Vijeće
Europske unije

Bruxelles, 6. prosinca 2022.
(OR. en)

15698/22

Međuinstitucijski predmet:
2021/0106(COD)

TELECOM 516
JAI 1633
COPEN 434
CYBER 399
DATAPROTECT 351
EJUSTICE 95
COSI 318
IXIM 291
ENFOPOL 626
RELEX 1674
MI 918
COMPET 1005
CODEC 1940

ISHOD POSTUPAKA

Od:	Glavno tajništvo Vijeća
Na datum:	6. prosinca 2022.
Za:	Delegacije
Br. preth. dok.:	14954/22 + ADD 1
Br. dok. Kom.:	8115/21
Predmet:	Prijedlog uredbe Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) i izmjeni određenih zakonodavnih akata Unije – opći pristup (6. prosinca 2022.)

Za delegacije se u Prilogu nalazi opći pristup Vijeća o navedenom prijedlogu kako ga je Vijeće (promet, telekomunikacije i energetika) odobrilo na 3917. sastanku održanom 6. prosinca 2022.

Opći pristup predstavlja privremeno stajalište Vijeća o tom prijedlogu i osnova je za pripreme za pregovore s Europskim parlamentom.

PRILOG

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

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

(Tekst značajan za EGP)

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

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

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrta zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora[1],

uzimajući u obzir mišljenje Odbora regija[2],

uzimajući u obzir mišljenje Europske središnje banke[3],

u skladu s redovnim zakonodavnim postupkom,

budući da:

[1] SL C […], […], str. […].
[2] SL C […], […], str. […].
[3] Upućivanje na mišljenje ESB-a.

(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, uvoze 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 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 infrastrukturom, 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 prihvaćanje 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 utvrđivanju tih pravila i nadogradnji na rad Stručne skupine na visokoj razini za umjetnu inteligenciju koji se odražava u Smjernicama za pouzdanu umjetnu inteligenciju u EU-u, doprinosi Unijinu cilju globalnog vodstva u razvoju sigurne, pouzdane i etične umjetne inteligencije koji je odredilo Europsko vijeće[4] i osigurava se zaštita etičkih načela u skladu s izričitim zahtjevom Europskog parlamenta[5].

---

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

[5] 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).

(5a) Usklađena pravila o stavljanju na tržište, stavljanju u uporabu i uporabi UI sustava utvrđena u ovoj Uredbi trebala bi se primjenjivati u svim sektorima i, u skladu s njezinim pristupom novog zakonodavnog okvira, ne bi trebala dovoditi u pitanje postojeće pravo Unije, posebno ono u području zaštite podataka, zaštite potrošača, temeljnih prava, zapošljavanja i sigurnosti proizvoda, koje ova Uredba dopunjuje. Stoga sva prava i pravni lijekovi koji su tim pravom Unije predviđeni za potrošače i druge osobe na koje bi UI sustavi mogli negativno utjecati, među ostalim u pogledu naknade moguće štete u skladu s Direktivom Vijeća 85/374/EEZ od 25. srpnja 1985. o približavanju zakona i drugih propisa država članica u vezi s odgovornošću za neispravne proizvode, ostaju nepromijenjeni i u potpunosti primjenjivi. Osim toga, cilj je ove Uredbe ojačati učinkovitost tih postojećih prava i pravnih lijekova utvrđivanjem posebnih zahtjeva i obveza, među ostalim u pogledu transparentnosti, tehničke dokumentacije i vođenja evidencije o UI sustavima. Nadalje, obveze koje su na temelju ove Uredbe nametnute različitim operaterima uključenima u lanac vrijednosti UI-ja trebale bi se primjenjivati ne dovodeći u pitanje nacionalne zakone, u skladu s pravom Unije, i imati učinak ograničavanja uporabe određenih UI sustava ako takvi zakoni nisu obuhvaćeni područjem primjene ove Uredbe ili ako se njima žele ostvariti drugi legitimni ciljevi od javnog interesa koji nisu ciljevi iz ove Uredbe. Na primjer, ova Uredba ne bi trebala utjecati na nacionalno radno pravo ni na zakone o zaštiti maloljetnika (tj. osoba mlađih od 18 godina), uzimajući u obzir Opću napomenu Ujedinjenih naroda br. 25 (2021.) o pravima djeteta, u mjeri u kojoj nisu specifični za UI sustave i imaju druge legitimne ciljeve od javnog interesa.

(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 umjetne inteligencije, kao što su njezine sposobnosti učenja, zaključivanja ili modeliranja, i u njoj bi umjetnu inteligenciju trebalo razlikovati od jednostavnijih softverskih sustava i programskih pristupa. Konkretno, za potrebe ove Uredbe UI sustavi trebali bi moći na temelju podataka i ulaznih podataka koje je generirao stroj i/ili čovjek izvoditi zaključke o načinu na koji se može postići skup konačnih ciljeva koje im je zadao čovjek, primjenom strojnog učenja i/ili pristupa koji se temelje na logici i pristupa koji se temelje na znanju, i generirati izlazne rezultate kao što su sadržaj kod generativnih UI sustava (npr. tekst, videozapisi ili slike), predviđanja, preporuke ili odluke koji utječu na okolinu s kojom je sustav u interakciji, bilo u fizičkoj bilo u digitalnoj dimenziji. Sustav koji za automatsko izvršavanje operacija upotrebljava pravila koja su definirale isključivo fizičke osobe ne bi trebalo smatrati UI sustavom. 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). Koncept autonomije UI sustava odnosi se na stupanj u kojem takav sustav funkcionira bez sudjelovanja čovjeka.

(6a) Pristupi strojnog učenja usmjereni su na razvoj sustava sposobnih za učenje i izvođenje zaključaka iz podataka radi rješavanja problema u području primjene, a da nisu izričito programirani nizom postupnih uputa od ulaznih podataka do izlaznog rezultata. Učenje se odnosi na računalni proces optimizacije parametara modela iz podataka, što je matematička konstrukcija koja proizvodi izlazni rezultat na temelju ulaznih podataka. Problemi koji se rješavaju strojnim učenjem obično uključuju zadatke u kojima drugi pristupi ne uspijevaju, i to ili zato što ne postoji odgovarajuća formalizacija problema ili zato što je problem teško riješiti pristupima koji ne uključuju učenje. Pristupi strojnog učenja uključuju, na primjer, nadzirano, nenadzirano i podržano učenje, pri čemu se primjenjuju različite metode, među ostalim duboko učenje s neuronskim mrežama, statističke tehnike učenja i inferencija (uključujući, na primjer, logističku regresiju i Bayesovsku procjenu) te metode pretraživanja i optimizacije.

(6b) Pristupi koji se temelje na logici i pristupi koji se temelje na znanju usmjereni su na razvoj sustavâ s logičkim sposobnostima zaključivanja o znanju radi rješavanja problema u području primjene. Takvi sustavi obično uključuju bazu znanja i modul za inferenciju koji generira izlazne rezultate zaključivanjem na temelju baze znanja. Baza znanja, koju obično kodiraju ljudski stručnjaci, predstavlja subjekte i logičke odnose relevantne za problem u području primjene s pomoću formalizama utemeljenih na pravilima, ontologija ili grafikona znanja. Modul za inferenciju djeluje na temelju baze znanja i izvlači nove informacije operacijama kao što su razvrstavanje, pretraživanje, uparivanje ili ulančavanje. Pristupi koji se temelje na logici i pristupi koji se temelje na znanju uključuju, na primjer, reprezentaciju znanja, induktivno (logičko) programiranje, baze znanja, module za inferenciju i dedukciju, (simboličko) zaključivanje, stručne sustave i metode pretraživanja i optimizacije.

(6c) Radi osiguravanja jedinstvenih uvjeta za provedbu ove Uredbe u pogledu pristupa strojnom učenju, pristupa koji se temelje na logici i pristupa koji se temelje na znanju i kako bi se uzeo u obzir tržišni i tehnološki razvoj, provedbene ovlasti trebalo bi dodijeliti Komisiji.

(6d) Pojam „korisnik” iz ove Uredbe trebalo bi tumačiti kao svaku fizičku ili pravnu osobu, uključujući tijela javne vlasti, agencije ili druga tijela, koja upotrebljava UI sustav pod čijom se nadležnošću sustav upotrebljava. Ovisno o vrsti UI sustava, uporaba tog sustava može utjecati na osobe koje nisu korisnici.

(7) Pojam biometrijskih podataka koji se upotrebljava u ovoj Uredbi trebalo bi tumačiti dosljedno pojmu biometrijskih podataka kako je definiran člankom 4. točkom 14. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća[6], člankom 3. točkom 18. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća[7] i člankom 3. točkom 13. Direktive (EU) 2016/680 Europskog parlamenta i Vijeća[8].

[6] 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.).

[7] 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.)

[8] 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.).

(8) Pojam sustava za daljinsku biometrijsku identifikaciju koji se upotrebljava u ovoj Uredbi trebalo bi definirati funkcionalno, kao UI sustav namijenjen identificiranju pojedinaca, obično na daljinu, bez njihova aktivnog sudjelovanja, usporedbom biometrijskih podataka dotične osobe s biometrijskim podacima iz referentnog repozitorija podataka, bez obzira na tehnologiju, postupke ili vrste biometrijskih podataka koji se upotrebljavaju. Takvi sustavi za daljinsku biometrijsku identifikaciju obično se upotrebljavaju za percepciju (skeniranje) više osoba ili njihova ponašanja u isto vrijeme kako bi se znatno olakšala identifikacija određenog broja osoba bez njihova aktivnog sudjelovanja. Takva definicija isključuje sustave provjere/autentifikacije čija bi jedina svrha bila potvrditi da određeni pojedinac doista jest ona osoba za koju tvrdi da jest, kao i sustave koji se upotrebljavaju za potvrđivanje identiteta pojedinca isključivo u svrhu pristupa usluzi, uređaju ili prostorima. To je isključenje opravdano činjenicom da će takvi sustavi vjerojatno imati manji utjecaj na temeljna prava pojedinaca u usporedbi sa sustavima za daljinsku biometrijsku identifikaciju koji se mogu upotrebljavati za obradu biometrijskih podataka velikog broja osoba. 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 iz 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 dotičnih 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 neodređenom broju pojedinaca, bez obzira na to je li dotično mjesto u privatnom ili javnom vlasništvu i bez obzira na aktivnost za koju se to mjesto može upotrebljavati, kao što je trgovina (na primjer trgovine, restorani, kafići), usluge (na primjer banke, profesionalne aktivnosti, ugostiteljstvo), sport (na primjer bazeni, teretane, stadioni), prijevoz (na primjer autobusne i željezničke postaje, postaje podzemne željeznice, zračne luke, prijevozna sredstva), zabava (na primjer kina, kazališta, muzeji, koncertne i konferencijske dvorane), aktivnosti u slobodno vrijeme ili druge svrhe (na primjer javne ceste i trgovi, parkovi, šume, igrališta). Mjesto bi trebalo klasificirati kao javno i ako, bez obzira na mogući kapacitet ili sigurnosna ograničenja, pristup podliježe određenim unaprijed utvrđenim uvjetima koje može ispuniti neodređen broj osoba, kao što su kupnja ulaznice ili prijevozne karte, prethodna registracija ili određena dob. S druge strane, mjesto se ne bi trebalo smatrati javnim ako je pristup ograničen na određene i definirane fizičke osobe putem prava Unije ili nacionalnog prava koje je izravno povezano s javnom sigurnošću ili zaštitom ili putem jasnog iskaza volje osobe koja ima odgovarajuće ovlasti na dotičnom mjestu. Sama činjenična mogućnost pristupa (npr. otključana vrata, otvoreni ulaz u ogradi) ne znači da je mjesto javno ako postoje naznake ili okolnosti koje upućuju na suprotno (npr. znakovi kojima se zabranjuje ili ograničava pristup). Poslovni prostori poduzeća i tvornica te uredi i mjesta rada kojima mogu pristupiti samo relevantni zaposlenici i pružatelji usluga nisu javna mjesta. Javna mjesta ne bi trebala uključivati zatvore ili područja granične kontrole. Neka druga područja mogu uključivati i područja koja nisu javna mjesta i područja koja jesu javna mjesta, kao što je hodnik privatne stambene zgrade potreban za pristup liječničkoj ordinaciji ili zračna luka. Nisu obuhvaćeni ni internetski prostori jer oni nisu fizički prostori. Ipak, to je li određeno mjesto javno trebalo bi utvrditi u svakom slučaju posebno i pritom uzeti u obzir specifične okolnosti konkretne situacije.

(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 među visokorizične sustave. 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 budućom suradnjom sa stranim partnerima s kojima se razmjenjuju informacije i dokazi, ova se Uredba ne bi trebala primjenjivati na tijela javne vlasti treće zemlje ni na međunarodne organizacije 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, Europola i drugih agencija EU-a te trećih zemalja i međunarodnih organizacija. Nadležna tijela država članica primateljica i institucije, uredi i tijela Unije koji se koriste takvim izlaznim rezultatima u Uniji i dalje snose odgovornost za osiguravanje da njihova uporaba bude usklađena s pravom Unije. Pri reviziji tih međunarodnih sporazuma ili sklapanju novih u budućnosti ugovorne stranke trebale bi uložiti najveće moguće napore u usklađivanje tih sporazuma sa zahtjevima iz ove Uredbe.

(12) Ova bi se Uredba trebala primjenjivati i na institucije, urede, tijela i agencije Unije ako djeluju kao dobavljači ili korisnici UI sustava.

(-12a) Ako se, i u mjeri u kojoj se UI sustavi stavljaju na tržište, stavljaju u uporabu ili upotrebljavaju s izmjenama ili bez njih u obrambene i vojne svrhe te svrhe povezane s nacionalnom sigurnošću, te bi sustave trebalo isključiti iz područja primjene ove Uredbe bez obzira na to koja vrsta subjekta obavlja te aktivnosti, na primjer bez obzira na to je li riječ o javnom ili privatnom subjektu. Kad je riječ o vojnim i obrambenim svrhama, takvo je isključenje opravdano i člankom 4. stavkom 2. UEU-a i posebnostima obrambene politike država članica i zajedničke obrambene politike Unije obuhvaćene glavom V. poglavljem 2. Ugovora o Europskoj uniji (UEU) koje podliježu međunarodnom javnom pravu, koje je stoga primjereniji pravni okvir za reguliranje UI sustavâ u kontekstu uporabe smrtonosne sile i drugih UI sustava u kontekstu vojnih i obrambenih aktivnosti. Što se tiče nacionalne sigurnosti, isključenje je opravdano činjenicom da nacionalna sigurnost ostaje isključiva odgovornost država članica, u skladu s člankom 4. stavkom 2. UEU-a, i posebnom prirodom i operativnim potrebama aktivnosti povezanih s nacionalnom sigurnošću i posebnim nacionalnim pravilima koja se primjenjuju na te aktivnosti. Međutim, ako se UI sustav koji je razvijen, stavljen na tržište, stavljen u uporabu ili se upotrebljava u vojne ili obrambene svrhe ili svrhe povezane s nacionalnom sigurnošću privremeno ili trajno upotrebljava u druge svrhe (na primjer u civilne ili humanitarne svrhe, za potrebe kaznenog progona ili za potrebe javne sigurnosti), takav bi sustav bio obuhvaćen područjem primjene ove Uredbe. U tom bi slučaju subjekt koji taj sustav upotrebljava u svrhe koje nisu vojne, obrambene ili povezane s nacionalnom sigurnošću trebao osigurati usklađenost sustava s ovom Uredbom, osim ako je sustav s njome već usklađen. UI sustavi koji se stavljaju na tržište ili u uporabu u isključene svrhe (tj. vojne, obrambene ili povezane s nacionalnom sigurnošću) i u jednu ili više svrha koje nisu isključene (npr. civilne svrhe, kazneni progon itd.) obuhvaćeni su područjem primjene ove Uredbe i dobavljači tih sustava trebali bi osigurati usklađenost s ovom Uredbom. U tim slučajevima činjenica da UI sustav može biti obuhvaćen područjem primjene ove Uredbe ne bi trebala utjecati na mogućnost da subjekti koji provode aktivnosti povezane s nacionalnom sigurnošću te obrambene i vojne aktivnosti, bez obzira na vrstu subjekta koji te aktivnosti obavlja, upotrebljavaju UI sustave čija je uporaba isključena iz područja primjene ove Uredbe u svrhe povezane s nacionalnom sigurnošću te vojne i obrambene svrhe. UI sustav koji se stavlja na tržište u civilne svrhe ili u svrhe kaznenog progona i koji se s izmjenama ili bez njih upotrebljava u vojne, obrambene ili s nacionalnom

sigurnošću povezane svrhe ne bi trebao biti obuhvaćen područjem primjene ove Uredbe, bez obzira na vrstu subjekta koji obavlja te aktivnosti.

(12a) 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].

(12b) Ovom se Uredbom ne bi trebale ugroziti aktivnosti istraživanja i razvoja i njome bi se trebala poštovati sloboda znanosti. Stoga je potrebno iz njezina područja primjene isključiti UI sustave koji su posebno razvijeni i stavljeni u uporabu isključivo u svrhu znanstvenog istraživanja i razvoja te osigurati da Uredba na drugi način ne utječe na aktivnosti znanstvenih istraživanja i razvoja UI sustava. Odredbe ove Uredbe ne bi se trebale primjenjivati ni na istraživačke aktivnosti dobavljača usmjerene na proizvode. Time se ne dovodi u pitanje obveza usklađivanja s ovom Uredbom kada se UI sustav obuhvaćen područjem primjene ove Uredbe stavlja na tržište ili u uporabu kao rezultat takve aktivnosti istraživanja i razvoja ni primjena odredaba o regulatornim izoliranim okruženjima i testiranju u stvarnim uvjetima. Nadalje, ne dovodeći u pitanje ono što je prethodno navedeno u vezi s UI sustavima koji su posebno razvijeni i stavljeni u uporabu isključivo u svrhu znanstvenog istraživanja i razvoja, svi drugi UI sustavi koji se mogu upotrebljavati za obavljanje bilo kakve aktivnosti istraživanja i razvoja trebali bi i dalje podlijegati odredbama ove Uredbe. Aktivnosti istraživanja i razvoja u svim se okolnostima trebaju provoditi u skladu s priznatim etičkim i profesionalnim standardima za znanstvena istraživanja.

(12c) S obzirom na prirodu i složenost lanca vrijednosti za UI sustave ključno je pojasniti ulogu aktera koji mogu doprinijeti razvoju UI sustava, posebno visokorizičnih UI sustava. Konkretno, treba pojasniti da su UI sustavi opće namjene UI sustavi koje je dobavljač namijenio obavljanju općenito primjenjivih funkcija, kao što je prepoznavanje slike/govora, i to u različitim kontekstima. Mogu se sami po sebi upotrebljavati kao visokorizični UI sustavi ili mogu biti sastavni dijelovi drugih visokorizičnih UI sustava. Stoga bi zbog svoje posebne prirode i radi osiguravanja pravedne raspodjele odgovornosti u cijelom lancu vrijednosti UI-ja takvi sustavi trebali podlijegati razmjernim i konkretnijim zahtjevima i obvezama na temelju ove Uredbe te istodobno osiguravati visoku razinu zaštite temeljnih prava, zdravlja i sigurnosti. Osim toga, dobavljači UI sustava opće namjene, neovisno o tome mogu li ih drugi dobavljači upotrebljavati kao visokorizične UI sustave same po sebi ili kao sastavne dijelove visokorizičnih UI sustava, trebali bi prema potrebi surađivati s dobavljačima dotičnih visokorizičnih UI sustava kako bi im se omogućilo ispunjavanje relevantnih obveza iz ove Uredbe i s nadležnim tijelima uspostavljenima na temelju ove Uredbe. Kako bi se uzele u obzir posebne značajke UI sustava opće namjene i brz tržišni i tehnološki razvoj u tom području, Komisiji bi trebalo dodijeliti provedbene ovlasti za utvrđivanje i prilagodbu primjene zahtjeva utvrđenih na temelju ove Uredbe na UI sustave opće namjene i za utvrđivanje koje informacije trebaju dijeliti dobavljači UI sustava opće namjene kako bi se dobavljačima dotičnog visokorizičnog UI sustava omogućilo da ispune svoje obveze iz ove Uredbe.

(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 operatere 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 Unijinim 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) Manipulativne tehnike omogućene umjetnom inteligencijom mogu se upotrebljavati kako bi se osobe uvjerilo na sudjelovanje u neželjenom ponašanju ili kako bi ih se obmanulo tako da ih se potiče na odluke na način kojim se podriva i narušava njihova autonomija, donošenje odluka i slobodan izbor. Osobito su opasni stavljanje na tržište, stavljanje u uporabu i uporaba određenih UI sustava kojima se bitno mijenja čovjekovo ponašanje, pri čemu je vjerojatna pojava tjelesne ili psihološke štete, i stoga ih treba zabraniti. U takvim UI sustavima upotrebljavaju se subliminalne komponente kao što su zvučni i slikovni podražaji te videopodražaji koje osobe ne mogu percipirati jer ti podražaji nadilaze ljudsku percepciju ili druge subliminalne tehnike kojima se podriva ili narušava autonomija, donošenje odluka ili slobodan izbor osobe na načine koje ljudi svjesno ne percipiraju ili koje čak i kad su ih svjesni ne mogu kontrolirati ili im se oduprijeti, na primjer u slučajevima sučeljâ mozga i uređaja ili virtualne stvarnosti. Osim toga, UI sustavi mogu na drugi način iskorištavati ranjivosti određene skupine osoba zbog njihove dobi, invaliditeta u smislu Direktive (EU) 2019/882 ili posebne socijalne ili gospodarske situacije zbog kojih bi te osobe mogle biti izloženije iskorištavanju, kao što su osobe koje žive u ekstremnom siromaštvu i etničke ili vjerske manjine. Takvi UI sustavi mogu se staviti na tržište, staviti u uporabu ili upotrebljavati s ciljem ili učinkom bitnog mijenjanja ponašanja osobe, i to na način kojim se toj ili drugoj osobi ili skupinama osoba uzrokuje tjelesna ili psihološka šteta, što uključuje štetu koja se može akumulirati s vremenom, ili je u razumnoj mjeri vjerojatno da će im se takva šteta uzrokovati. Namjera da se promijeni ponašanje ne može se pretpostaviti ako je narušavanje posljedica čimbenika izvan UI sustava koji su izvan kontrole dobavljača ili korisnika, odnosno čimbenika koje dobavljač ili korisnik UI sustava ne mogu u razumnoj mjeri predvidjeti i ublažiti. U svakom slučaju nije nužno da dobavljač ili korisnik ima namjeru nanijeti tjelesnu ili psihološku štetu, pod uvjetom da takva šteta proizlazi iz manipulativnih ili izrabljivačkih praksi koje su omogućene umjetnom inteligencijom. Zabrane takvih praksi umjetne inteligencije komplementarne su odredbama Direktive 2005/29/EZ, osobito u pogledu toga da su nepoštene poslovne prakse koje dovode do gospodarske ili financijske štete potrošačima zabranjene u svim okolnostima, bez obzira na to izvode li se putem UI sustavâ ili na drugi način. Zabrane manipulativnih i izrabljivačkih praksi iz ove Uredbe ne bi trebale utjecati na zakonite prakse u kontekstu liječenja, kao što je psihološko liječenje mentalnih bolesti ili fizička rehabilitacija, ako se te prakse provode u skladu s primjenjivim medicinskim standardima i zakonodavstvom. Osim toga, uobičajene i zakonite poslovne prakse koje su usklađene s primjenjivim pravom ne bi same po sebi trebalo smatrati štetnim manipulativnim praksama u području umjetne inteligencije.

(17) UI sustavi koji omogućuju društveno vrednovanje pojedinaca koje provode tijela javne vlasti ili privatni akteri 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 pojedince na temelju njihova društvenog ponašanja u različitim kontekstima ili na temelju 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 UI sustave koji uključuju takve neprihvatljive prakse vrednovanja trebalo zabraniti. Ta zabrana ne bi trebala utjecati na zakonite prakse evaluacije pojedinaca koje se provode u jednu ili više posebnih svrha u skladu sa zakonom.

(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 iscrpno navedenim 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 terorističke napade i otkrivanje, lociranje, identifikaciju ili progon počinitelja kaznenih djela ili osumnjičenika za kaznena djela iz Okvirne odluke Vijeća 2002/584/PUP[9] ako su ta kaznena djela u dotičnoj državi članici kažnjiva kaznom zatvora ili oduzimanjem slobode u najduljem trajanju od najmanje tri godine i definirana su u pravu te države članice. Takvim pragom za kaznu zatvora ili oduzimanje slobode u skladu s nacionalnim pravom pomaže se osigurati da ta djela budu dovoljno teška da se potencijalno 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 relevantnija od drugih, u smislu 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 i s obzirom na vjerojatne razlike u težini, vjerojatnosti i razmjeru štete ili mogućih negativnih posljedica. Osim toga, ovom bi se Uredbom trebala očuvati sposobnost tijela kaznenog progona, tijela nadležnih za nadzor granica, tijela nadležnih za imigraciju ili tijela nadležnih za azil da provode provjere identiteta u prisutnosti dotične osobe, u skladu s uvjetima utvrđenima za takve provjere u pravu Unije i nacionalnom pravu. Konkretno, tijela kaznenog progona, tijela nadležna za nadzor granica, tijela nadležna za imigraciju ili tijela nadležna za azil trebala bi se moći koristiti informacijskim sustavima, u skladu s pravom Unije ili nacionalnim pravom, za identifikaciju osobe koja se tijekom provjere identiteta odbija identificirati ili nije sposobna navesti ili dokazati svoj identitet, a da se od njih ovom Uredbom ne zahtijeva pribavljanje prethodnog odobrena. To bi, na primjer, mogla biti osoba uključena u kazneno djelo, koja nije spremna ili zbog nesreće ili zdravstvenog stanja nije sposobna otkriti svoj identitet tijelima kaznenog progona.

[9] 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.).

(20) Kako bi se osigurala odgovorna i proporcionalna uporaba tih sustava, važno je i utvrditi da bi u svakoj od tih iscrpno navedenih i usko definiranih situacija trebalo uzeti u obzir određene elemente, osobito u pogledu prirode situacije zbog koje se zahtijeva njihova uporaba i posljedica te uporabe za prava i slobode svih uključenih osoba te u pogledu zaštitnih mjera i uvjeta propisanih 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 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 sustava u cilju identifikacije osobe ili osoba. Trebalo bi dopustiti odstupanja od tog pravila 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 podlijegati 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 podrobnim 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 iz 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 podlijegati zahtjevu za odobrenje u skladu s ovom Uredbom te važećim podrobnim 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 u svrhu kaznenog progona kako je uređeno ovom Uredbom, i dalje bi trebala ispunjavati sve zahtjeve koji proizlaze iz članka 10. Direktive (EU) 2016/680. Za svrhe koje nisu kazneni progon, člankom 9. stavkom 1. Uredbe (EU) 2016/679 i člankom 10. stavkom 1. Uredbe (EU) 2018/1725 zabranjuje se obrada biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, osim ako se primjenjuje jedna od situacija iz drugog stavka navedenih dvaju članaka.

(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., 3. i 4. 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., 3. i 4. 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.

(27) UFEU-a. 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 Vijeća[10], Uredbe (EU) br. 167/2013 Europskog parlamenta i Vijeća[11], Uredbe (EU) br. 168/2013 Europskog parlamenta i Vijeća[12], Direktive 2014/90/EU Europskog parlamenta i Vijeća[13], Direktive (EU) 2016/797 Europskog parlamenta i Vijeća[14], Uredbe (EU) 2018/858 Europskog parlamenta i Vijeća[15], Uredbe (EU) 2018/1139 Europskog parlamenta i Vijeća[16] i Uredbe (EU) 2019/2144 Europskog parlamenta i Vijeća[17], primjereno je 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.

---

10 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.).

11 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.).

12 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.).

13 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.).

14 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.).

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

16 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.).

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

(30) Kad je riječ o UI sustavima koji su sigurnosni sastavni dijelovi proizvodâ 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 Vijeća[18] i Uredbu (EU) 2017/746 Europskog parlamenta i Vijeća[19] ako ocjenjivanje sukladnosti srednjorizičnih i visokorizičnih proizvoda provodi treća strana.

[18] 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.)

[19] 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.).

(32) Kad je riječ o 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. Važno je i pojasniti da u visokorizičnim scenarijima iz Priloga III. mogu postojati sustavi koji ne dovode do znatnog rizika za pravne interese zaštićene u tim scenarijima, uzimajući u obzir izlazne rezultate UI sustava. Stoga bi se UI sustav trebao smatrati visokorizičnim samo ako je izlazni rezultat koji proizvodi toliko važan (tj. nije isključivo pomoćni) za relevantnu radnju ili odluku da dovodi do znatnog rizika za zaštićene pravne interese. Na primjer, ako se informacije koje UI sustavi pružaju čovjeku sastoje od izrade profila pojedinaca u smislu članka 4. stavka 4. Uredbe (EU) 2016/679, članka 3. stavka 4. Direktive (EU) 2016/680 i članka 3. stavka 5. Uredbe (EU) 2018/1725, takve informacije obično ne bi trebalo smatrati dodatnima u kontekstu visokorizičnih UI sustava iz Priloga III. Međutim, ako izlazni rezultat UI sustava ima tek zanemarivu ili malu važnost za ljudsko djelovanje ili odlučivanje, može se smatrati isključivo dodatnim, što, na primjer, uključuje UI sustave koji se upotrebljavaju za prevođenje u informativne svrhe ili za upravljanje dokumentima.

(33) Tehničke netočnosti UI sustava namijenjenih daljinskoj biometrijskoj identifikaciji pojedinaca mogu prouzročiti pristrane rezultate i imati diskriminacijske učinke. To je osobito relevantno kad je riječ o dobi, etničkom podrijetlu, rasi, 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 infrastrukturom i njezinu radu, primjereno je kao visokorizične klasificirati one UI sustave koji su namijenjeni uporabi kao sigurnosni sastavni dijelovi u upravljanju kritičnom digitalnom infrastrukturom navedenom u Prilogu I. točki 8. Direktive o otpornosti kritičnih subjekata i radu takve infrastrukture, u cestovnom prometu i upravljanju njime te u opskrbi vodom, plinom, grijanjem i električnom energijom jer bi njihov kvar ili neispravnost mogli ugroziti život i zdravlje osoba u velikim razmjerima te znatno poremetiti uobičajeno odvijanje društvenih i gospodarskih aktivnosti. Sigurnosni sastavni dijelovi kritične infrastrukture, uključujući kritičnu digitalnu infrastrukturu, sustavi su koji se upotrebljavaju za izravnu zaštitu fizičkog integriteta kritične infrastrukture ili zdravlja i sigurnosti osoba i imovine, ali koji nisu neophodni za funkcioniranje sustava. Kvar ili neispravnost takvih sastavnih dijelova može izravno dovesti do rizika za fizički integritet kritične infrastrukture, a time i do rizika za zdravlje i sigurnost osoba i imovine. Sastavne dijelove namijenjene isključivo uporabi u kibersigurnosne svrhe ne bi trebalo smatrati sigurnosnim komponentama. Primjeri sigurnosnih sastavnih dijelova takve kritične infrastrukture mogu uključivati sustave za praćenje tlaka vode ili sustave za kontrolu protupožarnog alarma u centrima za računalstvo u oblaku.

(35) UI sustave koji se upotrebljavaju u obrazovanju ili strukovnom osposobljavanju, posebno za razvrstavanje osoba u ustanove za obrazovanje i strukovno osposobljavanje, za upis u te ustanove ili za određivanje pristupa tim ustanovama ili programima na svim razinama, ili pak za vrednovanje ishoda učenja osoba treba 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 sustave 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 dodjelu zadataka na temelju ponašanja pojedinca ili osobnih značajki odnosno karakteristika i za praćenje ili evaluaciju osoba u radnim ugovornim odnosima također bi trebalo klasificirati kao visokorizične 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 dobnih 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 korištenje je i dostupnost određenih osnovnih privatnih i javnih usluga i naknada potrebnih 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 za vlastite potrebe stavljaju mikropoduzeća ili mala poduzeća, kako su definirana u Prilogu Preporuci Komisije 2003/361/EZ. Pojedinci koji tijelima javne vlasti podnose zahtjev za naknade i usluge osnovne 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, uključujući određivanje imaju li korisnici legitimno pravo na takve naknade ili usluge, ti sustavi mogu znatno utjecati na životne uvjete tih osoba i mogu kršiti njihova temeljna prava, kao što je 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. UI sustavi sve se više upotrebljavaju i za procjenu rizika u vezi s pojedincima i određivanje cijena u slučaju životnog i zdravstvenog osiguranja, a to, ako nisu propisno projektirani i razvijeni i ako se ne upotrebljavaju propisno, može dovesti do ozbiljnih posljedica za život i zdravlje ljudi, uključujući financijsku isključenost i diskriminaciju. Kako bi se osigurao dosljedan pristup u sektoru financijskih usluga, navedena iznimka za mikropoduzeća ili mala poduzeća u vezi s uporabom za vlastite potrebe trebala bi se primjenjivati u mjeri u kojoj ona sama pružaju i stavljaju u uporabu UI sustav u svrhu prodaje vlastitih proizvoda osiguranja.

(38) Postupcima tijelâ kaznenog progona koji uključuju određene uporabe UI sustavâ 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 treniran 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 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. UI sustave posebno namijenjene za upravne postupke poreznih i carinskih tijela i financijsko-obavještajnih jedinica koje provode administrativne zadaće analize informacija na temelju zakonodavstva Unije o sprečavanju pranja novca ne bi trebalo 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 koji su namijenjeni tijelima javne vlasti nadležnima za zadaće u području upravljanja migracijama, azilom i nadzorom granica, 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 pomaganje nadležnim tijelima javne vlasti pri razmatranju zahtjeva za azil, vize i boravišne dozvole i s time 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 Vijeća[20], Uredbom (EZ) br. 810/2009 Europskog parlamenta i Vijeća[21] i drugim relevantnim propisima.

[20] 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.).

[21] 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.).

(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 tumačenju činjenica i prava i 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 ili administrativne zadaće.

(41) Činjenicu da je UI sustav klasificiran kao visokorizičan na temelju ove Uredbe ne bi trebalo tumačiti kao indikator da je uporaba sustava 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, osim ako je u ovoj Uredbi izričito navedeno drugačije.

(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, trebali bi se primjenjivati određeni obvezni zahtjevi s obzirom na namjenu sustava i sustav upravljanja rizikom koji uspostavlja dobavljač. Sustav upravljanja rizicima osobito bi se trebao sastojati od kontinuiranog iterativnog procesa koji se planira i izvodi tijekom cijelog životnog vijeka visokorizičnog UI sustava. Tim bi se postupkom trebalo osigurati da dobavljač utvrdi i analizira rizike za zdravlje, sigurnost i temeljna prava osoba na koje bi sustav mogao utjecati s obzirom na njegovu namjenu, uključujući moguće rizike koji proizlaze iz interakcije UI sustava i okruženja u kojem on radi, i da se u skladu s time donesu odgovarajuće mjere upravljanja rizikom s obzirom na najnovija dostignuća.

(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 kibersigurnosti. 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 treniranjem 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 treniranje, validaciju i testiranje potrebna je primjena odgovarajuće prakse upravljanja podacima. Skupovi podataka za treniranje, validaciju i testiranje trebali bi biti dovoljno relevantni, reprezentativni i imati odgovarajuća statistička obilježja, među ostalim u odnosu na osobe ili skupine osoba za koje se visokorizični UI sustav namjerava upotrebljavati. Ti skupovi podataka trebali bi biti u najvećoj mogućoj mjeri bez pogrešaka i potpuni s obzirom na namjenu UI sustava, uzimajući u obzir, na razmjeran način, tehničku izvedivost i najnovija dostignuća, dostupnost podataka i provedbu primjerenih mjera upravljanja rizikom kako bi se na odgovarajući način uklonili mogući nedostaci skupova podataka. Zahtjev da skupovi podataka budu potpuni i bez pogrešaka ne bi trebao utjecati na primjenu tehnika zaštite privatnosti u kontekstu razvoja i testiranja UI sustavâ. U skupovima podataka za treniranje, validaciju i testiranje trebalo uzeti u obzir, u mjeri u kojoj to iziskuju njihova namjena, obilježja, karakteristike ili elementi specifični 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 također trebali moći obrađivati posebne kategorije osobnih podataka, kao pitanje od značajnog javnog interesa u smislu članka 9. stavka 2. točke (g) Uredbe (EU) 2016/679 i članka 10. stavka 2. točke (g) Uredbe (EU) 2018/1725, kako bi se osiguralo praćenje, otkrivanje i ispravljanje pristranosti povezanih s visokorizičnim UI sustavima.

(44a) Pri primjeni načelâ iz članka 5. stavka 1. točke (c) Uredbe 2016/679 i članka 4. stavka 1. točke (c) Uredbe 2018/1725, osobito načela smanjenja količine podataka, u pogledu skupova podataka za treniranje, validaciju i testiranje iz ove Uredbe trebalo bi uzeti u obzir cijeli životni ciklus UI sustava.

(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 treniranje, validaciju i testiranje UI sustavâ. Na primjer, u području zdravstva zajednički europski prostor za zdravstvene podatke olakšat će nediskriminirajući pristup zdravstvenim podacima i treniranje algoritama umjetne inteligencije 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 treniranje, 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 treniranja, testiranja i validacije koji su primijenjeni, kao i dokumentaciju o relevantnom sustavu upravljanja rizikom. Tehnička dokumentacija trebala bi se redovito ažurirati. Nadalje, dobavljači ili korisnici trebali bi čuvati dnevnike događaja koje automatski generira visokorizični UI sustav, uključujući, na primjer, izlazne podatke, datum i vrijeme početka itd., u mjeri u kojoj su takav sustav i s njime povezani dnevnici događaja pod njihovom kontrolom, tijekom razdoblja koje je primjereno kako bi im se omogućilo da ispune svoje obveze.

(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 i uključivati sažete i jasne informacije, među ostalim, prema potrebi, o mogućim rizicima povezanim s temeljnim pravima i diskriminacijom osoba na koje bi sustav mogao utjecati s obzirom na njegovu namjenu. Kako bi se korisnicima olakšalo razumijevanje uputa za uporabu, one bi prema potrebi trebale sadržavati ilustrativne primjere.

(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. S obzirom na važne posljedice za osobe ako u određenim sustavima za biometrijsku identifikaciju dođe do netočnih rezultata, primjereno je za takve sustave predvidjeti zahtjev za pojačanim ljudskim nadzorom tako da korisnik ne može poduzeti nikakve radnje ili odluke na temelju identifikacije proizišle iz sustava ako je nisu zasebno provjerile i potvrdile najmanje dvije fizičke osobe. Te osobe mogu biti iz jednog ili više subjekata i mogu uključivati osobu koja upravlja sustavom ili ga upotrebljava. Taj zahtjev ne bi trebao predstavljati nepotrebno opterećenje ili uzrokovati kašnjenja i moglo bi biti dovoljno da se zasebne provjere koje provode različite osobe automatski evidentiraju u dnevnicima događaja koje generira sustav.

(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 u odnosu na štetno ili na drugi način nepoželjno ponašanje koje bi moglo proizići iz ograničenjâ unutar sustava ili okruženja u kojem sustavi rade (npr. pogreške, pogreške, nedosljednosti, neočekivane situacije). Visokorizične UI sustave trebalo bi stoga projektirati i razvijati s pomoću odgovarajućih tehničkih rješenja kako bi se štetno ili na drugi način neželjeno ponašanje spriječilo ili svelo na najmanju moguću mjeru, kao što su, na primjer, mehanizmi kojima se sustavu omogućuje da sigurno prekine rad (zaštitni planovi) u prisutnosti određenih nepravilnosti ili kada se rad odvija izvan određenih unaprijed utvrđenih granica. 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 sustavâ 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 treniranje (npr. trovanje podataka) ili istrenirani 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 Vijeća[22] o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta, Odlukom br. 768/2008/EZ Europskog parlamenta i Vijeća[23] o zajedničkom okviru za stavljanje na tržište proizvoda i Uredbom (EU) 2019/1020 Europskog parlamenta i Vijeća[24] o nadzoru tržišta i sukladnosti proizvoda („novi zakonodavni okvir za stavljanje proizvoda na tržište").

(52a) U skladu s načelima novog zakonodavnog okvira trebalo bi utvrditi posebne obveze za relevantne operatere u lancu vrijednosti UI-ja kako bi se postigla pravna sigurnost i olakšalo usklađivanje s ovom Uredbom. U određenim situacijama ti bi operateri mogli istodobno djelovati u više uloga i stoga bi trebali kumulativno ispuniti sve relevantne obveze povezane s tim ulogama. Na primjer, operater bi mogao istodobno djelovati kao distributer i uvoznik.

(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.

---

22 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.).

23 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.).

24 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.).

(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 dotičnog tijela javne vlasti.

(54a) Kako bi se osigurala pravna sigurnost, potrebno je pojasniti da bi se pod određenim posebnim uvjetima svaka fizička ili pravna osoba trebala smatrati dobavljačem novog visokorizičnog UI sustava i stoga preuzeti sve odgovarajuće obveze. To bi, na primjer, vrijedilo ako ta osoba stavlja svoje ime ili žig na visokorizični UI sustav koji je već stavljen na tržište ili u uporabu ili ako ta osoba izmijeni namjenu UI sustava koji nije visokorizičan i koji je već stavljen na tržište ili u uporabu tako da izmijenjeni sustav postane visokorizični UI sustav. Te bi se odredbe trebale primjenjivati ne dovodeći u pitanje detaljnije odredbe utvrđene u određenom sektorskom zakonodavstvu novog zakonodavnog okvira s kojim bi se ova Uredba trebala zajednički primjenjivati. Na primjer, članak 16. stavak 2. Uredbe 745/2017, u kojem se navodi da određene promjene ne bi trebalo smatrati izmjenama proizvoda koje mogu utjecati na njegovu usklađenost s primjenjivim zahtjevima, trebao bi se i dalje primjenjivati na visokorizične UI sustave koji su medicinski proizvodi u smislu te uredbe.

(55) Ako se visokorizični UI sustav koji je sigurnosni sastavni dio proizvoda obuhvaćenog relevantnim sektorskim propisima novog zakonodavnog okvira ne stavlja na tržište ili u uporabu neovisno o proizvodu, proizvođač proizvoda kako je definiran relevantnim propisima iz 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.

(56a) Za dobavljače koji nemaju poslovni nastan u Uniji ovlašteni zastupnik ima ključnu ulogu u osiguravanju usklađenosti visokorizičnih UI sustava koje ti dobavljači stavljaju na tržište ili u uporabu u Uniji i služi kao njihova osoba za kontakt s poslovnim nastanom u Uniji. S obzirom na tu ključnu ulogu i kako bi se osiguralo preuzimanje odgovornosti za potrebe izvršenja ove Uredbe, primjereno je da ovlašteni zastupnik bude solidarno i pojedinačno odgovoran s dobavljačem za neispravne visokorizične UI sustave. Odgovornost ovlaštenog zastupnika predviđena ovom Uredbom ne dovodi u pitanje odredbe Direktive 85/374/EEZ o odgovornosti za neispravne proizvode.

(57) [izbrisano]

(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. Tim se obvezama ne bi trebale dovoditi u pitanje druge obveze korisnika povezane s visokorizičnim UI sustavima na temelju prava Unije ili nacionalnog prava i ne bi se trebale primjenjivati ako je riječ o uporabi tijekom osobne neprofesionalne aktivnosti.

(58a) Primjereno je pojasniti da ova Uredba ne utječe na obveze dobavljača i korisnika UI sustavâ u njihovoj ulozi voditelja obrade ili izvršitelja obrade podataka koje proizlaze iz prava Unije o zaštiti osobnih podataka u mjeri u kojoj projektiranje, razvoj ili uporaba UI sustava uključuje obradu osobnih podataka. Također je primjereno pojasniti da ispitanici i dalje uživaju sva prava i jamstva koja su im dodijeljena tim pravom Unije, uključujući prava povezana s isključivo automatiziranim pojedinačnim donošenjem odluka, uključujući izradu profila. Usklađena pravila za stavljanje na tržište, stavljanje u uporabu i uporabu UI sustava uspostavljena ovom Uredbom trebala bi olakšati učinkovitu provedbu i omogućiti ostvarivanje prava ispitanikâ i drugih pravnih lijekova zajamčenih pravom Unije o zaštiti osobnih podataka i drugih temeljnih prava.

(59) [izbrisano]

(60) [izbrisano]

(61) Normizacija bi trebala imati ključnu ulogu u pružanju tehničkih rješenja dobavljačima kako bi se osigurala usklađenost s ovom Uredbom, u skladu s najnovijim dostignućima. Sukladnost s usklađenim normama kako su definirane u Uredbi (EU) br. 1025/2012 Europskog parlamenta i Vijeća[25], za koje se obično očekuje da odražavaju najnovija dostignuća, trebala bi biti sredstvo kojim će dobavljači dokazivati sukladnost sa zahtjevima iz ove Uredbe. Međutim, u nedostatku relevantnih upućivanja na usklađene norme Komisija bi trebala moći provedbenim aktima utvrditi zajedničke specifikacije za određene zahtjeve na temelju ove Uredbe kao iznimno zamjensko rješenje za olakšavanje obveze dobavljača da ispuni zahtjeve iz ove Uredbe ako je postupak normizacije blokiran ili ako dođe do kašnjenja u uspostavi odgovarajuće usklađene norme. Ako je takvo kašnjenje posljedica tehničke složenosti dotične norme, Komisija bi to trebala razmotriti prije razmatranja utvrđivanja zajedničkih specifikacija. Primjereno sudjelovanje malih i srednjih poduzeća u izradi normi kojima se podupire provedba ove Uredbe ključno je za promicanje inovacija i konkurentnosti u području umjetne inteligencije u Uniji. Takvo sudjelovanje trebalo bi osigurati na odgovarajući način, u skladu s člancima 5. i 6. Uredbe 1025/2012.

[25] 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.).

(61a) Ne dovodeći u pitanje primjenu usklađenih normi i zajedničkih specifikacija, primjereno je da se na dobavljače primijeni pretpostavka sukladnosti s relevantnim zahtjevom u pogledu podataka ako je njihov visokorizični UI sustav treniran i testiran na podacima koji odražavaju specifično zemljopisno, bihevioralno ili radno okruženje u kojem se UI sustav namjerava upotrebljavati. Slično tome, u skladu s člankom 54. stavkom 3. Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća za visokorizične UI sustave koji su certificirani ili za koje je izdana izjava o sukladnosti u okviru programa kibersigurnosti na temelju te uredbe i na koje su objavljena upućivanja objavljena u *Službenom listu Europske unije* trebalo bi pretpostaviti da ispunjavaju kibersigurnosni zahtjev iz ove Uredbe. Time se ne dovodi u pitanje dobrovoljna priroda tog programa kibersigurnosti.

(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.

(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. Kad je riječ o visokorizičnim UI sustavima povezanima s proizvodima koji su obuhvaćeni uredbama 745/2017 i 746/2017 o medicinskim proizvodima, primjenjivošću zahtjevâ iz ove Uredbe ne bi se trebala dovoditi u pitanje i trebala bi se uzimati u obzir logika upravljanja rizikom i ocjenjivanje odnosa između koristi i rizika koje se provodi na temelju okvira za medicinske proizvode.

(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. Nacionalna nadležna tijela trebala bi Komisiji i drugim državama članicama slati obavijesti o tim imenovanjima elektroničkim načinom obavješćivanja koji je razvila i kojim upravlja Komisija u skladu s člankom R23. Odluke 768/2008.

(66) U skladu sa zajednički utvrđenim pojmom znatne izmjene za proizvode regulirane zakonodavstvom Unije o usklađivanju primjereno je da se svaki put kad dođe do promjene koja može utjecati na usklađenost visokorizičnog UI sustava s ovom Uredbom (npr. promjena operativnog sustava ili softverske arhitekture) ili kad se promijeni namjena sustava, taj UI sustav smatra novim UI sustavom koji bi trebao proći novo ocjenjivanje sukladnosti. Međutim, promjene algoritma i sposobnosti UI sustava koji nakon stavljanja na tržište ili u uporabu nastavljaju „učiti” (tj. automatski prilagođavati način izvršavanja funkcija) ne bi trebale predstavljati znatnu izmjenu, pod uvjetom da je te promjene unaprijed odredio dobavljač i da su ocijenjene u trenutku ocjenjivanja sukladnosti.

(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 povezanima 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 i 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 sebe i informacije o svojem visokorizičnom UI sustavu registriraju u bazi podataka EU-a, koju će uspostaviti i kojom će upravljati Komisija. Prije uporabe visokorizičnog UI sustava navedenog u Prilogu III. korisnici visokorizičnih UI sustava koji su tijela javne vlasti, javne agencije ili javna tijela, uz iznimku tijela kaznenog progona, tijela za nadzor granica, tijela za imigraciju ili tijela za azil, i tijela koja su korisnici visokorizičnih UI sustava u području kritične infrastrukture također se registriraju u takvoj bazi podataka i odabiru sustav koji namjeravaju upotrebljavati. Komisija bi trebala biti voditelj obrade za tu bazu podataka, u skladu s Uredbom (EU) 2018/1725 Europskog parlamenta i Vijeća[26]. 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.

[26] 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.).

(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 podlijegati posebnim obvezama u pogledu transparentnosti, ne dovodeći u pitanje zahtjeve i obveze za visokorizične UI sustave. Osobito bi pojedince trebalo obavijestiti o tome da su u interakciji s UI sustavom, osim ako je to očito sa stajališta razmjerno dobro informiranog, pronicljivog i opreznog pojedinca, uzimajući u obzir okolnosti i kontekst uporabe. Pri provedbi te obveze trebalo bi uzeti u obzir karakteristike pojedinaca koji pripadaju ranjivim skupinama zbog svoje dobi ili invaliditeta u mjeri u kojoj je UI sustav namijenjen interakciji s tim skupinama. Nadalje, pojedince bi trebalo obavijestiti kada su izloženi sustavima koji obradom njihovih biometrijskih podataka mogu identificirati emocije, izvoditi zaključke o njihovim emocijama ili namjerama ili te pojedince razvrstati u određene kategorije. Te se određene kategorije mogu odnositi na aspekte kao što su spol, dob, boja kose, boja očiju, tetovaže, osobne značajke, etničko podrijetlo, osobne preferencije i interesi ili na druge aspekte, kao što su spolna ili politička orijentacija. 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. Sukladnost s navedenim obvezama u pogledu informiranja ne bi se trebala tumačiti kao da upućuje na to da je uporaba sustava ili njegovih izlaznih rezultata zakonita na temelju ove Uredbe ili drugog prava Unije i države članice i njome se ne bi trebale dovoditi u pitanje druge obveze u pogledu transparentnosti za korisnike UI sustava utvrđene u pravu Unije ili nacionalnom pravu. Nadalje, ne bi se trebala tumačiti niti kao da upućuje na to da se uporabom sustava ili njegovih izlaznih rezultata ugrožava pravo na slobodu izražavanja i pravo na slobodu umjetnosti i znanosti zajamčene Poveljom EU-a o temeljnim pravima, posebno ako je sadržaj očito dio kreativnog, satiričkog, umjetničkog ili fiktivnog djela ili programa, podložno odgovarajućim zaštitnim mjerama za prava i slobode trećih strana.

(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 za umjetnu inteligenciju trebali bi biti poticanje inovacija u području umjetne inteligencije uspostavom kontroliranog okruženja za eksperimentiranje i testiranje u fazi razvoja i prije stavljanja na tržište 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 MSP-ove, uključujući *start-up* poduzeća. Sudjelovanje u regulatornom izoliranom okruženju za umjetnu inteligenciju trebalo bi biti usmjereno na pitanja koja uzrokuju pravnu nesigurnost za dobavljače i potencijalne dobavljače u pogledu inovacija, eksperimentiranja s umjetnom inteligencijom u Uniji i trebalo bi doprinijeti regulatornom učenju utemeljenom na dokazima. Nadzor UI sustava u regulatornom izoliranom okruženju za umjetnu inteligenciju stoga bi trebao obuhvaćati njihov razvoj, treniranje, testiranje i validaciju prije stavljanja tih sustava na tržište ili u uporabu, kao i pojam i pojavu znatne izmjene koja bi mogla zahtijevati novi postupak ocjenjivanja sukladnosti. Nacionalna nadležna tijela koja uspostavljaju regulatorna izolirana okruženja za umjetnu inteligenciju trebala bi prema potrebi surađivati s drugim relevantnim tijelima, među ostalim s tijelima koja nadziru zaštitu temeljnih prava, i mogla bi omogućiti sudjelovanje drugih aktera iz ekosustava umjetne inteligencije, kao što su nacionalne ili europske organizacije za normizaciju, prijavljena tijela, objekti za testiranje i eksperimentiranje, laboratoriji za istraživanje i eksperimentiranje, inovacijski centri i relevantne organizacije dionika i civilnog društva. 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. Regulatornim izoliranim okruženjima za umjetnu inteligenciju uspostavljenima na temelju ove Uredbe ne bi se trebalo dovoditi u pitanje drugo zakonodavstvo kojim se omogućuje uspostava drugih izoliranih okruženja u cilju osiguravanja usklađenosti s drugim zakonodavstvom koje nije ova Uredba. Relevantna nadležna tijela zadužena za ta druga regulatorna izolirana okruženja trebala bi prema potrebi razmotriti prednosti uporabe tih izoliranih okruženja i za potrebe osiguravanja usklađenosti UI sustavâ s ovom Uredbom. Slijedom dogovora između nacionalnih nadležnih tijela i sudionika u regulatornom izoliranom okruženju za umjetnu inteligenciju testiranje u stvarnim uvjetima može se provoditi i nadzirati u okviru regulatornog izoliranog okruženja za umjetnu inteligenciju.

(-72a) Ovom bi se Uredbom sudionicima u regulatornom izoliranom okruženju za umjetnu inteligenciju trebala osigurati 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. i člankom 9. stavkom 2. točkom (g) Uredbe (EU) 2016/679 i člancima 5. i 10. Uredbe (EU) 2018/1725, ne dovodeći u pitanje članak 4. stavak 2. i članak 10. Direktive (EU) 2016/680. I dalje se primjenjuju sve druge obveze voditelja obrade podataka i prava ispitanika na temelju Uredbe (EU) 2016/679, Uredbe (EU) 2018/1725 i Direktive (EU) 2016/680. Ovom Uredbom osobito se ne bi trebala osigurati pravna osnova u smislu članka 22. stavka 2. točke (b) Uredbe (EU) 2016/679 i članka 24. stavka 2. točke (b) Uredbe (EU) 2018/1725. 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.

(72a) Kako bi se ubrzao proces razvoja i stavljanja na tržište visokorizičnih UI sustava navedenih u Prilogu III., važno je da se dobavljači ili potencijalni dobavljači takvih sustava mogu služiti posebnim režimom za testiranje tih sustava u stvarnim uvjetima, bez sudjelovanja u regulatornom izoliranom okruženju za umjetnu inteligenciju. Međutim, u takvim slučajevima, uzimajući u obzir moguće posljedice takvog testiranja na pojedince, trebalo bi osigurati da se ovom Uredbom uvedu odgovarajuća i dostatna jamstva i uvjeti za dobavljače ili potencijalne dobavljače. Takva bi jamstva među ostalim trebala uključivati traženje informiranog pristanka pojedinaca za sudjelovanje u testiranju u stvarnim uvjetima, uz iznimku tijela kaznenog progona u slučajevima u kojima bi traženje informiranog pristanka spriječilo testiranje UI sustava. Privola ispitanika za sudjelovanje u takvom testiranju na temelju ove Uredbe razlikuje se od privole ispitanika za obradu njihovih osobnih podataka na temelju relevantnog zakonodavstva o zaštiti podataka i njome se privola za obradu osobnih podataka ne dovodi u pitanje.

(73) Kako bi se promicale i štitile inovacije, posebno je važno uzeti u obzir interese malih i srednjih poduzeća dobavljača i malih i srednjih poduzeća 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 pri utvrđivanju naknada za ocjenjivanje sukladnosti uzeti u obzir posebne interese i potrebe malih i srednjih poduzeća dobavljača. 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.

(73a) Kako bi se promicale i zaštitile inovacije, ostvarivanju ciljeva ove Uredbe trebalo bi doprinositi putem platforme za umjetnu inteligenciju na zahtjev i svim relevantnim programima i projektima za financiranje sredstvima EU-a, poput programa Digitalna Europa i Obzor Europa, koje provode Komisija i države članice na nacionalnoj razini ili razini EU-a.

(74) Konkretno, kako bi se rizici za provedbu koji proizlaze iz nedostatka znanja i iskustva na tržištu sveli na najmanju moguću mjeru i kako bi se dobavljačima, posebno MSP-ovima, i prijavljenim tijelima olakšalo ispunjavanje obveza iz ove Uredbe, provedbi ove Uredbe trebalo bi eventualno doprinositi putem platforme za umjetnu inteligenciju na zahtjev, europskih centara za digitalne inovacije te centara za testiranje i eksperimentiranje koje uspostavljaju Komisija i države članice na nacionalnoj razini ili razini EU-a. U okviru svojih misija i područja kompetentnosti ponajprije mogu pružati tehničku i znanstvenu potporu dobavljačima i prijavljenim tijelima.

(74a) Nadalje, kako bi se s obzirom na vrlo malenu veličinu nekih operatera osigurala proporcionalnost u pogledu troškova inovacija, primjereno je izuzeti mikropoduzeća od najskupljih obveza, kao što je uspostava sustava upravljanja kvalitetom, čime bi se smanjili administrativno opterećenje i troškovi za ta poduzeća, a bez utjecanja na razinu zaštite i potrebu za usklađivanjem sa zahtjevima za visokorizične UI sustave.

(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 akreditiranima 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. U Odboru bi se trebali odražavati različiti interesi ekosustava umjetne inteligencije, a trebao bi biti sastavljen od predstavnika država članica. Kako bi se osiguralo sudjelovanje relevantnih dionika, trebalo bi osnovati stalnu podskupinu Odbora. Odbor bi trebao biti odgovoran za niz savjetodavnih zadaća, uključujući davanje mišljenja, preporuka i savjeta ili doprinošenje smjernicama o pitanjima povezanima s provedbom ove Uredbe, među ostalim pitanjima izvršenja, tehničkim specifikacijama ili postojećim normama povezanima sa zahtjevima iz ove Uredbe, te za davanje savjeta Komisiji i državama članicama te njihovim nacionalnim nadležnim tijelima u vezi sa specifičnim pitanjima povezanima s umjetnom inteligencijom. Kako bi se državama članicama pružila određena fleksibilnost u vezi s imenovanjem njihovih predstavnika u Odbor za umjetnu inteligenciju, ti predstavnici mogu biti sve osobe koje pripadaju javnim subjektima i trebale bi imati odgovarajuće nadležnosti i ovlasti za olakšavanje koordinacije na nacionalnoj razini i doprinošenje ostvarivanju zadaća Odbora. Odbor bi trebao uspostaviti dvije stalne podskupine kako bi osigurao platformu za suradnju i razmjenu između tijelâ za nadzor tržišta i tijela koja provode prijavljivanje o pitanjima koja se odnose na nadzor tržišta odnosno na prijavljena tijela. Stalna podskupina za nadzor tržišta trebala bi djelovati kao skupina za administrativnu suradnju (ADCO) za ovu Uredbu u smislu članka 30. Uredbe (EU) 2019/1020. U skladu s ulogom i zadaćama Komisije na temelju članka 33. Uredbe (EU) 2019/1020 Komisija bi trebala podupirati aktivnosti stalne podskupine za nadzor tržišta provođenjem evaluacija ili studija tržišta, osobito u cilju utvrđivanja aspekata ove Uredbe koji zahtijevaju posebnu i hitnu koordinaciju među tijelima za nadzor tržišta. Odbor prema potrebi može osnovati druge stalne ili privremene podskupine za razmatranje konkretnih pitanja. Odbor bi također prema potrebi trebao surađivati s relevantnim tijelima EU-a i stručnim skupinama i mrežama EU-a koje djeluju u kontekstu relevantnog zakonodavstva EU-a, uključujući posebno one koje djeluju na temelju relevantnih propisa EU-a o podacima, digitalnim proizvodima i uslugama.

(76a) Komisija bi trebala aktivno podupirati države članice i operatere u provedbi i izvršenju ove Uredbe. U tom bi pogledu Komisija trebala izraditi smjernice o posebnim temama s ciljem olakšavanja primjene ove Uredbe, posvećujući posebnu pozornost potrebama MSP-ova i *start-up* poduzeća u sektorima za koje je vjerojatnost da će biti pogođeni najveća. Kako bi se poduprlo odgovarajuće izvršavanje i kapaciteti država članica, trebalo bi uspostaviti objekte Unije za testiranje umjetne inteligencije i skupinu odgovarajućih stručnjaka i staviti ih na raspolaganje državama članicama.

(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. Države članice mogu odlučiti imenovati bilo koju vrstu javnog subjekta za obavljanje zadaća nacionalnih nadležnih tijela u smislu ove Uredbe, u skladu sa svojim posebnim nacionalnim organizacijskim značajkama i potrebama.

(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 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. Tijela za nadzor tržišta imenovana na temelju ove Uredbe trebala bi imati sve izvršne ovlasti na temelju ove Uredbe i Uredbe (EU) 2019/1020 i svoje bi ovlasti i dužnosti trebala izvršavati neovisno, nepristrano i bez predrasuda. Iako većina UI sustava ne podliježe posebnim zahtjevima i obvezama na temelju ove Uredbe, tijela za nadzor tržišta mogu poduzeti mjere u vezi sa svim UI sustavima kada oni predstavljaju rizik u skladu s ovom Uredbom. Zbog specifične prirode institucija, agencija i tijela Unije obuhvaćenih područjem primjene ove Uredbe primjereno je za njih imenovati Europskog nadzornika za zaštitu podataka tijelom nadležnim za nadzor tržišta. Time se ne bi trebalo dovoditi u pitanje imenovanje nacionalnih nadležnih tijela koje izvršavaju države članice. Aktivnosti nadzora tržišta ne bi trebale utjecati na sposobnost nadziranih subjekata da neovisno obavljaju svoje zadaće kada se takva neovisnost zahtijeva pravom Unije.

(79a) Ovom se Uredbom ne dovode u pitanje nadležnosti, zadaće, ovlasti i neovisnost relevantnih nacionalnih tijela javne vlasti ili javnopravnih tijela koja nadziru primjenu prava Unije o zaštiti temeljnih prava, uključujući tijela za ravnopravnost i tijela za zaštitu podataka. Ako je to potrebno za njihov mandat, ta nacionalna tijela javne vlasti ili javnopravna tijela trebala bi također imati pristup svoj dokumentaciji izrađenoj na temelju ove Uredbe. Trebalo bi utvrditi poseban zaštitni postupak kako bi se osigurala odgovarajuće i pravodobno izvršenje u pogledu UI sustava koji predstavljaju rizik za zdravlje, sigurnost i temeljna prava. Postupak za takve UI sustave koji predstavljaju rizik trebao bi se primjenjivati na visokorizične UI sustave koji predstavljaju rizik, zabranjene sustave koji su stavljeni na tržište, stavljeni u uporabu ili se upotrebljavaju protivno odredbama o zabranjenim praksama iz ove Uredbe i na UI sustave koji su stavljeni na raspolaganje protivno odredbama o zahtjevima u pogledu transparentnosti iz ove Uredbe i koji predstavljaju rizik.

(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 izvršenje obveza iz ove Uredbe te relevantnih pravila i zahtjeva iz zakonodavstva Unije o financijskim uslugama, tijela odgovorna za nadzor i izvršavanje zakonodavstva o financijskim uslugama 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, osim ako države članice odluče za obavljanje tih zadaća nadzora tržišta imenovati drugo tijelo. Ta bi nadležna tijela trebala imati sve ovlasti na temelju ove Uredbe i Uredbe (EU) 2019/1020 o nadzoru tržišta za izvršenje zahtjeva i obveza iz ove Uredbe, uključujući ovlasti za provođenje *ex post* aktivnosti nadzora tržišta koje se prema potrebi mogu integrirati u njihove postojeće nadzorne mehanizme i postupke na temelju relevantnog zakonodavstva Unije o financijskim uslugama. Primjereno je predvidjeti da, kada djeluju kao tijela za nadzor tržišta na temelju ove Uredbe, nacionalna tijela odgovorna za nadziranje kreditnih institucija reguliranih Direktivom 2013/36/EU, koja sudjeluju u jedinstvenom nadzornom mehanizmu (SSM) uspostavljenom Uredbom Vijeća br. 1024/2013, trebala bi bez odgode izvijestiti Europsku središnju banku o svim informacijama utvrđenima tijekom njihovih aktivnosti nadzora tržišta koje bi mogle biti od interesa za zadaće bonitetnog nadzora Europske središnje banke navedene u toj uredbi. 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 Vijeća[27], primjereno je i integrirati neke od postupovnih obveza dobavljača povezanih s upravljanjem rizikom, praćenjem nakon stavljanja na tržište i vođenjem dokumentacije u postojeće obveze i postupke na temelju Direktive 2013/36/EU. Kako bi se izbjegla preklapanja, trebalo bi predvidjeti i ograničena odstupanja u pogledu 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. Taj bi se režim trebao primjenjivati na društva za osiguranje i reosiguranje i osigurateljne holdinge u skladu s Direktivom 2009/138/EU (Solventnost II) i posrednike u osiguranju u skladu s Direktivom (EU) 2016/97 te na druge vrste financijskih institucija koje podliježu zahtjevima u pogledu unutarnjeg upravljanja,

[27] 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.).

aranžmana ili postupaka uspostavljenih na temelju relevantnog zakonodavstva Unije o financijskim uslugama kako bi se osigurala dosljednost i jednako postupanje u financijskom sektoru.

(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 zahtjeva za visokorizične UI sustave, prilagođene s obzirom na namjenu tih sustava i niži povezani rizik. 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 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 doprinijelo tom cilju, Direktiva 2001/95/EZ Europskog parlamenta i Vijeća[28] 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, u skladu s pravom Unije ili nacionalnim pravom,

---

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

(84) Države članice trebale bi poduzeti sve mjere potrebne za osiguravanje provedbe odredaba ove Uredbe, među ostalim određivanjem učinkovitih, proporcionalnih i odvraćajućih sankcija za povrede tih odredaba, i u pogledu načela *ne bis in idem*. 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 kada je to potrebno, Komisiji bi trebalo delegirati ovlast za donošenje akata u skladu s člankom 290. UFEU-a radi izmjene 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 tijekom svojeg pripremnog rada provede odgovarajuća savjetovanja, uključujući ona na razini stručnjaka, te da se ta savjetovanja provedu u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.[29] 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. Takva savjetovanja i savjetodavna potpora trebali bi se provoditi i u okviru aktivnosti Odbora za umjetnu inteligenciju i njegovih podskupina.

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

(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 Vijeća[30]. Posebno je važno da, u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016., kad god je u ranoj pripremi nacrta provedbenih akata potrebno šire stručno znanje, Komisija upotrebljava stručne skupine, savjetuje se s ciljanim dionicima ili provodi javna savjetovanja, prema potrebi. Takva savjetovanja i savjetodavna potpora trebali bi se provoditi i u okviru aktivnosti Odbora za umjetnu inteligenciju i njegovih podskupina, među ostalim u okviru pripreme provedbenih akata u pogledu članaka 4., 4.b i 6.

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

(87a) Kako bi se osigurala pravna sigurnost, osiguralo odgovarajuće razdoblje prilagodbe za operatere i izbjegli poremećaji na tržištu, među ostalim osiguravanjem kontinuiteta uporabe UI sustavâ, primjereno je da se ova Uredba primjenjuje na visokorizične UI sustave koji su stavljeni na tržište ili u uporabu prije općeg datuma njezine primjene samo ako od tog datuma u tim sustavima dođe do znatnih promjena u pogledu projektiranja ili namjene. Primjereno je pojasniti da bi u tom pogledu pojam znatne promjene trebalo tumačiti kao sadržajno istovjetan pojmu znatne izmjene, koji se upotrebljava samo u pogledu visokorizičnih UI sustava kako su definirani u ovoj Uredbi.

[30] 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.).

(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 određene UI sustave;

(d) pravila o praćenju tržišta, nadzoru tržišta i upravljanju;

(e) mjere za potporu inovacijama.

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 nalaze li se ti dobavljači fizički ili imaju li poslovni nastan u Uniji ili u trećoj zemlji;

(b) korisnike UI sustava koji se fizički nalaze ili imaju poslovni nastan u Uniji;

(c) dobavljače i korisnike UI sustava koji se fizički nalaze ili imaju poslovni nastan u trećoj zemlji ako se izlazni rezultati sustava upotrebljavaju u Uniji;

(d) uvoznike i distributere UI sustava;

(e) proizvođače proizvoda koji stavljaju na tržište ili u uporabu UI sustav zajedno sa svojim proizvodom i pod vlastitim imenom ili žigom;

(f) ovlaštene predstavnike dobavljača s poslovnim nastanom u Uniji.

2. Na UI sustave klasificirane kao visokorizične u skladu s člankom 6. stavcima 1. i 2. u odnosu na proizvode obuhvaćene zakonodavstvom Unije o usklađivanju iz Priloga II. odjeljka B primjenjuje se samo članak 84. ove Uredbe. Članak 53. primjenjuje se samo u mjeri u kojoj su zahtjevi za visokorizične UI sustave iz ove Uredbe uključeni u to zakonodavstvo Unije o usklađivanju.

3. Ova se Uredba ne primjenjuje na UI sustave ako i u mjeri u kojoj se stavljaju na tržište, stavljaju u uporabu ili upotrebljavaju s izmjenom ili bez izmjena tih sustava za potrebe aktivnosti koje nisu obuhvaćene područjem primjene prava Unije, a u svakom slučaju ni na aktivnosti povezane s vojskom, obranom ili nacionalnom sigurnošću, bez obzira na vrstu subjekta koji obavlja te aktivnosti.

   Osim toga, ova se Uredba ne primjenjuje na UI sustave koji se ne stavljaju na tržište ni u uporabu u Uniji ako se izlazni rezultati upotrebljavaju u Uniji za potrebe aktivnosti koje nisu obuhvaćene područjem primjene prava Unije, a u svakom slučaju ni na aktivnosti povezane s vojskom, obranom ili nacionalnom sigurnošću, bez obzira na vrstu subjekta koji obavlja te aktivnosti.

4. Ova se Uredba ne primjenjuje na tijela javne vlasti u trećoj zemlji ni na međunarodne organizacije obuhvaćene područjem primjene ove Uredbe na temelju stavka 1. ako ta tijela ili 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 Vijeća[31] [*kako će biti zamijenjena odgovarajućim odredbama Akta o digitalnim uslugama*].

6. Ova Uredba ne primjenjuje se na UI sustave, uključujući njihove izlazne rezultate, koji su posebno razvijeni i stavljeni u uporabu isključivo u svrhu znanstvenih istraživanja i razvoja.

7. Ova se Uredba ne primjenjuje na aktivnosti istraživanja i razvoja u vezi s UI sustavima.

8. Ova se Uredba ne primjenjuje na obveze korisnika koji su fizičke osobe koje upotrebljavaju UI sustave tijekom isključivo osobne neprofesionalne aktivnosti, osim članka 52.

---

[31] 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.)

Članak 3.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

(1) „sustav umjetne inteligencije” (UI sustav) znači sustav koji je projektiran za rad s elementima autonomije i koji na temelju podataka i ulaznih podataka koje je generirao stroj ili čovjek izvodi zaključke o tome kako postići zadani skup ciljeva primjenom strojnog učenja i/ili pristupa koji se temelje na logici i pristupa koji se temelje na znanju i proizvodi izlazne rezultate koje je generirao sustav, kao što su sadržaj (generativni UI sustavi), predviđanja, preporuke ili odluke, koji utječu na okolinu s kojom je UI sustav u interakciji;

(1a) „životni ciklus UI sustava” znači trajanje UI sustava, od projektiranja do umirovljenja. Ne dovodeći u pitanje ovlasti tijelâ za nadzor tržišta, takvo umirovljenje može se dogoditi u bilo kojem trenutku tijekom faze praćenja nakon stavljanja na tržište slijedom odluke dobavljača i podrazumijeva da se sustav ne smije dalje upotrebljavati. Životni ciklus UI sustava završava i znatnom izmjenom UI sustava koju izvrši dobavljač ili bilo koja druga fizička ili pravna osoba, a u tom se slučaju znatno izmijenjeni UI sustav smatra novim UI sustavom.

(1b) „UI sustav opće namjene” znači UI sustav koji je, neovisno o načinu na koji je stavljen na tržište ili u uporabu, među ostalim kao softver otvorenog koda, dobavljač namijenio obavljanju općih primjenjivih funkcija kao što su prepoznavanje slike i govora, generiranje audiosadržaja i videosadržaja, otkrivanje uzoraka, odgovaranje na pitanja, prevođenje i drugo; UI sustav opće namjene može se upotrebljavati u različitim kontekstima i može se integrirati u različite druge UI sustave;

(2) „dobavljač” znači fizička ili pravna osoba, tijelo javne vlasti, javna agencija ili drugo javno tijelo koje razvija UI sustav ili ima UI sustav razvijen i stavlja ga na tržište ili u uporabu pod vlastitim imenom ili žigom, uz plaćanje ili besplatno;

(3) [izbrisano];

(3a) „mala i srednja poduzeća” (MSP-ovi) znači poduzeća kako su definirana u Prilogu Preporuci Komisije 2003/361/EZ o definiranju mikropoduzeća te malih i srednjih poduzeća;

(4) „korisnik” znači svaka fizička ili pravna osoba, uključujući tijelo javne vlasti, javnu agenciju ili drugo javno tijelo u okviru čije se nadležnosti sustav upotrebljava;

(5) „ovlašteni zastupnik” znači svaka fizička ili pravna osoba koja se fizički nalazi ili ima poslovni nastan u Uniji, koju je dobavljač UI sustava napismeno ovlastio da u njegovo ime izvršava i provodi obveze i postupke utvrđene u ovoj Uredbi i koja je takvo ovlaštenje prihvatila;

(5a) „proizvođač proizvoda” znači proizvođač u smislu bilo kojeg akta iz zakonodavstva Unije o usklađivanju navedenog u Prilogu II.;

(6) „uvoznik” znači svaka fizička ili pravna osoba koja se fizički nalazi ili ima poslovni nastan u Uniji i koja stavlja na tržište 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;

(8) „operater” znači dobavljač, proizvođač proizvoda, korisnik, ovlašteni zastupnik, uvoznik ili 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 u Uniji 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;

(16) „opoziv UI sustava” znači svaka mjera čiji je cilj vraćanje dobavljaču UI sustava stavljenog na raspolaganje korisnicima ili njegovo izuzimanje iz usluge ili onemogućavanje njegove uporabe;

(17) „povlačenje UI sustava” znači svaka mjera čija je svrha sprečavanje da se UI sustav u opskrbnom lancu stavi na raspolaganje na tržištu;

(18) „sposobnost UI sustava” znači sposobnost UI sustava da ostvari svoju namjenu;

(19) „ocjenjivanje sukladnosti” znači postupak kojim se provjerava jesu li ispunjeni zahtjevi iz glave III. poglavlja 2. ove Uredbe koji se odnose na visokorizični UI sustav;

(20) „tijelo koje provodi prijavljivanje” znači nacionalno tijelo odgovorno za utvrđivanje i provedbu postupaka potrebnih za ocjenjivanje, imenovanje, obavješćivanje i praćenje tijela za ocjenjivanje sukladnosti;

(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 u uporabu koja utječe na sukladnost UI sustava sa zahtjevima iz glave III. poglavlja 2. ove Uredbe ili promjena namjene prema kojoj je UI sustav bio ocijenjen. Za visokorizične UI sustave koji nastavljaju učiti nakon stavljanja na tržište ili 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.

(24) „oznaka sukladnosti CE” ili „oznaka CE” znači oznaka kojom dobavljač označuje da je UI sustav sukladan sa zahtjevima iz glave III. poglavlja 2. ili iz članka 4.b ove Uredbe i drugim primjenjivim pravnim aktom Unije o usklađivanju uvjeta za stavljanje proizvoda na tržište („zakonodavstvo Unije o usklađivanju”) kojim se propisuje označivanje tom oznakom;

(25) „sustav praćenja nakon stavljanja na tržište” znači sve aktivnosti kojima dobavljači UI sustava prikupljaju i analiziraju iskustva stečena uporabom 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) „zajednička specifikacija” znači skup tehničkih specifikacija kako su definirane u članku 2. točki 4. Uredbe (EU) br. 1025/2012 kojim se opisuje način ispunjavanja određenih zahtjeva utvrđenih na temelju ove Uredbe;

(29) „podaci za treniranje” znači podaci koji se upotrebljavaju za treniranje UI sustava prilagođavanjem njegovih poučivih parametara;

(30) „podaci za validaciju” znači podaci koji se upotrebljavaju za evaluaciju istreniranog 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 treniranje;

(31) „podaci za testiranje” znači podaci koji se upotrebljavaju za neovisnu evaluaciju istreniranog i validiranog UI sustava kako bi se potvrdila očekivana sposobnost tog sustava prije njegova stavljanja na tržište ili 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, kao što su fotografije lica ili daktiloskopski podaci;

(34) „sustav za prepoznavanje emocija” znači UI sustav namijenjen prepoznavanju psihološkog stanja, emocija ili namjera pojedinaca ili izvođenju zaključaka o njihovu psihološkom stanju, emocijama ili namjerama na temelju njihovih biometrijskih podataka;

(35) „sustav za biometrijsku kategorizaciju” znači UI sustav namijenjen razvrstavanju pojedinaca u određene kategorije na temelju njihovih biometrijskih podataka;

(36) „sustav za daljinsku biometrijsku identifikaciju” znači UI sustav namijenjen identificiranju pojedinaca, obično na daljinu, bez njihova aktivnog sudjelovanja, usporedbom biometrijskih podataka dotične osobe s biometrijskim podacima iz referentnog repozitorija podataka;

(37) „sustav za daljinsku biometrijsku identifikaciju u stvarnom vremenu” znači sustav za daljinsku biometrijsku identifikaciju koji trenutačno ili gotovo trenutačno prikuplja biometrijske podatke, vrši usporedbe i provodi identifikaciju;

(38) [izbrisano]

(39) „javno mjesto” znači svako fizičko mjesto u javnom ili privatnom vlasništvu dostupno neodređenom broju pojedinaca, bez obzira na to jesu li za pristup određeni neki uvjeti ili okolnosti i bez obzira na moguća ograničenja kapaciteta;

(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 kaznenog progona ili koje se provode u njihovo ime radi sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje;

(42) [izbrisano]

(43) „nacionalno nadležno tijelo” znači jedno od sljedećeg: tijelo koje provodi prijavljivanje i tijelo za nadzor tržišta; Kad je riječ o UI sustavima koje stavljaju u uporabu ili koriste institucije, agencije, uredi i tijela EU-a, odgovornosti koje su u državama članicama povjerene nacionalnom nadležnom tijelu ispunjava Europski nadzornik za zaštitu podataka, a, prema potrebi, svako upućivanje na nacionalna nadležna tijela ili tijela za nadzor tržišta u ovoj Uredbi smatra se upućivanjem na Europskog nadzornika za zaštitu podataka;

(44) „ozbiljan incident” znači svaki incident ili neispravnost UI sustava koji je izravno ili neizravno doveo do bilo kojeg od sljedećeg:

(a) smrti osobe ili znatne štete za zdravlje osobe;

(b) ozbiljnog i nepovratnog poremećaja u upravljanju kritičnom infrastrukturom i njezinu radu;

(c) kršenja obveza na temelju prava Unije namijenjenih zaštiti temeljnih prava;

(d) znatne štete za imovinu ili okoliš.

(45) „kritična infrastruktura” znači resurs, sustav ili njegov dio koji je potreban za pružanje usluge koja je ključna za održavanje vitalnih društvenih funkcija ili gospodarskih djelatnosti u smislu članka 2. stavaka 4. i 5. Direktive …../….. o otpornosti kritičnih subjekata;

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

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

(48) „testiranje u stvarnim uvjetima” znači privremeno testiranje UI sustava za predviđenu namjenu u stvarnim uvjetima, izvan laboratorija ili drugog simuliranog okruženja u cilju prikupljanja pouzdanih i utemeljenih podataka te procjene i provjere sukladnosti UI sustava sa zahtjevima ove Uredbe; testiranje u stvarnim uvjetima ne smatra se stavljanjem UI sustava na tržište ili u uporabu u smislu ove Uredbe ako su ispunjeni svi uvjeti iz članka 53. ili članka 54.a;

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

(50) „ispitanik” za potrebe testiranja u stvarnim uvjetima znači fizička osoba koja sudjeluje u testiranju u stvarnim uvjetima;

(51) „informirani pristanak” znači ispitanikov slobodan i dobrovoljan iskaz spremnosti da sudjeluje u određenom testiranju u stvarnim uvjetima nakon što je obaviješten o svim aspektima testiranja relevantnima za njegovu odluku o sudjelovanju; u slučaju maloljetnikâ i ispitanikâ koji nisu u stanju dati pristanak, informirani pristanak daje njihov zakonito imenovani zastupnik;

(52) „regulatorno izolirano okruženje za umjetnu inteligenciju” znači konkretan okvir koji je uspostavilo nacionalno nadležno tijelo i kojim se dobavljačima ili potencijalnim dobavljačima UI sustavâ nudi mogućnost razvoja, treniranja, validacije i testiranja inovativnog UI sustava, prema potrebi u stvarnim uvjetima, u skladu s određenim planom, na ograničeno vrijeme i pod regulatornim nadzorom.

Članak 4.

Provedbeni akti

Kako bi se osigurali jedinstveni uvjeti za provedbu ove Uredbe u pogledu pristupâ strojnog učenja, pristupa koji se temelje na logici i pristupa koji se temelje na znanju iz članka 3. stavka 1., Komisija može donijeti provedbene akte radi određivanja tehničkih elemenata tih pristupa, uzimajući u obzir tržišni i tehnološki razvoj. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 74. stavka 2.

GLAVA I.A

UI SUSTAVI OPĆE NAMJENE

Članak 4.a

Usklađenost UI sustavâ opće namjene s ovom Uredbom

1. Ne dovodeći u pitanje članke 5., 52., 53. i 69. ove Uredbe, UI sustavi opće namjene moraju ispunjavati samo zahtjeve i obveze iz članka 4.b.

2. Ti zahtjevi i obveze primjenjuju se neovisno o tome stavlja li se UI sustav opće namjene na tržište ili u uporabu kao prethodno istreniran model i treba li korisnik UI sustava opće namjene dodatno doraditi model.

Članak 4.b

Zahtjevi za UI sustave opće namjene i obveze za dobavljače takvih sustava

1. UI sustavi opće namjene koji se mogu upotrebljavati kao visokorizični UI sustavi ili kao sastavni dijelovi visokorizičnih UI sustava u smislu članka 6. moraju ispunjavati zahtjeve utvrđene u glavi III. poglavlju 2. ove Uredbe od datuma početka primjene provedbenih akata koje Komisija donese u skladu s postupkom ispitivanja iz članka 74. stavka 2. najkasnije 18 mjeseci nakon stupanja na snagu ove Uredbe. U tim provedbenim aktima utvrđuje se primjena zahtjevâ iz glave III. poglavlja 2. i prilagođava UI sustavima opće namjene s obzirom na njihove značajke, tehničku izvedivost, posebnosti lanca vrijednosti UI-ja te tržišni i tehnološki razvoj. Pri ispunjavanju tih zahtjeva u obzir se uzimaju općepriznata najnovija dostignuća.

2. Dobavljači UI sustavâ opće namjene iz stavka 1. od datuma početka primjene provedbenih akata iz stavka 1. moraju ispunjavati obveze utvrđene u člancima 16.aa, 16.e, 16.f, 16.g, 16.i, 16.j, 25., 48. i 61.

3. Kako bi ispunili obveze iz članka 16.e, dobavljači primjenjuju postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole iz Priloga VI. točaka 3. i 4.

4. Dobavljači takvih usto sustava stavljaju tehničku dokumentaciju iz članka 11. na raspolaganje nacionalnim nadležnim tijelima tijekom razdoblja koje završava deset godina nakon što je UI sustav opće namjene stavljen na tržište Unije ili stavljen u uporabu u Uniji.

5. Dobavljači UI sustava opće namjene surađuju s drugim dobavljačima koji namjeravaju staviti takve sustave u uporabu ili na tržište Unije kao visokorizične UI sustave ili sastavne dijelove visokorizičnih UI sustava te im pružaju potrebne informacije kako bi im se omogućilo da ispune svoje obveze na temelju ove Uredbe. U okviru takve suradnje među dobavljačima čuvaju se, ako je to primjenjivo, prava intelektualnog vlasništva i povjerljive poslovne informacije ili poslovne tajne u skladu s člankom 70. Kako bi se osigurali jedinstveni uvjeti za provedbu ove Uredbe u pogledu informacija koje dobavljači UI sustava opće namjene trebaju dijeliti, Komisija može donijeti provedbene akte u skladu s postupkom ispitivanja iz članka 74. stavka 2.

6. Kad je riječ o ispunjavanju zahtjeva i obveza iz stavaka 1., 2. i 3.:

– smatra se da se svako upućivanje na namjenu odnosi na moguću uporabu UI sustavâ opće namjene kao visokorizičnih UI sustava ili sastavnih dijelova visokorizičnih UI sustava u smislu članka 6.;

– svako upućivanje na zahtjeve za visokorizične UI sustave u glavi III. poglavlju II. smatra se upućivanjem samo na zahtjeve iz ovog članka.

Članak 4.c

Iznimke od članka 4.b

1. Članak 4.b ne primjenjuje se ako je dobavljač u uputama za uporabu ili informacijama priloženima UI sustavu opće namjene izričito isključio svaku visokorizičnu uporabu.

2. Takvo isključenje provodi se u dobroj vjeri i ne smatra se opravdanim ako dobavljač ima razloga vjerovati da bi se sustav mogao zloupotrijebiti.

3. Ako dobavljač otkrije zlouporabu na tržištu ili o njoj bude obaviješten, poduzima sve potrebne i razmjerne mjere kako bi spriječio takvu daljnju zlouporabu, posebno uzimajući u obzir razmjer zlouporabe i ozbiljnost povezanih rizika.

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 koje nadilaze svijest osobe s ciljem ili s učinkom bitnog mijenjanja ponašanja te osobe na način koji toj ili nekoj drugoj osobi uzrokuje tjelesnu ili psihološku štetu ili se može razumno očekivati da će je prouzročiti;

   (b) stavljanje na tržište, stavljanje u uporabu ili korištenje UI sustava koji iskorištava bilo koju slabost određene skupine osoba zbog njihove dobi, invaliditeta ili specifičnog društvenog ili ekonomskog položaja s ciljem ili s učinkom bitnog mijenjanja ponašanja osobe koja pripada toj skupini na način koji toj ili nekoj drugoj osobi uzrokuje tjelesnu ili psihološku štetu ili se može razumno očekivati da će je prouzročiti;

   (c) stavljanje na tržište, stavljanje u uporabu ili korištenje UI sustavâ u svrhu vrednovanja ili klasifikacije 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 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 skupinama pojedinaca koje je neopravdano ili nerazmjerno njihovu društvenom ponašanju ili ozbiljnosti postupanja;

(d) uporaba sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima od strane tijela kaznenog progona ili u njihovo ime za potrebe kaznenog progona, osim ako i u mjeri u kojoj je takva uporaba neophodna radi jednog od sljedećih ciljeva:

i. ciljane potrage za konkretnim potencijalnim žrtvama kaznenih djela;

ii. sprečavanja konkretne i znatne prijetnje kritičnoj infrastrukturi odnosno životu, zdravlju ili tjelesnoj sigurnosti pojedinaca ili sprečavanja terorističkih napada;

iii. lociranja ili identifikacije pojedinca u svrhu provođenja kaznene istrage ili progona odnosno izvršenja kaznene sankcije za kaznena djela iz članka 2. stavka 2. Okvirne odluke Vijeća 2002/584/PUP[32] koja su u dotičnoj državi članici kažnjiva zatvorskom kaznom ili mjerom oduzimanja slobode tijekom maksimalnog razdoblja od najmanje tri godine ili za druga specifična kaznena djela koja su u dotičnoj državi članici kažnjiva zatvorskom kaznom ili mjerom oduzimanja slobode tijekom maksimalnog razdoblja od najmanje pet godina, kako je propisano 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;

[32] 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.).

(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 uporabu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima 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 podrobnim pravilima nacionalnog prava iz stavka 4. Međutim, u propisno opravdanim hitnim situacijama sustav se može početi upotrebljavati bez odobrenja pod uvjetom da se to odobrenje zatraži bez nepotrebne odgode tijekom uporabe UI sustava, a ako se izdavanje odobrenja odbije, sustav se smjesta prestaje upotrebljavati.

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 podrobna pravila o podnošenju zahtjeva za odobrenja iz stavka 3., izdavanju, izvršavanju i nadzoru tih odobrenja te izvješćivanju u vezi s njima. 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 o klasifikaciji visokorizičnih UI sustava

1. UI sustav koji je sam po sebi proizvod obuhvaćen zakonodavstvom Unije o usklađivanju iz Priloga II. smatra se visokorizičnim ako se zahtijeva njegovo ocjenjivanje sukladnosti koje provodi treća strana radi stavljanja tog proizvoda na tržište ili u uporabu u skladu s navedenim zakonodavstvom.

2. UI sustav namijenjen za uporabu kao sigurnosni sastavni dio proizvoda obuhvaćenog zakonodavstvom iz stavka 1. smatra se visokorizičnim ako se zahtijeva njegovo ocjenjivanje sukladnosti koje provodi treća strana radi stavljanja tog proizvoda na tržište ili u uporabu u skladu s navedenim zakonodavstvom. Ova se odredba primjenjuje bez obzira na to stavlja li se UI sustav na tržište ili u uporabu neovisno o proizvodu.

3. UI sustavi iz Priloga III. smatraju se visokorizičnima, osim ako izlazni rezultati sustava imaju isključivo pomoćni učinak u odnosu na dotičnu radnju koju treba poduzeti ili odluku koju treba donijeti te stoga nije vjerojatno da će prouzročiti znatan rizik za zdravlje, sigurnost ili temeljna prava.

Kako bi se osigurali jedinstveni uvjeti za provedbu ove Uredbe, Komisija najkasnije godinu dana nakon stupanja ove Uredbe na snagu donosi provedbene akte u kojima se određuju okolnosti u kojima bi izlazni rezultati UI sustavâ iz Priloga III. imali isključivo pomoćni učinak u odnosu na dotičnu radnju koju treba poduzeti ili odluku koju treba donijeti. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 74. stavka 2.

Članak 7.

Izmjene Priloga II.

1. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 73. u svrhu izmjene 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 krajnji ishod uporabe UI sustava nije lako poništiv, pri čemu se krajnji ishodi koji utječu na zdravlje ili sigurnost osoba ne smatraju lako poništivima;

(h) stupanj u kojem se postojećim zakonodavstvom 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;

(i) razmjer i vjerojatnost koristi od uporabe UI sustava za pojedince, skupine ili društvo u cjelini.

3. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 73. u svrhu izmjene popisa iz Priloga III. uklanjanjem visokorizičnih UI sustava ako su ispunjena oba sljedeća uvjeta:

(a) dotični visokorizični UI sustav više ne predstavlja znatan rizik za temeljna prava, zdravlje ili sigurnost, uzimajući u obzir kriterije iz stavka 2.;

(b) brisanjem se ne smanjuje ukupna razina zaštite zdravlja, sigurnosti i temeljnih prava na temelju prava Unije.

POGLAVLJE 2.

ZAHTJEVI ZA VISOKORIZIČNE UI SUSTAVE

Članak 8.

Ispunjavanje zahtjeva

1. Visokorizični UI sustavi moraju ispunjavati zahtjeve utvrđene u ovom poglavlju, uzimajući u obzir općepriznata najnovija dostignuća.

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 podrazumijeva kontinuiran iterativan proces koji se planira i izvodi tijekom cijelog životnog vijeka visokorizičnog UI sustava i koji je potrebno redovito sustavno ažurirati. Čine ga sljedeći koraci:

   (a) utvrđivanje i analiza poznatih i predvidivih rizika koji će najvjerojatnije nastati za zdravlje, sigurnost i temeljna prava s obzirom na namjenu visokorizičnog UI sustava;

   (b) [izbrisano];

   (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.

   Rizici iz ovog stavka odnose se samo na one rizike koji se mogu razumno ublažiti ili ukloniti u sklopu razvoja ili projektiranja visokorizičnog UI sustava ili osiguravanjem odgovarajućih tehničkih informacija.

3. U mjerama upravljanja rizicima iz stavka 2. točke (d) uzimaju se u obzir učinci i moguća interakcija koji proizlaze iz kombinirane primjene zahtjeva iz ovog poglavlja, u cilju djelotvornijeg smanjenja rizika i istodobnog postizanja odgovarajuće ravnoteže u provedbi mjera za ispunjavanje tih zahtjeva.

4. Mjere upravljanja rizicima iz stavka 2. točke (d) moraju biti takve da se procijeni da je eventualni preostali rizik povezan sa svakom pojedinom opasnošću i cjelokupni preostali rizik visokorizičnih UI sustava prihvatljiv.

Kao najprikladnije mjere upravljanja rizicima utvrđuju se one kojima se osigurava sljedeće:

(a) uklanjanje rizika utvrđenih i evaluiranih na temelju stavka 2. ili njihovo svođenje na najmanju moguću mjeru odgovarajućim projektiranjem i razvojem visokorizičnog UI sustava;

(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.

U cilju 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. Visokorizični UI sustavi testiraju se kako bi se osiguralo da rade u skladu s namjenom i da ispunjavaju zahtjeve utvrđene u ovom poglavlju.

6. Postupci testiranja mogu uključivati testiranje u stvarnim uvjetima u skladu s člankom 54.a.

7. Visokorizični UI sustavi testiraju se prema potrebi u bilo kojem trenutku razvojnog procesa, a u svakom slučaju prije stavljanja na tržište ili u uporabu. Testiranje se provodi u odnosu na preliminarno definirane parametre i probabilističke pragove koji su primjereni za namjenu visokorizičnog UI sustava.

8. U okviru sustava upravljanja rizicima opisanog u stavcima od 1. do 7. posebno se vodi računa o vjerojatnosti da će visokorizičnom UI sustavu pristup imati osobe mlađe od 18 godina ili da će UI sustav na njih utjecati.

9. Kad je riječ o dobavljačima visokorizičnih UI sustava na koje se primjenjuju zahtjevi u pogledu internih procesa upravljanja rizicima na temelju relevantnog sektorskog prava Unije, aspekti opisani u stavcima od 1. do 8. mogu biti dio postupaka upravljanja rizicima uspostavljenih na temelju tog prava.

Članak 10.

Podaci i upravljanje podacima

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

2. Na skupove podataka za treniranje, validaciju i testiranje primjenjuju se odgovarajuće prakse upravljanja podacima. Te se prakse ponajprije odnose na:

   (a) relevantne odluke o organizaciji podataka;

   (b) postupke prikupljanja 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 koje će vjerojatno utjecati na zdravlje i sigurnost pojedinaca ili dovesti do diskriminacije koja je zabranjena pravom Unije;

(g) utvrđivanje svih mogućih nepotpunosti i nedostataka podataka te načina na koje se te nepotpunosti i nedostaci mogu ukloniti.

3. Skupovi podataka za treniranje, validaciju i testiranje relevantni su i reprezentativni te u najvećoj mogućoj mjeri 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 treniranje, 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. Kad je riječ o razvoju visokorizičnih UI sustava u kojima se ne upotrebljavaju tehnike koje uključuju treniranje modelâ, stavci od 2. do 5. primjenjuju se samo na skupove podataka za testiranje.

Članak 11.

Tehnička dokumentacija

1. Tehnička dokumentacija visokorizičnog UI sustava sastavlja se prije njegova stavljanja na tržište ili u 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 na jasan i sveobuhvatan način pruže sve informacije potrebne za ocjenjivanje sukladnosti UI sustava s tim zahtjevima. Sadržava barem elemente utvrđene u Prilogu IV. ili, ako je riječ o MSP-ovima, uključujući *start-up* poduzeća, bilo koju jednakovrijednu dokumentaciju koja ispunjava iste ciljeve, osim ako nadležno tijelo ustanovi da to nije primjereno.

2. U slučaju stavljanja na tržište ili 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. Kod visokorizičnih UI sustava tehnički je omogućeno automatsko evidentiranje događaja („dnevnici događaja”) tijekom životnog ciklusa sustava.

2. Kako bi se osigurala određena razina sljedivosti funkcioniranja UI sustava koja je u skladu s namjenom sustava, funkcije bilježenja događaja omogućuju evidentiranje događaja relevantnih za:

   i. utvrđivanje situacija koje mogu dovesti do toga da UI sustav predstavlja rizik u smislu članka 65. stavka 1. ili do znatne izmjene;

   ii. olakšavanje praćenja nakon stavljanja na tržište iz članka 61.; i

   iii. praćenje rada visokorizičnih UI sustava iz članka 29. stavka 4.

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 se osigura da je njihov rad dovoljno transparentan kako bi korisnici i dobavljači mogli ispuniti relevantne obveze iz poglavlja 3. ove glave i kako bi korisnici sustav mogli primjereno razumjeti i upotrebljavati.

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, uključujući specifično zemljopisno, bihevioralno ili funkcionalno okruženje u kojem se visokorizični UI sustav namjerava upotrebljavati;

      ii. razine točnosti, uključujući njezine parametre, otpornosti i kibersigurnosti iz članka 15. u odnosu na koje je visokorizični UI sustav testiran i validiran i koje se mogu očekivati te sve poznate i predvidljive okolnosti koje mogu utjecati na tu očekivanu razinu točnosti, otpornosti i kibersigurnosti;

      iii. sve poznate ili predvidljive okolnosti povezane s uporabom visokorizičnog UI sustava u skladu s njegovom namjenom koje mogu prouzročiti rizike za zdravlje i sigurnost ili temeljna prava iz članka 9. stavka 2.;

iv. prema potrebi, ponašanje sustava u odnosu na konkretne 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 treniranje, validaciju i testiranje, uzimajući u obzir namjenu UI sustava;

vi. prema potrebi, opis očekivanih izlaznih rezultata 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) potrebni računalni i hardverski resursi, očekivani životni vijek visokorizičnog UI sustava i sve potrebne mjere održavanja i brige, uključujući njihovu učestalost, kako bi se osiguralo pravilno funkcioniranje tog UI sustava, što se odnosi i na softverska ažuriranja;

(f) opis mehanizma uključenog u UI sustav s pomoću kojeg korisnici mogu pravilno prikupljati, pohranjivati i tumačiti dnevnike događaja, ako je to relevantno.

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 jednom od sljedećih vrsta mjera ili svima njima:

(a) mjerama koje dobavljač utvrđuje i ugrađuje, ako je to tehnički izvedivo, u visokorizični UI sustav prije stavljanja na tržište ili u uporabu;

(b) mjerama koje dobavljač utvrđuje prije stavljanja visokorizičnog UI sustava na tržište ili u uporabu, a koje su primjerene da ih provodi korisnik.

4. Za potrebe provedbe stavaka od 1. do 3. visokorizični UI sustav isporučuje se korisniku tako da pojedinci kojima je povjeren ljudski nadzor, u mjeri u kojoj je to primjereno i razmjerno s obzirom na okolnosti, mogu:

(a) razumjeti sposobnosti i ograničenja visokorizičnog UI sustava i propisno pratiti njegov rad;

(b) biti svjesni moguće tendencije automatskog oslanjanja ili pretjeranog oslanjanja na izlazne rezultate visokorizičnog UI sustava („automatizacijska pristranost”);

(c) točno protumačiti izlazne rezultate visokorizičnog UI sustava, uzimajući u obzir primjerice dostupne alate i metode za tumačenje;

(d) u bilo kojoj situaciji odustati od korištenja visokorizičnog UI sustava ili na neki drugi način zanemariti, zaobići ili poništiti izlazni rezultat visokorizičnog UI sustava;

(e) intervenirati u rad visokorizičnog UI sustava ili prekinuti sustav pritiskom gumba za zaustavljanje ili sličnim postupkom.

5. Kad je riječ o visokorizičnim UI sustavima iz točke 1. podtočke (a) Priloga III., mjerama iz stavka 3. mora se usto osigurati da korisnik ne poduzima nikakvu radnju i ne donosi nikakvu odluku na temelju identifikacije koja je rezultat sustava ako je nisu zasebno provjerila i potvrdila barem dva pojedinca. Zahtjev da najmanje dva pojedinca moraju provesti zasebnu provjeru ne primjenjuje se na visokorizične UI sustave koji se upotrebljavaju u svrhu kaznenog progona, migracija, nadzora državne granice ili azila ako se u pravu Unije ili nacionalnom pravu primjena tog zahtjeva smatra nerazmjernom.

Članak 15.

Točnost, otpornost i 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 pričuvne ili zaštitne planove.

   Visokorizični UI sustavi koji nastavljaju učiti nakon stavljanja na tržište ili u uporabu razvijaju se tako da se rizik od izlaznih rezultata koji bi mogli biti pristrani, a utječu na ulazne podatke u budućim operacijama („povratne veze”), otkloni ili svedi na najmanju moguću mjeru te da se primjene odgovarajuće mjere za ublažavanje tog rizika.

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 treniranje („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;

(aa) na visokorizičnom UI sustavu ili, ako to nije moguće, na ambalaži ili popratnoj dokumentaciji, ovisno o slučaju, navesti svoje ime, registrirano trgovačko ime ili registrirani žig i adresu na koju im se moguće obratiti u vezi s tim sustavom.

(b) imati uspostavljen sustav upravljanja kvalitetom koji je u skladu s člankom 17.;

(c) voditi dokumentaciju iz članka 18.;

(d) čuvati dnevnike događaja koje automatski generiraju njihovi visokorizični UI sustavi dok su pod njihovom kontrolom, kako je navedeno u članku 20.;

(e) pobrinuti se da visokorizični UI sustav prije stavljanja na tržište ili u uporabu prođe relevantni postupak ocjenjivanja sukladnosti iz članka 43.;

(f) ispuniti obveze registracije iz članka 51. stavka 1.;

(g) poduzeti potrebne korektivne mjere iz članka 21. ako visokorizični UI sustav nije sukladan sa zahtjevima iz poglavlja 2. ove glave;

(h) o neusklađenosti i svim poduzetim korektivnim mjerama obavijestiti relevantno nacionalno nadležno tijelo 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 visokorizičnih UI sustava na tržište ili u uporabu;

(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 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.

2.a Kad je riječ o dobavljačima visokorizičnih UI sustava na koje se primjenjuju obveze u pogledu sustavâ upravljanja kvalitetom na temelju relevantnog sektorskog prava Unije, aspekti opisani u stavku 1. mogu biti dio sustava upravljanja kvalitetom uspostavljenih na temelju tog prava.

3. Kad je riječ o dobavljačima koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu internog upravljanja, aranžmana ili postupaka na temelju zakonodavstva Unije o financijskim uslugama, obveza uspostave sustava upravljanja kvalitetom, uz iznimku stavka 1. točaka (g), (h) i (i), smatra se ispunjenom ako dobavljači poštuju pravila o aranžmanima ili procesima internog upravljanja na temelju relevantnog zakonodavstva Unije o financijskim uslugama. U tom se kontekstu u obzir uzimaju sve usklađene norme iz članka 40. ove Uredbe.

Članak 18.

Čuvanje dokumentacije

1. 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.

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

2. Dobavljači koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu internog upravljanja, aranžmana ili postupaka na temelju zakonodavstva Unije o financijskim uslugama čuvaju tehničku dokumentaciju u sklopu dokumentacije koja se čuva na temelju relevantnog zakonodavstva Unije o financijskim uslugama.

Članak 19.

Ocjenjivanje sukladnosti

1. Dobavljači visokorizičnih UI sustava dužni su se pobrinuti da njihovi sustavi prije stavljanja na tržište ili 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. [izbrisano]

Članak 20.

Automatski generirani dnevnici događaja

1. Dobavljači visokorizičnih UI sustava čuvaju dnevnike događaja iz članka 12. stavka 1. koje automatski generiraju njihovi visokorizični UI sustavi u mjeri u kojoj su takvi dnevnici događaja pod njihovom kontrolom na temelju ugovornog aranžmana s korisnikom ili neke druge pravne osnove. Čuvaju ih tijekom razdoblja od najmanje šest mjeseci, osim ako je primjenjivim pravom Unije ili nacionalnim pravom, osobito pravom Unije o zaštiti osobnih podataka, predviđeno drukčije.

2. Dobavljači koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu internog upravljanja, aranžmana ili postupaka na temelju zakonodavstva Unije o financijskim uslugama čuvaju dnevnike događaja koje automatski generiraju njihovi visokorizični UI sustavi u sklopu dokumentacije koja se čuva na temelju relevantnog zakonodavstva o financijskim uslugama.

Članak 21.

Korektivne radnje

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 smjesta istražuju uzroke za to, ako je primjenjivo, u suradnji s korisnikom koji je prijavio nesukladnost te poduzimaju potrebne korektivne radnje kako bi osigurali sukladnost tog sustava, povukli ga ili opozvali, ovisno o slučaju. 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 dostavljaju sve informacije i dokumentaciju potrebne za dokazivanje sukladnosti visokorizičnog UI sustava sa zahtjevima iz poglavlja 2. ove glave na jeziku koji tijelo dotične države članice može bez poteškoća razumjeti. Na obrazloženi zahtjev nacionalnog nadležnog tijela dobavljači tom tijelu daju i pristup dnevnicima događaja iz članka 12. stavka 1. koje je automatski generirao visokorizični UI sustav u mjeri u kojoj su takvi dnevnici događaja pod njihovom kontrolom na temelju ugovornog aranžmana s korisnikom ili neke druge pravne osnove.

Članak 23.a

Uvjeti pod kojima druge osobe podliježu obvezama dobavljača.

1. Sve fizičke ili pravne osobe smatraju se dobavljačima novih visokorizičnih UI sustava za potrebe ove Uredbe i podliježu obvezama dobavljača na temelju članka 16. u bilo kojoj od sljedećih okolnosti:

   (a) ako stavljaju svoje ime ili žig na visokorizični UI sustav koji je već stavljen na tržište ili u uporabu, ne dovodeći u pitanje ugovorne aranžmane kojima je propisano da se obveze raspodjeljuju drukčije;

(b) [izbrisano]

(c) ako znatno izmijene visokorizični UI sustav koji je već stavljen na tržište ili u uporabu;

(d) ako izmijene namjenu UI sustava koji nije visokorizičan i koji je već stavljen na tržište ili u uporabu tako da izmijenjeni sustav postane visokorizičan UI sustav;

(e) ako UI sustav opće namjene stave na tržište ili u uporabu kao visokorizični UI sustav ili kao sastavni dio visokorizičnog UI sustava.

2. Ako nastupe okolnosti iz stavka 1. točke (a) ili (c), dobavljač koji je prvobitno stavio visokorizični UI sustav na tržište ili u uporabu više se ne smatra dobavljačem za potrebe ove Uredbe.

3. Kad je riječ o visokorizičnim UI sustavima koji su sigurnosni sastavni dio proizvodâ na koje se primjenjuju pravni akti navedeni u Prilogu II. odjeljku A, proizvođač tih proizvoda smatra se dobavljačem visokorizičnog UI sustava i podliježe obvezama iz članka 16. u bilo kojoj od sljedećih okolnosti:

i. visokorizični UI sustav stavljen je na tržište zajedno s dotičnim proizvodom pod imenom ili žigom proizvođača proizvoda;

ii. visokorizični UI sustav stavljen je u uporabu pod imenom ili žigom proizvođača dotičnog proizvoda nakon što je proizvod stavljen na tržište.

Članak 24.

[izbrisano]

Članak 25.

Ovlašteni zastupnici

1. Prije stavljanja svojih sustava na raspolaganje na tržištu Unije 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. Za potrebe ove Uredbe ovlaštenjem se ovlaštenom zastupniku daje ovlast da obavlja samo sljedeće zadaće:

   (-a) provjerava je li dobavljač sastavio EU izjavu o sukladnosti i tehničku dokumentaciju te proveo relevantni postupak ocjenjivanja sukladnosti;

   (a) nacionalnim nadležnim tijelima i nacionalnim tijelima iz članka 63. stavka 7., u razdoblju koje završava deset godina nakon što je visokorizični UI sustav stavljen na tržište ili u uporabu, stavlja na raspolaganje podatke za kontakt dobavljača koji je imenovao ovlaštenog zastupnika, primjerak EU izjave o sukladnosti, tehničku dokumentaciju i, ako je primjenjivo, potvrdu koju je izdalo prijavljeno tijelo;

   (b) nacionalnom nadležnom tijelu na obrazloženi zahtjev dostavlja sve informacije i dokumentaciju, uključujući one koje se čuvaju u skladu s točkom (b), potrebne za dokazivanje sukladnosti visokorizičnog UI sustava sa zahtjevima iz poglavlja 2. ove glave, što uključuje i davanje pristupa dnevnicima događaja iz članka 12. stavka 1. koje automatski generira visokorizični UI sustav u mjeri u kojoj su takvi dnevnici događaja pod kontrolom dobavljača na temelju ugovornog aranžmana s korisnikom ili druge pravne osnove;

   (c) na obrazloženi zahtjev surađuje s nacionalnim nadležnim tijelima u svim radnjama koje ta tijela poduzimaju u vezi s visokorizičnim UI sustavom;

(d) ispunjava obveze registracije iz članka 51. stavka 1. i, ako registraciju sustava provodi sam dobavljač, provjerava jesu li informacije iz Priloga VIII. dijela II. točaka od 1. do 11. točne.

Ovlašteni zastupnik prekida ovlaštenje ako ima razloga vjerovati da dobavljač postupa protivno svojim obvezama na temelju ove Uredbe. Ako dođe do toga, o prekidu ovlaštenja i razlozima za prekid ujedno bez odgode obavješćuje tijelo za nadzor tržišta države članice u kojoj ima poslovni nastan i, prema potrebi, relevantno prijavljeno tijelo,.

Kad je riječ o njegovoj potencijalnoj odgovornosti na temelju Direktive Vijeća 85/374/EEZ, ovlašteni zastupnik pravno je odgovoran za neispravne UI sustave na istoj osnovi kao i dobavljač te pojedinačno i solidarno s njim.

Članak 26.

Obveze uvoznika

1. Prije stavljanja visokorizičnog UI sustava na tržište uvoznici takvog sustava osiguravaju da je sustav u skladu s ovom Uredbom tako da provjere je li:

(a) dobavljač tog UI sustava proveo relevantni postupak ocjenjivanja sukladnosti iz članka 43.;

(b) dobavljač sastavio tehničku dokumentaciju u skladu s Prilogom IV.;

(c) sustav označen oznakom sukladnosti CE te jesu li mu priložene EU izjava o sukladnosti i upute za upotrebu;

(d) dobavljač imenovao ovlaštenog zastupnika iz članka 25.

2. Ako uvoznik ima razloga vjerovati da visokorizični UI sustav nije sukladan s ovom Uredbom, da je krivotvoren ili da mu je priložena krivotvorena dokumentacija, ne stavlja taj sustav na tržište dok on ne postane sukladan. Ako visokorizični UI sustav predstavlja rizik u smislu članka 65. stavka 1., uvoznik o tome obavješćuje dobavljača UI sustava, ovlaštene zastupnike 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.

4.a Uvoznici u razdoblju od deset godina nakon što je UI sustav stavljen na tržište ili u uporabu čuvaju primjerak potvrde koju je izdalo prijavljeno tijelo, ako je primjenjivo, uputa za uporabu i EU izjave o sukladnosti.

5. Uvoznici nacionalnim nadležnim tijelima na obrazloženi zahtjev dostavljaju sve informacije i dokumentaciju, uključujući one koje se čuvaju u skladu sa stavkom 5., potrebne za dokazivanje sukladnosti visokorizičnog UI sustava sa zahtjevima iz poglavlja 2. ove glave na jeziku koji to nacionalno nadležno tijelo može bez poteškoća razumjeti. U tu svrhu osiguravaju da se tim tijelima na raspolaganje može staviti i tehnička dokumentacija.

5.a Uvoznici surađuju s nacionalnim nadležnim tijelima u svim radnjama koje ta tijela poduzimaju u vezi s UI sustavom čiji su uvoznici.

Članak 27.

Obveze distributera

1. Prije stavljanja visokorizičnog UI sustava na raspolaganje na tržištu distributeri provjeravaju ima li taj visokorizični UI sustav potrebnu oznaku sukladnosti CE, jesu li mu priloženi primjerak EU izjave o sukladnosti i upute za uporabu te jesu li dobavljač i uvoznik sustava, ovisno o slučaju, ispunili obveze iz članka 16. točke (b) odnosno članka 26. stavka 3.

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, da ga se povuče ili opozove 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 dostavljaju sve informacije i dokumentaciju u vezi sa svojim aktivnostima iz stavaka od 1. do 4.

5.a Distributeri surađuju s nacionalnim nadležnim tijelima u svim radnjama koje ta tijela poduzimaju u vezi s UI sustavom čiji su distributeri.

Članak 28.

[izbrisano]

Članak 29.

Obveze korisnika visokorizičnih UI sustava

1. Korisnici visokorizičnih UI sustava upotrebljavaju takve sustave u skladu s uputama za uporabu priloženima sustavima i u skladu sa stavcima 2. i 5. ovog članka.

1.a Korisnici dodjeljuju zadaću ljudskog nadzora pojedincima koji imaju potrebne kompetencije i nadležnosti te su prošli potrebno osposobljavanje.

2. Obvezama iz stavaka 1. i 1.a 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 provode ljudski nadzor i 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 prijavljuju i svaki ozbiljan incident te prekidaju uporabu UI sustava. Ako korisnik ne može stupiti u kontakt s dobavljačem, članak 62. primjenjuje se *mutatis mutandis*. Ta obveza ne obuhvaća osjetljive operativne podatke korisnika UI sustavâ koji su tijela kaznenog progona.

Kad je riječ o korisnicima koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu internog upravljanja, aranžmana ili postupaka na temelju zakonodavstva Unije o financijskim uslugama, obveza praćenja iz prvog podstavka smatra se ispunjenom ako korisnici poštuju pravila o aranžmanima, procesima i mehanizmima internog upravljanja na temelju relevantnog zakonodavstva o financijskim uslugama.

5. Korisnici visokorizičnih UI sustava čuvaju dnevnike događaja iz članka 12. stavka 1. koje automatski generira taj visokorizični UI sustavi u mjeri u kojoj su takvi dnevnici događaja pod njihovom kontrolom. Čuvaju ih tijekom razdoblja od najmanje šest mjeseci, osim ako je primjenjivim pravom Unije ili nacionalnim pravom, osobito pravom Unije o zaštiti osobnih podataka, predviđeno drukčije.

Korisnici koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu internog upravljanja, aranžmana ili postupaka na temelju zakonodavstva Unije o financijskim uslugama čuvaju dnevnike o događajima u sklopu dokumentacije koja se čuva na temelju relevantnog zakonodavstva Unije o financijskim uslugama.

5.a Korisnici visokorizičnih UI sustava koji su tijela javne vlasti, javne agencije ili javna tijela, uz iznimku tijela kaznenog progona, tijela za nadzor državne granice, tijela za imigraciju ili tijela za azil, dužni su ispunjavati obveze registracije iz članka 51. Ako utvrde da sustav koji namjeravaju upotrebljavati nije registriran u bazi podataka EU-a iz članka 60., taj sustav ne upotrebljavaju i o tome obavješćuju dobavljača ili distributera.

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.

6.a Korisnici surađuju s nacionalnim nadležnim tijelima u svim radnjama koje ta tijela poduzimaju u vezi s UI sustavom čiji su korisnici.

POGLAVLJE 4.

TIJELA KOJA PROVODE PRIJAVLJIVANJE I PRIJAVLJENA TIJELA

Članak 30.

Tijela koja provode prijavljivanje

1. Svaka država članica imenuje ili osniva barem jedno tijelo koje provodi prijavljivanje, koje je odgovorno za utvrđivanje i provedbu postupaka potrebnih za ocjenjivanje, imenovanje, prijavljivanje i praćenje tijelâ za ocjenjivanje sukladnosti.

2. Države članice mogu odlučiti da ocjenjivanje i praćenje iz stavka 1. provodi nacionalno akreditacijsko tijelo u smislu Uredbe (EZ) br. 765/2008 i u skladu s njom.

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 tijelâ 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 u skladu s člankom 70.

7. Tijela koja provode prijavljivanje moraju na raspolaganju imati primjeren broj članova stručnog osoblja za propisno obavljanje zadaća.

8. [izbrisano]

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 UI sustavâ 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 redovito 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. Prijavljeno tijelo ažurira dokumentaciju iz stavaka 2. i 3. u slučaju bilo kakvih bitnih promjena kako bi tijelu odgovornom za prijavljena tijela omogućilo da prati i provjerava kontinuiranu usklađenost sa svim zahtjevima iz članka 33.

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 prijavljuju ta tijela Komisiji i drugim državama članicama putem alata za elektroničko prijavljivanje koji je razvila i kojim upravlja Komisija.

3. Prijavljivanje iz stavka 2. obuhvaća sve pojedinosti o aktivnostima ocjenjivanja sukladnosti, modulu ili modulima za ocjenjivanje sukladnosti i dotičnom UI sustavu te relevantnu potvrdu o stručnosti. Ako se prijavljivanje ne temelji na potvrdi o akreditaciji iz članka 31. stavka 2., tijelo koje provodi prijavljivanje dostavlja Komisiji i ostalim državama članicama pisane dokaze kojima se potvrđuje stručnost tijela za ocjenjivanje sukladnosti i obavješćuje ih o aranžmanima koji su uspostavljeni kako bi se osiguralo da će se to tijelo redovito pratiti i da će nastaviti ispunjavati zahtjeve iz članka 33.

4. Dotično tijelo za ocjenjivanje sukladnosti može obavljati aktivnosti prijavljenog tijela samo ako Komisija ili druge države članice ne podnesu prigovor u roku od dva tjedna od prijavljivanja koje je izvršilo tijelo koje provodi prijavljivanje ako prijava uključuje potvrdu o akreditaciji iz članka 31. stavka 2. odnosno u roku od dva mjeseca od prijavljivanja koje je izvršilo tijelo koje provodi prijavljivanje ako prijava uključuje pisane dokaze iz članka 31. stavka 3.

5. [izbrisano]

Članak 33.

Zahtjevi koji se odnose na prijavljena tijela

1. Prijavljeno tijelo mora biti osnovano na temelju nacionalnog prava i imati pravnu osobnost.

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 imaju dokumentirane postupke kojima se osigurava da njihovo osoblje, odbori, društva kćeri, podizvođači i sva povezana tijela ili osoblje vanjskih tijela poštuju povjerljivost informacija u skladu s člankom 70. 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 država članica u kojoj se nalaze 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. Prijavljeno tijelo trajno raspolaže dovoljnim brojem članova administrativnog, tehničkog, pravnog i znanstvenog osoblja koji posjeduju iskustvo i znanje u vezi 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. [izbrisano]

Članak 33.a

Pretpostavka sukladnosti sa zahtjevima koji se odnose na prijavljena tijela

Ako tijelo za ocjenjivanje sukladnosti dokaže da ispunjava kriterije utvrđene u relevantnim usklađenim normama ili njihovim dijelovima, upućivanja na koje su objavljena u Službenom listu Europske unije, pretpostavlja se da ispunjava zahtjeve iz članka 33. u mjeri u kojoj primjenjive usklađene norme obuhvaćaju te zahtjeve.

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. Relevantni dokumenti koji se odnose na ocjenjivanje kvalifikacija podizvođača ili društva kćeri i zadaća koje su oni obavili na temelju ove Uredbe stavljaju se na raspolaganje tijelu koje provodi prijavljivanje tijekom razdoblja od pet godina od datuma prestanka podugovaranja.

Članak 34.a

Operativne obveze prijavljenih tijela

1. Prijavljena tijela provjeravaju sukladnost visokorizičnog UI sustava u skladu s postupcima ocjenjivanja sukladnosti iz članka 43.

2. Prijavljena tijela pri obavljanju svojih aktivnosti izbjegavaju nepotrebno opterećivanje dobavljača, uzimajući u obzir veličinu poduzeća, sektor u kojem ono posluje, strukturu poduzeća i stupanj složenosti dotičnog visokorizičnog UI sustava. Prijavljeno tijelo pritom ipak poštuje stupanj strogosti i razinu zaštite koji su potrebni kako bi visokorizični UI sustav bio sukladan sa zahtjevima ove Uredbe.

3. Prijavljena tijela tijelu koje provodi prijavljivanje iz članka 30. stavljaju na raspolaganje i na zahtjev dostavljaju svu relevantnu dokumentaciju, uključujući dokumentaciju dobavljača, kako bi to tijelo moglo provoditi svoje aktivnosti ocjenjivanja, imenovanja, prijavljivanja i praćenja te kako bi se olakšalo ocjenjivanje opisano u ovom poglavlju.

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 vezi s prijavama

1. Tijelo koje provodi prijavljivanje obavješćuje Komisiju i druge države članice o svim relevantnim promjenama u vezi s prijavom prijavljenog tijela putem alata za elektroničko prijavljivanje iz članka 32. stavka 2.

2. Na proširenja opsega prijave primjenjuju se postupci opisani u člancima 31. i 32. Na promjene u vezi s prijavom, uz iznimku proširenja njezina opsega, primjenjuju se postupci utvrđeni u sljedećim stavcima.

Ako prijavljeno tijelo odluči prestati obavljati svoje aktivnosti ocjenjivanja sukladnosti, obavješćuje tijelo koje provodi prijavljivanje i dotične dobavljače u najkraćem mogućem roku, a u slučaju planiranog prestanka obavljanja aktivnosti godinu dana prije prestanka. Potvrde mogu ostati privremeno valjane u razdoblju od devet mjeseci nakon prestanka obavljanja aktivnosti prijavljenog tijela pod uvjetom da je neko drugo prijavljeno tijelo u pisanom obliku potvrdilo da će preuzeti odgovornost za UI sustave na koje se te potvrde odnose. Novo prijavljeno tijelo provodi cjelokupno ocjenjivanje UI sustava na koje utječe kraj tog razdoblja prije nego što izda nove potvrde za te sustave. Ako je prijavljeno tijelo prestalo obavljati aktivnosti, tijelo koje provodi prijavljivanje povlači imenovanje.

3. Ako tijelo koje provodi prijavljivanje ima razloga smatrati da prijavljeno tijelo više ne ispunjava zahtjeve iz članka 33. ili da ne ispunjava svoje obveze, tijelo koje provodi prijavljivanje – pod uvjetom da je prijavljeno tijelo imalo priliku izjasniti se – prema potrebi ograničava, suspendira ili povlači prijavu, ovisno o ozbiljnosti neispunjavanja tih zahtjeva ili obveza. O tome odmah obavješćuje Komisiju i druge države članice.

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

5. U slučaju ograničenja, suspenzije ili povlačenja prijave, tijelo koje provodi prijavljivanje poduzima odgovarajuće mjere kako bi osiguralo da se predmeti dotičnog prijavljenog tijela sačuvaju i stavlja ih na raspolaganje tijelima koja provode prijavljivanje u drugim državama članicama i tijelima za nadzor tržišta na njihov zahtjev.

6. U slučaju ograničenja, suspenzije ili povlačenja imenovanja, tijelo koje provodi prijavljivanje:

   (a) ocjenjuje učinak koji to ima na potvrde koje je izdalo prijavljeno tijelo;

   (b) Komisiji i drugim državama članicama podnosi izvješće o svojim nalazima u roku od tri mjeseca nakon što ih je obavijestilo o promjenama u vezi s prijavom;

   (c) od prijavljenog tijela zahtijeva da u razumnom roku koji određuje tijelo koje provodi prijavljivanje suspendira ili povuče sve nepropisno izdane potvrde kako bi se osigurala sukladnost UI sustavâ na tržištu;

   (d) obavješćuje Komisiju i države članice o potvrdama za koje je zatražilo suspenziju ili povlačenje;

(e) nacionalnim nadležnim tijelima države članice u kojoj dobavljač ima registrirano mjesto poslovanja dostavlja sve relevantne informacije o potvrdama za koje je zatražilo suspenziju ili povlačenje. To nadležno tijelo prema potrebi poduzima odgovarajuće mjere kako bi se izbjegao potencijalni rizik za zdravlje, sigurnost ili temeljna prava.

7. Osim ako su potvrde nepropisno izdane i ako je prijava suspendirana ili ograničena, potvrde ostaju valjane u sljedećim okolnostima:

(a) tijelo koje provodi prijavljivanje potvrdilo je, u roku od mjesec dana od suspenzije ili ograničenja, da potvrde na koje se odnosi suspenzija ili ograničenje ne predstavljaju rizik za zdravlje, sigurnost ili temeljna prava te je navelo rok i mjere s pomoću kojih bi se suspenzija ili ograničenje mogli prekinuti; ili

(b) tijelo koje provodi prijavljivanje potvrdilo je da se tijekom razdoblja suspenzije ili ograničenja neće izdavati, mijenjati ili ponovno izdavati potvrde relevantne za suspenziju te navodi je li prijavljeno tijelo sposobno nastaviti pratiti već izdane potvrde i odgovarati za njih tijekom razdoblja suspenzije ili ograničenja. U slučaju da tijelo odgovorno za prijavljena tijela utvrdi da prijavljeno tijelo nije sposobno podupirati već izdane potvrde, dobavljač u roku od tri mjeseca od suspenzije ili ograničenja nacionalnim nadležnim tijelima države članice u kojoj dobavljač sustava na koji se potvrda odnosi ima registrirano mjesto poslovanja dostavlja pisanu potvrdu da neko drugo kvalificirano prijavljeno tijelo privremeno preuzima funkcije prijavljenog tijela u pogledu praćenja potvrda i odgovaranja za njih tijekom razdoblja suspenzije ili ograničenja.

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

(a) ako je nacionalno nadležno tijelo države članice u kojoj dobavljač UI sustava na koji se potvrda odnosi ima registrirano mjesto poslovanja potvrdilo da dotični sustavi ne predstavljaju rizik za zdravlje, sigurnost i temeljna prava; i

(b) drugo prijavljeno tijelo potvrdilo je u pisanom obliku da će preuzeti neposrednu odgovornost za te sustave i da će dovršiti njihovo ocjenjivanje u roku od dvanaest mjeseci od opoziva imenovanja.

U okolnostima iz prvog podstavka nacionalno nadležno tijelo države članice u kojoj dobavljač sustava na koji se potvrda odnosi ima registrirano mjesto poslovanja može produljiti privremenu valjanost potvrda za dodatna razdoblja od tri mjeseca, koja sveukupno ne smiju biti dulja od dvanaest mjeseci.

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

Članak 37.

Osporavanje nadležnosti 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 povjerljiv način u skladu s člankom 70.

4. Ako Komisija utvrdi da prijavljeno tijelo ne zadovoljava ili je prestalo zadovoljavati zahtjeve iz članka 33., obavješćuje tijelo koje provodi prijavljivanje o razlozima na temelju kojih je to utvrdila te zahtijeva od njega da poduzme potrebne korektivne mjere, uključujući, prema potrebi, suspenziju, ograničenje ili povlačenje imenovanja. Ako tijelo koje provodi prijavljivanje ne provede potrebne korektivne mjere, Komisija provedbenim aktima može suspendirati, ograničiti ili povući prijavu. 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, kad je riječ o visokorizičnim UI sustavima, uspostave i pravilno provode primjerena koordinacija i suradnja prijavljenih tijela koja se bave postupcima ocjenjivanja sukladnosti na temelju ove Uredbe, i to u okviru sektorske skupine prijavljenih tijela.

2. Tijelo koje provodi prijavljivanje osigurava da tijela koja je prijavilo sudjeluju u radu te skupine, izravno ili preko imenovanih predstavnika.

Članak 39.

Tijela za ocjenjivanje sukladnosti iz trećih zemalja

Tijela za ocjenjivanje sukladnosti uspostavljena na temelju prava određene treće zemlje s kojom je Unija sklopila sporazum mogu biti ovlaštena za obavljanje aktivnosti prijavljenih tijela na temelju ove Uredbe, pod uvjetom da ispunjavaju zahtjeve iz članka 33.

POGLAVLJE 5.

NORME, OCJENJIVANJE SUKLADNOSTI, POTVRDE, REGISTRACIJA

Članak 40.

Usklađene norme

1. Za visokorizične UI sustave ili UI sustave opće namjene 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 odnosno sa zahtjevima iz članaka 4.a i 4.b, ovisno o slučaju, u mjeri u kojoj te norme obuhvaćaju dotične zahtjeve.

2. Pri izdavanju zahtjeva za normizaciju europskim organizacijama za normizaciju u skladu s člankom 10. Uredbe 1025/2012 Komisija navodi da su norme usklađene, jasne i izrađene tako da im je svrha osobito ostvarivanje sljedećih ciljeva:

   (a) osigurati da su UI sustavi stavljeni na tržište ili u uporabu u Uniji sigurni i da poštuju vrijednosti Unije i jačaju otvorenu stratešku autonomiju Unije;

   (b) promicati ulaganja i inovacije u području umjetne inteligencije, među ostalim zahvaljujući većoj pravnoj sigurnosti, kao i konkurentnost i rast tržišta Unije;

   (c) povećati višedioničko upravljanje, u kojem su zastupljeni svi relevantni europski dionici (npr. industrija, MSP-ovi, civilno društvo, istraživači);

   (d) doprinositi jačanju globalne suradnje u normizaciji u području umjetne inteligencije koja je u skladu s vrijednostima i interesima Unije.

Komisija od europskih organizacija za normizaciju zahtijeva da dostave dokaze o tome da su uložile maksimalne napore u ispunjavanje prethodno navedenih ciljeva.

Članak 41.

Zajedničke specifikacije

1. Komisija je ovlaštena, nakon savjetovanja s Odborom za umjetnu inteligenciju iz članka 56., za donošenje provedbenih akata u skladu s postupkom ispitivanja iz članka 74. stavka 2. kojima se utvrđuju zajedničke tehničke specifikacije za zahtjeve iz poglavlja 2. ove glave odnosno sa zahtjevima iz članaka 4.a i 4.b, ovisno o slučaju, ako su ispunjeni sljedeći uvjeti:

   (a) u Službenom listu Europske unije nisu objavljena upućivanja na usklađene norme koje se odnose na relevantne bitne bojazni u vezi sa sigurnošću ili temeljnim pravima u skladu s Uredbom (EU) br. 1025/2012;

   (b) Komisija je na temelju članka 10. stavka 1. Uredbe (EU) br. 1025/2012 zatražila od jedne ili više europskih organizacija za normizaciju da izrade usklađenu normu za zahtjeve iz poglavlja 2. ove glave;

   (c) nijedna europska organizacija za normizaciju nije prihvatila zahtjev iz točke (b) ili usklađene norme koje se odnose na taj zahtjev nisu dostavljene u roku utvrđenom u skladu s člankom 10. stavkom 1. Uredbe (EU) br. 1025/2012 ili te norme nisu u skladu sa zahtjevom.

1.a Prije nego što izradi nacrt provedbenog akta Komisija obavješćuje odbor iz članka 22. Uredbe (EU) br. 1025/2012 da smatra da su uvjeti iz stavka 1. ispunjeni.

2. Tijekom rane faze izrade nacrta provedbenog akta kojim se utvrđuju zajedničke specifikacije Komisija ispunjava ciljeve iz članka 40. stavka 2. i prikuplja stajališta relevantnih tijela ili stručnih skupina osnovanih na temelju relevantnog sektorskog prava Unije. Komisija na temelju tog savjetovanja izrađuje nacrt provedbenog akta.

3. Za visokorizične UI sustave ili UI sustave opće namjene koji su sukladni sa zajedničkim specifikacijama iz stavka 1. pretpostavlja se da su sukladni sa zahtjevima iz poglavlja 2. ove glave odnosno sa zahtjevima iz članaka 4.a i 4.b, ovisno o slučaju, u mjeri u kojoj te zajedničke specifikacije obuhvaćaju dotične zahtjeve.

4. Ako se upućivanja na usklađenu normu objave u Službenom listu Europske unije, provedbeni akti iz stavka 1., koji obuhvaćaju zahtjeve iz poglavlja 2. ove glave odnosno zahtjeve iz članaka 4.a i 4.b, ovisno o slučaju, stavljaju se izvan snage.

5. Ako neka država članica smatra da zajednička specifikacija ne ispunjava u potpunosti zahtjeve iz poglavlja 2. ove glave odnosno zahtjeve iz članaka 4.a i 4.b, ovisno o slučaju, o tome obavješćuje Komisiju i dostavlja joj detaljno objašnjenje, a Komisija je dužna razmotriti te informacije i, prema potrebi, izmijeniti provedbeni akt kojim se utvrđuje dotična zajednička specifikacija.

Članak 42.

Pretpostavka sukladnosti s određenim zahtjevima

1. Za visokorizične UI sustave koji su trenirani i testirani na podacima koji odražavaju specifično zemljopisno, bihevioralno ili radno okruženje u kojem je predviđena njihova uporaba pretpostavlja se da ispunjavaju odgovarajuće zahtjeve iz članka 10. stavka 4.

2. Za visokorizične UI sustave ili UI sustave opće namjene koji su certificirani ili za koje je izdana izjava o sukladnosti u okviru programa kibersigurnosti na temelju Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća[33] 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 bira jedan od sljedećih postupaka:

   (a) postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole iz Priloga VI.; ili

   (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.

[33] 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.).

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. i za UI sustave opće namjene iz glave 1.a dobavljači primjenjuju postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole iz Priloga VI., kojim se ne predviđa sudjelovanje prijavljenog tijela.

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 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. [izbrisano]

5. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 73. u svrhu ažuriranja priloga VI. i VII. 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. sastavljaju se na jeziku koji relevantna tijela u državi članici u kojoj prijavljeno tijelo ima poslovni nastan mogu bez poteškoća razumjeti.

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. Svaka dopuna potvrde ostaje valjana dok god je valjana potvrda koju dopunjuje.

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

Protiv odluka prijavljenih tijela mora se moći uložiti žalba.

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 UI sustave dostavlja relevantne informacije o pitanjima u vezi s negativnim i, na zahtjev, pozitivnim rezultatima ocjenjivanja sukladnosti.

4. Obveze iz stavaka od 1. do 3. ispunjavaju se u skladu s člankom 70.

Članak 47.

Odstupanje od postupka ocjenjivanja sukladnosti

1. Odstupajući od članka 43. i na propisno obrazložen zahtjev, svako tijelo za nadzor tržišta može odobriti stavljanje određenih visokorizičnih UI sustava na tržište ili u uporabu na državnom području dotične države članice zbog iznimnih razloga u pogledu 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, uzimajući u obzir iznimne razloge zbog kojih je odstupanje opravdano. Ti se postupci dovršavaju bez nepotrebne odgode.

1.a U propisno opravdanoj hitnoj situaciji zbog iznimnih razloga u pogledu javne sigurnosti ili u slučaju konkretne, znatne i neposredne prijetnje životu ili fizičkoj sigurnosti pojedinaca, tijela kaznenog progona ili tijela civilne zaštite određeni visokorizični UI sustav mogu staviti u uporabu bez odobrenja iz stavka 1. pod uvjetom da se to odobrenje bez nepotrebne odgode zatraži tijekom ili nakon uporabe, a ako se odobrenje odbije, uporaba tog sustava smjesta se prekida te se svi rezultati te uporabe i izlazni podaci odmah odbacuju.

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. Ta obveza ne obuhvaća osjetljive operativne podatke u vezi s aktivnostima tijela kaznenog progona.

3. [izbrisano]

4. [izbrisano]

5. [izbrisano]

6. Kad je riječ o visokorizičnim UI sustavima koji su povezani s proizvodima obuhvaćenima zakonodavstvom Unije o usklađivanju iz Priloga II. odjeljka A, primjenjuje se samo odstupanje od postupaka ocjenjivanja sukladnosti utvrđeno u tom zakonodavstvu.

Članak 48.

EU izjava o sukladnosti

1. Dobavljač sastavlja EU izjavu o sukladnosti potpisanu rukom ili elektronički za svaki UI sustav i drži je na raspolaganju nacionalnim nadležnim tijelima u razdoblju od deset 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. Primjerak EU izjave o sukladnosti dostavlja se relevantnim nacionalnim nadležnim tijelima na njihov zahtjev.

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

3. Ako visokorizični UI sustavi podliježu drugom zakonodavstvu Unije o usklađivanju kojim se također zahtijeva EU izjava o sukladnosti, sastavlja se jedinstvena EU izjava o sukladnosti 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. Za oznaku sukladnosti CE vrijede opća načela utvrđena u članku 30. Uredbe (EZ) br. 765/2008.

2. 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.

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.

[izbrisano]

Članak 51.

Registracija relevantnih operatera i visokorizičnih UI sustava navedenih u Prilogu III.

1. Prije stavljanja visokorizičnog UI sustava navedenog u Prilogu III. na tržište ili u uporabu, uz iznimku visokorizičnih UI sustava iz točaka 1., 6. i 7. Priloga III. u područjima kaznenog progona, migracija, azila i upravljanja nadzorom državne granice te visokorizičnih UI sustava iz točke 2. Priloga III., dobavljač i, ako je primjenjivo, ovlašteni zastupnik registriraju se u bazi podataka EU-a iz članka 60. Dobavljač ili, ako je primjenjivo, ovlašteni zastupnik u toj bazi podataka registrira i svoje sustave.

2. Prije uporabe visokorizičnog UI sustava navedenog u Prilogu III. korisnici visokorizičnih UI sustava koji su tijela javne vlasti, javne agencije ili javna tijela ili pak subjekti koji djeluju u njihovo ime registriraju se u bazi podataka EU-a iz članka 60. i odabiru sustav koji namjeravaju upotrebljavati.

   Obveze utvrđene u prethodnom podstavku ne primjenjuju se na tijela vlasti, agencije ili druga tijela iz područja kaznenog progona, nadzora državne granice, imigracija ili azila, kao ni na tijela vlasti, agencije ili druga tijela koji upotrebljavaju visokorizične UI sustave iz točke 2. Priloga III. ni na subjekte koji djeluju u njihovo ime.

GLAVA IV.

OBVEZE U POGLEDU TRANSPARENTNOSTI ZA DOBAVLJAČE I KORISNIKE ODREĐENIH UI SUSTAVA

Članak 52.

Obveze u pogledu transparentnosti za dobavljače i korisnike određenih UI sustava

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 sa stajališta razmjerno dobro informiranog, pronicljivog i opreznog pojedinca, uzimajući u obzir okolnosti i kontekst uporabe. Ta se obveza ne primjenjuje na UI sustave koji su zakonski odobreni za otkrivanje, sprečavanje, istragu i kazneni progon kaznenih djela, podložno odgovarajućim zaštitnim mjerama za prava i slobode trećih strana, osim ako su ti sustavi dostupni javnosti za prijavu kaznenog djela.

2. Korisnici 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 odobreni za otkrivanje, sprečavanje i istragu kaznenih djela, podložno odgovarajućim zaštitnim mjerama za prava i slobode trećih strana.

2.a Korisnici sustava za prepoznavanje emocija informiraju pojedince koji su izloženi tom sustavu o njegovu radu. Ta se obveza ne primjenjuje na UI sustave za prepoznavanje emocija koji su zakonski odobreni za otkrivanje, sprečavanje i istragu kaznenih djela, podložno odgovarajućim zaštitnim mjerama za prava i slobode trećih strana.

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 dotična upotreba zakonski odobrena za otkrivanje, sprečavanje, istragu i kazneni progon kaznenih djela ili ako je sadržaj naočigled dio kreativnog, satiričkog, umjetničkog ili fiktivnog rada ili programa, podložno odgovarajućim zaštitnim mjerama za prava i slobode trećih strana.

3.a Informacije iz stavaka od 1. do 3. pojedincima se pružaju na jasan i raspoznatljiv način najkasnije u trenutku prve interakcije ili izloženosti.

4. Stavci 1., 2., 2.a, 3. i 3.a ne utječu na zahtjeve i obveze iz glave III. ove Uredbe i njima se ne dovode u pitanje druge obveze u pogledu transparentnosti za korisnike UI sustava utvrđene u pravu Unije ili nacionalnom pravu.

GLAVA V.

MJERE ZA POTPORU INOVACIJAMA

Članak 53.

Regulatorna izolirana okruženja za umjetnu inteligenciju

–1.a Nacionalna nadležna tijela mogu uspostaviti regulatorna izolirana okruženja za umjetnu inteligenciju namijenjena za razvoj, treniranje, testiranje i validaciju inovativnih UI sustava pod izravnim nadzorom, vodstvom i potporom nacionalnog nadležnog tijela prije nego što se ti sustavi stave na tržište ili u uporabu. Takva regulatorna izolirana okruženja mogu uključivati testiranje u stvarnim uvjetima pod nadzorom nacionalnih nadležnih tijela.

–1.b [izbrisano]

–1.c Nacionalna nadležna tijela prema potrebi surađuju s drugim relevantnim tijelima i mogu dopustiti sudjelovanje drugih aktera iz ekosustava umjetne inteligencije.

–1.d Ovaj članak ne utječe na druga regulatorna izolirana okruženja uspostavljena na temelju nacionalnog prava ili prava Unije, među ostalim u slučajevima kada su proizvodi ili usluge koji se u njima testiraju povezani s uporabom inovativnih UI sustava. Države članice osiguravaju odgovarajuću razinu suradnje između tijela koja nadziru ta druga izolirana okruženja i nacionalnih nadležnih tijela.

1. [izbrisano]

1.a [izbrisano]

1.b Uspostavom regulatornih izoliranih okruženja za umjetnu inteligenciju na temelju ove Uredbe nastoji se doprinijeti jednom ili više sljedećih ciljeva:

a) poticanju inovacija i konkurentnosti te olakšavanju razvoja ekosustava umjetne inteligencije;
b) olakšavanju i ubrzavanju pristupa UI sustavâ tržištu Unije, posebno ako su njihovi dobavljači mala i srednja poduzeća (MSP-ovi), uključujući *start-up* poduzeća;
c) poboljšanju pravne sigurnosti i razmjeni najbolje prakse putem suradnje s tijelima koja sudjeluju u regulatornom izoliranom okruženju za umjetnu inteligenciju s ciljem osiguravanja buduće usklađenosti s ovom Uredbom i, prema potrebi, drugim zakonodavstvom Unije i država članica;
d) regulatornom učenju koje se temelji na dokazima.

2. [izbrisano]

2.a Pristup regulatornim izoliranim okruženjima za umjetnu inteligenciju imaju svi dobavljači ili potencijalni dobavljači UI sustava koji ispunjavaju kriterije prihvatljivosti i kriterije za odabir iz stavka 6. točke (a) i koje su odabrala nacionalna nadležna tijela na temelju postupka odabira iz stavka 6. točke (b). Dobavljači ili potencijalni dobavljači mogu se prijaviti i u partnerstvu s korisnicima ili bilo kojom drugom relevantnom trećom stranom.

Sudjelovanje u regulatornom izoliranom okruženju za umjetnu inteligenciju ograničeno je na razdoblje koje je primjereno složenosti i opsegu projekta. Nacionalno nadležno tijelo može produljiti to razdoblje.

Sudjelovanje u regulatornom izoliranom okruženju za umjetnu inteligenciju temelji se na posebnom planu iz stavka 6. ovog članka, koji dogovaraju sudionici i nacionalna nadležna tijela, ovisno o slučaju.

3. Sudjelovanje u regulatornom izoliranom okruženju za umjetnu inteligenciju ne utječe na nadzorne i korektivne ovlasti tijela koja nadziru to okruženje. Ta tijela izvršavaju svoje nadzorne ovlasti na fleksibilan način, u granicama relevantnog zakonodavstva, i primjenjuju svoje diskrecijske ovlasti pri provedbi pravnih odredaba za određeni projekt u izoliranom okruženju za umjetnu inteligenciju, s ciljem podupiranja inovacija u području umjetne inteligencije u Uniji.

Pod uvjetom da sudionici poštuju plan izoliranog okruženja i uvjete sudjelovanja iz stavka 6. točke (c) te u dobroj vjeri slijede smjernice nadležnih tijela, nadležna tijela ne izriču administrativne kazne zbog kršenja primjenjivog zakonodavstva Unije ili države članice koje se odnosi na UI sustav koji se nadzire u izoliranom okruženju, što uključuje i odredbe ove Uredbe.

4. Sudionici na temelju primjenjivog zakonodavstva Unije i država članica o odgovornosti ostaju odgovorni za svu štetu prouzročenu tijekom njihova sudjelovanja u regulatornom izoliranom okruženju za umjetnu inteligenciju.

4.a Na zahtjev dobavljača ili potencijalnog dobavljača UI sustava nacionalno nadležno tijelo dostavlja, ako je to primjenjivo, pisani dokaz o aktivnostima koje su uspješno provedene u izoliranom okruženju. Nacionalno nadležno tijelo dostavlja i završno izvješće koje sadržava pojedinosti o aktivnostima provedenima u izoliranom okruženju te povezanim rezultatima i ishodima učenja. Tijela za nadzor tržišta ili prijavljena tijela, ovisno o slučaju, mogla bi takav pisani dokaz i završno izvješće uzeti u obzir u kontekstu postupaka ocjenjivanja sukladnosti ili provjera u okviru nadzora tržišta.

Podložno odredbama o povjerljivosti iz članka 70. i uz suglasnost sudionika izoliranog okruženja, Europska komisija i Odbor za umjetnu inteligenciju mogu ostvariti uvid u završna izvješća i prema potrebi ih uzeti u obzir pri izvršavanju svojih zadaća na temelju ove Uredbe. Ako se sudionik i nacionalno nadležno tijelo izričito dogovore o tome, završno izvješće može biti objavljeno na jedinstvenoj informacijskoj platformi iz članka 55. stavka 3. točke (b).

4.b Regulatorna izolirana okruženja za umjetnu inteligenciju projektiraju se i provode tako da se njima olakšava prekogranična suradnja među nacionalnim nadležnim tijelima, ako je to relevantno.

5. Nacionalna nadležna tijela objavljuju godišnja izvješća o provedbi regulatornih izoliranih okruženja za umjetnu inteligenciju, koja sadržavaju dobre primjere iz prakse, stečena iskustva i preporuke za uspostavu tih okruženja, te, prema potrebi, o primjeni ove Uredbe i drugog zakonodavstva Unije koje se nadzire u izoliranom okruženju. Ta godišnja izvješća podnose se Odboru za umjetnu inteligenciju, koji objavljuje sažetak svih dobrih primjera iz prakse, stečenih iskustava i preporuka. Ta obveza objave godišnjih izvješća ne obuhvaća osjetljive operativne podatke u vezi s aktivnostima tijela kaznenog progona, tijela za nadzor granica, tijela za imigraciju ili tijela za azil. Komisija i Odbor za umjetnu inteligenciju ta godišnja izvješća prema potrebi uzimaju u obzir pri izvršavanju svojih zadaća na temelju ove Uredbe.

5.b Komisija osigurava da su informacije o regulatornim izoliranim okruženjima za umjetnu inteligenciju, među ostalim o onima uspostavljenima na temelju ovog članka, dostupne putem jedinstvene informacijske platforme iz članka 55. stavka 3. točke (b).

6. Modaliteti i uvjeti uspostave i rada regulatornih izoliranih okruženja za umjetnu inteligenciju na temelju ove Uredbe utvrđuju se provedbenim aktima u skladu s postupkom ispitivanja iz članka 74. stavka 2.

Tim modalitetima i uvjetima u što većoj mjeri podupire se fleksibilnost nacionalnih nadležnih tijela u uspostavi regulatornih izoliranih okruženja za umjetnu inteligenciju i upravljanju njima, potiču se inovacije i regulatorno učenje te se osobito uzimaju u obzir posebne okolnosti i kapaciteti MSP-ova koji sudjeluju u njima, što uključuje i *start-up* poduzeća.

Ti provedbeni akti sadržavaju zajednička glavna načela o sljedećim pitanjima:

a) prihvatljivosti i odabiru sudionika u regulatornom izoliranom okruženju za umjetnu inteligenciju;
b) postupku za provedbu, praćenje i obustavu regulatornog izoliranog okruženja za umjetnu inteligenciju te za sudjelovanje u njemu i izlazak iz njega, što uključuje plan izoliranog okruženja i završno izvješće;
c) uvjetima koji se primjenjuju na sudionike.

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

Članak 54.

Daljnja obrada osobnih podataka za razvoj određenih UI sustava od javnog interesa u regulatornom izoliranom okruženju za umjetnu inteligenciju

1. Osobni podaci koji su u regulatornom izoliranom okruženju za umjetnu inteligenciju zakonito prikupljeni u druge svrhe mogu se obrađivati za potrebe razvoja, testiranja i treniranja inovativnih UI sustava u izoliranom okruženju pod sljedećim kumulativnim uvjetima:

   (a) inovativne UI sustave razvija tijelo javne vlasti ili neka druga fizička ili pravna osoba koja posluje sukladno javnom pravu ili privatnom pravu, i to u svrhu zaštite znatnog javnog interesa, u jednom ili više sljedećih područja:

      i. [izbrisano]

      ii. javna sigurnost i zdravlje, uključujući prevenciju, kontrolu i liječenje bolesti te poboljšanje zdravstvenih sustava;

      iii. zaštita okoliša i poboljšanje kvalitete okoliša, uključujući zelenu tranziciju, ublažavanje klimatskih promjena i prilagodbu klimatskim promjenama;

      iv. energetska održivost, promet i mobilnost;

      v. učinkovitost i kvaliteta javne uprave i javnih usluga;

      vi. kibersigurnost i otpornost kritične infrastrukture;

   (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 može utvrditi mogu li se tijekom eksperimentiranja u izoliranom okruženju pojaviti bilo kakvi veliki rizici za prava i slobode ispitanika, kako je navedeno u članku 35. Uredbe (EU) 2016/679 i u članku 39. Uredbe (EU) 2018/1725, kao i mehanizmi za odgovor kojima se mogu brzo smanjiti ti rizici 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) druge strane koje nisu sudionici u izoliranom okruženju ne smiju prenositi i prosljeđivati osobne podatke koji se obrađuju niti im na drugi način pristupati, osim ako se to odvija u skladu s Uredbom (EU) 2016/679 ili, ako je primjenjivo, Uredbom 2018/725 i svi su sudionici na to pristali;

(f) svaka obrada osobnih podataka u kontekstu izoliranog okruženja ne utječe na primjenu pravâ ispitanika kako su predviđena pravom Unije o zaštiti osobnih podataka, a posebno člankom 22. Uredbe (EU) 2016/679 i člankom 24. Uredbe (EU) 2018/1725;

(g) svi osobni podaci koji se obrađuju u kontekstu izoliranog okruženja zaštićeni su odgovarajućim tehničkim i organizacijskim mjerama i brišu se nakon završetka sudjelovanja u izoliranom okruženju ili završetka razdoblja čuvanja osobnih podataka;

(h) evidencija obrade osobnih podataka u kontekstu izoliranog okruženja čuva se tijekom trajanja sudjelovanja u izoliranom okruženju, osim ako je pravom Unije ili nacionalnim pravom predviđeno drukčije;

(i) u sklopu tehničke dokumentacije iz Priloga IV. zajedno s rezultatima testiranja čuva se potpuni i detaljni opis procesa i temelja treniranja, testiranja i validacije dotičnog UI sustava;

(j) na internetskim stranicama nadležnih tijela objavljuju se kratak sažetak projekta umjetne inteligencije razvijenog u izoliranom okruženju te njegovi ciljevi i očekivani rezultati. Ta obveza ne obuhvaća osjetljive operativne podatke u vezi s aktivnostima tijela kaznenog progona, tijela za nadzor granica, tijela za imigraciju ili tijela za azil.

1.a U svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, što uključuje mjere za zaštitu od prijetnji javnoj sigurnosti i sprečavanje tih prijetnji, pod kontrolom i odgovornošću tijela kaznenog progona, obrada osobnih podataka u regulatornim izoliranim okruženjima za umjetnu inteligenciju temelji se na pravu određene države članice ili Unije i podliježe kumulativnim uvjetima iz stavka 1.

2. Stavkom 1. ne dovodi se u pitanje zakonodavstvo Unije ili država članica kojim se utvrđuje osnova za obradu osobnih podataka koja je potrebna u svrhu razvoja, testiranja i treniranja inovativnih UI sustava ili bilo koja druga pravna osnova, u skladu s pravom Unije o zaštiti osobnih podataka.

Članak 54.a

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

1. Testiranje UI sustavâ u stvarnim uvjetima izvan regulatornih izoliranih okruženja za umjetnu inteligenciju mogu provoditi dobavljači ili potencijalni dobavljači visokorizičnih UI sustava navedenih u Prilogu III. u skladu s odredbama ovog članka i planom testiranja u stvarnim uvjetima iz ovog članka.

Pojedinosti plana testiranja u stvarnim uvjetima utvrđuju se u provedbenim aktima koje Komisija donosi u skladu s postupkom ispitivanja iz članka 74. stavka 2.

Ovom se odredbom ne dovodi u pitanje zakonodavstvo Unije ili država članica o testiranju visokorizičnih UI sustava povezanih s proizvodima obuhvaćenima zakonodavstvom iz Priloga II. u stvarnim uvjetima.

2. Dobavljači ili potencijalni dobavljači mogu provesti testiranje visokorizičnih UI sustava iz Priloga III. u stvarnim uvjetima samostalno ili u partnerstvu s jednim ili više potencijalnih korisnika u bilo kojem trenutku prije stavljanja UI sustava na tržište ili u uporabu.

3. Testiranjem visokorizičnih UI sustava u stvarnim uvjetima na temelju ovog članka ne dovodi se u pitanje etičko preispitivanje koje može biti potrebno na temelju nacionalnog prava ili prava Unije.

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

(a) dobavljač ili potencijalni dobavljač izradio je plan testiranja u stvarnim uvjetima i dostavio ga tijelima za nadzor tržišta u državama članicama u kojima će provesti testiranje u stvarnim uvjetima;

(b) tijela za nadzor tržišta u državama članicama u kojima će se provesti testiranje u stvarnim uvjetima nisu uložila prigovor na testiranje u roku od 30 dana od podnošenja tog plana;

(c) dobavljač ili potencijalni dobavljač UI sustavâ, uz iznimku visokorizičnih UI sustava iz točaka 1., 6. i 7. Priloga III. u područjima kaznenog progona, migracija, azila i upravljanja nadzorom državne granice te visokorizičnih UI sustava iz točke 2. Priloga III., testiranje u stvarnim uvjetima registrirao je u bazi podataka EU-a iz članka 60. stavka 5.a, pri čemu je naveo jedinstveni identifikacijski broj na razini Unije i informacije iz Priloga VIII.a;

(d) dobavljač ili potencijalni dobavljač koji provodi testiranje u stvarnim uvjetima ima poslovni nastan u Uniji ili je za potrebe testiranja u stvarnim uvjetima imenovao pravnog zastupnika s poslovnim nastanom u Uniji;

(e) podaci prikupljeni i obrađeni u svrhu testiranja u stvarnim uvjetima ne prenose se u zemlje izvan Unije, osim ako se prijenosom i obradom pružaju zaštitne mjere istovjetne onima koje su predviđene na temelju prava Unije;

(f) testiranje u stvarnim uvjetima ne traje dulje nego što je potrebno za postizanje njegovih ciljeva, a u svakom slučaju ne dulje od 12 mjeseci;

(g) osobe koje pripadaju ranjivim skupinama zbog svoje dobi, fizičkog invaliditeta ili intelektualnih teškoća primjereno su zaštićene;

(h) [izbrisano]

(i) ako dobavljač ili potencijalni dobavljač organizira testiranje u stvarnim uvjetima u suradnji s jednim ili više potencijalnih korisnika, potonji su obaviješteni o svim aspektima testiranja koji su relevantni za njihovu odluku o sudjelovanju i pružene su im relevantne upute o tome kako upotrebljavati UI sustav iz članka 13.; dobavljač ili potencijalni dobavljač i korisnik ili korisnici sklapaju sporazum kojim se određuju njihove uloge i odgovornosti kako bi se osigurala usklađenost s odredbama za testiranje u stvarnim uvjetima na temelju ove Uredbe i drugog primjenjivog zakonodavstva Unije i država članica;

(j) ispitanici koji sudjeluju u testiranju u stvarnim uvjetima dali su informirani pristanak u skladu s člankom 54.b ili, u slučaju tijela kaznenog progona, ako bi traženje informiranog pristanka spriječilo testiranje UI sustava, sâmo testiranje i ishod testiranja u stvarnim uvjetima nemaju negativan učinak na ispitanika;

(k) testiranje u stvarnim uvjetima učinkovito nadzire dobavljač ili potencijalni dobavljač i korisnik ili korisnici s osobama koje imaju odgovarajuće kvalifikacije u relevantnom području te potrebne kapacitete, osposobljavanje i ovlasti za obavljanje svojih zadaća;

(l) predviđanja, preporuke ili odluke UI sustava mogu se učinkovito poništiti ili zanemariti.

5. Svaki ispitanik koji sudjeluje u testiranju u stvarnim uvjetima ili, prema potrebi, njegov zakonito imenovani zastupnik mogu se povući iz testiranja u bilo kojem trenutku povlačenjem svojeg informiranog pristanka, a da to nema nikakve negativne posljedice i da pritom ne moraju pružiti obrazloženje. Povlačenje informiranog pristanka ne utječe na aktivnosti koje su već provedene ni na upotrebu podataka dobivenih na temelju informiranog pristanka prije njegova povlačenja.

6. Svaki ozbiljni incident utvrđen tijekom testiranja u stvarnim uvjetima prijavljuje se nacionalnom tijelu za nadzor tržišta u skladu s člankom 62. ove Uredbe. Dobavljač ili potencijalni dobavljač odmah donosi mjere ublažavanja ili, ako to nije moguće, obustavlja testiranje u stvarnim uvjetima dok se takve mjere ublažavanja ne provedu ili ga u suprotnom prekida. Dobavljač ili potencijalni dobavljač uspostavlja postupak za promptni opoziv UI sustava nakon takvog završetka testiranja u stvarnim uvjetima.

7. Dobavljači ili potencijalni dobavljači obavješćuju nacionalno tijelo za nadzor tržišta u državi članici odnosno državama članicama u kojima se provodi testiranje u stvarnim uvjetima o obustavi ili završetku testiranja u stvarnim uvjetima i konačnim ishodima.

8. Dobavljač i potencijalni dobavljač odgovorni su na temelju primjenjivog zakonodavstva Unije i država članica o odgovornosti za svu štetu prouzročenu tijekom njihova sudjelovanja u testiranju u stvarnim uvjetima.

Članak 54.b

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

1. Za potrebe testiranja u stvarnim uvjetima na temelju članka 54.a ispitanik dobrovoljno daje informirani pristanak prije svojeg sudjelovanja u takvom testiranju i nakon što je propisno obaviješten s pomoću jezgrovitih, jasnih, relevantnih i razumljivih informacija o sljedećem:

i. prirodi i ciljevima testiranja u stvarnim uvjetima i mogućih neugodnosti koje mogu biti povezane sa sudjelovanjem ispitanika;

ii. uvjetima pod kojima će se provoditi testiranje u stvarnim uvjetima, uključujući očekivano trajanje sudjelovanja ispitanika;

iii. pravima i jamstvima ispitanika u pogledu njegova sudjelovanja, osobito o njegovu pravu na odbijanje sudjelovanja u testiranju u stvarnom vremenu i pravu na povlačenje iz njega u svakom trenutku, a da to nema nikakve negativne posljedice i da pritom ne mora pružiti obrazloženje;

iv. načinima podnošenja zahtjeva za poništenje ili zanemarivanje predviđanjâ, preporuka ili odluka UI sustava;

v. jedinstvenom identifikacijskom broju na razini Unije za testiranje u stvarnim uvjetima u skladu s člankom 54.a stavkom 4. točkom (c) i kontaktnim podacima dobavljača ili njegova pravnog zastupnika od kojeg se mogu dobiti dodatne informacije.

2. Informirani pristanak mora biti datiran i dokumentiran, a primjerak se daje ispitaniku ili njegovu pravnom zastupniku.

Članak 55.

Mjere potpore za operatere, posebno za MSP-ove, uključujući start-up poduzeća

1. Države članice poduzimaju sljedeće mjere:

(a) MSP-ovima, uključujući *start-up* poduzeća, daju prioritetni pristup regulatornim izoliranim okruženjima za umjetnu inteligenciju u onoj mjeri u kojoj ispunjavaju uvjete prihvatljivosti i odabira;

(b) organiziraju specifične aktivnosti podizanja svijesti i osposobljavanja o primjeni ove Uredbe prilagođene potrebama MSP-ova, uključujući *start-up* poduzeća, te, prema potrebi, lokalnih tijela javne vlasti;

(c) prema potrebi uspostavljaju namjenski kanal za komunikaciju s MSP-ovima, uključujući *start-up* poduzeća, te, prema potrebi, s lokalnim tijelima javne vlasti, radi pružanja savjeta i odgovaranja na upite u vezi s provedbom ove Uredbe, među ostalim u pogledu sudjelovanja u regulatornim izoliranim okruženjima za umjetnu inteligenciju.

2. Pri određivanju naknada za ocjenjivanje sukladnosti na temelju članka 43. uzimaju se u obzir specifični interesi i potrebe malih i srednjih poduzeća dobavljača, uključujući *start-up* poduzeća, a naknade se smanjuju razmjerno njihovoj veličini, veličini tržišta i drugim relevantnim pokazateljima.

3. Komisija poduzima sljedeće mjere:

(a) na zahtjev Odbora za umjetnu inteligenciju osigurava standardizirane predloške za područja obuhvaćena ovom Uredbom;

(b) razvija i održava jedinstvenu informacijsku platformu na kojoj se svim operaterima diljem Unije pružaju informacije u vezi s ovom Uredbom koje su jednostavne za uporabu;

(c) organizira odgovarajuće komunikacijske kampanje za podizanje svijesti o obvezama koje proizlaze iz ove Uredbe;

(d) evaluira i promiče konvergenciju najboljih praksi u postupcima javne nabave u vezi s UI sustavima.

Članak 55.a

Odstupanja za specifične operatere

1. Obveze utvrđene u članku 17. ove Uredbe ne primjenjuju se na mikropoduzeća kako su definirana u članku 2. stavku 3. Priloga Preporuci Komisije 2003/361/EZ o definiciji mikropoduzeća te malih i srednjih poduzeća, pod uvjetom da ta poduzeća nemaju partnerska poduzeća ili povezana poduzeća kako su definirana u članku 3. istog Priloga.

2. Stavak 1. ne tumači se kao izuzimanje tih operatera od ispunjavanja bilo kojih drugih zahtjeva i obveza utvrđenih u ovoj Uredbi, uključujući one utvrđene u člancima 9., 61. i 62.

3. Zahtjevi i obveze za UI sustave opće namjene utvrđeni u članku 4.b ne primjenjuju se na mikropoduzeća te mala i srednja poduzeća, pod uvjetom da ta poduzeća nemaju partnerska poduzeća ili povezana poduzeća kako su definirana u članku 3. Priloga Preporuci Komisije 2003/361/EZ o definiciji mikropoduzeća te malih i srednjih poduzeća.

GLAVA VI.

UPRAVLJANJE

POGLAVLJE 1.

EUROPSKI ODBOR ZA UMJETNU INTELIGENCIJU

Članak 56.

Osnivanje i struktura Europskog odbora za umjetnu inteligenciju

1. Osniva se „Europski odbor za umjetnu inteligenciju” („Odbor”).

2. Odbor se sastoji od jednog predstavnika iz svake države članice. Europski nadzornik za zaštitu podataka sudjeluje u njemu kao promatrač. Komisija također prisustvuje sastancima Odbora bez sudjelovanja u glasovanju.

   Odbor može na pojedinačnoj osnovi pozvati druga nacionalna ili Unijina tijela ili stručnjake na sastanke ako su pitanja o kojima se raspravlja relevantna za njih.

2.a Svakog predstavnika imenuje njegova država članica na razdoblje od tri godine, koje se može jednom produljiti.

2.aa Države članice osiguravaju da njihovi predstavnici u Odboru:

   i. posjeduju relevantne kompetencije i ovlasti u svojoj državi članici kako bi aktivno doprinosili ostvarivanju zadaća Odbora iz članka 58.;

   ii. određeni su kao jedinstvena kontaktna točka u odnosu na Odbor i, prema potrebi, uzimajući u obzir potrebe država članica, kao jedinstvena kontaktna točka za dionike;

iii. ovlašteni su olakšavati dosljednost i koordinaciju među nacionalnim nadležnim tijelima u svojoj državi članici u pogledu provedbe ove Uredbe, među ostalim prikupljanjem relevantnih podataka i informacija u svrhu ispunjavanja svojih zadaća u Odboru.

3. Imenovani predstavnici država članica donose poslovnik Odbora dvotrećinskom većinom.

Poslovnikom se posebno utvrđuju postupci za postupak odabira, trajanje mandata i specifikacije zadaća predsjednika, načini glasovanja te organizacija aktivnosti Odbora i njegovih podskupina.

Odbor osniva stalnu podskupinu koja služi kao platforma za dionike za savjetovanje Odbora o svim pitanjima povezanima s provedbom ove Uredbe, među ostalim o pripremi provedbenih i delegiranih akata. U tu se svrhu organizacije koje zastupaju interese dobavljača i korisnika UI sustava, uključujući MSP-ove i *start-up* poduzeća, kao i organizacije civilnog društva, predstavnici pogođenih osoba, istraživači, organizacije za normizaciju, prijavljena tijela te laboratoriji i objekti za testiranje i eksperimentiranje pozivaju na sudjelovanje u toj podskupini. Odbor uspostavlja dvije stalne podskupine kako bi osigurao platformu za suradnju i razmjenu između tijelâ za nadzor tržišta i tijela koja provode prijavljivanje o pitanjima koja se odnose na nadzor tržišta odnosno na prijavljena tijela.

Odbor prema potrebi može osnovati druge stalne ili privremene podskupine u svrhu razmatranja konkretnih pitanja. Prema potrebi, dionici iz prethodnog podstavka mogu biti pozvani u takve podskupine ili na posebne sastanke tih podskupina u svojstvu promatrača.

3.a Odbor je organiziran i djeluje tako da čuva objektivnost i nepristranost svojih aktivnosti.

4. Odborom predsjeda jedan od predstavnika država članica. Na zahtjev predsjednika Komisija saziva sastanke i priprema dnevni red u skladu sa zadaćama Odbora na temelju ove Uredbe i njegovim poslovnikom. Komisija pruža administrativnu i analitičku podršku aktivnostima Odbora na temelju ove Uredbe.

Članak 57.
[izbrisano]

Članak 58.
Zadaće Odbora

Odbor savjetuje Komisiju i države članice i pomaže im kako bi se olakšala dosljedna i učinkovita primjena ove Uredbe. U tu svrhu Odbor posebno može:

(a) prikupljati i razmjenjivati stručno znanje i najbolje primjere iz prakse među državama članicama;

(b) doprinositi usklađivanju administrativnih praksi u državama članicama, među ostalim u pogledu odstupanja od postupaka ocjenjivanja sukladnosti iz članka 47., funkcioniranja regulatornih izoliranih okruženja i testiranja u stvarnim uvjetima iz članaka 53., 54. i 54.a;

(c) na zahtjev Komisije ili na vlastitu inicijativu izdavati preporuke i pisana mišljenja o svim relevantnim pitanjima povezanima s provedbom ove Uredbe te njezinom dosljednom i učinkovitom primjenom, među ostalim:

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.

(d) savjetovati Komisiju o mogućoj potrebi za izmjenom Priloga III. u skladu s člancima 4. i 7., uzimajući u obzir relevantne dostupne dokaze i najnoviji tehnološki razvoj;

(e) savjetovati Komisiju tijekom pripreme delegiranog ili provedbenog akta u skladu s ovom Uredbom;

(f) surađivati, prema potrebi, s relevantnim tijelima EU-a, stručnim skupinama i mrežama, posebno u područjima sigurnosti proizvoda, kibersigurnosti, tržišnog natjecanja, digitalnih i medijskih usluga, financijskih usluga, kriptovaluta, zaštite potrošača te zaštite podataka i temeljnih prava;

(g) doprinositi i pružati odgovarajuće savjete Komisiji u razvoju smjernica iz članka 58.a ili zatražiti razvoj takvih smjernica;

(h) pružati pomoć pomoći tijelima za nadzor tržišta i, u suradnji s dotičnim tijelima za nadzor tržišta i uz njihovu suglasnost, promicati i podupirati prekogranične istrage nadzora tržišta, među ostalim u pogledu pojave rizika sustavne prirode koji mogu proizlaziti iz UI sustava;

(i) doprinositi procjeni potreba za osposobljavanjem osoblja država članica koje sudjeluje u provedbi ove Uredbe;

(j) savjetovati Komisiju o međunarodnim pitanjima u vezi s umjetnom inteligencijom.

POGLAVLJE 1.A

SMJERNICE KOMISIJE

Članak 58.a

Smjernice Komisije o provedbi ove Uredbe

1. Na zahtjev država članica ili Odbora ili na vlastitu inicijativu Komisija izdaje smjernice o praktičnoj provedbi ove Uredbe, a posebno o:

   i. primjeni zahtjeva iz članaka od 8. do 15.;

   ii. zabranjenim praksama iz članka 5.;

   iii. praktičnoj provedbi odredaba povezanih s bitnom izmjenom;

   iv. praktičnoj provedbi jedinstvenih uvjeta iz članka 6. stavka 3., uključujući primjere povezane s visokorizičnim UI sustavima iz Priloga III.;

   v. praktičnoj provedbi obveza u pogledu transparentnosti utvrđenih u članku 52.;

   vi. odnosu ove Uredbe s drugim relevantnim zakonodavstvom Unije, među ostalim u pogledu dosljednosti u njihovoj provedbi.

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

POGLAVLJE 2.

NACIONALNA NADLEŽNA TIJELA

Članak 59.

Imenovanje nacionalnih nadležnih tijela:

1. [izbrisano]

2. Za potrebe ove Uredbe svaka država članica osniva ili imenuje nacionalnim nadležnim tijelima barem jedno tijelo koje provodi prijavljivanje i barem jedno tijelo za nadzor tržišta. Ta nacionalna nadležna tijela organiziraju se tako da se zajamče načela objektivnosti i nepristranosti njihovih aktivnosti i zadaća. Pod uvjetom da se poštuju ta načela, takve aktivnosti i zadaće može obavljati jedno ili više imenovanih tijela, u skladu s organizacijskim potrebama države članice.

3. Države članice obavješćuju Komisiju o tom imenovanju ili imenovanjima.

4. Države članice osiguravaju da nacionalna nadležna tijela imaju dostatne financijske resurse, tehničku opremu i kvalificirane ljudske resurse za učinkovito obavljanje svojih zadaća na temelju ove Uredbe.

5. Do *[godinu dana nakon stupanja na snagu ove Uredbe]*, a nakon toga šest mjeseci prije roka iz članka 84. stavka 2., države članice obavješćuju Komisiju o stanju financijskih resursa, tehničke opreme i ljudskih resursa nacionalnih nadležnih tijela uz procjenu njihove primjerenosti. 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 savjete o provedbi ove Uredbe, što obuhvaća i savjete prilagođene malim i srednjim poduzećima dobavljačima, uključujući *start-up* poduzeća. 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 na temelju tog zakonodavstva 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 VISOKORIZIČNE UI SUSTAVE NAVEDENE U PRILOGU III.

Članak 60.

Baza podataka EU-a za visokorizične UI sustave navedene u Prilogu III.

1. Komisija u suradnji s državama članicama uspostavlja i vodi bazu podataka EU-a koja sadržava informacije iz stavka 2. o relevantnim operaterima i visokorizičnim UI sustavima s popisa u Prilogu III. koji su registrirani u skladu s člancima 51. i 54.a. Pri utvrđivanju funkcionalnih specifikacija takve baze podataka Komisija se savjetuje s Odborom za umjetnu inteligenciju.

2. Podatke navedene u Prilogu VIII. dijelu I. u bazu podataka EU-a unose dobavljači, ovlašteni zastupnici i relevantni korisnici, ovisno o slučaju, nakon svoje registracije. Podatke navedene u Prilogu VIII. dijelu II. točkama od 1. do 11. u bazu podataka EU-a unose dobavljači ili, ako je primjenjivo, ovlašteni zastupnik, u skladu s člankom 51. Podaci iz Priloga VIII. dijela II. točke 12. automatski se generiraju u bazi podataka na temelju informacija koje su dostavili relevantni korisnici u skladu s člankom 51. stavkom 2. Podatke navedene u Prilogu VIII.a potencijalni dobavljači ili dobavljači unose u bazu podataka u skladu s člankom 54.a.

3. [izbrisano]

4. Baza podataka EU-a ne sadržava osobne podatke, osim informacija navedenih u Prilogu VIII., i njome se ne dovodi u pitanje članak 70.

5. Komisija je nadzornik baze podataka EU-a. Dobavljačima, potencijalnim dobavljačima i korisnicima stavlja na raspolaganje odgovarajuću tehničku i administrativnu potporu.

5.a Informacije sadržane u bazi podataka EU-a registrirane u skladu s člankom 51. dostupne su javnosti. Informacije registrirane u skladu s člankom 54.a dostupne su samo tijelima za nadzor tržišta i Komisiji, osim ako je potencijalni dobavljači ili dobavljači dao suglasnost da te informacije budu dostupne i javnosti.

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 rizicima visokorizičnog UI sustava.

2. Kako bi dobavljač mogao ocijeniti usklađenost UI sustavâ sa zahtjevima iz glave III. poglavlja 2. tijekom njihova životnog ciklusa, u sustavu praćenja nakon stavljanja na tržište prikupljaju se, dokumentiraju i analiziraju relevantni podaci o sposobnosti visokorizičnih UI sustava, koje mogu dostaviti korisnici ili koji se mogu prikupiti iz drugih izvora. Ta obveza ne obuhvaća osjetljive operativne podatke korisnika UI sustavâ koji su tijela kaznenog progona.

3. Sustav praćenja nakon stavljanja na tržište temelji se na planu praćenja nakon stavljanja na tržište. Plan praćenja nakon stavljanja na tržište dio je tehničke dokumentacije iz Priloga IV. Komisija 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. odjeljka A, ako su sustav i plan praćenja nakon stavljanja na tržište već uspostavljeni na temelju tog zakonodavstva, dokumentacija o planu praćenja nakon stavljanja na tržište smatra se dostatnom pod uvjetom da se upotrebljava predložak iz stavka 3.

Prvi podstavak primjenjuje se i na visokorizične UI sustave iz Priloga III. točke 5. koje na tržište ili u uporabu stavljaju financijske institucije na koje se primjenjuju zahtjevi u pogledu njihova internog upravljanja, mehanizama ili procesa na temelju zakonodavstva Unije o financijskim uslugama.

POGLAVLJE 2.

RAZMJENA INFORMACIJA O OZBILJNIM INCIDENTIMA

Članak 62.

Prijavljivanje ozbiljnih incidenata

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

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

2. Nakon primitka obavijesti o ozbiljnom incidentu iz članka 3. stavka 44. točke (c) relevantno tijelo za nadzor tržišta o tome informira 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 Priloga III. točke 5. koje na tržište ili u uporabu stavljaju dobavljači koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu njihova internog upravljanja, mehanizama ili procesa na temelju zakonodavstva Unije o financijskim uslugama, obavješćivanje o ozbiljnim incidenatima ograničeno je samo na one iz članka 3. stavka 44. točke (c).

4. Za visokorizične UI sustave koji su sigurnosni sastavni dijelovi uređajâ ili su sami uređaji, obuhvaćeni Uredbom (EU) 2017/745 i Uredbom (EU) 2017/746, obavješćivanje o ozbiljnim incidentima ograničava se na one iz članka 3. stavka 44. točke (c) i podnosi se nacionalnom nadležnom tijelu koje su u tu svrhu odabrale države članice u kojima je došlo do tog incidenta.

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 članka 2. ove Uredbe;

   (b) smatra se da svako upućivanje na proizvod na temelju Uredbe (EU) 2019/1020 uključuje sve UI sustave obuhvaćene područjem primjene ove Uredbe.

2. U okviru svojih obveza prijavljivanja na temelju članka 34. stavka 4. Uredbe (EU) 2019/1020 tijela za nadzor tržišta izvješćuju Komisiju o ishodima relevantnih aktivnosti nadzora tržišta na temelju ove Uredbe.

3. Za visokorizične UI sustave povezane s proizvodima na koje se primjenjuju pravni akti navedeni u Prilogu II. odjeljku A, tijelo za nadzor tržišta za potrebe ove Uredbe jest tijelo odgovorno za aktivnosti nadzora tržišta imenovano na temelju tih pravnih akata ili, u opravdanim okolnostima i pod uvjetom da je osigurana koordinacija, drugo relevantno tijelo koje je utvrdila država članica.

Postupci iz članaka 65., 66., 67. i 68. ove Uredbe ne primjenjuju se na UI sustave povezane s proizvodima na koje se primjenjuju pravni akti navedeni u Prilogu II. odjeljku A ako su tim pravnim aktima već predviđeni postupci s istim ciljem. U takvim se slučajevima primjenjuju ti sektorski postupci.

4. Za visokorizične UI sustave koji se stavljaju na tržište, stavljaju u uporabu ili koje upotrebljavaju financijske institucije regulirane zakonodavstvom Unije o financijskim uslugama, tijelo za nadzor tržišta za potrebe ove Uredbe relevantno je nacionalno tijelo odgovorno za financijski nadzor tih institucija na temelju tog zakonodavstva ako su stavljanje na tržište, stavljanje u uporabu ili uporaba UI sustava u izravnoj vezi s pružanjem tih financijskih usluga.

Odstupajući od prethodnog podstavka, u opravdanim okolnostima i pod uvjetom da je osigurana koordinacija, država članica može odrediti drugo relevantno tijelo kao tijelo za nadzor tržišta za potrebe ove Uredbe.

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

5. Za visokorizične UI sustave navedene u točki 1. podtočki (a) ako se ti sustavi upotrebljavaju za potrebe kaznenog progona, i u točkama 6., 7. i 8. Priloga III., države članice za potrebe ove Uredbe kao tijela za nadzor tržišta imenuju ili nacionalna tijela koja nadziru aktivnosti tijela kaznenog progona, tijela za nadzor granica, tijela za imigraciju, tijela za azil ili pravosudna tijela, ili nadležna nadzorna tijela za zaštitu podataka na temelju Direktive (EU) 2016/680 ili Uredbe 2016/679. Aktivnosti nadzora tržišta ni na koji način ne utječu na neovisnost pravosudnih tijela niti na drugi način utječu na njihove aktivnosti kada djeluju u okviru svoje sudske nadležnosti.

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.

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

9. Tijelima za nadzor tržišta odobrava se pristup izvornom kodu visokorizičnog UI sustava na obrazložen zahtjev i samo ako su ispunjeni sljedeći kumulativni uvjeti:

a) pristup izvornom kodu potreban je za ocjenjivanje sukladnosti visokorizičnog UI sustava sa zahtjevima iz glave III. poglavlja 2. i

b) postupci testiranja/revizije i provjera na temelju podataka i dokumentacije koje je dostavio dobavljač iscrpljeni su ili su se pokazali nedostatnima.

10. Sa svim informacijama i svom dokumentacijom koje su tijela za nadzor tržišta dobila postupa se u skladu s obvezama povjerljivosti utvrđenima u članku 70.

11. Pritužbe relevantnom tijelu za nadzor tržišta može podnijeti svaka fizička ili pravna osoba koja ima razloga smatrati da je došlo do kršenja odredaba ove Uredbe.

U skladu s člankom 11. stavkom 3. točkom (e) i člankom 11. stavkom 7. točkom (a) Uredbe (EU) 2019/1020 pritužbe se uzimaju u obzir za potrebe provođenja aktivnosti nadzora tržišta i s njima se postupa u skladu s posebnim postupcima koje su u tu svrhu utvrdila tijela za nadzor tržišta.

Članak 63.a

Nadzor testiranja u stvarnim uvjetima koji provode tijela za nadzor tržišta

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

2. Ako se testiranje u stvarnim uvjetima provodi za UI sustave koji se nadziru u regulatornom izoliranom okruženju za umjetnu inteligenciju na temelju članka 54., tijela za nadzor tržišta provjeravaju usklađenost s odredbama članka 54.a u okviru svoje nadzorne uloge za regulatorno izolirano okruženje za umjetnu inteligenciju. Ta tijela mogu, prema potrebi, dopustiti da dobavljač ili potencijalni dobavljač provodi testiranje u stvarnim uvjetima odstupajući od uvjeta utvrđenih u članku 54.a stavku 4. točkama (f) i (g).

3. Ako su potencijalni dobavljač, dobavljač ili treća stranka obavijestili tijelo za nadzor tržišta o ozbiljnom incidentu ili ono ima drugih razloga vjerovati da uvjeti iz članaka 54.a i 54.b nisu ispunjeni, ono može na svojem državnom području prema potrebi donijeti jednu od sljedećih odluka:

(a) obustaviti ili prekinuti testiranje u stvarnim uvjetima;

(b) zahtijevati od dobavljača ili potencijalnog dobavljača i korisnika (korisnikâ) da izmijene bilo koji aspekt testiranja u stvarnim uvjetima.

4. Ako je tijelo za nadzor tržišta donijelo odluku iz stavka 3. ovog članka ili je izdalo prigovor u smislu članka 54.a stavka 4. točke (b), u odluci ili prigovoru navode se razlozi za njihovo donošenje te načini i uvjeti za osporavanje odluke ili prigovora od strane dobavljača ili potencijalnog dobavljača.

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

Članak 64.

Ovlasti tijela za zaštitu temeljnih prava

1. [izbrisano]

2. [izbrisano]

3. Nacionalna tijela javne vlasti ili javnopravna tijela koja nadziru ili izvršavaju poštovanje obveza na temelju prava Unije kojima se štite temeljna prava, uključujući pravo na nediskriminaciju, u pogledu uporabe visokorizičnih UI sustava iz Priloga III. ovlaštena su zatražiti i pristupiti svoj 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 tih 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 toga 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 na temelju odredaba ovog članka postupa se u skladu s obvezama povjerljivosti utvrđenima u članku 70.

Članak 65.

Postupak za UI sustave koji predstavljaju rizik na nacionalnoj razini

1. UI sustavi koji predstavljaju rizik tumače se kao proizvodi koji predstavljaju rizik definirani u članku 3. točki 19. Uredbe (EU) 2019/1020 s obzirom na rizike za zdravlje ili sigurnost 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 su utvrđeni rizici za temeljna 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 nepotrebne 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 opoziv u roku koji ono 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 bez nepotrebne odgode 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 opoziv. To tijelo bez nepotrebne odgode obavješćuje Komisiju i druge države članice o tim mjerama.

6. Obavijest iz stavka 5. uključuje sve dostupne pojedinosti, posebno informacije 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) nepoštovanje zabrane praksi u području umjetne inteligencije iz članka 5.;

(a) visokorizični 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.

(c) neusklađenost s odredbama iz članka 52.;

(d) neusklađenost UI sustava opće namjene sa zahtjevima i obvezama iz članka 4.a.

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

8. Ako u roku od tri mjeseca od primitka obavijesti navedene 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. Razdoblje iz prve rečenice ovog stavka skraćuje se na 30 dana u slučaju neusklađenosti sa zabranom praksi u području umjetne inteligencije iz članka 5.

9. Tijela za nadzor tržišta svih država članica zatim osiguravaju da se bez nepotrebne odgode poduzmu prikladne restriktivne mjere u odnosu na dotični UI sustav, 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., ili 30 dana u slučaju neusklađenosti sa zabranom praksi u području umjetne inteligencije iz članka 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 nepotrebne odgode započinje savjetovanje s tijelom za nadzor tržišta i operaterom ili operaterima relevantne države članice te evaluira nacionalnu mjeru. Na temelju rezultata te evaluacije Komisija odlučuje je li nacionalna mjera opravdana u roku od devet mjeseci, ili 60 dana u slučaju neusklađenosti sa zabranom praksi u području umjetne inteligencije iz članka 5., počevši od trenutka obavijesti iz članka 65. stavka 5. Dotičnu državu članicu obavješćuje o takvoj odluci. Komisija također obavješćuje sve druge države članice o takvoj odluci.

2. Ako Komisija mjeru koju je poduzelo relevantno tijelo za nadzor tržišta države članice smatra opravdanom, tijela za nadzor tržišta svih država članica bez nepotrebne odgode osiguravaju poduzimanje odgovarajućih restriktivnih mjera u pogledu dotičnog UI sustava, kao što je povlačenje UI sustava s njihova tržišta, te o tome obavješćuju Komisiju. Ako Komisija smatra da je nacionalna mjera neopravdana, tijelo za nadzor tržišta dotične države članice povlači mjeru i o tome obavješćuje Komisiju.

3. Ako se nacionalna mjera smatra opravdanom i ako se neusklađenost UI sustava pripisuje nedostacima u usklađenim normama ili zajedničkim specifikacijama iz članaka 40. i 41. ove Uredbe, Komisija primjenjuje postupak iz članka 11. Uredbe (EU) br. 1025/2012.

Članak 67.

Usklađeni visokorizični UI sustavi ili UI sustavi opće namjene koji prestavljaju rizik

1. Ako tijelo za nadzor tržišta države članice nakon provedene evaluacije na temelju članka 65. ustanovi da visokorizični UI sustav ili UI sustav opće namjene koji je u skladu s ovom Uredbom ipak predstavlja rizik za zdravlje ili sigurnost osoba ili za temeljna prava, 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 opoziv bez nepotrebne odgode u roku koje ono 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 nepotrebne odgode započinje savjetovanje s dotičnim 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 dotičnim državama članicama i obavješćuje sve druge države članice.

Članak 68.

Formalna neusklađenost

1. Tijelo za nadzor tržišta države članice zahtijeva od relevantnog dobavljača da otkloni neusklađenost u roku koji ono propiše 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 opoziv ili povlačenje s tržišta.

Članak 68.a

Objekti Unije za ispitivanje u području umjetne inteligencije

1. Komisija imenuje jedan ili više objekata Unije za ispitivanje u području umjetne inteligencije u skladu s člankom 21. Uredbe (EU) 1020/2019.

2. Ne dovodeći u pitanje aktivnosti objekata Unije za ispitivanje iz članka 21. stavka 6. Uredbe (EU) 1020/2019, objekti Unije za testiranje iz stavka 1. pružaju i neovisne tehničke ili znanstvene savjete na zahtjev Odbora ili tijelâ za nadzor tržišta.

Članak 68.b

Središnja skupina neovisnih stručnjaka

1. Na zahtjev Odbora za umjetnu inteligenciju Komisija provedbenim aktom donosi odredbe o osnivanju, održavanju i financiranju središnje skupine neovisnih stručnjaka za potporu provedbenim aktivnostima na temelju ove Uredbe.

2. Komisija odabire stručnjake i uključuje ih u središnju skupinu na temelju najnovijeg znanstvenog ili tehničkog stručnog znanja u području umjetne inteligencije, uzimajući u obzir tehnička područja obuhvaćena zahtjevima i obvezama iz ove Uredbe i aktivnosti tijelâ za nadzor tržišta u skladu s člankom 11. Uredbe (EU) 1020/2019. Komisija određuje broj stručnjaka u skupini u skladu s potrebama.

3. Stručnjaci mogu imati sljedeće zadaće:

(a) savjetovati i podupirati rad tijela za nadzor tržišta na njihov zahtjev;

(b) podupirati prekogranične istrage nadzora tržišta iz članka 58. točke (h), ne dovodeći u pitanje ovlasti tijelâ za nadzor tržišta;

(c) savjetovati i podupirati Komisiju pri izvršavanju njezinih dužnosti u kontekstu zaštitne klauzule na temelju članka 66.

4. Stručnjaci svoje zadaće obavljaju nepristrano i objektivno te osiguravaju povjerljivost informacija i podataka dobivenih pri obavljanju svojih zadaća i aktivnosti. Svaki stručnjak sastavlja izjavu o interesima koja je javno dostupna. Komisija uspostavlja sustave i postupke za aktivno upravljanje mogućim sukobima interesa i njihovo sprečavanje.

5. Od država članica može se zahtijevati plaćanje naknada za savjete i potporu stručnjaka. Komisija provedbenim aktom iz stavka 1. donosi strukturu i visinu naknada te ljestvicu i strukturu troškova čiju je naknadu moguće zatražiti, uzimajući u obzir ciljeve odgovarajuće provedbe ove Uredbe, troškovnu učinkovitost i potrebu da se svim državama članicama osigura učinkovit pristup stručnjacima.

6. Komisija državama članicama olakšava pravodoban pristup stručnjacima, prema potrebi, i osigurava da je kombinacija potpornih aktivnosti koje provode objekti Unije za ispitivanje u skladu s člankom 68.a i stručnjaci u skladu s ovim člankom učinkovito organizirana i da pruža najbolju moguću dodanu vrijednost.

GLAVA IX.

KODEKSI PONAŠANJA

Članak 69.

Kodeksi ponašanja za dobrovoljnu primjenu specifičnih zahtjeva

1. Komisija i države članice u najvećoj mogućoj mjeri olakšavaju izradu kodeksa ponašanja namijenjenih poticanju dobrovoljne primjene jednog ili više zahtjeva iz glave III. poglavlja 2. ove Uredbe na UI sustave koji nisu visokorizični, uzimajući u obzir dostupna tehnička rješenja kojima se omogućuje primjena takvih zahtjeva.

2. Komisija i države članice potiču i olakšavaju izradu kodeksa ponašanja namijenjenih poticanju toga da se na sve UI sustave dobrovoljno primjenjuju specifični zahtjevi koji se odnose primjerice na okolišnu održivost, među ostalim u pogledu energetski učinkovitog programiranja, 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. Komisija i države članice također olakšavaju, prema potrebi, izradu kodeksa ponašanja primjenjivih na dobrovoljnoj osnovi u vezi s obvezama korisnikâ u pogledu UI sustava.

3. Kodekse ponašanja primjenjive na dobrovoljnoj osnovi mogu sastavljati pojedinačni dobavljači UI sustava i/ili organizacije koje ih zastupaju, među ostalim uz sudjelovanje korisnikâ i svih zainteresiranih dionika i njihovih predstavničkih organizacija, ili, ako je to primjereno, korisnici u pogledu svojih obveza. Kodeksi ponašanja mogu obuhvaćati jedan ili više UI sustava uzimajući u obzir sličnost namjene relevantnih sustava.

4. Pri poticanju i olakšavanju izrade kodeksâ ponašanja iz ovog članka Komisija i države članice uzimaju u obzir posebne interese i potrebe malih i srednjih poduzeća dobavljača, uključujući *start-up* poduzeća.

GLAVA X.

POVJERLJIVOST I SANKCIJE

Članak 70.

Povjerljivost

1. Nacionalna nadležna tijela, prijavljena tijela, Komisija, Odbor i sve druge fizičke ili pravne osobe uključene u primjenu ove Uredbe, u skladu s pravom Unije ili nacionalnim pravom, uspostavljaju odgovarajuće tehničke i organizacijske mjere kako bi osigurali povjerljivost informacija i podataka dobivenih pri obavljanju svojih zadaća i aktivnosti tako da osobito štite:

(a) prava intelektualnog vlasništva i povjerljive poslovne informacije ili poslovne tajne fizičke ili pravne osobe, uključujući izvorni kôd, osim 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;

(d) integritet kaznenih ili upravnih postupaka.

(e) integritet informacija klasificiranih u skladu s pravom Unije ili nacionalnim pravom.

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 nadzor granica, 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. Ta obveza razmjene informacija ne obuhvaća osjetljive operativne podatke u vezi s aktivnostima tijela kaznenog progona, tijela za nadzor granica, tijela za imigraciju ili tijela za azil.

Ako su tijela kaznenog progona, tijela za imigraciju ili tijela za azil dobavljači visokorizičnih UI sustava iz točaka 1., 6. 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 njihovih relevantnih tijela, kao i prijavljenih tijela, u pogledu razmjene informacija i širenja upozorenja, među ostalim u kontekstu prekogranične suradnje, ni na obveze dotičnih stranaka da pruže informacije na temelju kaznenog prava država članica.

Članak 71.

Sankcije

1. U skladu s uvjetima utvrđenima u ovoj Uredbi, države članice utvrđuju pravila o sankcijama, uključujući upravne novčane kazne, koje se primjenjuju na kršenje 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 veličina i interesi malih i srednjih poduzeća dobavljača, uključujući *start-up* poduzeća, te njihova gospodarska održivost. Njima se uzima u obzir i činjenica upotrebljava li se UI sustav u kontekstu osobne neprofesionalne djelatnosti.

2. Države članice bez odgode obavješćuju Komisiju o tim pravilima i mjerama te o svim naknadnim izmjenama koje na njih utječu.

3. Za neusklađenost s bilo kojim zabranama praksi u području umjetne inteligencije iz članka 5. 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. U slučaju MSP-ova, uključujući *start-up* poduzeća, te novčane kazne iznose do 3 % njihova godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu.

4. Za kršenje sljedećih odredaba u vezi s operaterima ili prijavljenim tijelima 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:

   (-a) obveza dobavljačâ u skladu s člancima 4.b i 4.c;

   (a) obveza dobavljačâ u skladu s člankom 16.;

   (b) obveza određenih drugih osoba u skladu s člankom 23.a;

(c) obveza ovlaštenih zastupnika u skladu s člankom 25.;

(d) obveza uvoznika u skladu s člankom 26.;

(e) obveza distributera u skladu s člankom 27.;

(f) obveza korisnika u skladu s člankom 1. stavcima od 1. do 6.a;

(g) zahtjeva i obveza prijavljenih tijela u skladu s člankom 33., člankom 34. stavkom 1., člankom 34. stavkom 3., člankom 34. stavkom 4. i člankom 34.a;

(h) obveza transparentnosti za dobavljače i korisnike u skladu s člankom 52.

U slučaju MSP-ova, uključujući *start-up* poduzeća, te novčane kazne iznose do 2 % njihova godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu.

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. U slučaju MSP-ova, uključujući *start-up* poduzeća, te novčane kazne iznose do 1 % njihova godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu.

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;

(aa) tome ima li povreda obilježje namjere ili nepažnje;

(ab) svakoj aktivnosti koju operater poduzima kako bi se otklonilo kršenje i ublažili mogući štetni učinci tog kršenja;

(b) eventualnim upravnim novčanim kaznama koje su druga tijela za nadzor tržišta u drugim državama članicama već izrekla istom operateru za istu povredu;

(ba) eventualnim upravnim novčanim kaznama koje su druga tijela već izrekla istom operateru za povrede drugog prava Unije ili nacionalnog prava, ako su takve povrede posljedica iste aktivnosti ili propusta koji predstavljaju relevantnu povredu ovog akta;

(c) veličini, godišnjem prometu i tržišnom udjelu operatera koji je počinio povredu;

(d) svim ostalim otegotnim ili olakotnim čimbenicima koji su primjenjivi na okolnosti slučaja, kao što su financijska dobit ostvarena kršenjem ili gubici izbjegnuti, izravno ili neizravno, tim kršenjem.

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.

9. Na izvršavanje ovlasti tijela za nadzor tržišta na temelju ovog članka primjenjuju se odgovarajuće postupovne zaštitne mjere u skladu s pravom Unije i pravom države članice, uključujući učinkoviti sudski pravni lijek i pravilno postupanje.

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, agenciji ili tijelu Unije u vezi s istim predmetom;

   (c) svim sličnim prijašnjim povredama koje je počinila dotična institucija, agencija ili tijelo Unije;

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

3. Za neusklađenost UI sustava s bilo kojim zahtjevima ili obvezama na temelju 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 7. stavka 1., članka 7. stavka 3., članka 11. stavka 3., članka 43. stavaka 5. i 6. i članka 48. stavka 5. dodjeljuje se Komisiji na razdoblje od pet godina počevši od [*datuma stupanja na snagu ove Uredbe*].

Komisija izrađuje izvješće o delegiranju ovlasti najkasnije devet mjeseci prije kraja razdoblja od pet godina. Delegiranje ovlasti prešutno se produljuje za razdoblja jednakog trajanja, osim ako se Europski parlament ili Vijeće tom produljenju usprotive najkasnije tri mjeseca prije kraja svakog razdoblja.

3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 7. stavka 1., članka 7. stavka 3., 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. On 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 7. stavka 1., članka 7. stavka 3., 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 podrobnih mjera povezanih s tehničkim specifikacijama i postupcima za odobravanje i uporabu zaštitne opreme koje se odnose na sustave umjetne inteligencije u smislu Uredbe (EU) YYY/XX [o umjetnoj inteligenciji] Europskog parlamenta i Vijeća* uzimaju se u obzir zahtjevi utvrđeni u glavi III. poglavlju 2. te uredbe.”

_____

* Uredba (EU) YYY/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) 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 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) YYY/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) 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 ...).”

(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) YYY/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) YYY/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) YYY/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) YYY/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) YYY/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) 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 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. [izbrisano]

1.b Komisija procjenjuje potrebu za izmjenom popisa iz Priloga III. svaka 24 mjeseca nakon stupanja na snagu ove Uredbe i do kraja razdoblja delegiranja ovlasti. Rezultati te procjene dostavljaju se Europskom parlamentu i Vijeću.

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 resursa, tehničke opreme 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 evaluira učinak i djelotvornost dobrovoljnih kodeksa ponašanja kako bi se potaknula primjena zahtjeva iz glave III. poglavlja 2. za UI sustave koji nisu visokorizični, a možda i drugih dodatnih zahtjeva za UI sustave, među ostalim u pogledu okolišne održivosti.

5. Odbor, države članice i nacionalna nadležna tijela Komisiji na zahtjev dostavljaju informacije za potrebe stavaka od 1.a do 4.

6. Pri provedbi evaluacija i preispitivanjâ iz stavaka od 1.a 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 [36 mjeseci nakon stupanja na snagu Uredbe].

3. Odstupajući od stavka 2.:

   (a) glava III. poglavlje 4. i glava VI. primjenjuju se od [12 mjeseci nakon stupanja na snagu ove Uredbe];

   (b) članak 71. primjenjuje se od [12 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	*Za Vijeće*
Predsjednik/Predsjednica	*Predsjednik/Predsjednica*

PRILOG I.

[izbrisano]

PRILOG II.

POPIS ZAKONODAVSTVA UNIJE O USKLAĐIVANJU

Odjeljak A – Popis zakonodavstva Unije o usklađivanju koje se temelji na novom zakonodavnom okviru

1. Direktiva 2006/42/EZ Europskog parlamenta i Vijeća od 17. svibnja 2006. o strojevima o izmjeni Direktive 95/16/EZ (SL L 157, 9.6.2006., str. 24.) [stavljena izvan snage Uredbom o strojevima];

2. Direktiva 2009/48/EZ Europskog parlamenta i Vijeća od 18. lipnja 2009. o sigurnosti igračaka (SL L 170, 30.6.2009., str. 1.);

3. Direktiva 2013/53/EU Europskog parlamenta i Vijeća od 20. studenoga 2013. o rekreacijskim plovilima i osobnim plovilima na vodomlazni pogon i o stavljanju izvan snage Direktive Vijeća 94/25/EZ (SL L 354, 28.12.2013., str. 90.);

4. Direktiva 2014/33/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o usklađivanju zakonodavstava država članica u odnosu na dizala i sigurnosne komponente za dizala (SL L 96, 29.3.2014., str. 251.);

5. Direktiva 2014/34/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o usklađivanju zakonodavstava država članica u odnosu na opremu i zaštitne sustave namijenjene za uporabu u potencijalno eksplozivnim atmosferama (SL L 96, 29.3.2014., str. 309.);

6. Direktiva 2014/53/EU Europskog parlamenta i Vijeća od 16. travnja 2014. o usklađivanju zakonodavstava država članica o stavljanju na raspolaganje radijske opreme na tržištu i stavljanju izvan snage Direktive 1999/5/EZ (SL L 153, 22.5.2014., str. 62.);

7. Direktiva 2014/68/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o usklađivanju zakonodavstava država članica o stavljanju na raspolaganje na tržištu tlačne opreme (SL L 189, 27.6.2014., str. 164.);

8. Uredba (EU) 2016/424 Europskog parlamenta i Vijeća od 9. ožujka 2016. o žičarama i stavljanju izvan snage Direktive 2000/9/EZ (SL L 81, 31.3.2016., str. 1.);

9. Uredba (EU) 2016/425 Europskog parlamenta i Vijeća od 9. ožujka 2016. o osobnoj zaštitnoj opremi i o stavljanju izvan snage Direktive Vijeća 89/686/EEZ (SL L 81, 31.3.2016., str. 51.);

10. Uredba (EU) 2016/426 Europskog parlamenta i Vijeća od 9. ožujka 2016. o aparatima na plinovita goriva i stavljanju izvan snage Direktive 2009/142/EZ (SL L 81, 31.3.2016., str. 99.);

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

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

Odjeljak B – Popis ostalog zakonodavstva Unije o usklađivanju

1. 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.).

2. 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.);

3. 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.);

4. 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.);

5. 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.).

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

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

8. Uredba (EU) 2018/1139 Europskog parlamenta i Vijeća od 4. srpnja 2018. o zajedničkim pravilima u području civilnog zrakoplovstva i osnivanju Agencije Europske unije za sigurnost zračnog prometa i izmjeni uredbi (EZ) br. 2111/2005, (EZ) br. 1008/2008, (EU) br. 996/2010, (EU) br. 376/2014 i direktiva 2014/30/EU i 2014/53/EU Europskog parlamenta i Vijeća te stavljanju izvan snage uredbi (EZ) br. 552/2004 i (EZ) br. 216/2008 Europskog parlamenta i Vijeća i Uredbe Vijeća (EEZ) br. 3922/91 (SL L 212, 22.8.2018., str. 1.), kada je riječ o projektiranju, proizvodnji i stavljanju na tržište zrakoplova iz članka 2. stavka 1. točaka (a) i (b), u vezi s bespilotnim zrakoplovima i njihovim motorima, propelerima, dijelovima i opremi za daljinsko upravljanje tim zrakoplovima.

PRILOG III.
VISOKORIZIČNI UI SUSTAVI IZ ČLANKA 6. STAVKA 3.

U svakom od područja navedenih u točkama od 1. do 8. UI sustavi koji su posebno navedeni pod svakim slovom smatraju se visokorizičnim UI sustavima u skladu s člankom 6. stavkom 3.:

1. Biometrija:

   (a) sustavi za daljinsku biometrijsku identifikaciju.

2. Kritična infrastruktura:

   (a) UI sustavi namijenjeni za uporabu kao sigurnosni sastavni dijelovi za upravljanje kritičnom infrastrukturom, cestovnim prometom i opskrbom vodom, plinom, grijanjem i električnom energijom te za njihov rad;

3. Obrazovanje i strukovno osposobljavanje:

   (a) UI sustavi namijenjeni za određivanje pristupa, primanja ili raspoređivanja pojedinaca u ustanove ili programe za obrazovanje i strukovno osposobljavanje na svim razinama;

   (b) UI sustavi namijenjeni za evaluaciju ishodâ učenja, među ostalim kada se ti ishodi upotrebljavaju za usmjeravanje procesa učenja pojedinaca u ustanovama ili programima za obrazovanje i strukovno osposobljavanje na svim razinama.

4. Zapošljavanje, upravljanje radnicima i pristup samozapošljavanju:

   (a) UI sustavi namijenjeni za zapošljavanje ili odabir pojedinaca, posebno za postavljanje ciljanih oglasa za posao, za analizu i filtriranje prijava za posao te za evaluaciju kandidata;

(b) UI sustavi namijenjeni za donošenje odluka o promaknućima i prestanku radnih ugovornih odnosa, za dodjelu zadataka na osnovi individualnog ponašanja ili osobnih značajki odnosno karakteristika te za praćenje i evaluaciju uspješnosti i ponašanja osoba u takvim odnosima;

5. Pristup i korištenje osnovnim privatnim uslugama te osnovnim javnim uslugama i naknadama:

(a) UI sustavi namijenjeni tijelima javne vlasti, ili drugima u njihovo ime, za evaluaciju prihvatljivosti pojedinaca za osnovne naknade i usluge javne pomoći te za odobravanje, smanjenje, ukidanje ili povrat takvih naknada i usluga;

(b) UI sustavi namijenjeni za ocjenjivanje kreditne sposobnosti pojedinaca ili utvrđivanje njihove kreditne ocjene, osim UI sustava koje dobavljači koji su mikropoduzeća te mala i srednja poduzeća definirana u Prilogu Preporuke Komisije 2003/361/EZ stavljaju u uporabu za vlastite potrebe;

(c) UI sustavi namijenjeni za dispečiranje ili određivanje prioriteta pri dispečiranju hitnih službi, uključujući vatrogasce i medicinsku pomoć;

(d) UI sustavi namijenjeni za procjenu rizika i određivanje cijena u odnosu na pojedince u slučaju životnog i zdravstvenog osiguranja, osim UI sustava koje dobavljači koji su mikropoduzeća te mala i srednja poduzeća definirana u Prilogu Preporuke Komisije 2003/361/EZ stavljaju u uporabu za vlastite potrebe.

6. Kazneni progon:

(a) UI sustavi namijenjeni za upotrebu od strane tijela kaznenog progona ili u njihovo ime radi procjene rizika u vezi s time hoće li pojedinac počiniti ili ponovno počiniti kazneno djelo ili postati potencijalna žrtva kaznenih djela;

(b) UI sustavi namijenjeni za upotrebu od strane tijela kaznenog progona kao poligrafi i slični instrumenti ili za otkrivanje emocionalnog stanja pojedinaca;

(c) [izbrisano]

(d) UI sustavi namijenjeni za upotrebu od strane tijela kaznenog progona ili u njihovo ime radi evaluacije pouzdanosti dokaza tijekom istrage ili progona kaznenih djela;

(e) UI sustavi namijenjeni za upotrebu od strane tijela kaznenog progona ili u njihovo ime radi predviđanja počinjenja ili ponovnog počinjenja stvarnog ili potencijalnog kaznenog djela na temelju izrade profila pojedinaca kako je navedeno u članku 3. točki 4. Direktive (EU) 2016/680 ili procjene osobina i karakteristika ili prethodnog kriminalnog ponašanja pojedinaca ili skupina;

(f) UI sustavi namijenjeni za upotrebu od strane tijela kaznenog progona ili u njihovo ime radi izrade profila pojedinaca kako je navedeno u članku 3. točki 4. Direktive (EU) 2016/680 tijekom otkrivanja, istrage ili progona kaznenih djela.

(g) [izbrisano]

7. Upravljanje migracijama, azilom i nadzorom državne granice:

(a) UI sustavi namijenjeni za upotrebu od strane nadležnih tijela javne vlasti ili u njihovo ime kao poligrafi i slični instrumenti ili za otkrivanje emocionalnog stanja pojedinca;

(b) UI sustavi namijenjeni za upotrebu od strane nadležnih tijela javne vlasti ili u njihovo ime za procjenu rizika, uključujući rizik za sigurnost, rizik od nezakonitih migracija ili rizik za zdravlje, koji predstavlja pojedinac koji namjerava ući ili je ušao na državno područje države članice;

(c) [izbrisano]

(d) UI sustavi namijenjeni za upotrebu od strane nadležnih tijela javne vlasti ili u njihovo ime pri razmatranju zahtjeva za azil, vize i boravišne dozvole te povezanih pritužbi u pogledu prihvatljivosti pojedinaca koji podnose zahtjev za status.

8. Pravosuđe i demokratski procesi:

(a) UI sustavi namijenjeni za upotrebu od strane pravosudnih tijela ili u njihovo ime radi tumačenja činjenica ili prava te primjene prava na konkretan skup činjenica.

PRILOG IV.

TEHNIČKA DOKUMENTACIJA iz članka 11. stavka 1.

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

1. općenit opis UI sustava, uključujući:

   (a) njegovu namjenu, imena osoba koje ga razvijaju te datum i verziju sustava;

   (b) način na koji je UI sustav u interakciji, ili se može upotrijebiti za interakciju, s hardverom ili softverom koji nije dio samog UI sustava, ako je primjenjivo;

   (c) verzije relevantnog softvera ili integriranog softvera i sve zahtjeve povezane s ažuriranjem verzija;

   (d) opis svih oblika u kojima se UI sustav stavlja na tržište ili u uporabu (npr. kao softverski paket ugrađen u hardver, u formatu koji se može preuzeti s interneta, API itd.);

   (e) opis hardvera na kojem bi UI sustav trebao raditi;

   (f) ako je UI sustav sastavni dio proizvoda, fotografije ili ilustracije koje prikazuju vanjske značajke, oznake i unutarnju konstrukciju tih proizvoda;

   (g) korisničke upute za uporabu i, prema potrebi, upute za instalaciju;

2. detaljan opis elemenata UI sustava i postupka njegova razvoja, uključujući:

   (a) metode i korake provedene u razvoju UI sustava, uključujući, prema potrebi, korištenje prethodno treniranih sustava ili alata trećih strana te način na koji ih je dobavljač upotrijebio, integrirao ili izmijenio;

(b) projektne specifikacije sustava, odnosno opću logiku UI sustava i algoritama; najvažnije projektne odabire, uključujući razloge i pretpostavke za njih, među ostalim u vezi s osobama ili skupinama osoba na kojima se sustav namjerava upotrebljavati; glavna primijenjena klasifikacijska rješenja; informacije o tome što bi sustav trebao optimizirati te relevantnost različitih parametara; opis očekivanih izlaznih rezultata sustava; odluke o eventualnim kompromisima u tehničkim rješenjima koji su doneseni radi poštovanja zahtjeva iz glave III. poglavlja 2.;

(c) opis arhitekture sustava s objašnjenjem kako se softverske komponente međusobno nadopunjuju ili potpomažu te kako su uključene u cjelokupnu obradu; računalne resurse korištene za razvoj, učenje, testiranje i validaciju UI sustava;

(d) ako je primjenjivo, potrebne podatke u smislu tablica s opisom metodologije i tehnika treniranja te skupova podataka korištenih za treniranje, uključujući općenit opis tih skupova podataka i informacije o njihovu podrijetlu, sadržaju i glavnim karakteristikama; način na koji su podaci dobiveni i odabrani; postupke označivanja (npr. za nadzirano učenje), metodologije čišćenja podataka (npr. otkrivanje netipičnih vrijednosti);

(e) procjenu mjera ljudskog nadzora potrebnih u skladu s člankom 14., uključujući procjenu tehničkih mjera potrebnih kako bi se korisnicima olakšalo tumačenje izlaznih rezultata UI sustava, u skladu s člankom 13. stavkom 3. točkom (d);

(f) ako je primjenjivo, detaljan opis unaprijed određenih promjena UI sustava i njegove sposobnosti, zajedno sa svim relevantnim informacijama o tehničkim rješenjima primijenjenima radi kontinuirane usklađenosti UI sustava s relevantnim zahtjevima iz glave III. poglavlja 2.;

(g) primijenjene postupke validacije i testiranja, uključujući informacije o podacima korištenima za validaciju i testiranje te njihovim glavnim karakteristikama; parametre za mjerenje točnosti, otpornosti, kibersigurnosti i usklađenosti s drugim relevantnim zahtjevima iz glave III. poglavlja 2., kao i potencijalno diskriminirajuće učinke; dnevnike događaja tijekom testiranja i sva izvješća o testiranju s datumom i potpisom odgovornih osoba, među ostalim u vezi s unaprijed određenim promjenama iz točke (f);

3. detaljne informacije o praćenju, funkcioniranju i kontroli UI sustava, posebno u pogledu: njegovih mogućnosti i ograničenja u radu, uključujući stupnjeve točnosti za konkretne osobe ili skupine osoba na kojima se sustav namjerava upotrebljavati te ukupnu očekivanu razinu točnosti u odnosu na namjenu sustava; predvidljivih neplaniranih krajnjih ishoda i izvora rizika za zdravlje i sigurnost, temeljna prava i diskriminaciju s obzirom na namjenu UI sustava; mjera ljudskog nadzora potrebnih u skladu s člankom 14., uključujući tehničke mjere primijenjene kako bi se korisnicima olakšalo tumačenje izlaznih rezultata UI sustava; specifikacije ulaznih podataka, prema potrebi;

4. detaljan opis sustava upravljanja rizicima u skladu s člankom 9.;

5. opis svih relevantnih promjena koje je dobavljač unio u sustav tijekom njegova životnog ciklusa;

6. popis u cijelosti ili djelomično primijenjenih usklađenih normi na koje su objavljena upućivanja u Službenom listu Europske unije; ako nisu primijenjene takve usklađene norme, detaljan opis rješenja koja su upotrijebljena radi ispunjavanja zahtjeva iz glave III. poglavlja 2., uključujući popis drugih primijenjenih relevantnih normi i tehničkih specifikacija;

7. primjerak EU izjave o sukladnosti;

8. detaljan opis sustava uvedenog za evaluaciju sposobnosti UI sustava u fazi nakon stavljanja na tržište u skladu s člankom 61., uključujući plan praćenja nakon stavljanja na tržište iz članka 61. stavka 3.

PRILOG V.

EU IZJAVA O SUKLADNOSTI EU

EU izjava o sukladnosti iz članka 48. sadržava sve sljedeće informacije:

1. ime i vrstu UI sustava te sve dodatne nedvosmislene referentne oznake koje omogućuju identifikaciju i sljedivost UI sustava;

2. ime i adresu dobavljača ili, prema potrebi, njegova ovlaštenog zastupnika;

3. navod da je za izdavanje EU izjave o sukladnosti odgovoran isključivo dobavljač;

4. izjavu da je dotični UI sustav u skladu s ovom Uredbom i, ako je primjenjivo, sa svim drugim relevantnim propisima Unije kojima je predviđeno izdavanje EU izjave o sukladnosti;

5. upućivanja na sve korištene relevantne usklađene norme ili druge zajedničke specifikacije u odnosu na koje se izjavljuje sukladnost;

6. ako je primjenjivo, ime i identifikacijski broj prijavljenog tijela, opis provedenog postupka ocjenjivanja sukladnosti te identifikacijsku oznaku izdane potvrde;

7. mjesto i datum izdavanja izjave, ime i funkciju osobe koja ju je potpisala, uključujući navod za koga i u čije ime je potpisana, te potpis.

PRILOG VI.

POSTUPAK OCJENJIVANJA SUKLADNOSTI NA TEMELJU UNUTARNJE KONTROLE

1. Postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole postupak je ocjenjivanja sukladnosti na temelju točaka od 2. do 4.

2. Dobavljač provjerava je li uvedeni sustav upravljanja kvalitetom u skladu sa zahtjevima iz članka 17.

3. Dobavljač pregledava informacije iz tehničke dokumentacije kako bi ocijenio usklađenost UI sustava s relevantnim temeljnim zahtjevima iz glave III. poglavlja 2.

4. Osim toga, dobavljač provjerava i jesu li postupak projektiranja i razvoja UI sustava te njegovo praćenje nakon stavljanja na tržište iz članka 61. u skladu s tehničkom dokumentacijom.

PRILOG VII.

SUKLADNOST NA TEMELJU OCJENJIVANJA SUSTAVA UPRAVLJANJA KVALITETOM I OCJENJIVANJA TEHNIČKE DOKUMENTACIJE

1. Uvod

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

2. Pregled

Odobreni sustav upravljanja kvalitetom za projektiranje, razvoj i testiranje UI sustavâ u skladu s člankom 17. ispituje se u skladu s točkom 3. i podliježe nadzoru kako je utvrđeno u točki 5. Tehnička dokumentacija UI sustava pregledava se u skladu s točkom 4.

3. Sustav upravljanja kvalitetom

3.1. Zahtjev dobavljača sadržava:

(a) ime i adresu dobavljača te ime i adresu ovlaštenog zastupnika ako je on podnio zahtjev;

(b) popis UI sustava obuhvaćenih istim sustavom upravljanja kvalitetom;

(c) tehničku dokumentaciju za svaki UI sustav obuhvaćen istim sustavom upravljanja kvalitetom;

(d) dokumentaciju o sustavu upravljanja kvalitetom koja obuhvaća sve aspekte navedene u članku 17.;

(e) opis uvedenih postupaka kojima se osigurava da sustav upravljanja kvalitetom ostane primjeren i djelotvoran;

(f) pisanu izjavu da isti zahtjev nije podnesen nijednom drugom prijavljenom tijelu.

3.2. Prijavljeno tijelo ocjenjuje sustav upravljanja kvalitetom i utvrđuje udovoljava li on zahtjevima iz članka 17.

O toj se odluci obavješćuje dobavljač ili njegov ovlašteni zastupnik.

Ta obavijest sadržava zaključke ocjenjivanja sustava upravljanja kvalitetom i obrazloženu odluku o ocjeni.

3.3. Dobavljač je dužan nastaviti primjenjivati i održavati odobreni sustav upravljanja kvalitetom tako da ostane primjeren i djelotvoran.

3.4. Dobavljač obavješćuje prijavljeno tijelo o svakoj planiranoj promjeni odobrenog sustava upravljanja kvalitetom ili popisa UI sustava koji su njime obuhvaćeni.

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

Prijavljeno tijelo obavješćuje dobavljača o svojoj odluci. Ta obavijest sadržava zaključke pregleda promjena i obrazloženu odluku o ocjeni.

4. Kontrola tehničke dokumentacije

4.1. Uz zahtjev iz točke 3. dobavljač podnosi prijavljenom tijelu po vlastitom izboru zahtjev za ocjenjivanje tehničke dokumentacije UI sustava koji dobavljač namjerava staviti na tržište ili u uporabu i koji je obuhvaćen sustavom upravljanja kvalitetom iz točke 3.

4.2. Taj zahtjev sadržava:

(a) ime i adresu dobavljača;

(b) pisanu izjavu da isti zahtjev nije podnesen nijednom drugom prijavljenom tijelu;

(c) tehničku dokumentaciju iz Priloga IV.

4.3. Prijavljeno tijelo pregledava tu tehničku dokumentaciju. Ako je to relevantno i ograničeno na ono što je potrebno za ispunjavanje njihovih zadaća, tijela za nadzor tržišta imaju puni pristup skupovima podataka koji se upotrebljavaju za treniranje, validaciju i testiranje, među ostalim, prema potrebi i podložno sigurnosnim zaštitnim mjerama, putem aplikacijskih programskih sučelja („API”) ili drugih relevantnih tehničkih sredstava i alata koji omogućuju daljinski pristup.

4.4. Pri pregledu tehničke dokumentacije prijavljeno tijelo može zatražiti da dobavljač dostavi dodatne dokaze ili provede dodatna testiranja kako bi se omogućilo pravilno ocjenjivanje sukladnosti UI sustava sa zahtjevima iz glave III. poglavlja 2. Kad prijavljeno tijelo nije zadovoljno testiranjima koja je proveo dobavljač, ono prema potrebi samo provodi potrebna testiranja.

4.5. Prijavljenim tijelima odobrava se pristup izvornom kodu visokorizičnog UI sustava na obrazložen zahtjev i samo ako su ispunjeni sljedeći kumulativni uvjeti:

a) pristup izvornom kodu potreban je za ocjenjivanje sukladnosti visokorizičnog UI sustava sa zahtjevima iz glave III. poglavlja 2. i

b) postupci testiranja/revizije i provjere na temelju podataka i dokumentacije koje je dostavio dobavljač iscrpljeni su ili su se pokazali nedostatnima.

4.6. O toj se odluci obavješćuje dobavljač ili njegov ovlašteni zastupnik. Ta obavijest sadržava zaključke ocjene tehničke dokumentacije i obrazloženu odluku o ocjeni.

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

Potvrda i njezini prilozi sadržavaju sve relevantne informacije potrebne za ocjenjivanje sukladnosti UI sustava i, prema potrebi, za kontrolu UI sustava tijekom uporabe.

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

Ako UI sustav ne ispunjava zahtjev koji se odnosi na podatke korištene za njegovo treniranje, prije podnošenja zahtjeva za novo ocjenjivanje sukladnosti bit će potrebno ponovno treniranje dotičnog UI sustava. U tom slučaju obrazložena odluka prijavljenog tijela o odbijanju izdavanja potvrde EU-a o ocjenjivanju tehničke dokumentacije mora sadržavati konkretne argumente o kvaliteti podataka korištenih za treniranje UI sustava, a posebno o razlozima za utvrđivanje neusklađenosti.

4.7. Svaku promjenu UI sustava koja bi mogla utjecati na usklađenost UI sustava sa zahtjevima ili na njegovu namjenu mora odobriti prijavljeno tijelo koje je izdalo potvrdu EU-a o ocjenjivanju tehničke dokumentacije. Dobavljač je dužan obavijestiti to prijavljeno tijelo ako namjerava uvesti bilo koju od prethodno navedenih promjena ili ako na neki drugi način sazna za pojavu takvih promjena. Prijavljeno tijelo ocjenjuje planirane promjene i odlučuje je li zbog njih potrebno novo ocjenjivanje sukladnosti u skladu s člankom 43. stavkom 4. ili se za njih može izdati dodatak potvrdi EU-a o ocjenjivanju tehničke dokumentacije. U potonjem slučaju prijavljeno tijelo ocjenjuje promjene, obavješćuje dobavljača o svojoj odluci te, ako promjene odobri, dobavljaču izdaje dodatak potvrdi EU-a o ocjenjivanju tehničke dokumentacije.

5. Nadzor odobrenog sustava upravljanja kvalitetom

5.1. Svrha nadzora koji provodi prijavljeno tijelo iz točke 3. jest osigurati da dobavljač ispunjava uvjete odobrenog sustava upravljanja kvalitetom.

5.2. Za potrebe ocjenjivanja dobavljač prijavljenom tijelu omogućuje pristup prostorima u kojima se odvijaju projektiranje, razvoj i testiranje UI sustavâ. Osim toga, dobavljač prijavljenom tijelu daje sve potrebne informacije.

5.3. Prijavljeno tijelo provodi periodične revizije kako bi potvrdilo da dobavljač provodi i primjenjuje sustav upravljanja kvalitetom te dobavljaču dostavlja izvješće o reviziji. U okviru tih revizija prijavljeno tijelo može provesti dodatna testiranja UI sustava za koje je izdana potvrda EU-a o ocjenjivanju tehničke dokumentacije.

PRILOG VIII.

INFORMACIJE KOJE SE MORAJU DOSTAVITI NAKON REGISTRACIJI OPERATERA I VISOKORIZIČNIH UI SUSTAVA U SKLADU S ČLANKOM 51.

Dobavljači, ovlašteni zastupnici i korisnici koji su tijela javne vlasti, javne agencije ili javna tijela dostavljaju informacije iz dijela I. Dobavljači ili, ako je to primjenjivo, ovlašteni zastupnici osiguravaju da su informacije o njihovim visokorizičnim UI sustavima iz dijela II. točaka od 1. do 11. potpune, točne i ažurirane. Baza podataka automatski generira informacije utvrđene u točki II.12.

Dio I. – Informacije o operaterima (nakon registracije operatera)

-1. Vrsta operatera (dobavljač, ovlašteni zastupnik ili korisnik);

1. ime, adresa i kontaktni podaci dobavljača;

2. ako informacije dostavlja druga osoba u ime operatera, ime, adresa i kontaktni podaci te osobe;

Dio II. Informacije povezane s visokorizičnim UI sustavom

1. ime, adresa i kontaktni podaci dobavljača;

2. ime, adresa i kontaktni podaci ovlaštenog zastupnika, prema potrebi;

3. trgovačko ime UI sustava i sve dodatne nedvosmislene referentne oznake koje omogućuju identifikaciju i sljedivost UI sustava;

4. opis namjene UI sustava;

5. status UI sustava (na tržištu ili u uporabi; više nije stavljen na tržište/u uporabu, opozvan);

6. vrsta, broj i datum isteka potvrde koju je izdalo prijavljeno tijelo te, prema potrebi, ime ili identifikacijski broj tog prijavljenog tijela;

7. skeniran primjerak potvrde iz točke 6., prema potrebi;

8. imena država članica u kojima se UI sustav stavlja ili je stavljen na tržište, u uporabu ili na raspolaganje u Uniji;

9. primjerak EU izjave o sukladnosti iz članka 48.;

10. upute za uporabu u elektroničkom formatu;

11. internetska poveznica za dodatne informacije (nije obvezno);

12. ime, adresa i kontaktni podaci korisnikâ.

PRILOG VIII.a

INFORMACIJE KOJE TREBA PODNIJETI NAKON REGISTRACIJE VISOKORIZIČNIH UI SUSTAVA S POPISA IZ PRILOGA III. U VEZI S TESTIRANJEM U STVARNIM UVJETIMA U SKLADU S ČLANKOM 54.a

U vezi s testiranjem u stvarnim uvjetima koje se treba registrirati u skladu s člankom 54.a dostavljaju se i ažuriraju sljedeće informacije:

1. jedinstveni identifikacijski broj na razini Unije za testiranje u stvarnim uvjetima;

2. ime i kontaktni podaci dobavljača ili potencijalnog dobavljača i korisnikâ uključenih u testiranje u stvarnim uvjetima;

3. kratak opis UI sustava i njegove namjene te druge informacije potrebne za identifikaciju sustava;

4. sažetak glavnih značajki plana testiranja u stvarnim uvjetima;

5. informacije o obustavi ili prekidu testiranja u stvarnim uvjetima.

PRILOG IX.

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

1. Schengenski informacijski sustav

   (a) Uredba (EU) 2018/1860 Europskog parlamenta i Vijeća od 28. studenoga 2018. o upotrebi Schengenskog informacijskog sustava za vraćanje državljana trećih zemalja s nezakonitim boravkom (SL L 312, 7.12.2018., str. 1.);

   (b) Uredba (EU) 2018/1861 Europskog parlamenta i Vijeća od 28. studenoga 2018. o uspostavi, radu i upotrebi Schengenskog informacijskog sustava (SIS) u području granične kontrole i o izmjeni Konvencije o provedbi Schengenskog sporazuma te o izmjeni i stavljanju izvan snage Uredbe (EZ) br. 1987/2006 (SL L 312, 7.12.2018., str. 14.);

   (c) Uredba (EU) 2018/1862 Europskog parlamenta i Vijeća od 28. studenoga 2018. o uspostavi, radu i upotrebi Schengenskog informacijskog sustava (SIS) u području policijske suradnje i pravosudne suradnje u kaznenim stvarima, izmjeni i stavljanju izvan snage Odluke Vijeća 2007/533/PUP i stavljanju izvan snage Uredbe (EZ) br. 1986/2006 Europskog parlamenta i Vijeća i Odluke Komisije 2010/261/EU (SL L 312, 7.12.2018., str. 56.).

2. Vizni informacijski sustav

   (a) Prijedlog UREDBE EUROPSKOG PARLAMENTA I VIJEĆA o izmjeni Uredbe (EZ) br. 767/2008, Uredbe (EZ) br. 810/2009, Uredbe (EU) 2017/2226, Uredbe (EU) 2016/399, Uredbe XX/2018 [Uredba o interoperabilnosti] i Odluke 2004/512/EZ te o stavljanju izvan snage Odluke Vijeća 2008/633/PUP – COM(2018) 302 final. Ažurirat će se nakon što suzakonodavci donesu Uredbu (travanj/svibanj 2021.).

3. Eurodac

(a) Izmijenjeni Prijedlog UREDBE EUROPSKOG PARLAMENTA I VIJEĆA o uspostavi sustava „Eurodac” za usporedbu otisaka prstiju za učinkovitu primjenu Uredbe (EU) XXX/XXX [Uredba o upravljanju azilom i migracijama] i Uredbe (EU) XXX/XXX [Uredba o preseljenju] radi identificiranja državljanina treće zemlje ili osobe bez državljanstva s nezakonitim boravkom, o zahtjevima tijela kaznenog progona država članica i Europola za usporedbu s podacima iz Eurodaca u svrhu kaznenog progona te o izmjeni uredaba (EU) 2018/1240 i (EU) 2019/818 – COM(2020) 614 final.

4. Sustav ulaska/izlaska

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

5. Europski sustav za informacije o putovanjima i odobravanje putovanja

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

(b) Uredba (EU) 2018/1241 Europskog parlamenta i Vijeća od 12. rujna 2018. o izmjeni Uredbe (EU) 2016/794 u svrhu uspostave europskog sustava za informacije o putovanjima i odobravanje putovanja (ETIAS) (SL L 236, 19.9.2018., str. 72.).

6. Europski informacijski sustav kaznene evidencije za državljane trećih zemalja i osobe bez državljanstva

(a) Uredba (EU) 2019/816 Europskog parlamenta i Vijeća od 17. travnja 2019. o uspostavi centraliziranog sustava za utvrđivanje država članica koje imaju podatke o osuđujućim presudama protiv državljana trećih zemalja i osoba bez državljanstva (sustav ECRIS-TCN) za dopunu Europskog informacijskog sustava kaznene evidencije te o izmjeni Uredbe (EU) 2018/1726 (SL L 135, 22.5.2019., str. 1.).

7. Interoperabilnost

(a) Uredba (EU) 2019/817 Europskog parlamenta i Vijeća od 20. svibnja 2019. o uspostavi okvira za interoperabilnost informacijskih sustava EU-a u području granica i viza (SL L 135, 22.5.2019., str. 27.);

(b) Uredba (EU) 2019/818 Europskog parlamenta i Vijeća od 20. svibnja 2019. o uspostavi okvira za interoperabilnost informacijskih sustava EU-a u području policijske i pravosudne suradnje, azila i migracija (SL L 135, 22.5.2019., str. 85.).