni sastavni dijelovi u smislu Uredbe (EU) YYYY/XX [o umjetnoj inteligenciji]

Europskog parlamenta i Vijeća* uzimaju se u obzir zahtjevi iz glave III. poglavlja 2. te uredbe.

* Uredba (EU) YYYY/XX [o umjetnoj inteligenciji] (SL ...).”.

Članak 83.

UI sustavi koji su već stavljeni na tržište ili u uporabu

1. Ova se Uredba ne primjenjuje na UI sustave koji su sastavni dijelovi opsežnih informacijskih sustava uspostavljenih pravnim aktima navedenima u Prilogu IX. koji su stavljeni na tržište ili u uporabu prije [*12 mjeseci nakon datuma početka primjene ove Uredbe iz članka 85. stavka 2.*], osim ako zamjena ili izmjena tih pravnih akata dovodi do znatne promjene u konceptu ili namjeni dotičnog UI sustava ili dotičnih UI sustava.

Zahtjevi utvrđeni u ovoj Uredbi uzimaju se u obzir, ako je primjenjivo, pri evaluaciji svakog opsežnog informacijskog sustava uspostavljenog pravnim aktima navedenima u Prilogu IX. koju treba provesti kako je predviđeno u tim aktima.

2. Ova se Uredba primjenjuje na visokorizične UI sustave, osim onih iz stavka 1., koji su stavljeni na tržište ili u uporabu prije [*datum početka primjene ove Uredbe iz članka 85. stavka 2.*] samo ako se nakon tog datuma znatno promijeni koncept ili namjena tih sustava.

Članak 84.

Evaluacija i preispitivanje

1. Komisija procjenjuje potrebu za izmjenom popisa iz Priloga III. jednom godišnje nakon stupanja na snagu ove Uredbe.
2. Do [*tri godine nakon datuma početka primjene ove Uredbe iz članka 85. stavka 2.*] i svake četiri godine nakon toga Komisija Europskom parlamentu i Vijeću podnosi izvješće o evaluaciji i preispitivanju ove Uredbe. Ta se izvješća objavljuju.
3. U izvješćima iz stavka 2. posebna se pozornost pridaje sljedećem:
 - (a) stanju financijskih i ljudskih resursa nacionalnih nadležnih tijela radi djelotvornog obavljanja zadaća koje su im dodijeljene na temelju ove Uredbe;
 - (b) stanju sankcija, a posebno upravnih novčanih kazni iz članka 71. stavka 1., koje države članice primjenjuju na povrede odredaba ove Uredbe.
4. Do [*tri godine nakon datuma početka primjene ove Uredbe iz članka 85. stavka 2.*] i svake četiri godine nakon toga Komisija evaluiira učinak i djelotvornost kodeksâ ponašanja kako bi se potaknula primjena zahtjeva iz glave III. poglavlja 2., a možda i drugih dodatnih zahtjeva, na UI sustave koji nisu visokorizični.
5. Odbor, države članice i nacionalna nadležna tijela Komisiji na zahtjev dostavljaju informacije za potrebe stavaka od 1. do 4.
6. Pri provedbi evaluacija i preispitivanjâ iz stavaka od 1. do 4. Komisija uzima u obzir stajališta i zaključke Odbora, Europskog parlamenta, Vijeća i drugih relevantnih tijela ili izvora.

7. Komisija prema potrebi podnosi odgovarajuće prijedloge s ciljem izmjene ove Uredbe, posebno uzimajući u obzir razvoj tehnologije te s obzirom na napredak informacijskog društva.

Članak 85.

Stupanje na snagu i primjena

1. Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.
2. Ova Uredba primjenjuje se od [24 mjeseca nakon stupanja na snagu Uredbe].
3. Odstupajući od stavka 2.:
 - (a) glava III. poglavlje 4. i glava VI. primjenjuju se od [*tri mjeseca nakon stupanja na snagu ove Uredbe*];
 - (b) članak 71. primjenjuje se od [dvanaest mjeseci nakon stupanja na snagu ove Uredbe].

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

Sastavljeno u Bruxellesu,

Za Europski parlament
Predsjednik

Za Vijeće
Predsjednik

ZAKONODAVNI FINACIJSKI IZVJEŠTAJ

1. OKVIR PRIJEDLOGA/INICIJATIVE

- 1.1. Naslov prijedloga/inicijative
- 1.2. Predmetna područja politike
- 1.3. Prijedlog/inicijativa odnosi se na:
- 1.4. Ciljevi
 - 1.4.1. Opći ciljevi
 - 1.4.2. Posebni ciljevi
 - 1.4.3. Očekivani rezultati i učinak
 - 1.4.4. Pokazatelji uspješnosti
- 1.5. Osnova prijedloga/inicijative
 - 1.5.1. Zahtjevi koje treba ispuniti u kratkoročnom ili dugoročnom razdoblju, uključujući detaljan vremenski plan provedbe inicijative
 - 1.5.2. Dodana vrijednost sudjelovanja Unije (može proizlaziti iz različitih čimbenika, npr. prednosti koordinacije, pravne sigurnosti, veće djelotvornosti ili komplementarnosti). Za potrebe ove točke „dodana vrijednost sudjelovanja Unije” vrijednost je koja proizlazi iz intervencije Unije i predstavlja dodatnu vrijednost u odnosu na vrijednost koju bi države članice inače ostvarile same.
 - 1.5.3. Pouke iz prijašnjih sličnih iskustava
 - 1.5.4. Usklađenost s višegodišnjim financijskim okvirom i moguće sinergije s drugim prikladnim instrumentima
 - 1.5.5. Ocjena različitih dostupnih mogućnosti financiranja, uključujući mogućnost preraspodjele
- 1.6. Trajanje i financijski učinak prijedloga/inicijative
- 1.7. Predviđeni načini upravljanja

2. MJERE UPRAVLJANJA

- 2.1. Pravila praćenja i izvješćivanja
- 2.2. Sustav upravljanja i kontrole
 - 2.2.1. Obrazloženje načina upravljanja, mehanizama provedbe financiranja, načina plaćanja i predložene strategije kontrole
 - 2.2.2. Informacije o utvrđenim rizicima i uspostavljenim sustavima unutarnje kontrole za smanjenje rizika
 - 2.2.3. Procjena i obrazloženje troškovne učinkovitosti kontrola (omjer troškova kontrole i vrijednosti sredstava kojima se upravlja) i procjena očekivane razine rizika od pogreške (pri plaćanju i pri zaključenju)

2.3. Mjere za sprečavanje prijevara i nepravilnosti

3. PROCIJENJENI FINANCIJSKI UČINAK PRIJEDLOGA/INICIJATIVE

3.1. Naslovi višegodišnjeg financijskog okvira i proračunske linije rashoda na koje prijedlog/inicijativa ima učinak

3.2. Procijenjeni financijski učinak prijedloga na odobrena sredstva

3.2.1. Sažetak procijenjenog učinka na odobrena sredstva za poslovanje

3.2.2. Procijenjeni rezultati financirani odobrenim sredstvima za poslovanje

3.2.3. Sažetak procijenjenog učinka na administrativna odobrena sredstva

3.2.4. Usklađenost s aktualnim višegodišnjim financijskim okvirom

3.2.5. Doprinos trećih strana

3.3. Procijenjeni učinak na prihode

ZAKONODAVNI FINACIJSKI IZVJEŠTAJ

1. OKVIR PRIJEDLOGA/INICIJATIVE

1.1. Naslov prijedloga/inicijative

Uredba Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) i izmjeni određenih zakonodavnih akata Unije

1.2. Predmetna područja politike

Komunikacijske mreže, sadržaji i tehnologija

Unutarnje tržište, industrija, poduzetništvo te mala i srednja poduzeća

Učinak na proračun odnosi se na nove zadaće povjerene Komisiji, uključujući podršku Europskom odboru za umjetnu inteligenciju

Aktivnost: izgradnja digitalne budućnosti Europe

1.3. Prijedlog/inicijativa odnosi se na:

☒ **novo djelovanje**

☐ **novo djelovanje nakon pilot-projekta/pripremnog djelovanja**⁶⁴

☐ **produženje postojećeg djelovanja**

☐ **djelovanje koje je preusmjereno na novo djelovanje**

1.4. Ciljevi

1.4.1. Opći ciljevi

Opći je cilj intervencije osiguravanje pravilnog funkcioniranja jedinstvenog tržišta stvaranjem uvjeta za razvoj i uporabu pouzdane umjetne inteligencije u Uniji.

1.4.2. Posebni ciljevi

Posebni cilj br. 1

Utvrđiti zahtjeve specifične za UI sustave i obveze za sve sudionike lanca vrijednosti kako bi se osiguralo da su UI sustavi koji se stavljaju na tržište i upotrebljavaju sigurni i usklađeni s postojećim pravom o temeljnim pravima i vrijednostima Unije.

Posebni cilj br. 2

Zajamčiti pravnu sigurnost kako bi se olakšala ulaganja i inovacije u području umjetne inteligencije tako što će se jasno utvrditi koji se temeljni zahtjevi, obveze te postupci ocjenjivanja sukladnosti i usklađenosti moraju poštovati da bi se UI sustav stavio na tržište Unije ili upotrebljavao na njemu.

Posebni cilj br. 3

Poboljšati upravljanje i učinkovito provođenje postojećeg prava o temeljnim pravima i sigurnosnim zahtjevima koje je primjenjivo na UI sustave reguliranjem novih ovlasti, sredstava i jasnih pravila za relevantna tijela u pogledu postupaka

⁶⁴

Kako je navedeno u članku 54. stavku 2. točkama (a) ili (b) Financijske uredbe.

ocjenjivanja sukladnosti i *ex post* praćenja te podjelom zadaća u području upravljanja i nadzora između nacionalne razine i razine EU-a.

Posebni cilj br. 4

Olakšati razvoj jedinstvenog tržišta za zakonite, sigurne i pouzdane primjene umjetne inteligencije te spriječiti fragmentaciju tržišta djelovanjem na razini EU-a s ciljem utvrđivanja minimalnih zahtjeva za stavljanje UI sustavâ na tržište Unije i uporabu na njemu u skladu s postojećim pravom o temeljnim pravima i sigurnosti.

1.4.3. Očekivani rezultati i učinak

Navesti očekivane učinke prijedloga/inicijative na ciljane korisnike/skupine.

Dobavljači UI-ja trebali bi imati koristi od minimalnog, ali jasnog skupa zahtjeva kojim se stvara pravna sigurnost i osigurava pristup cijelom jedinstvenom tržištu.

Korisnici UI-ja trebali bi imati koristi od pravne sigurnosti da su visokorizični UI sustavi koje kupuju u skladu s europskim zakonima i vrijednostima.

Potrošači bi trebali imati koristi od smanjenja rizika od ugrožavanja njihove sigurnosti ili temeljnih prava.

1.4.4. Pokazatelji uspješnosti

Navesti pokazatelje koji omogućuju praćenje provedbe prijedloga/inicijative.

Pokazatelj 1

broj ozbiljnih incidenata ili radnih učinaka UI-ja koji se smatraju ozbiljnim incidentom ili kršenjem obveza u pogledu temeljnih prava (polugodišnje) prema području primjene i izračunati (a) u apsolutnim vrijednostima, (b) kao udio primjena i (c) kao udio pogođenih građana

Pokazatelj 2

(a) ukupna ulaganja u umjetnu inteligenciju u EU-u (godišnje)

(b) ukupna ulaganja u umjetnu inteligenciju po državi članici (godišnje)

(c) udio poduzeća u kojima se upotrebljava umjetna inteligencija (godišnje)

(d) udio malih i srednjih poduzeća u kojima se upotrebljava umjetna inteligencija (godišnje)

(a) i (b) izračunat će se na temelju službenih izvora i usporediti s privatnim procjenama

(c) i (d) prikupljat će se redovnim anketama u poduzećima

1.5. Osnova prijedloga/inicijative

1.5.1. *Zahtjevi koje treba ispuniti u kratkoročnom ili dugoročnom razdoblju, uključujući detaljan vremenski plan provedbe inicijative*

Uredba bi trebala biti u potpunosti primjenjiva godinu i pol nakon njezina donošenja. Međutim, elementi strukture upravljanja trebali bi biti uspostavljeni prije toga. Države članice trebaju ponajprije imenovati postojeća tijela i/ili uspostaviti nova tijela koja će obavljati zadaće prethodno utvrđene zakonodavstvom te bi Europski odbor za umjetnu inteligenciju trebao biti osnovan i na snazi. Europska baza podataka za UI sustave trebala bi prije početka primjene biti u potpunosti funkcionalna. Stoga je nužno izraditi bazu podataka usporedno s postupkom donošenja kako bi bila spremna kad Uredba stupi na snagu.

- 1.5.2. *Dodana vrijednost sudjelovanja Unije (može proizlaziti iz različitih čimbenika, npr. prednosti koordinacije, pravne sigurnosti, veće djelotvornosti ili komplementarnosti). Za potrebe ove točke „dodana vrijednost sudjelovanja Unije” vrijednost je koja proizlazi iz intervencije Unije i predstavlja dodatnu vrijednost u odnosu na vrijednost koju bi države članice inače ostvarile same.*

Okvir sastavljen od mnoštva novih potencijalno različitih nacionalnih pravila otežat će nesmetano dobavljanje UI sustavâ u cijelom EU-u te nije djelotvorno jamstvo sigurnosti i zaštite temeljnih prava i vrijednosti Unije u različitim državama članicama. Zajedničko zakonodavno djelovanje EU-a u području UI-ja moglo bi ojačati unutarnje tržište te ima velik potencijal da europskoj industriji omogućiti konkurentsku prednost na svjetskoj razini i ekonomije razmjera koje pojedinačne države članice ne mogu ostvariti same.

- 1.5.3. *Pouke iz prijašnjih sličnih iskustava*

Direktivom 2000/31/EZ o elektroničkoj trgovini pruža se temeljni okvir za funkcioniranje jedinstvenog tržišta i nadzor digitalnih usluga te utvrđuje osnovna struktura općeg mehanizma suradnje među državama članicama, i u načelu se odnosi na sve zahtjeve primjenjive na digitalne usluge. Evaluacija Direktive ukazala je na nedostatke u određenim aspektima tog mehanizma suradnje, uključujući važne postupovne aspekte, kao što je nepostojanje jasnih rokova za odgovor država članica u kombinaciji s općim izostankom odgovora na zahtjeve njihovih partnera. To je s godinama dovelo do nedostatka povjerenja među državama članicama u rješavanju pitanja povezanih s pružateljima prekograničnih digitalnih usluga. Evaluacija Direktive pokazala je potrebu za definiranjem različitih pravila i zahtjeva na europskoj razini. Zbog toga je za provedbu posebnih obveza utvrđenih u ovoj Uredbi potreban poseban mehanizam suradnje na razini EU-a, sa strukturom upravljanja kojom se osigurava koordinacija konkretnih odgovornih tijela na razini EU-a.

- 1.5.4. *Usklađenost s višegodišnjim financijskim okvirom i moguće sinergije s drugim prikladnim instrumentima*

Uredbom o utvrđivanju usklađenih pravila o UI-ju i izmjeni određenih zakonodavnih akata Unije utvrđuje se novi zajednički okvir zahtjeva koji se primjenjuju na UI sustave, što uvelike nadilazi okvir predviđen postojećim zakonodavstvom. Zbog toga je ovim prijedlogom potrebno uspostaviti novu nacionalnu i europsku regulatornu i koordinacijsku funkciju.

Kad je riječ o mogućim sinergijama s drugim prikladnim instrumentima, ulogu tijela koja provode prijavljivanje na nacionalnoj razini mogu izvršavati nacionalna tijela koja obavljaju slične funkcije u skladu s drugim propisima EU-a.

Osim toga, jačanjem povjerenja u UI, a time i poticanjem ulaganja u razvoj i primjenu UI-ja nadopunjuje se program Digitalna Europa, kojemu je promicanje širenja primjene UI-ja jedan od pet prioriteta.

- 1.5.5. *Ocjena različitih dostupnih mogućnosti financiranja, uključujući mogućnost preraspodjele*

Osoblje će biti preraspoređeno. S obzirom na to da se ovom Uredbom, odnosno osiguravanjem pouzdanog UI-ja, izravno pridonosi jednom od ključnih ciljeva programa Digitalna Europa, odnosno ubrzanju razvoja i uvođenja UI-ja u Europi, ostali troškovi pokrit će se iz omotnice za program Digitalna Europa.

1.6. Trajanje i financijski učinak prijedloga/inicijative

☐ **Ograničeno trajanje**

- ☐ na snazi od [DD/MM]GGGG do [DD/MM]GGGG
- ☐ financijski učinak od GGGG do GGGG za odobrena sredstva za preuzete obveze i od GGGG do GGGG za odobrena sredstva za plaćanje

☒ **Neograničeno trajanje**

- provedba s početnim razdobljem od **jedne/dvije (još nije potvrđeno)** godine,
- nakon čega slijedi redovna provedba.

1.7. Predviđeni načini upravljanja⁶⁵

☒ **Izravno upravljanje** koje provodi Komisija

- ☐ putem svojih službi, uključujući osoblje u delegacijama Unije
- ☐ putem izvršnih agencija

☐ **Podijeljeno upravljanje** s državama članicama

☐ **Neizravno upravljanje** povjeravanjem zadaća izvršenja proračuna:

- ☐ trećim zemljama ili tijelima koja su one odredile
- ☐ međunarodnim organizacijama i njihovim agencijama (navesti)
- ☐ EIB-u i Europskom investicijskom fondu
- ☐ tijelima iz članaka 70. i 71. Financijske uredbe
- ☐ tijelima javnog prava
- ☐ tijelima uređenima privatnim pravom koja pružaju javne usluge u mjeri u kojoj daju odgovarajuća financijska jamstva
- ☐ tijelima uređenima privatnim pravom države članice kojima je povjerena provedba javno-privatnog partnerstva i koja daju odgovarajuća financijska jamstva
- ☐ osobama kojima je povjerena provedba određenih djelovanja u području ZVSP-a u skladu s glavom V. UEU-a i koje su navedene u odgovarajućem temeljnom aktu.
- *Ako je navedeno više načina upravljanja, potrebno je pojasniti u odjeljku „Napomene”.*

Napomene

--

⁶⁵

Informacije o načinima upravljanja i upućivanja na Financijsku uredbu dostupni su na internetskim stranicama BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. MJERE UPRAVLJANJA

2.1. Pravila praćenja i izvješćivanja

Navesti učestalost i uvjete.

Uredba će se preispitati i evaluirati pet godina nakon njezina stupanja na snagu. Komisija će podnijeti izvješće o rezultatima evaluacije Europskom parlamentu, Vijeću i Europskom gospodarskom i socijalnom odboru.

2.2. Sustavi upravljanja i kontrole

2.2.1. *Obrazloženje načina upravljanja, mehanizama provedbe financiranja, načina plaćanja i predložene strategije kontrole*

Uredbom se uspostavlja nova politika u pogledu usklađenih pravila za dobavljanje UI sustava na unutarnjem tržištu te se istodobno osigurava poštovanje sigurnosti i temeljnih prava. Za ta nova pravila potreban je mehanizam konzistentnosti za prekograničnu primjenu obveza iz ove Uredbe u obliku nove savjetodavne skupine koja koordinira aktivnosti nacionalnih tijela.

Kako bi mogle obavljati te nove zadaće, službama Komisije potrebno je osigurati odgovarajuća sredstva. Procjenjuje se da će za provedbu nove Uredbe biti potrebno 10 EPRV-a (pet EPRV-a za potporu aktivnostima Odbora i pet EPRV-a za rad Europskog nadzornika za zaštitu podataka koji djeluje kao tijelo koje provodi prijavljivanje UI sustava razvijenih u okviru tijela Europske unije).

2.2.2. *Informacije o utvrđenim rizicima i uspostavljenim sustavima unutarnje kontrole za smanjenje rizika*

Kako bi članovi Odbora mogli provoditi analize utemeljene na činjeničnim dokazima, predviđeno je da administrativne strukture Komisije pružaju podršku Odboru i da se osnuje stručna skupina koja bi, prema potrebi, davala dodatna stručna mišljenja.

2.2.3. *Procjena i obrazloženje troškovne učinkovitosti kontrola (omjer troškova kontrole i vrijednosti sredstava kojima se upravlja) i procjena očekivane razine rizika od pogreške (pri plaćanju i pri zaključenju)*

S obzirom na nisku vrijednost transakcija (npr. nadoknada putnih troškova izaslaniku za sastanak), čini se da su standardni postupci kontrole dostatni za rashode za sastanke. Kad je riječ o izradi baze podataka, za dodjelu ugovorâ u Glavnoj upravi CNECT u okviru centralizirane javne nabave postoji učinkovit sustav unutarnje kontrole.

2.3. Mjere za sprečavanje prijevара i nepravilnosti

Navesti postojeće ili predviđene mjere za sprečavanje i zaštitu, npr. iz strategije za borbu protiv prijevara.

Postojećim mjerama za sprečavanje prijevara za koje je nadležna Komisija pokrit će se dodatna odobrena sredstva potrebna za ovu Uredbu.

3. PROCIJENJENI FINANCIJSKI UČINAK PRIJEDLOGA/INICIJATIVE

3.1. Naslovi višegodišnjeg financijskog okvira i proračunske linije rashoda na koje prijedlog/inicijativa ima učinak

- Postojeće proračunske linije

Prema redoslijedu naslova višegodišnjeg financijskog okvira i proračunskih linija.

Naslov višegodišnjeg financijskog okvira	Proračunska linija	Vrsta rashoda	Doprinos			
	Broj	dif./nedif. 66	zemalja EFTA-e ⁶⁷	zemalja kandidatkinja ⁶⁸	trećih zemalja	u smislu članka 21. stavka 2. točke (b) Financijske uredbe
7.	20 02 06 administrativni rashodi	nedif.	NE	NE	NE	NE
1.	02 04 03 program Digitalna Europa, umjetna inteligencija	dif.	DA	NE	NE	NE
1.	02 01 30 01 rashodi za potporu programu Digitalna Europa	nedif.	DA	NE	NE	NE

3.2. Procijenjeni financijski učinak prijedloga na odobrena sredstva

3.2.1. Sažetak procijenjenog učinka na rashode za odobrena sredstva za poslovanje

- ☐ Za prijedlog/inicijativu nisu potrebna odobrena sredstva za poslovanje.
- ☒ Za prijedlog/inicijativu potrebna su sljedeća odobrena sredstva za poslovanje:

U milijunima EUR (do 3 decimalna mjesta)

⁶⁶ Dif. = diferencirana odobrena sredstva; nedif. = nediferencirana odobrena sredstva.

⁶⁷ EFTA: Europsko udruženje slobodne trgovine.

⁶⁸ Zemlje kandidatkinje i, ako je primjenjivo, potencijalni kandidati sa zapadnog Balkana.

Naslov višegodišnjeg financijskog okvira	1.	
---	----	--

Glavna uprava: CNECT				Godina 2022.	Godina 2023.	Godina 2024.	Godina 2025.	Godina 2026.	Godina 2027. ⁶⁹	UKUPNO	
• Odobrena sredstva za poslovanje											
Proračunska linija ⁷⁰ 02 04 03	Obveze	(1a)			1,000						1,000
	Plaćanja	(2a)			0,600	0,100	0,100	0,100	0,100		1,000
Proračunska linija	Obveze	(1b)									
	Plaćanja	(2b)									
Administrativna odobrena sredstva koja se financiraju iz omotnice za posebne programe ⁷¹											
Proračunska linija 02 01 30 01		(3)			0,240	0,240	0,240	0,240	0,240		1,200
UKUPNA odobrena sredstva za Glavnu upravu CNECT	Obveze	=1a+1b+3			1,240		0,240	0,240	0,240		2,200
	Plaćanja	=2a+2b+3			0,840	0,340	0,340	0,340	0,340		2,200

⁶⁹ Indikativno i ovisi o raspoloživosti proračunskih sredstava.

⁷⁰ Prema službenoj proračunskoj nomenklaturi.

⁷¹ Tehnička i/ili administrativna pomoć i rashodi za potporu provedbi programa i/ili djelovanja EU-a (prijašnje linije „BA”), neizravno istraživanje, izravno istraživanje.

• UKUPNA odobrena sredstva za poslovanje	Obveze	(4)		1,000						1,000
	Plaćanja	(5)		0,600	0,100	0,100	0,100	0,100		1,000
• UKUPNA administrativna odobrena sredstva koja se financiraju iz omotnice za posebne programe		(6)		0,240	0,240	0,240	0,240	0,240		1,200
UKUPNA odobrena sredstva iz NASLOVA 1. višegodišnjeg financijskog okvira	Obveze	=4+6		1,240	0,240	0,240	0,240	0,240		2,200
	Plaćanja	=5+6		0,840	0,340	0,340	0,340	0,340		2,200

Ako prijedlog/inicijativa utječe na više od jednog naslova, ponovite prethodni odjeljak:

• UKUPNA odobrena sredstva za poslovanje (svi naslovi za poslovanje)	Obveze	(4)								
	Plaćanja	(5)								
• UKUPNA administrativna odobrena sredstva koja se financiraju iz omotnice za posebne programe (svi naslovi za poslovanje)		(6)								
UKUPNA odobrena sredstva iz NASLOVA 1.–6. višegodišnjeg financijskog okvira (referentni iznos)	Obveze	=4+6								
	Plaćanja	=5+6								

Naslov višegodišnjeg financijskog okvira	7.	„Administrativni rashodi”
---	-----------	---------------------------

U ovaj se dio unose „administrativni proračunski podaci”, koji se najprije unose u [prilog zakonodavnom financijskom izvještaju](#) (Prilog V. internim pravilima), koji se učitava u sustav DECIDE za potrebe savjetovanja među službama.

U milijunima EUR (do 3 decimalna mjesta)

		Godina 2023.	Godina 2024.	Godina 2025.	Godina 2026.	Godina 2027.	Nakon ⁷² 2027.	UKUPNO
Glavna uprava: CNECT								
• Ljudski resursi		0,760	0,760	0,760	0,760	0,760	0,760	3,800
• Ostali administrativni rashodi		0,010	0,010	0,010	0,010	0,010	0,010	0,050
UKUPNO ZA GLAVNU UPRAVU CNECT	Odobrena sredstva	0,760	0,760	0,760	0,760	0,760	0,760	3,850
Europski nadzornik za zaštitu podataka								
• Ljudski resursi		0,760	0,760	0,760	0,760	0,760	0,760	3,800
• Ostali administrativni rashodi								
UKUPNO ZA EUROPSKOG NADZORNIKA ZA ZAŠTITU PODATAKA	Odobrena sredstva	0,760	0,760	0,760	0,760	0,760	0,760	3,800
UKUPNA odobrena sredstva iz NASLOVA 7. višegodišnjeg financijskog okvira	(ukupne obveze = ukupna plaćanja)	1,530	1,530	1,530	1,530	1,530	1,530	7,650

U milijunima EUR (do 3 decimalna mjesta)

⁷² Svi iznosi u ovom stupcu okvirni su i ovise o nastavku programâ i raspoloživosti odobrenih sredstava.

		Godina 2022.	Godina 2023.	Godina 2024.	Godina 2025.	Godina 2026.	Godina 2027.		UKUPNO	
UKUPNA odobrena sredstva iz NASLOVA 1.–7. višegodišnjeg financijskog okvira	Obveze		2,770	1,770	1,770	1,770	1,770		9,850	
	Plaćanja		2,370	1,870	1,870	1,870	1,870		9,850	

3.2.2. Procijenjeni rezultati financirani odobrenim sredstvima za poslovanje

Odobrena sredstva za preuzimanje obveza u milijunima EUR (do 3 decimalna mjesta)

Navesti ciljeve i rezultate ↓			Godina 2022.		Godina 2023.		Godina 2024.		Godina 2025.		Godina 2026.		Godina 2027.		Nakon 2027. ⁷³		UKUPNO	
	REZULTATI																	
	Vrsta	Prosječni trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Ukupn i broj	Ukupni trošak
POSEBNI CILJ br. 1 ⁷⁴ ...																		
Baza podataka					1	1,000	1		1		1		1		1	0,100	1	1,000
Sastanci – rezultati					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Komunikacijske aktivnosti					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Međubroj za posebni cilj br. 1																		
POSEBNI CILJ br. 2...																		
– Rezultat																		
Međubroj za posebni cilj br. 2																		
UKUPNO					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

⁷³ Svi iznosi u ovom stupcu okvirni su i ovise o nastavku programâ i raspoloživosti odobrenih sredstava.

⁷⁴ Kako je opisan u odjeljku 1.4.2. „Posebni ciljevi...”.

3.2.3. Sažetak procijenjenog učinka na administrativna odobrena sredstva

- ☐ Za prijedlog/inicijativu nisu potrebna administrativna odobrena sredstva.
- ☒ Za prijedlog/inicijativu potrebna su sljedeća administrativna odobrena sredstva:

U milijunima EUR (do 3 decimalna mjesta)

	Godina 2022.	Godina 2023.	Godina 2024.	Godina 2025.	Godina 2026.	Godina 2027.	Godišnje nakon 2027. ⁷⁵	UKUPNO
--	-----------------	-----------------	-----------------	-----------------	-----------------	-----------------	--	--------

NASLOV 7. višegodišnjeg financijskog okvira								
Ljudski resursi		1,520	1,520	1,520	1,520	1,520	1,520	7,600
Ostali administrativni rashodi		0,010	0,010	0,010	0,010	0,010	0,010	0,050
Međuzbroj za NASLOV 7. višegodišnjeg financijskog okvira		1,530	1,530	1,530	1,530	1,530	1,530	7,650

izvan NASLOVA 7.⁷⁶ višegodišnjeg financijskog okvira								
Ljudski resursi								
Ostali administrativni rashodi		0,240	0,240	0,240	0,240	0,240	0,240	1,20
Međuzbroj izvan NASLOVA 7. višegodišnjeg financijskog okvira		0,240	0,240	0,240	0,240	0,240	0,240	1,20

UKUPNO		1,770	1,770	1,770	1,770	1,770	1,770	8,850
---------------	--	--------------	--------------	--------------	--------------	--------------	--------------	--------------

Potrebna odobrena sredstva za ljudske resurse i ostale administrativne rashode pokrit će se odobrenim sredstvima glavne uprave koja su već dodijeljena za upravljanje djelovanjem i/ili su preraspodijeljena unutar glavne uprave te, prema potrebi, dodatnim sredstvima koja se mogu dodijeliti nadležnoj glavnoj upravi u okviru godišnjeg postupka dodjele sredstava uzimajući u obzir proračunska ograničenja.

⁷⁵

Svi iznosi u ovom stupcu okvirni su i ovise o nastavku programâ i raspoloživosti odobrenih sredstava.

⁷⁶

Tehnička i/ili administrativna pomoć i rashodi za potporu provedbi programa i/ili djelovanja EU-a (prijašnje linije „BA”), neizravno istraživanje, izravno istraživanje.

3.2.3.1. Procijenjene potrebe u pogledu ljudskih resursa

- ☐ Za prijedlog/inicijativu nisu potrebni ljudski resursi.
- ☒ Za prijedlog/inicijativu potrebni su sljedeći ljudski resursi:

Procjenu navesti u ekvivalentima punog radnog vremena

	Godina 2023.	Godina 2024.	Godina 2025.	2026.	2027.	Nakon 2027. ⁷⁷	
• Radna mjesta prema planu radnih mjesta (dužnosnici i privremeno osoblje)							
20 01 02 01 (sjedište i predstavništva Komisije)	10	10	10	10	10	10	
20 01 02 03 (delegacije)							
01 01 01 01 (neizravno istraživanje)							
01 01 01 11 (izravno istraživanje)							
Druge proračunske linije (navesti)							
• Vanjsko osoblje (u ekvivalentu punog radnog vremena: EPRV)⁷⁸							
20 02 01 (UO, UNS, UsO iz „globalne oмотnice”)							
20 02 03 (UO, LO, UNS, UsO i MSD u delegacijama)							
XX 01 xx yy zz ⁷⁹	– u sjedištima						
	– u delegacijama						
01 01 01 02 (UO, UNS, UsO – neizravno istraživanje)							
01 01 01 12 (UO, UNS, UsO – izravno istraživanje)							
Druge proračunske linije (navesti)							
UKUPNO	10	10	10	10	10	10	

XX se odnosi na odgovarajuće područje politike ili glavu proračuna.

Potrebe za ljudskim resursima pokrit će se osobljem glavne uprave kojemu je već povjereno upravljanje djelovanjem i/ili koje je preraspoređeno unutar glavne uprave te, prema potrebi, resursima koji se mogu dodijeliti nadležnoj glavnoj upravi u okviru godišnjeg postupka dodjele sredstava uzimajući u obzir proračunska ograničenja.

Od Europskog nadzornika za zaštitu podataka očekuje se da će osigurati polovicu potrebnih resursa.

Opis zadaća:

Dužnosnici i privremeno osoblje	U cilju pripreme ukupno 13–16 sastanaka, nacрта izvješća, nastavka političkog rada, npr. u vezi s budućim izmjenama popisa visokorizičnih primjena umjetne inteligencije, te održavanja odnosa s tijelima država članica bit će potrebna četiri EPRV-a AD i jedan EPRV AST. Za UI sustave koje razvijaju institucije EU-a odgovoran je Europski nadzornik za zaštitu podataka (EDPS). Na temelju prošlih iskustava može se procijeniti da je potrebno pet EPRV-a AD kako bi se ispunile odgovornosti EDPS-a u skladu s nacrtom zakonodavstva.
Vanjsko osoblje	

⁷⁷ Svi iznosi u ovom stupcu okvirni su i ovise o nastavku programâ i raspoloživosti odobrenih sredstava.

⁷⁸ UO = ugovorno osoblje; LO = lokalno osoblje; UNS = upućeni nacionalni stručnjaci; UsO = ustupljeno osoblje; MSD = mladi stručnjaci u delegacijama.

⁷⁹ U okviru gornje granice za vanjsko osoblje iz odobrenih sredstava za poslovanje (prijašnje linije „BA”).

3.2.4. Usklađenost s aktualnim višegodišnjim financijskim okvirom

Prijedlog/inicijativa:

- ☒ može se u potpunosti financirati preraspodjelom unutar relevantnog naslova višegodišnjeg financijskog okvira (VFO).

Nije potrebno reprogramiranje.

- ☐ zahtijeva upotrebu nedodijeljene razlike u okviru relevantnog naslova VFO-a i/ili upotrebu posebnih instrumenata kako su definirani u Uredbi o VFO-u.

Objasniti što je potrebno te navesti predmetne naslove i proračunske linije, odgovarajuće iznose te instrumente čija se upotreba predlaže.

- ☐ zahtijeva reviziju VFO-a.

Objasniti što je potrebno te navesti predmetne naslove i proračunske linije te odgovarajuće iznose.

3.2.5. Doprinos trećih strana

U prijedlogu/inicijativi:

- ☒ ne predviđa se sudjelovanje trećih strana u sufinanciranju.
- ☐ predviđa se sudjelovanje trećih strana u sufinanciranju prema sljedećoj procjeni:

Odobrena sredstva u milijunima EUR (do 3 decimalna mjesta)

	Godina N ⁸⁰	Godina N+1	Godina N+2	Godina N+3	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)			Ukupno
Navedi tijelo koje sudjeluje u financiranju								
UKUPNO sufinancirana odobrena sredstva								

⁸⁰

Godina N je godina početka provedbe prijedloga/inicijative. Umjesto „N” upisati predviđenu prvu godinu provedbe (na primjer: 2021.). Isto vrijedi i za ostale godine.

3.3. Procijenjeni učinak na prihode

- ☐ Prijedlog/inicijativa ima sljedeći financijski učinak:
- ☐ Prijedlog/inicijativa ima sljedeći financijski učinak:
 - ☐ na ostale prihode
 - ☐ na ostale prihode
 - navesti jesu li prihodi namijenjeni proračunskim linijama rashoda ☐

U milijunima EUR (do 3 decimalna mjesta)

Proračunska prihoda:	linija	Odobrena sredstva dostupna za tekuću financijsku godinu	Učinak prijedloga/inicijative ⁸¹						
			Godina N	Godina N+1	Godina N+2	Godina N+3	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)		
Članak									

Za namjenske prihode navesti odgovarajuće proračunske linije rashoda.

--

Ostale napomene (npr. metoda/formula za izračun učinka na prihode ili druge informacije)

--

⁸¹

Kad je riječ o tradicionalnim vlastitim sredstvima (carine, pristojbe na šećer) navedeni iznosi moraju biti neto iznosi, to jest bruto iznosi nakon odbitka od 20 % na ime troškova naplate.